UAV 기반 재난 재해 감시 시스템에서 GPS 스푸핑 방지를 위한 연합학습 모델링

김동희*, 도인실**, 채기준***
*이화여자대학교 인공지능·소프트웨어학부
**이화여자대학교 사이버보안전공
***이화여자대학교 컴퓨터공학전공
ddonghe.kim@ewhain.net, isdoh1@ewha.ac.kr, kjchae@ewha.ac.kr

Federated Learning modeling for defense against GPS Spoofing in UAV-based Disaster Monitoring Systems

DongHee Kim*, InShil Doh**, KiJoon Chae***
*Div. of Artificial Intelligence and Software, Ewha Womans University
**Dept. of Cyber Security, Ewha Womans University
***Dept. of Computer Science and Engineering, Ewha Womans University

요 약

무인 항공기(UAV, Unmanned Aerial Vehicles)는 높은 기동성을 가지며 설치 비용이 저렴하다는 이점이 있어 홍수, 지진 등의 재난 재해 감시 시스템에 이용되고 있다. 재난 재해 감시 시스템에서 UAV는 지상에 위치한 사물인터넷(IoT, Internet of Things) 기기로부터 데이터를 수집하는 임무를 수행하기 위해 계획된 항로를 따라 비행한다. 이때 UAV가 정상 경로로 비행하기 위해서는 실시간으로 GPS 위치 확인이 가능해야 한다. 만일 UAV가 계산한 현재 위치의 GPS 정보가 잘못될 경우 비행경로에 대한 통제권을 상실하여 임무 수행을 완료하지 못하는 결과가 초래될 수 있다는 취약점이 존재한다. 이러한 취약점으로 인해 UAV는 공격자가 악의적으로 거짓 GPS 위치 신호를 전송하는 GPS 스푸핑(Spoofing) 공격에 쉽게 노출된다. 본 논문에서는 신뢰할 수 있는 시스템을 구축하기 위해 지상에 위치한 기기가 송신하는 신호의 세기와 GPS 정보를 이용하여 UAV에 GPS 스푸핑 공격 여부를 탐지하고 공격당한 UAV가 경로를 이탈하지 않도록 대응하기 위해 연합학습(Federated Learning)을 이용하는 방안을 제안한다.

1. 서론

무인 항공기(UAV, Unmanned Aerial Vehicles)는 사용자의 조작 없이도 자동으로 비행하는 비행체로 높은 기동성을 가져 배치하기에 용이하다는 이점이 있다. 따라서 최근 넓은 지역을 커버하는 운송, 재난 감시, 레저, 정찰, 탐사 등 여러 분야에서 사용되고 있다. 특히 시스템의 운영 영역보다 통신 수요가 적은 경우 기지국을 설치하는 것보다 UAV를 이용해 통신하는 것이 비용적인 측면에서 효과적이므로 홍수, 지진, 산사태와 같은 재난 재해 감시 시스템에서 UAV를 활용한 시스템 구축이 활발하게 이루어지고 있다 [1].

재난 재해 감시 시스템은 소형 사물인터넷(IoT, Internet of Things) 센서를 이용해 수심 또는 지면 온도와 같은 환경 정보를 측정하여 재난 재해가 발생하기 전 미리 방지할 수 있는 시스템이다. 이는 감시 영역이 광범위한 데 비해 지상에서 정보를 수집하는 장치는 국소적으로 위치해 있으며, 또한 센서 기기는 환경을 측정하는 데 시간이 소요되기 때문에 실시간으로 데이터를 전송하지 않아 UAV를 사용하여 필요한 지역의 데이터를 수집하는 것이 효과적이다. 따라서 재난 재해 감시 시스템에서 UAV는 주기적으로 비행을 통해 사물인터넷 센서가 송신하는 데이터를 수집하는 임무를 수행하게 되는데 이때 비행경로는 임무 수행률과 소요되는 시간의 효율을 최적화할 수 있도록 미리 설정된다.

UAV는 GPS 위치 정보에 의해 경로를 따라 비행하기 때문에 비행하는 동안 GPS 센서를 통해 위치 정보를 실시간으로 수집해야 한다. 때문에 GPS 전파에 대한 방해 공격에 쉽게 노출될 수 있다. 특히, 공격자가 실제 GPS 값을 조작하여 교란된 신호를 송신하는 GPS 스푸핑(Spoofing) 공격이 발생할 수 있는데 이는 잡음이 포함된 GPS 신호를 수신한 UAV가 현재 위치를 잘못 계산하게 하여 항로 이탈

을 유도하거나 추락으로 인한 사고를 야기한다. 때문에 GPS 스푸핑 공격을 탐지하고 이에 대응하는 신뢰 가능한 기법이 적용되어야 한다.

반면 UAV는 물리적인 제한으로 인해 저장 장치 및 컴퓨팅 자원에 대한 제약이 존재한다. 만약 공격을 방어하는 방안에서 계산 과정이 복잡하면 공격에 대응할 수 있는 적절한 시간 안에 탐지하기 어렵다.

따라서 본 논문에서는 UAV의 제한적인 자원을 효율적으로 사용하기 위해 지상의 IoT 기기가 전송하는 GPS 정보와 신호 세기를 통해 UAV의 GPS 스푸핑 공격이 탐지되면 연합학습(Federated Learning)의 결과로 UAV 위치를 재설정하는 방안에 대해 제안한다.

본 논문의 구성은 2장에서는 GPS 스푸핑 공격과 연합학습에 대해 살펴보고 3장에서는 제안하는 GPS 스푸핑 방지를 위한 연합학습 모델링을 설명한다. 마지막으로 4장에서 결론과 향후 연구에 관해 기술한다.

2. 관련 연구

a. UAV-GPS 스푸핑

GPS 스푸핑 공격은 GPS 신호 수신자에게 거짓 GPS 위치 신호를 전송하여 수신자가 실제 GPS 위치 값을 상실하게 하는 공격을 의미한다. 공격자는 실제 GPS 신호를 탈취하여 위조된 복제 신호를 만든다 [2]. GPS 신호는 GPS 신호를 송신하는 위성과 수신하는 UAV 사이의 거리가 멀어질수록 약해진다. 따라서 공격자가 조작한 거짓 신호를 GPS 위성의 정상적인 신호보다 높은 세기로 전송하면 주파수가 위·변조되어 UAV는 오차가 인가된 위치 정보를 생성한다. UAV가 계산한 위치 정보가 변경됨에 따라 공격자가 원하는 항로로 유도되거나 장애물과의 충돌로 인해 추락할 수 있다. 따라서 GPS 스푸핑 공격에 의해 UAV가 정상적으로 임무를 수행할 수 없는 결과가 초래된다.

이를 해결하기 위해 GPS 신호에 대해 암호화 프로토콜을 사용한 신호 인증 방안과 UAV가 촬영한 주변 환경 이미지에서 물체의 속력 벡터를 분석하여 GPS 스푸핑 공격을 탐지 방안이 연구되었다 [3], [4]. 그러나 이러한 방법은 암복호화와 이미지 처리를 위한 계산 과정이 추가된다는 문제점이 여전히 존재한다. 따라서 본 논문은 UAV의 자원을 효율적으로 사용할 수 있도록 GPS 스푸핑 공격 탐지를 위한 계산 과정을 간소화하는 방안을 제안한다.

b. 연합학습

심층학습(Deep Learning)은 4차 산업 혁명의 핵심 기술로 모델의 예측 정확도 향상을 위한 여러 가지 학습 기법에 대한 연구가 활발히 진행되고 있다. 그러나 심층학습은 모델을 학습하기 위한 컴퓨팅 자원을 많이 요구하기 때문에 자원이 한정적인 기기가 사용되는 분산 시스템에 적용하는 것은 어려움이 있다. 이를 해결하기 위해 참여 노드들에 학습 모델의 일부를 배분하여 자원 사용 부담을 줄이는 분산학습(Distributed Learning)이 연구되고 있다.

연합학습은 분산학습의 일종으로 데이터 세트(Data Set)를 교환하지 않고 동일한 학습 모델을 각각의 참여 노드에서 발생하는 데이터를 이용해 학습하는 기법이다. 심층학습에서 학습 모델의 예측 정확도는 다양한 데이터를 이용해 학습할수록 높아지게 되므로 연합학습은 학습 성능 향상을 위해 전체 노드의 데이터를 학습 모델에 반영할 수 있도록 모델을 하나로 통합하고 재분배하여 다시 학습하는 과정을 진행한다. 이때, 모델을 하나로 통합하기 위해 데이터 세트가 아니라 모델의 파라미터만을 교환하기 때문에 데이터의 보안성을 높일 뿐만 아니라 학습 정확도 향상을 달성할 수 있다는 장점이 있다 [5]. 또한 중앙집중식 모델 학습 방법보다 상대적으로 계산 부담이 적어 저장 장치와 계산 비용이 제한적인 IoT 기기에서 적합한 학습 방법이다. 이러한 이점으로 인해 여러 UAV가 사용되는 분산 시스템에서 연합학습을 적용하기 위한 연구가 증가하고 있다 [6]. 특히 UAV는 실시간 비행에 의해 토폴로지가 빠르게 변하기 때문에 중앙 집중식 공격 탐지는 적합하지 않다. 이러한 이유로 본 논문은 연합학습을 적용하여 UAV의 전파 공격을 탐지하고자 한다.

3. GPS 스푸핑 방어 방안 제안

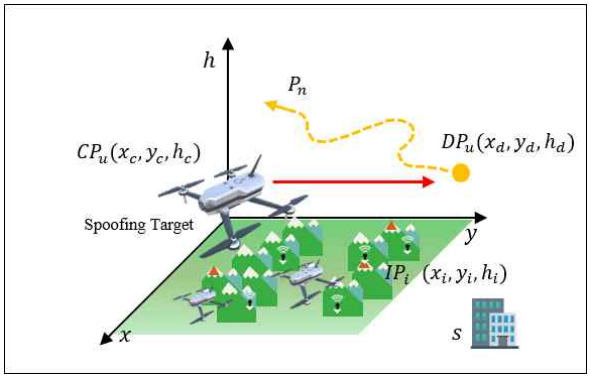
a. 시스템 모델

UAV를 이용한 재난 재해 감시 시스템 모델은 그림1과 같이 항공을 주행하는 UAV 그룹 U와 지상에서 환경을 감지하는 IoT 센서 기기 그룹 I로 이루어져 있다. 그룹 U는 UAV의 개수가 n이라고 할 때 $U=\{u_1,u_2,...,u_n\}$이며 u_n의 현재 위치(Current Position)는 $CP_u(x_c,y_c,h_c)$로 나타낼 수 있다. 재난 재해 감시 시스템에서 I는 일정 주기 동안 데이터를 측정하므로 특정 시간 t마다 측정한 데이터를 전송하는 I는 고정적이다. 따라서 출발 지점(Start Position) S에 위치한 시스템 제어 기관은 비

행 시작 시각 t_s부터 비행 종료 시각 t_e 구간 동안 데이터를 전송할 I의 데이터를 모두 수집할 수 있도록 위치, 속도, 방향과 같은 항법 정보를 기반으로 최적의 비행경로(Path) P를 설정한다. P는 UAV가 비행해야 하는 l개의 목적지 위치(Destination Position) $DP_u(x_d, y_d, h_d)$ 집합을 포함하고 있다. DP는 k-means 알고리즘을 이용해 t에 데이터를 송신하는 I의 데이터를 효율적으로 수집할 수 있도록 클러스터링하여 UAV들의 P에 포함한다. P의 l번째 DP에서 u_n이 데이터를 수집하기 위해 클러스터링된 IoT 기기의 개수가 m개라고 할 때 $I_u^l = \{ i_{n1}^l, i_{n2}^l, ..., i_{nm}^l \}$로 나타낼 수 있으며 i_{nm}^l의 위치는 $IP_{nm}^l(x_i, y_i, h_i)$으로 표현한다. 또한 i가 전송하는 신호의 세기(Signal Strength)는 SS_{nm}^l로 표현한다.

<표 1> 주요 기호 설명

기호	설명
U	n개의 UAV u집합
CP_u	u_n이 계산한 현재 GPS 위치 정보
P	u_n이 비행하는 경로
DP_u	P를 구성하는 목적지 집합
l	DP_u의 순서
I_u^l	u_n이 데이터를 수집하기 위해 클러스터링된 IoT 기기 집합
S	U의 출발 지점
IP_{nm}	u_n으로 데이터를 송신하는 기기 i_{nm}^l의 GPS위치 정보 집합
SS_{nm}^l	i_{nm}^l이 송신하는 신호의 세기
R	u_n과 i_{nm}^l 사이의 거리 집합
$complete\ rate$	i_{nm}^l가 송신한 데이터 양과 u_n이 수신한 데이터 양의 비율



(그림 1) 시스템 모델

b. UAV-GPS 스푸핑 방어 기법

본 논문은 통신 대상 간의 거리가 가까울수록 높은 신호 세기를 가진다는 특성을 사용하여 공격 여부를 탐지한다. IoT 기기와 UAV의 GPS 값을 기반으로 거리에 따른 신호 세기를 비교하면 UAV가 기만 표적(Spoofing Target)이 되었는지 탐지할 수 있다. 따라서 공격에 대응하기 위해 경로를 이동하는 에피소드마다 UAV가 위치하게 되는 GPS 값에서 IoT 기기의 위치 및 신호 세기 관계를 파악한 데이터를 수집하여 실제로 위치를 파악할 수 있도록 심층학습을 적용하는 기법을 제안한다. 해당 기법을 통해 UAV가 GPS 스푸핑 공격에 의해 실제 GPS 값을 모르더라도 기존에 설정된 최적의 경로를 이탈하지 않고 원래 위치를 찾아갈 수 있다. 또한 UAV가 학습한 모델을 통합하는 연합학습을 적용하여 자원을 효율적으로 사용하면서 학습 정확도를 높이고자 한다. 이에 대한 결과로 UAV가 기지국과 같은 중앙 서버와 통신 없이 스스로 GPS 스푸핑을 탐지할 수 있다. 본 논문에서 제안하는 UAV-GPS 스푸핑 방어 과정은 다음과 같다.

1) 데이터 수집: UAV는 공격 탐지 및 방어를 위해 비행하는 동안 IoT 기기 간의 거리와 신호 세기의 관계를 파악하기 위한 데이터를 저장한다. UAV u_n는 현재 위치 CP_u와 IP_{nm}^l들의 거리를 계산한다. 그리고 SS_{nm}^l와 함께 데이터 세트 DS_u에 저장한다. 또한 DP^l을 예측하기 위해서는 신호 세기가 정상 범위인지 판단하기 위해 UAV의 임무 수행률(Complete Rate)을 계산해야 한다. 따라서 I_u^l로 부터 데이터 수신이 종료되었을 때 I_u^l가 UAV와 통신을 시작할 때 송신했던 전송할 데이터의 크기와 수신된 데이터의 크기를 이용해 임무 수행률을 계산하여 DS_u에 저장한다. 결과적으로 UAV가 비행하는 동안 공격을 탐지하기 위해 l, CP_u, IP_{nm}^l, SS_{nm}^l, R에 대한 데이터를 저장한다.

2) 정상 경로 예측을 위한 연합학습: UAV는 비행 중 생성한 DS_u를 사용하여 목적지를 예측하는 모델을 학습한다. DP^l는 데이터 수집의 효율성을 최적화할 수 있도록 계산된 목적지 위치이다. 따라서 DP^l를 계산하기 위해 변수에 따라 UAV가 데이터 수집률이 최대가 되는 최적의 위치를 계산해야 한다. 그러나 UAV의 비행에 따른 환경이 계속해서 변하기 때문에 UAV에 학습 모델을 구축하여 DP^l을 예상한다.

본 논문에서 적용하는 연합학습을 진행하기 위해 먼저 각각의 UAV u_n가 학습하고 U의 모델을 통합하며 진행된다. UAV u_n는 손실 함수(Loss Function) L을 최소화할 수 있는 지역 가중치(Local

Weight) 집합 LW_u을 반복하여 계산한다. 그리고 출발 지점 s로 돌아오면 출발 지점에 위치한 기지국은 각 UAV의 학습 모델 파라미터 집합 LW_u를 이용해 전역 가중치(Global Weight) GW를 계산하고 배포함으로써 모델을 통합한다. 이는 다음과 같이 표현할 수 있다.

$$GW = \frac{1}{N}\sum_{u=1}^{n} LW_u$$

3) 신호 세기를 이용한 GPS 스푸핑 공격 탐지: UAV는 DS_u를 사용하여 심층학습 모델 학습 뿐만 아니라 공격 탐지를 위한 계산을 진행해야한다. 만약 CP_u와 IP_{nm}^{l} 사이의 거리에 기대되는 신호 세기보다 SS_{nm}^{l}가 너무 크거나 작은 이상치를 가지면 CP_u가 잘못되었을 수 있다. 그러나 신호 세기는 전파의 잡음 등 영향을 받는 다른 요소들이 존재하므로 CP_u 값이 오류라고 단정 지을 수는 없다. 따라서 거리에 따른 신호 세기의 오차 범위를 벗어나는 기기가 과반수 이상이라면 CP_u 값의 오류로 판단하고 GPS 스푸핑 공격을 당한 것으로 탐지한다.

4) GPS 스푸핑 공격이 탐지되면 경로로부터 이탈된 위치를 재설정하기위해 학습 모델이 예측한 결과인 DP^{l}로 이동한다.

5) 현재 위치 CP_u는 거짓 정보이므로 CP_u의 상대적인 위치를 계산한 DP^{l} 또한 이상 수치이다. 따라서 UAV는 이동 후 CP_u를 원래의 DP^{l}로 재설정한 후 정상 경로 P를 따라 비행을 진행한다.

4. 결론

UAV 기반 재난 재해 감시 시스템은 UAV 센서의 취약점을 이용한 GPS 스푸핑 공격 위협이 존재한다. GPS 스푸핑 공격은 악의적으로 조작한 GPS 신호를 주입하여 UAV의 항로를 변경함으로써 UAV가 임무를 수행할 수 없도록 한다. 이에 대한 해결책으로 본 논문은 UAV가 자체적으로 지상의 IoT 기기의 위치 및 신호 세기 정보를 이용하여 GPS 스푸핑이 발생했는지 탐지하고 연합학습을 통해 실제 위치로 이동하는 기법을 제안했다. 결과적으로 UAV의 자원을 효율적으로 사용하여 GPS 스푸핑 공격에 대응할 수 있어 UAV가 기존에 설정된 경로를 따라 임무 수행을 완료할 수 있을 것으로 기대된다.

향후 연구에서 시뮬레이션을 통해 GPS 스푸핑 공격 탐지율을 확인하고 학습을 통해 계산한 재설정 위치의 정확도를 확인하여 제안하는 메커니즘의 타당성을 제시하고자 한다.

Acknowledgement

이 논문은 2019년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2019R1F1A1063194). 또한, 이 논문은 2020년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2020R1A2C1006497). (교신저자: 채기준)

참고문헌

[1] M. Evita, A. Zakiyyatuddin, W. Srigutomo, N. Aminah, I. Meilano, and M. Djamal, "Photogrammetry using Intelligent-Battery UAV in Different Weather for Volcano Early Warning System Application," in Journal of Physics: Conference Series, 2021, vol. 1772, no. 1: IOP Publishing, p. 01, 2017.

[2] E. Basan, A. Basan, A. Nekrasov, C. Fidge, J. Gamec, and M. Gamcová, "A self-diagnosis method for detecting UAV cyber attacks based on analysis of parameter changes," Sensors, vol. 21, no. 2, p. 509, 2021.

[3] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-time GPS spoofing detection via correlation of encrypted signals," NAVIGATION, Journal of the Institute of Navigation, vol. 60, no. 4, pp. 267-278, 2013.

[4] Qiao, Yinrong, Yuxing Zhang, and Xiao Du. "A vision-based GPS-spoofing detection method for small UAVs." 2017 13th International Conference on Computational Intelligence and Security (CIS). IEEE, 2017.

[5] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50-60, 2020.

[6] N. I. Mowla, N. H. Tran, I. Doh, and K. Chae, "AFRL: Adaptive federated reinforcement learning for intelligent jamming defense in FANET," Journal of Communications and Networks, vol. 22, no. 3, pp. 244-258, 2020.