Wi-Fi RTT 기반 드론 상호 거리 검증을 통한 경량 GPS 스푸핑 탐지 기법

지채연, *이선영
순천향대학교

wlcodus1262@gmail.com, *sunlee@sch.ac.kr

Lightweight GPS spoofing detection technique based on Wi-Fi RTT-based drone mutual distance verification

Chae Yeon Ji, Sun-Young Lee*
Dept. of Information Security Engineering Soonchunhyang Univ.

요 약

본 논문은 드론의 GPS 스푸핑 공격을 탐지하기 위해 Wi-Fi RTT 기반 드론 간 상호거리 검증 기법을 제안한다.기존탐지 기법의 고비용 문제를 해결하기 위해 추가 센서 없이 Wi-Fi RTT 로 측정한 거리와 GPS 위치를 교차 검증하며,IMU 에서 획득한 상대 속도 벡터를 활용해 고속 비행 시 RTT 패킷 왕복 시간 동안 발생하는 이동 오차를 보정한다. 시뮬레이션 결과, 20m 이상의 스푸핑 공격에 대해 85% 이상, 30m 이상에서는 99% 이상의 탐지율을 달성하여 상용 드론 네트워크의 보안 강화에 효과적임을 입증하였다.

Ⅰ. 서 론

드론(UAV)은 감시, 물류, 재난 대응 등 다양한 분야에서 활용되고 있으며, 대부분 GPS 를 기반으로 위치 추정 및 경로 계획을 수행한다. 그러나 GPS 신호는 암호화되지 않은 민간 신호의 특성상 상대적으로 낮은 비용으로도 위조가 가능하다. 해커가 생성한 허위 GPS 신호는 드론을 비행 금지 구역으로 유도하거나 추락시킬 수 있어 심각한 보안 위협이 된다[1].

기존의 스푸핑 탐지 기법은 다중 안테나 배열, 암호화된 군용 GPS,또는 고정밀 관성 항법 장치(INS)와의 융합에 의존해 왔다. 하지만 이러한 방법은 하드웨어 비용 증가와 배터리 소모 문제를 수반하여 저가형 군집 드론에는 적합하지 않다[2][3].

최근 IEEE 802.11mc 표준에 정의된 Wi-Fi RTT(Fine Timing Measurement) 기술은 별도의 동기화 없이도 미터(m)급 거리 측정이 가능하여 차세대 실내외 측위 기술로 주목받고 있다[5][7].

본 연구에서는 이러한 RTT 기술을 활용하여,인접 드론 간의 '통신 거리'와 'GPS 표시 거리'를 실시간으로 비교함으로써 스푸핑 공격을 탐지하는 기법을 제안한다.

특히, 기존 연구에서 간과되었던 고속 비행 중의 RTT 측정 오차를 분석하고 이를 보정하는 알고리즘을 통해 동적 성능을 검증하고자 한다.

Ⅱ. 관련연구

2.1 GPS 스푸핑 및 탐지 기술

GPS 스푸핑은 수신기가 실제 위성 신호보다 강력한 위조 신호를 추적하도록 유도하는 공격이다. 이를 방어하기 위해 신호 강도(RSS) 모니터링, 도래각(AoA) 분석 등의 물리 계층 보안 기술이 연구되었다[2][3]. 그러나 이러한 방식은 전용 하드웨어가 필요하거나 환경 잡음에 민감하다는 단점이 있다. 최근에는 군집 드론 환경에서의 스푸핑 탐지 메커니즘에 대한 연구도 진행되고 있다[8].

2.2 Wi-Fi RTT 기반 거리 측정

Wi-Fi RTT 송수신 디바이스 간의 프레임 왕복 시간을 측정하여 거리를 산출한다[5][7]. Pagliari et al.의 연구에 따르면 RTT 는 RSSI(신호 세기) 기반 방식보다 다중 경로 페이딩에 강인하며, 드론과 같은 이동체 환경에서도 안정적인 거리 추정이 가능하다[4]. Sugiyama et al.은 실제 드론 호버링 실험을 통해 RTT 가 드론 위치 추정에 유효함을 입증하였으나, 기체 진동에 의한 측정 오차 증가 가능성을 지적하였다[6].

Ⅲ. 제안기법

3.1 시스템 모델

N 개의 드론이 군집 비행을 수행하며, 각 드론은 GPS 와 Wi-Fi RTT 모듈, IMU 센서를 탑재하고 있다고 가정한다. 각 드론 i 는 자신의 GPS 좌표 P_{i}를 주기적으로 브로드캐스팅하며, 인접 드론 j 는 이를 수신하여 상호 거리를 검증한다.

3.2 이동 오차 보정 알고리즘

드론이 고속으로 이동할 경우, RTT 패킷이 왕복하는 시간(Delta t) 동안 드론의 위치가 변하여 거리 측정 오차(epsilon_{motion}) 가 발생한다[4][6].

$$d_{measured} = d_{true} + \epsilon_{noise} + \epsilon_{motion}$$

<수식 1> RTT 측정 거리의 오차 구성

본 연구에서는 IMU 에서 획득한 상대 속도 벡터(v_{rel})를 이용하여 이 이동 오차를 역산하여 제거한다.

$$d_{corrected} = d_{measured} - (v_{rel} \cdot \Delta t)$$

<수식 2> IMU 기반 이동 오차 보정식

이를 통해 순수한 통신 노이즈 (epsilon_{noise})만을 남겨 거리 측정의 정밀도를 높인다[7].

3.3 스푸핑 판정 로직

최종적으로 GPS 좌표 기반 거리(d_{GPS})와 보정된 RTT 거리(d_{corrected})의 차이가 임계값(T_{th})을 초과하면 공격으로 간주한다[8].

$|dGPS - dcorrected| > Tth$

<수식 3> 스푸핑 판정 임계값 비교

Ⅳ. 성능 평가

4.1 실험 환경

제안 기법의 유효성을 검증하기 위해 Python 을 이용한 몬테카를로 시뮬레이션을 수행하였다. 선행 연구의 실측 데이터를 기반으로 보수적인 환경을 설정하였다[4][6][7].

드론 속도 : 15m/s m (고속이동)

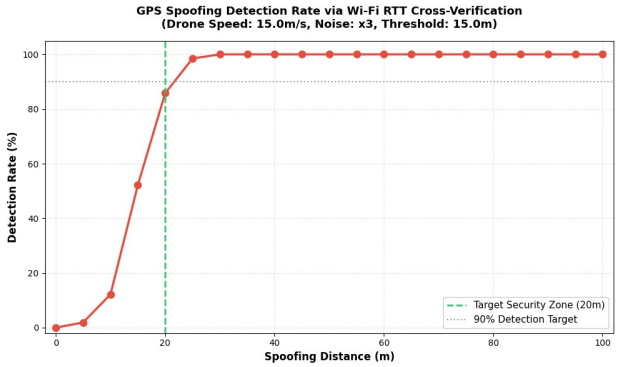
통신 지연 : 100ms

측정 노이즈 : sigma = 4.5 m (지상 환경 대비 3 배)

탐지 임계값 : 15m

4.2 실험 결과 및 결과 분석

스푸핑 거리를 0m 에서 100m 까지 증가시키며 탐지율을 측정한 결과



<그림 1> 스푸핑 거리에 따른 탐지율 변화

10m 이하의 정상 오차 구간에서는 오탐(False Alarm)이 거의 발생하지 않았으며, 20m 이상의 위조 시도에 대해서는 탐지율이 급격히 상승하여 S 자형 곡선을 그렸다. 특히 25m 이상 구간에서는 99% 이상의 탐지율을 기록하여, 제안 기법이 대규모 위치 기만 공격 방어에 매우 효과적임을 확인하였다.

Ⅴ. 결론

본 논문에서는 추가적인 고가 장비 없이 Wi-Fi RTT 기술만을 활용하여 드론 GPS 스푸핑을 탐지하는 실용적인 기법을 제안하였다[4][5][7].기존 탐지 기법들이 다중 안테나 배열이나 암호화된 군용 GPS 등 고비용 하드웨어를 요구하는 것과 달리[2][3],본 기법은 사용 드론에 이미 탑재된 Wi-Fi 모듈과 IMU 센서만을 활용하여 경제성과 실용성을 확보하였다.시뮬레이션 결과 25m 이상의 스푸핑 공격에 대해 99% 이상의 탐지율을 달성하여 군집 드론 환경에 실질적으로 적용 가능함을 입증하였다[8].

향후 연구에서는 제안하는 Wi-Fi RTT 기반 탐지 기법을 실제 드론 플랫폼에 구현하여 다양한 비행 패턴 및 기상 조건에서의 현장 실험을 통해 실용성을 검증할 필요가 있다.또한 UWB 등 다른 거리측정 기술과의 비교 실험을 통해 RTT 기반 접근법의 상대적 우수성을 입증하고, 기계학습 기반 이상 탐지 알고리즘과의 융합을 통해 탐지 정확도를 더욱 향상시키는 연구가 필요하다[2][3].

ACKNOWLEDGMENT

본 연구는 정부(과학기술통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (NO. RS-2024-00346749)

참 고 문 헌

[1] Restivo, P., & Dodson, A., “GPS Spoofing on UAV: A Survey,” *Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS)*, pp. 1- 10, 2018.

[2] Ma, X. et al., “Detection of GPS Spoofing Attacks in UAVs Based on Adversarial Machine Learning,” *Sensors*, vol. 24, no. 19, 2024.

[3] AlAbidy, A. et al., “A Survey on AI-Based Detection Methods of GPS Spoofing Attacks on UAVs,” *IEEE Conference on Artificial Intelligence*, Aug. 2024.

[4] Davoli, L. et al., “Wi-Fi-Based Real-Time UAV Localization: A Comparative Analysis Between RSSI-Based and FTM-Based Approaches,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 60, no. 4, 2024.

[5] Kosek-Szott, K. et al., “Indoor Positioning with Wi-Fi Location: A Survey of IEEE 802.11mc Fine Timing Measurement,” *IEEE Communications Surveys & Tutorials*, 2020.

[6] Sugiyama, Y. et al., “Experimental Study on Indoor Drone Positioning Using Wi-Fi RTT,” *IEICE Communications Express*, vol. 13, no. 9, 2024.

[7] Gupta, A. et al., “Accurate Indoor Positioning Using IEEE 802.11mc Round Trip Time,” *Computer Communications*, vol. 119, pp. 24- 34, 2018.

[8] Mykytyn, P. et al., “GPS-Spoofing Attack Detection Mechanism for UAV Swarms,” *Informatica*, vol. 48, no. 3, pp. 345- 360, 2024.