드론 안정성/보안성을 높이기 위한 드론 스푸핑 퍼저 연구

박정찬* 윤여정 정일훈 정승훈
국방과학연구소
*jcpark97@gmail.com

A Study on Drone Spoofing Fuzzer for Improving Stability and Security

Park Jeongchan
Agency for Defense Development

요 약

최근 활용도가 점점 높아지고 있는 드론에 대한 안정성과 보안성을 높이기 위해서는 다양한 실험이 요구된다. 물리적인 공격을 수반한 연구에 필요한 과도한 비용/시간/공간의 문제를 해결하며 공격에 의한 영향도를 효과적으로 분석할 수 있는 환경이 필요하다. 본 논문에서는 이를 위해 스푸핑 퍼저와 HILS기반 환경을 구성하여 공격 수행과 드론의 안정성을 평가할 수 있는 환경을 설계 및 구현하였다.

Ⅰ. 서 론

최근 무인이동체의 활용도는 몇 년 사이 급격하게 증가하고 있고 드론의 경우 인력이나 유인 장비로는 접근하기 어려운 작업을 신속하게 수행하고 있다. 드론의 활용도가 다양해짐에 따라 기체에 다양한 센서와 모듈들이 탑재되고 있고 외부로부터 위협받는 공격 스페이스가 증가하여 여러 잠재적인 보안 문제를 가지고 있다. 이러한 문제들을 해결하기 위해서는 드론 실기체 중심의 다양한 보안 위협을 시험하고 검증해야 하는데 장소, 비용, 시간 등 현실적인 문제들이 많이 존재한다. 본 논문에서는 SITL (Software in the Loop)에서 드론의 보안성과 안정성을 높이기 위한 스푸핑 퍼저에 관련된 설계와 구현을 바탕으로 HITL (Hardware in the Loop)과 연동하였다. 이를 통해 실제 드론을 활용하는 막대한 비용과 시간이 소요된다는 문제점을 해결할 수 있을 것으로 기대한다.

Ⅱ. 본론

1. SITL 기반 구조

본 논문에서는 SITL 기반으로 IMU 센서 내부 구조의 물리적 특성을 이용하여 임의의 센서 출력값을 발생시켜 비행 제어부의 자세 제어를 방해하도록 구현하였다. [1]에 의해 MEMS 자이로스코프의 공진 주파수를 이용하여 음향 노이즈를 주입함으로써 비행 제어부의 자세 및 위치 제어 기능을 무력화할 수 있음을 실험적으로 입증하였다. 자이로스코프가 특정 주파수에서 공진 현상을 일으키며, 이로 인해 센서 출력이 비정상적으로 변동함으로써 발생한 잘못된 센서 출력값이 비행 제어부에 입력되어 오작동 또는 추락을 유발한다[2][3][4]. IMU 센서의 공진 주파수를 활용한 센서 스푸핑 공격은 실제 드론의 자세 제어를 방해하고 기체를 추락시키는 등 큰 위협이다. 하지만 아직 알려지지 않은 센서 스푸핑 공격 기법이 존재하며 실제 드론을 대상으로 모든 공격 실험을 수행하기에는 어려움이 존재한다. 드론 기체 구매, 실험을 위한 안전한 공간 확보, 반복적인 실험 과정에서 발생할 수 있는 드론의 손상 및 복구 비용 등이 요구되며, 공격 실험을 위한 환경 구성 등 상당한 시간이 필요한 작업이 요구되고 안정상의 문제도 고려해야 한다. 본 논문에서는 다양한 임무 환경에서 변형된 센서값이 임무 수행에 미치는 영향을 평가하기 위하여 스푸핑 퍼저 설계와 구현을 하였으며, 이를 시뮬레이터와 연결하여 확장하였다(그림1).

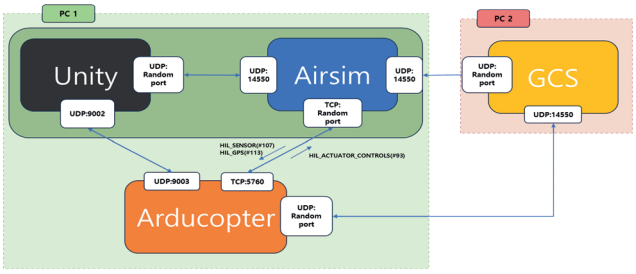

그림 1 SITL 연결 구조

FC(Flight Controller)는 드론의 안정성과 성능을 제어하는 중요한 장치로서 센서 데이터를 수집하고 이를 처리하여 드론의 모터(ESC)를 비롯한 다른 하위 시스템들을 제어한다. 센서 허브 역할을 하는 Sensors 모듈은 IMU 센서에서 수집하고 센서 드라이버를 통해 디코딩한 각속도, 가속도, 자성 정보 등을 통합하여 다른 모듈에서 활용할 수 있는 SensorCombined 토픽으로 발행한다(그림2).

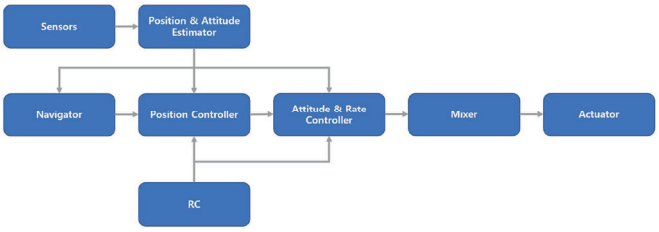

그림 2 FC(Flight Controller) 센서값 처리 과정

자세 및 위치 제어기에서는 자세 추정 모듈에서 계산한 현재 기체의 자세 및 위치 정보를 기반으로 다음 목표 지점에 도달하기 위한 목표 기체 상태와 차이를 계산하여 목표 상태에 도달하기 위한 구동기 출력을 계산함으로써 모터를 제어한다.

2. IMU 영향 분석을 위한 스푸핑 퍼저 설계 및 구현

스푸핑퍼저는 센서값을 변형하고 제어 오류를 기반으로 기체 이상 상태를 탐지하는 방식으로 동작한다. 퍼저는 크게 제어기와 퍼저 부분으로 구성되는데 퍼저는 구동기/수집기/임무영향분석기/센서 입력값 변형기로 구성되고 실행된다(그림3). 데이터 수집기는 자세 추정 및 제어 모듈, 센서 모듈 등에서 발행(Publish)되는 기체 상태와 관련된 토픽을 구독(Subscribe)하고 퍼저에서 활용할 수 있는 형태로 재가공하고 새로운 토픽으로 발행하여 임무 영향 분석기에서 변형된 센서값에 의한 임무 영향도를 평가할 수 있도록 제공한다.

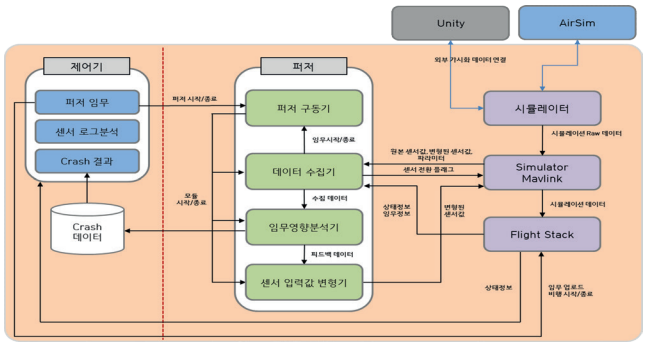

그림 3 IMU영향 분석 구조

임무영향분석기는 첫 번째로 변형된 센서값이 FC에 미치는 영향도를 평가하기 위해서 데이터 수집기에서 발행하는 CollectData 메시지가 업데이트 될 때마다 기체의 제어 오류를 계산하고 이를 기반으로 기체 상태의 이상 여부를 평가한다. 두 번째는 퍼저가 생성한 변형된 센서값이 기체에 미치는 영향을 극대화하기 위하여 발생한 제어 오류를 피드백 스코어로 변환하여 발행한다. 임무 영향 분석기가 수행하는 기능은 퍼저가 변형된 센서값에 의한 공격 성공 여부를 평가하고 퍼징 효율을 향상시키는데 핵심 역할을 한다. 제어 오류 통계는 그림4처럼 계산될 수 있는데 이를 기반으로 그림 5처럼 임계값의 평균을 계산할 수 있다.

	method	field	lower	upper	mean	median	threshold	log file
11	zscore	Roll	-101.9439572	125.7468833	11.90146305	1.707250055	113.8454202	b72c3e0b-124e-40c3-a0e3-066963671cc5.ulg
12	IQR	Roll	-10.04687848	17.09739997	11.90146305	1.707250055	13.57213922	b72c3e0b-124e-40c3-a0e3-066963671cc5.ulg
13	zscore	Roll	-0.177764698	0.214185949	0.018210626	0.006349125	0.195975323	a1c7ee6a-2f88-44c9-82f8-38a03d85dffc.ulg
14	IQR	Roll	-0.010555143	0.025423232	0.018210626	0.006349125	0.017989188	a1c7ee6a-2f88-44c9-82f8-38a03d85dffc.ulg
15	zscore	Roll	-0.558976072	0.638906652	0.03996379	0.009297544	0.598842862	df5d6463-6705-49c9-beb7-84b1980cf762.ulg
16	IQR	Roll	-0.023702376	0.045212947	0.03996379	0.009297544	0.034457661	df5d6463-6705-49c9-beb7-84b1980cf762.ulg
17	zscore	Roll	-0.444867677	0.519997639	0.037064979	0.000289798	0.491932656	a62e7f6b-a176-4eee-839f-0d04892e5f12.ulg
18	IQR	Roll	-0.019999147	0.006962151	0.037064979	0.000289798	0.025480649	a62e7f6b-a176-4eee-839f-0d04892e5f12.ulg
19	zscore	Roll	-192.631975	224.8854576	16.12674129	0.043064704	208.7587163	3ac48412-54bd-405a-956a-e1a31167e1a0.ulg
20	IQR	Roll	-0.798047349	1.332368879	16.12674129	0.043064704	1.065208114	3ac48412-54bd-405a-956a-e1a31167e1a0.ulg
21	zscore	Roll	-371.3830503	536.9157086	82.76632912	0.009130195	454.1493795	2f899655-48c8-4ca7-a587-526294b16346.ulg
22	IQR	Roll	-0.912233555	1.526959777	82.76632912	0.009130195	1.219599666	2f899655-48c8-4ca7-a587-526294b16346.ulg
23	zscore	Roll	-278.5201959	345.1761279	33.32796603	0.010911364	311.8481619	00d8c8cb-0949-4b45-8a9d-80b2f48da5b7.ulg
24	IQR	Roll	-0.036377729	0.067645833	33.32796603	0.010911364	0.052011781	00d8c8cb-0949-4b45-8a9d-80b2f48da5b7.ulg

그림 4 각 비행 로그에서 추출한 제어 오류의 임계값

임계값을 사용하려면 극단부의 영향이 적은 평균치를 사용하는 것이 합리적이다. 데이터가 정규 분포를 따른 경향을 통해 임계치보다 더 클 때 기체 상태 이상을 판단했다고 볼 수 있다. 이를 통해 Crash 정보를 획득할 수 있다.

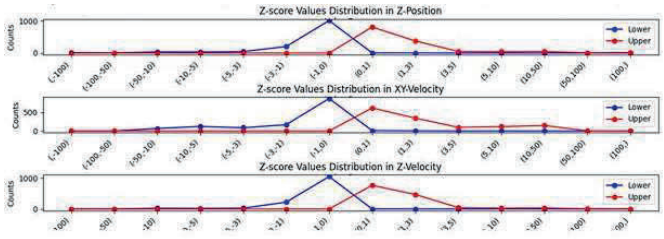

그림 5 임계값의 평균치(일부)

이를 통해 기체의 각 상태에 대한 제어 오류의 누적값을 계산하여 피드백 스코어로 활용하였다. 센서값 변형기는 새로운 센서값이 시뮬레이터로부터 전달될 때마다 호출되고 특정한 진폭과 주파수를 선정하여 사인값을 생성한 후 원본 센서값에 해당 값을 더한 변형된 센서값을 반환하도록 구현하였다.

3. 실험 및 고찰

시그널 앨리어싱(Signal Aliasing) 현상에 의해 센서 출력값이 왜곡되는 점을 이용하기 위하여 진폭과 위상을 조정함으로써 센서 출력값을 원하는 값으로 제어하도록 물리적인 실험환경을 구성하였다.

그림 6 물리적인 구성/AirSim 화면

실제 그림6의 물리 구성도를 기반으로 SITL로부터 나오는 데이터를 Airsim으로 들어가 HILS 장비에 영향을 주도록 구성하였다(그림7).

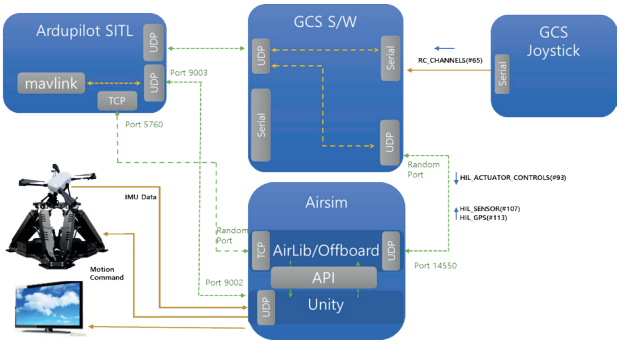

그림 7 공격 영향 실험 구성

변형된 센서값이 동작하도록 자동으로 임무생성이 되도록 구성하였고, 200여개의 CrashData를 획득할 수 있었다. SITL로부터 변형된 센서값을 통해 FC에 미치는 영향을 분석할 수 있었다.

Ⅲ. 결론

본 논문에서는 드론의 안정성과 보안성을 높이기 휘해서 공격에 의한 영향도를 분석할 수 있는 퍼저와 물리적인 환경을 구성하여 실험하였다. 이러한 환경을 활용하여 다양한 임무 상황과 공격 조건을 시뮬레이션 환경에서 실험하고 이를 통해 확보한 데이터를 분석하여 FC의 안정성을 확보하는 데 도움이 될 것으로 기대한다. 향후 연구에서는 시뮬레이션 환경에서 확보한 공격 실험 데이터를 기반으로 IMU 센서 공격에 대응하기 위한 공격 탐지와 대응기술을 연계하여야 할 것이다.

참 고 문 헌

[1] Son, Yunmok, et al. "Rocking drones with intentional sound noise on gyroscopic sensors." 24th USENIX security symposium (USENIX Security 15). 2015.

[2] Trippel, Timothy, et al. "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks." 2017 IEEE European symposium on security and privacy (EuroS&P). IEEE, 2017.

[3] Tu, Yazhou, et al. "Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors." 27th USENIX security symposium (USENIX Security 18). 2018.

[4] Kim, Taegyu, et al. “RVFuzzer: Finding input validation bugs in robotic vehicles through Control-Guided testing.” 28th USENIX Security Symposium (USENIX Security 19). 2019.