

디지털 트윈 기반 GPS 스푸핑 탐지 관한 연구

오석원¹, 송수빈¹, 이정범¹, 정경현², 김현수², 이창건³, 권태경³

¹서울대학교 컴퓨터공학부 석사과정

²서울대학교 컴퓨터공학부 박사수료

³서울대학교 컴퓨터공학부 교수

swoh@mmlab.snu.ac.kr, sbsong@mmlab.snu.ac.kr, jblee@mmlab.snu.ac.kr, ghjeong@mmlab.snu.ac.kr,
hskim@mmlab.snu.ac.kr, cglee@snu.ac.kr, tkkwon@snu.ac.kr

A Study on GPS Spoofing Detection Based on Digital Twin

Seokwon Oh¹, Subin Song¹, Jungbum Lee¹, Gyeongheon Jeong², Hyunsoo Kim²,
Chang-gun Lee³, Taekyoung (Ted) Kwon³

¹Dept. of Computer Science and Engineering, Seoul National University

²Dept. of Computer Science and Engineering, Seoul National University

³Dept. of Computer Science and Engineering, Seoul National University

요 약

DT(Digital Twin)는 물리적 현실 세계 데이터를 실시간으로 수집하여 디지털 세계에서 동일하게 구현하는 기술이다. DT 활용하여 현실 세계의 위험상황을 예측하고 방지할 수 있다. 본 연구는 DT가 디지털 디바이스의 현실 세계 현재 위치 데이터를 실시간으로 수집하고 디지털 세계에서 동일하게 구현하여 GPS(Global Positioning System) 스푸핑(Spoofing) 공격을 탐지하는 기법을 제시한다. 추가로 현실 세계 도심 항공 교통(Urban Air Mobility)과 사용자 디지털 디바이스에 적용 가능하다는 점을 제시한다. 도심 항공 교통의 경우 DT 서버는 모든 비행체의 GPS 위치 정보와 각 비행체의 인접 비행체 거리 정보를 실시간으로 수집한다. 두 가지 종류의 위치 정보 비교를 통해 비행체 위치 정보의 이상 상황을 탐지한다. 사용자 디지털 디바이스의 경우 DT 서버는 모든 디바이스의 GPS 위치 정보와 각 디바이스의 인접 디바이스 거리 정보를 실시간으로 수집한다. 두 가지 종류의 위치 정보 비교를 통해 디바이스 위치 정보 이상 상황을 탐지한다.

1. 서론

DT(Digital Twin)는 물리적 현실 세계를 디지털 세계에서 모방하는 기술이다. 물리적 현실 세계의 데이터를 실시간으로 수집하고 디지털 세계에서 구현한다. DT를 활용하여 안전성, 보안성 등의 이점을 확보할 수 있다.

도시 지상교통 혼잡 해결 수단으로 UAM(Urban Air Mobility)이 주목된다. 또한 UAM 시장 발전 가능성에 맞춰 다양한 도전과 경쟁이 확대되고 있다. K-UAM 로드맵의 주요 가치는 안전성, 지속 가능성, 국민 편의다[1]. 본 연구는 DT를 활용하여 비행체가 GPS(Global Positioning System) 스푸핑(Spoofing) 공격을 받는 상황을 탐지하며 안전성을 보장하는 기법을 제시한다. GPS 스푸핑 공격을 받은 비행체가 가짜 GPS 위치 정보로 인해 의도하지 않는 장소로 비행하는 이상 현상을 방지하는 것이다.

이를 달성하기 위해서는 UAM 비행체와 DT 서버

의 실시간 통신이 요구된다. 비행체의 GPS 위치 정보를 DT 서버에게 실시간으로 전송하는 것이 필요하다. 또한 비행체와 인접 비행체까지의 거리를 계산하여 DT 서버에게 실시간으로 전송할 것이 요구된다. DT 서버는 비행체의 GPS 위치 정보와 인접 비행체까지의 거리를 비교하여 GPS 스푸핑 여부를 탐지한다.

GPS 스푸핑이 탐지되면 DT 서버는 현실 세계의 데이터를 수집하여 디지털 세계를 구현한 내용을 토대로 현재 상황을 고려한 위험 등급을 판단하고 일부 혹은 전체 비행체에 알람을 주고 제어하는 것이 가능할 것이다. 건물, 사람, 지형, 기후에 따라 위험 등급 실시간 파악하는 것이 가능할 것이다.

또한 인터넷에 연결되는 기기들이 빠르게 증가하고 있고[2] 2023년 한국 성인 스마트폰 사용률은 97%이다[3]. 내비게이션 애플리케이션, 지도 애플리케이션도 존재하는 만큼 사용자 디지털 디바이스도 GPS 스푸핑 공격에 대한 방어가 요구된다.

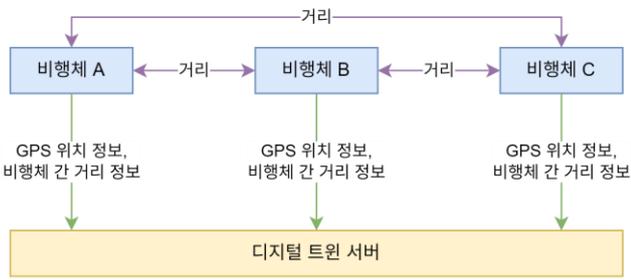
이에 따라 사용자 모바일 디바이스, IoT 디바이스, TV 디바이스에도 동일한 기법을 적용할 수 있다. 디바이스의 GPS 위치 정보를 DT 서버에 실시간으로 송신하고 인접 디바이스까지의 거리를 측정하여 DT 서버에 실시간으로 전송한다. DT 서버는 두 종류의 위치 정보를 비교하여 GPS 스푸핑 여부를 탐지한다. 탐지되면 DT 서버가 현재 상황을 고려한 위험 등급을 판단하고 알림을 주고 제어하는 것이 가능할 것이다.

2. 본론

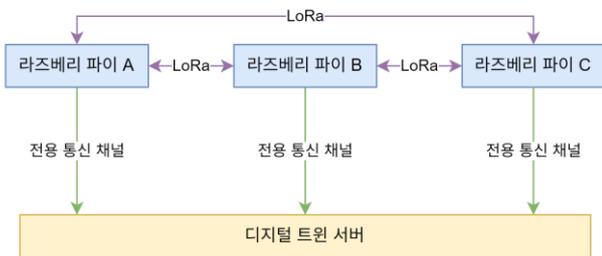
그림 1 과 같이 UAM 비행체 A, 비행체 B, 비행체 C 가 존재한다고 가정하겠다. 비행체 모두 DT 서버에 GPS 위치 정보를 실시간으로 송신한다.

또한 본 연구에서는 고도 차이는 고려하지 않는다. 실제 비행체 운영 환경에서는 GPS 고도 측정값, 기압 센서 등의 활용이 추가로 요구된다.

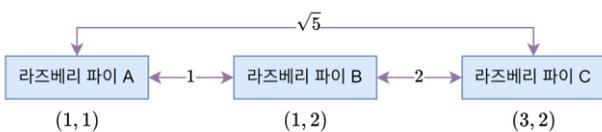
동시에 각 비행체는 인접 비행체에서 받은 무선 신호의 RSSI(Received Signal Strength Indicator)를 측정한다. RSSI 는 수신된 신호 강도이다. 거리가 가까울수록 값이 커지고 멀어질수록 값이 작아진다. 이를 통해 수신기와 송신기 사이의 거리 계산을 수행한다. 즉 그림 1 과 같이 비행체 간의 거리 계산을 수행한다.



(그림 1) GPS 스푸핑 탐지 실험 구상도



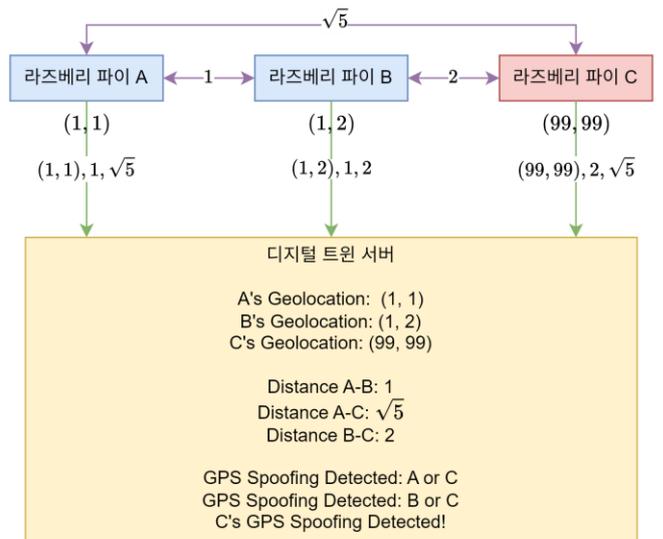
(그림 2) GPS 스푸핑 탐지 실험 환경



(그림 3) 라즈베리 파이 간 거리 예시

그림 2 와 같이 비행체 A, B, C 를 라즈베리 파이 A, B, C 로 대체 및 실험 환경 구성 가능하다. 라즈베리 파이에는 GPS 센서와 LoRa 통신 모듈 탑재가 요구된다. 라즈베리 파이가 자신의 GPS 신호를 받는 것이 확인된다. 또한 다른 위치의 2 개 라즈베리 파이에서 LoRa 통신 수행되는 것이 확인되고, 이를 이용해 RSSI 기반 거리 계산 수행 가능하다는 것이 확인된다. 개념 검증 환경에서 LoRa 통신 활용하지만, 실제 비행체 운영 환경에서는 UAM 전용 통신 기술이 활용될 것으로 예상된다.

그림 4 와 같이 라즈베리 파이 C 가 GPS 스푸핑 되었다고 가정하겠다. 라즈베리 파이 C 의 GPS 위치 정보는 가짜 위치 정보일 것이다. 그러면 DT 서버는 라즈베리 파이 C 의 가짜 위치 정보를 수신한다. 하지만 라즈베리 파이 간의 거리 정보는 LoRa 무선 신호 통해 계산하기 때문에 GPS 스푸핑 공격에 영향 받지 않는다. 이에 따라 라즈베리 파이 간의 거리 정보는 가짜 정보가 아닌 실제 비행체의 위치 정보 토대로 계산되어 전달된다.



(그림 4) GPS 스푸핑 탐지 시나리오 예시

그림 4 와 같이 DT 서버는 라즈베리 파이 C 의 GPS 위치 정보가 라즈베리 파이 A-C, B-C 거리 정보와 일치하지 않는다는 점을 탐지할 수 있다. 이에 따라 라즈베리 파이 C 의 위치 정보 이상 현상을 탐지할 수 있다.

라즈베리 파이 A, B, C 는 서로 LoRa 통신을 수행하기 때문에 독립적인 라즈베리 파이 간의 거리 정보를 보유한다. 파이썬, C 언어로 거리 계산 프로그램 구현하고 파일 형태로 거리 정보를 DT 서버에게 전송 가능하다.

라즈베리 파이 A, B, C 는 DT 서버와 전용 통신 채널

널로 통신한다. 전용 통신 채널로 GPS 위치 정보, 거리 정보 전송한다.

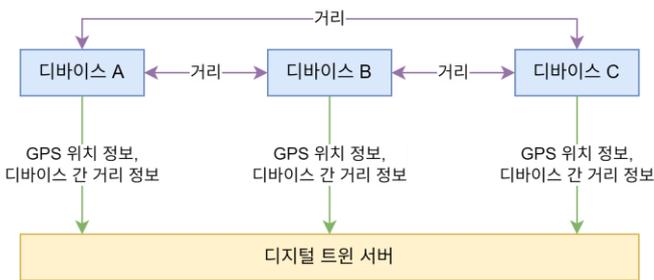
GPS 스푸핑은 SDR(Software Defined Radio)로 구현 가능하다. 가짜 GPS 신호를 생성하여 타겟 라즈베리 파이의 GPS 모듈에만 영향을 주는 방식이다. 라즈베리 파이는 가짜 GPS 위치 정보를 보유하고, 이를 DT 서버에게 전달하게 된다.

DT 서버는 현실 세계의 데이터 기반 디지털 세계를 구현하고 있다. 이에 따라 GPS 스푸핑이 탐지되는 경우 스푸핑 된 비행체를 인접 건물, 사람, 지형, 기후에 따라 비행체를 제어하는 것이 가능할 것이다. GPS 스푸핑이 탐지되면 GPS 신호를 무시하도록 제어하거나 속도를 감속하는 등의 조치가 가능할 것이다.

모바일 디바이스, TV 디바이스, IoT 디바이스와 같은 사용자 디지털 디바이스에도 동일한 기법 적용 가능하다. 그림 5 와 같이 사용자 디지털 디바이스의 경우 디바이스 A, B, C 가 존재한다고 가정하겠다. 또한 디바이스 A, B, C 는 LoRa 통신 모듈 탑재 및 LoRa 통신이 가능하다고 가정하겠다.

디바이스 모두 DT 서버에게 GPS 위치 정보를 실시간으로 송신한다. 동시에 디바이스 A 는 디바이스 B, C 와 무선 신호 RSSI 추출 후 거리 계산한다. 디바이스 B, C 도 동일하게 거리 계산한다.

디바이스 C 에 GPS 스푸핑이 발생하면 DT 서버는 디바이스 C 의 가짜 GPS 위치 정보를 받을 것이다. 하지만 디바이스 A-C, B-C 거리 정보는 가짜가 아니기 때문에 DT 서버는 디바이스 C 의 GPS 스푸핑을 탐지할 수 있다.



(그림 5) 디바이스의 GPS 스푸핑 공격 탐지 실험 구성도

```

Geolocation
A's Geolocation: (37.45028, 126.953012)
B's Geolocation: (37.450017, 126.952445)
C's Geolocation: (37.449565, 126.951702)
Distance
A - B: 58.043955989008445
A - C: 140.47572860351568
B - C: 82.69753116442531
    
```

(그림 6) 개념 실험 결과 - 정상 상황

```

Geolocation
A's Geolocation: (37.46218, 126.956162)
B's Geolocation: (37.448757, 126.951815)
C's Geolocation: (37.363275, 126.715814)
Distance
A - B: 1538.6148000805601
A - C: 757.4245948345315
B - C: 928.5763232956364
WARNING! GPS spoofing detected
A or C
WARNING! GPS spoofing detected
B or C
== C is under attacked ==
    
```

(그림 7) 개념 실험 결과 - 공격 탐지 상황

그림 6 과 7 은 각각 정상 상황과 공격을 탐지하는 상황의 개념 실험 출력 형태를 보여준다. 전용 통신 채널 통해 A, B, C 의 위치 정보 실시간 전송된 것으로 가정한다. A, B, C 의 좌표는 위경도로 나타나고 이를 이용하여 GPS 를 이용한 이들 간의 거리를 계산한다. 해당 결과와 A, B, C 가 전달한 각 거리를 비교하여 오차 범위 내면 정상, 오차 범위 외면 공격 탐지로 판단한다.

반면, GPS 기기 오작동 하는 경우에도 DT 위치 인식의 오차가 발생 가능하다. 현재 솔루션에서 해당 상황도 GPS 스푸핑으로 탐지된다는 한계점을 가진다. 이를 대비하여 일정 거리 범위 내에서 발생하는 오차는 GPS 스푸핑으로 탐지하지 않는 것이 필요할 것으로 예상된다. 또한 추가 검증 수단을 혼합하는 것도 가능하다. 멀티 팩터 검증을 통해 DT 위치 인식 오차를 탐지하는 것이다. 예를 들어 시각 정보, 레이더(Radar), LiDAR 등 다양한 정보를 종합하여 해당 오차가 실제 공격에 의한 것인지 장비 오작동 문제인지 판단할 수 있다.

3. 결론

DT(Digital Twin) 기술을 활용하여 비행체, 디바이스의 GPS 스푸핑을 탐지하는 기법을 제시한다. 비행체, 디바이스의 GPS 위치 정보와 RSSI 통해 계산한 인접 비행체, 인접 디바이스와의 거리 정보를 DT 서버에게 전달하고, 이를 통해 DT 서버는 비행체, 디바이스의 GPS 스푸핑을 탐지하고 위험 상황을 감지할 수 있다. 도시 지상 교통이 혼잡해지고 인터넷에 연결되는 기기의 종류와 개수가 다양해지면서 GPS 스푸핑 탐지는 더욱 중요해질 것으로 예상된다.

ACKNOWLEDGMENT

이 연구는 정부 (과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. RS-2023-00220985)

참고문헌

- [1] 관계부처 합동, “도시의 하늘은 여는 한국형 도심 항공교통(K-UAM) 로드맵”, 2020.5
- [2] 한국스마트헬스케어협회 신중훈 사업본부장, “일상 속 IoT(Internet Of Things) 활용과 남겨진 과제”, https://www.kca.kr/hot_clips/vol70/sub01.html?lang=ko, 2021.11
- [3] 갤럽리포트, “2012-2023 스마트폰 사용률&브랜드, 스마트워치, 무선이어폰에 대한 조사”, <https://www.gallup.co.kr/gallupdb/reportContent.asp?seqNo=1405>, 2023.7