Technical Journal of Advanced Mobility

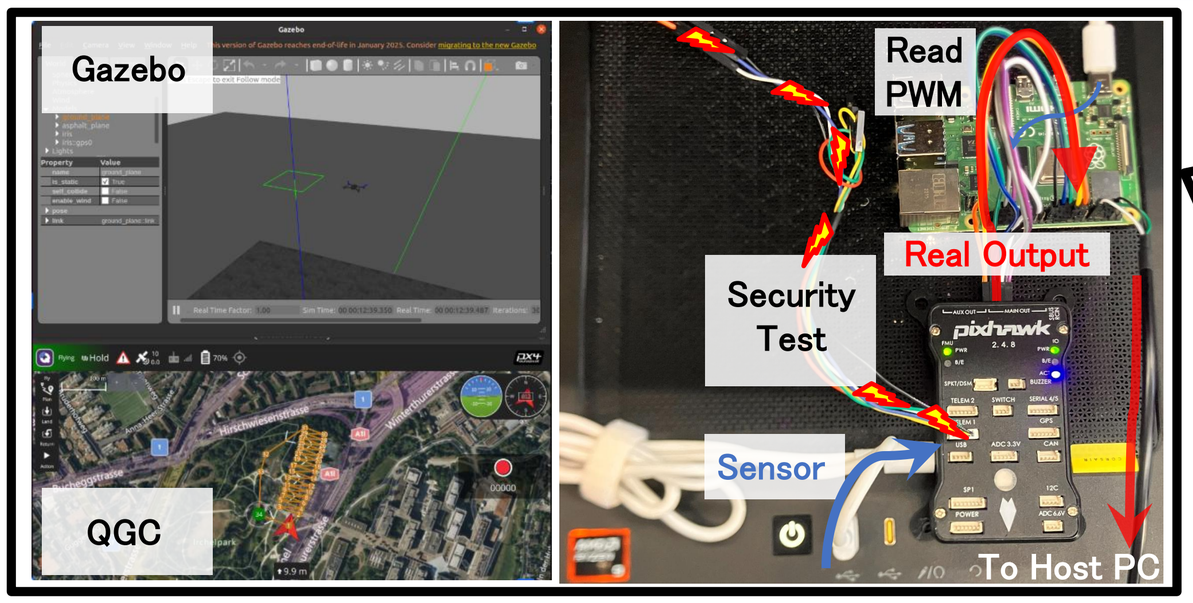
セキュリティテストを目的としたROHITLの提案

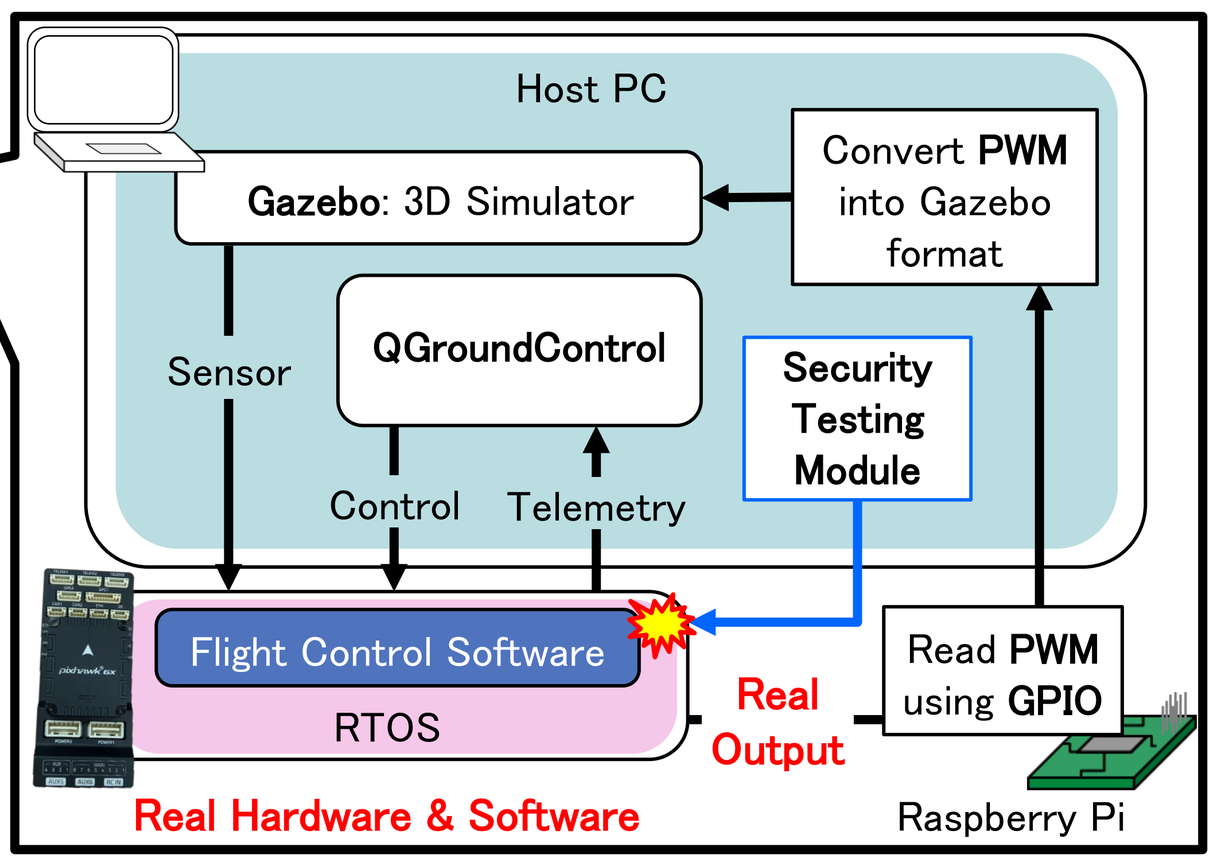
惣島雅樹，須崎有康　　情報セキュリティ大学院大学

① 背景（シミュレータにおけるサイバー攻撃の再現性問題）

オープンソースコミュニティが提供する既存のシミュレータでサイバー攻撃を正確に再現することはできない。近年広く活用されているSITL（Software-in-the-Loop）も、サイバー攻撃時の実機フライトコントローラやRTOS上での動作が確認できないため、セキュリティテストの目的には十分に適した環境とは言えない。

② 提案手法　ROHITL：Real-Output Hardware-in-the-Loop





■ オープンソースの主要ソフトウェアPX4およびArduPilotに対応

Open Source Software ＼ Existing Simulation	SITL	HITL	ROHITL（提案手法）
PX4	○	○※	○
ArduPilot	○	×	○

※ community supported and maintained

■ 実機フライトコントローラやRTOS上の動作が確認可能
■ モータ指令値の物理的な出力まで実機と同じ動作

③ セキュリティテストの事例（PX4、ArduPilotの既存シミュレーション環境と比較）

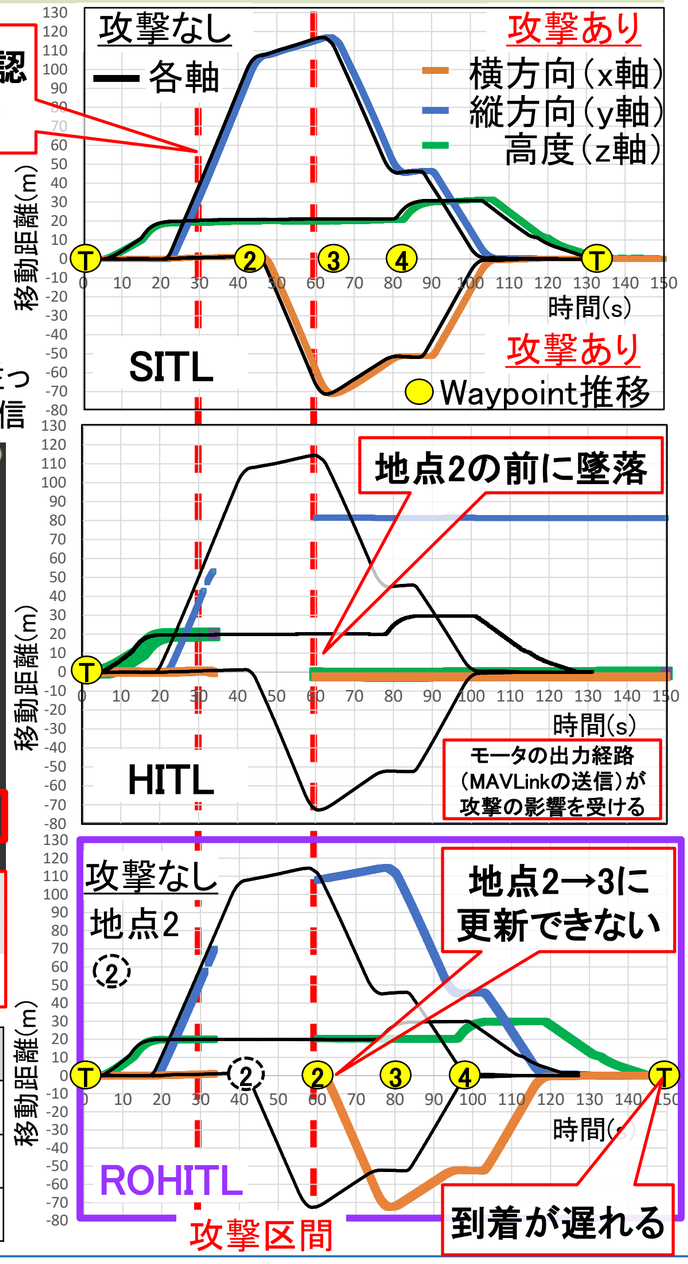
■ PX4のMAVLinkメッセージの大量送信

事前にアップロードしたWaypointに従って自律飛行中にメッセージを大量送信

```
COMMAND                 CPU(ms) CPU(%)  USED/STACK PRIO(BASE)
Idle Task               1281864  6.146   288/  768   0 (  0)
hpwork                        0  0.000   284/ 1224 249 (249)
lpwork                        0  0.000   284/ 1576  50 ( 50)
nsh_main                      0  0.000  2324/ 3144 100 (100)
wq:manager                    0  0.000   548/ 1232 255 (255)
wq:lp_default                 9  0.054  1444/ 1896 205 (205)
wq:rate_ctrl               1584 10.965  2492/ 3120 255 (255)
wq:hp_default                 2  0.017   964/ 2776 237 (237)
dataman                       0  0.001   908/ 1376  90 ( 90)
wq:I2C2                       3  0.026   700/ 2312 245 (245)
log_writer_file              43  0.111   692/ 1144  60 ( 60)
commander                    68  0.197  1860/ 3184 140 (140)
wq:nav_and_controllers      936  6.315  1452/ 2216 242 (242)
wq:INS0                    1744 11.757  3644/ 5976 241 (241)
mavlink_if0                 151  0.409  1980/ 2704 100 (100)
mavlink_rcv_if0            4738 42.831  1524/ 4776 175 (175)
navigator                    25  0.079  1820/ 2104 105 (105)
logger                      527  3.584  3452/ 3616 230 (230)
```

navigatorの優先度の方が低い
⇓
Waypointを更新できないはず

Simulation	評価
SITL	過少評価
HITL	過大評価
ROHITL	**適正に評価可能**



■ ArduPilotのSERIAL_CONTROLメッセージの不具合

ArduPilot

main_loop
飛行制御系のFastTaskなど

GCS_serial_control.cpp
```
...
while (packet.timeout != 0 &&
       stream->available() <
(int16_t)sizeof(packet.data)) {
    hal.scheduler->delay(1);
    packet.timeout--;
}
...
```

外部からのMAVLinkメッセージ
```
from pymavlink import mavutil
...
m.mav.serial_control_send(
    mavutil.mavlink.SERIAL_CONTROL_SERIAL0 + X,
    mavutil.mavlink.SERIAL_CONTROL_FLAG_RESPOND,
    3000,
...
)
```

長いタイムアウトを設定して、
SERIAL_CONTROLメッセージを送信すると
飛行制御タスクを含むmain_loopが停止するはず

ROHITLでの検証結果

```
Notice: Saved crash_dump.bin
Critical: WDG: T44 SL0 FL217 FT3 FA200180E0 FTP183 FLR2C000007 FICSR4196355 MM126 MC0 IE32768 IEC14 TN:moni
```

main_loopが停止して、**Watchdog Timer**によりTask44（MAVLink受信処理）実行中にFT3（HardFault）でリセット

Simulation	評価
SITL	評価不可
ROHITL	**適正に評価可能**

④ まとめ

- ドローンのセキュリティテストを目的として、サイバー攻撃を正確に再現可能なシミュレーション環境**ROHITLを提案**
- PX4とArduPilotのそれぞれで、**既存のSITL/HITLでは正確に再現できない攻撃をROHITL上で再現可能**であることを確認した

須崎研究室HP　JUIDAジャーナル