Check for updates

Path Planning for UAVs Under GPS Permanent Faults

M HANI SULIEMAN, Electrical Engineering and Computer Science, Syracuse University, USA
MENGYU LIU, Computer Science and Engineering, University of Notre Dame, USA
M CENK GURSOY, Electrical Engineering and Computer Science, Syracuse University, USA
FANXIN KONG, Computer Science and Engineering, University of Notre Dame, USA

Unmanned aerial vehicles (UAVs) have various applications in different settings, including e.g., surveillance, packet delivery, emergency response, data collection in the Internet of Things (IoT), and connectivity in cellular networks. However, this technology comes with many risks and challenges such as vulnerabilities to malicious cyber-physical attacks. This paper studies the problem of path planning for UAVs under GPS sensor permanent faults in a cyber-physical system (CPS) perspective. Based on studying and analyzing the CPS architecture of the UAV, the cyber "attacks and threats" are differentiated from attacks on sensors and communication components. An efficient way to address this problem is to introduce a novel approach for UAV's path planning resilience to GPS permanent faults artificial potential field algorithm (RCA-APF). The proposed algorithm completes the three stages in a coordinated manner. In the first stage, the permanent faults on the GPS sensor of the UAV are detected, and the UAV starts to divert from its initial path planning. In the second stage, we estimated the location of the UAV under GPS permanent fault using Received Signal Strength (RSS) trilateration localization approach. In the final stage of the algorithm, we implemented the path planning of the UAV using an open-source UAV simulator. Experimental and simulation results demonstrate the performance of the algorithm and its effectiveness, resulting in efficient path planning for the UAV.

CCS Concepts: • **Computer systems organization** → **Robotic autonomy**; *Reliability*.

Additional Key Words and Phrases: Permanent Faults, unmanned aerial vehicles, path planning, artificial potential field, Received Signal Strength (RSS) trilateration localization.

1 INTRODUCTION

Unmanned aerial vehicles (UAVs) have attracted significant interest in civilian and military applications. Indeed, many new technologies have been involved in designing and building UAVs that have different capabilities in rescue missions and emergency response. Additionally, UAV technology is expected to become a crucial part of aerial surveillance systems, particularly in smart cities. Also, in wireless communication systems, UAVs will play a significant role in assisting and improving the existing communication infrastructure and helping the deployment of the 5G technology in rural and remote regions [52]. UAV trajectory planning is one of the most critical components in controlling and monitoring UAVs during flight. Therefore, the UAV must stay connected with its associated ground base station (GBS) to make sure that the position and location of the UAV have been updated regularly. Additionally, the path planning and the trajectory design of a UAV becomes a key challenge to provide the best wireless connectivity and enhance the system's security and robustness. The air-to-ground

Authors' addresses: M Hani Sulieman, Electrical Engineering and Computer Science, Syracuse University, P.O. Box 1212, Syracuse, New York, USA, 13244, mhsuliem@syr.edu; Mengyu Liu, Computer Science and Engineering, University of Notre Dame, South Bend, USA, mliu9@nd.edu; M Cenk Gursoy, Electrical Engineering and Computer Science, Syracuse University, Syracuse, USA, mcgursoy@syr.edu; Fanxin Kong, Computer Science and Engineering, University of Notre Dame, South Bend, USA, fkong@nd.edu.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2024 Copyright held by the owner/author(s).
ACM 2378-962X/2024/3-ART
https://doi.org/10.1145/3653074

Just Accepted

channel model has been studied in [2]. Also, new studies started to look at UAVs as aerial base stations [22], [37]. Authors in [26], have studied the optimal position for UAVs to maximize the throughput. In UAV positions and placement scenarios, authors in [41] have considered the entire trajectory design for multiple UAVs to jointly optimize scheduling and user association. In the deployment and trajectory planning in UAV communication with jamming, authors in [36] proposed a trajectory planning method in 3D and introduced an anti-jamming approach by dynamically adjusting the UAV's trajectory. Moreover, authors in [39] present an intelligent UAV anti-jamming strategy, in which the optimal trajectory of the typical UAV is obtained via dueling double deep Q-network (D3QN). A low-power robust learning framework to deal with adversarial attacks has been introduced in [29], the authors propose a staged ensemble defense strategy in the framework, which achieves better defensive performance than a single defense algorithm.

One approach in trajectory design planning is to apply the artificial potential field (APF) algorithm. The APF method is a virtual force method that was first introduced by Khatib in [13]. The APF algorithm is developed to avoid collisions among multiple real-time autonomous vehicles and robots operating in a complex environment [13]. Recently, several studies have been conducted on UAV path planning using APF. For instance, the authors in [31] study the optimized APF for multiple UAVs operating in a 3-D dynamic environment. Similarly, the adaptive particle swarm optimization algorithm (APSO) designed for introduction to APF has been introduced in [50] where authors combine the global virtual navigation path (VNP) calculated by the particle swarm optimization algorithm (PSO) with the artificial potential field method for UAV path planning. In [19], the authors propose two algorithms, one is an obstacle avoidance control algorithm for a distributed multi-UAV formation system, and the other is the velocity-based artificial potential field (VAPF) algorithm which helps a UAV to avoid dynamic obstacles and overcome the APF problems of local minimum. The key idea behind the APF algorithm is to calculate the distance between the moving object and the obstacle.

Cyber-physical systems (CPS) are intelligent computer systems that are engineered in a way combining algorithmic computation and communication processes while sensing and interacting with the physical world. The rapid development of CPS technology encourages the development of key technologies and products in autonomous systems such as UAVs and self-driving cars. The mutual interaction between the physical world and information technology puts CPS at risk and makes it vulnerable to malicious attacks that are beyond traditional cyber attacks [1, 3, 24]. This is becoming a real threat to many technologies sometimes resulting in potential breaches of sensitive information about individuals and entities. Therefore, UAVs are one of the most targeted elements by the attackers to take advantage of and wreak havoc by taking control of the UAVs' movement and position. However, since it is difficult to ensure the safe movement of UAVs with the autopilot system against various cyber security attacks, many new studies have proposed new approaches to discovering the attackers and providing a recovery procedure for the system. The authors in [7] discuss the security threat coming from cyber attacks and how it will affect the safety performance of the UAVs, and they analyze the Cross-domain security risk mechanism of UAVs. Furthermore, in [38], the authors propose a new GPS spoofing attack detection method based on a machine learning algorithm that allows UAVs to detect GPS spoofing attacks. An attacker implementing GPS spoofing sends fake information either by generating new signals or by altering legitimately received signals, leading to an inaccurate display of GPS positions of the targeted device [21]. By the same token, a detection attack using the Bayesian network model has been proposed in [34], authors use their proposed model to analyze and detect the fake GPS signal data which is injected by the attackers. In the same direction, the authors in [6] carry out three studies involving GPS attacks in UAVs detecting GPS fraud, counterfeiting GPS on real UAVs, and implementing security measurements to avoid the attack. In [42], the authors propose an effective real-time cyber attack detection method using modified sliding innovation sequences (MSIS) detector. Also, in [47] the authors develop a GP-based approach to estimate the unknown disturbance and propose an approach to adapt the system performance (i.e., speed) along the planned trajectory based on environmental constraints and the GP-based estimation and to dynamically update the GP model.

Just Accepted

These results have motivated further research efforts on studying problems of adversarial attacks on UAVs. The adversarial training and defensive distillation methods are evaluated and discussed in [32]. The authors in [33] propose two adversarial attack methods based on forward derivative and optimization to conduct adversarial attacks against DL-based navigation systems of UAVs. To the best of our knowledge, prior work has not taken into account the impact of the cyber-physical attack on the path planning of the UAV and how it affects the entire flight mission of the UAV by sending wrong information to the GBS on the location of the UAV. Furthermore, in many cases, it can cause a real danger to the entire mechanism and the components of the autopilot system, which controls the movement of the UAV.

To address this challenge, we propose an efficient approach to detect and recover the UAV path planning under cyber-physical attacks on the GPS, knowing that the UAV is equipped with a detector. Attack detection occurs when the UAV loses connectivity with the nearest ground base station (GBS). By injecting false data, the attack diverts the UAV from following its planned path and dictates it to follow a different path. In addition, the GBS loses track of the UAV information such as the coordinates at a certain time and location. We design a new detection and estimation architecture based on two steps. Firstly, we estimate the UAV location under GPS attack using received signal strength (RSS) based trilateration. Secondly, we develop a procedure of resilience to permanent faults method based on the artificial potential field (RCA-APF) algorithm.

In essence, the RCA-APF algorithm is a specific method that handles both GPS permanent fault detection and estimated UAV path planning. Such an algorithm can be developed based on feeding the system with the coordinates of the UAV during its flight from an initial to a final location. To be specific, our method is applicable to deal with compromised sensor measurements caused by faults and false data injection. In this sense, detection, and estimation are presented as cause and effect in this paper. Finally, we evaluate our design by conducting simulation-based experiments which demonstrate the performance of the proposed approach.

Particularly, the RCA-APF algorithm, while indeed serving as an obstacle avoidance mechanism, is intrinsically designed to complement our system's resilience to GPS permanent fault. In scenarios where GPS fault might mislead the UAV path into hazardous zones, the RCA-APF algorithm serves as a critical layer of defense. It enables the UAV to make context-aware decisions, avoiding obstacles that might not be evident through compromised GPS data. In addition, the RCA-APF algorithm works in collaboration with our RSS trilateration technique. While RSS trilateration provides accurate localization in the absence of reliable GPS data, RCA-APF ensures safe navigation through potential threats, forming a comprehensive solution to GPS faults.

Regarding the advantages of RCA-APF over traditional APF algorithms, we have identified several key improvements:

- Unlike traditional APF algorithms [13], which have static response behaviors, our RCA-APF algorithm adapts its response based on the context, such as the proximity and size of obstacles and the severity of GPS fault.
- Our algorithm demonstrates superior robustness in dynamic and unpredictable environments, a common challenge for the UAV, especially in GPS-compromised scenarios.

The rest of the paper is organized as follows. Section 2 presents the design overview and the system model. Section 3 introduces the UAV cyber-physical system and the threat model. Section 4 describes the UAV cyber-physical system approach. Section 5 demonstrates the simulation results. Finally, Section 6 concludes the paper.

2 PRELIMINARIES AND DESIGN OVERVIEW

In this section, we delineate the system model, illustrating the trajectory of each UAV as it navigates from a starting point to its destination. We detail the communication channel model between UAVs and Ground-Based Stations (GBSs).

Just Accepted

2.1 System Model

In this work, we consider a graphical area with a $3D$ Cartesian coordinate system, where the horizontal coordinate of a ground base station (GBS) k is fixed at $W_k = [x_k, y_k]$. The UAV communicates with each of the ground base stations with time length T. All UAVs are assumed to fly at an altitude of H_u above the ground, and the time-varying horizontal coordinate of the UAV at time instant t is denoted by $\mathbf{L_u} = [x_u(t), y_u(t)]$. In this model, potential permanent faults on the UAV path planning can be introduced, as shown in Figure 1. Also, we assume that each UAV starts from a fixed initial location $\mathbf{L_s} = [x_s, y_s]$, and aims to reach the destination/goal $\mathbf{L_g} = [x_g, y_g]$. Also, we assume that the fixed obstacles are randomly distributed and the location of the obstacle j is denoted by $\mathbf{L_o} = [x_j, y_j]$.

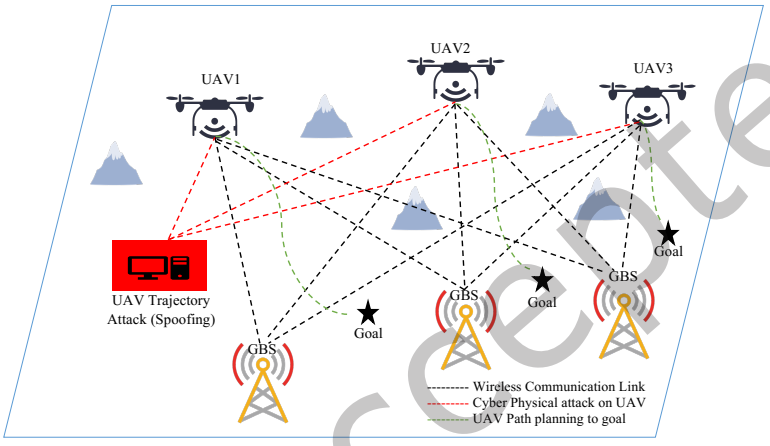

Fig. 1. UAVs attack system model.

2.2 Channel Model between UAV and GBS

The communication link between a UAV and the k^{th} GBS is typically dominated by line-of-sight (LOS) [49]. The LOS probability is given by

$$P_{LOS} = \frac{1}{1 + aexp(-b(arctan\frac{h}{d_i} - a))}. \tag{1}$$

where a and b are constant values depending on the environment. The relative NLOS probability is $P_{NLOS} = 1 - P_{LOS}$. The UAV exchanges data packets with the GBS, assuming that all GBS locations are known. The distance from the i^{th} UAV to the k^{th} GBS at time t is given by

$$d_k(t) = \sqrt{H_u^2 + (x_i(t) - x_k)^2 + (y_i(t) - y_k)^2}. \tag{2}$$

Similarly, the distance from the i^{th} UAV to the j^{th} obstacle at time t is given by

$$d_j(t) = \sqrt{H_u^2 + (x_i(t) - x_j)^2 + (y_i(t) - y_j)^2}. \tag{3}$$

Just Accepted

3 UAV CYBER-PHYSICAL SYSTEM AND THREAT MODEL

3.1 System Model of UAVs Wireless Networks

UAVs are drones or aircraft that can fly without the need for a pilot on board. Also, UAVs are equipped with many essential components such as the flight control unit, sensor payloads, and wireless communications module. In addition, reliable and very high-speed wireless communication networks are required for the UAV to execute its flying mission successfully. The payload sensors are equipped with onboard sensors and GPS modules for position and navigation purposes. The communication module includes a high-speed wireless interface and antennas to transmit and receive control signals and data. There are mainly two types of radio communications that occur in a typical UAV-assisted communication network; UAV-to-UAV and the communication between UAV to the nearest GBS. Moreover, network communication plays an important role to ensure smooth wireless networking and uninterrupted services. The integrated system of the UAV works by collecting data, exchanging information, making decisions, and eventually executing those decisions [10].

3.2 Cyber-Physical System Architecture of UAV

We consider that a single UAV is used to execute complex missions. During these missions, the UAV communicates with the GBS through the uplink and downlink channels. Moreover, the onboard GPS sensor in the cyber-physical system architecture plays an essential role in cooperating and achieving efficient coordination. In addition, the GPS sensor helps the UAV with mission allocation and monitors path planning in addition to exchanging the data between the UAV and the nearest GBS.

In this paper, we focus on the GPS permanent faults in cyber-physical systems. It is important to have an attack detector deployed on the UAV to maintain the safety of the system [11, 18, 51]. Additionally, the attack detector should be computing-efficient due to the limited resources on the UAV in real-time scenarios. Usually, the attack detector monitors the data streams from the sensors to check whether there is a statistically abnormal signal [17, 51]. For example, CUSUM-based methods can be applied onboard at the UAV to monitor the residuals between the sensor measurements and estimation over a time window [17]. Figure 2 depicts the UAV hardware components within the cyber-physical system architecture. Notably, the GPS sensor of the UAV emerges as an appealing target for potential attackers, posing a significant risk of system damage. The errors in the GPS readings affect the movements of the UAV. These errors instruct the UAV to follow a specific path. In other words, the GPS permanent faults divert the UAV to an arbitrary location of the attacker's choosing. It is worth noting that the UAV is equipped with an onboard detector. This onboard attack detector is further used to estimate the UAV position when the attacker caused the permanent fault for the UAV-GPS sensor. Figure 3 illustrates the primary sensors mounted on the UAV, which include the onboard attack detection system, the GPS sensor, and the camera sensor.

3.3 Cyber-Physical Attack to UAV and Threat Model

In general, a cyber-physical attack can target each of the components of any cyber-physical system. Indeed, UAV security threats should be analyzed from the perspective of a new type of attack, which dismantles the physical operation of the UAV. Moreover, sensors are critical components for the UAV to receive data about itself and the surrounding environment. Essentially, UAVs rely on the collaboration of various sensors, including GPS. With this crucial sensor, UAV can obtain the obstacle's location, altitude, and other important information related to the flight mission, for the safe and successful completion of a task. Additionally, the GPS sensor provides the necessary data to make sure the UAV reaches its final destination. However, false data leads the UAV to make the wrong decision, affecting flight safety and reliability. It can further cause a catastrophic crash. Therefore, sensor attacks have been categorized as one of the most critical threats in cyber-physical attacks.

Just Accepted

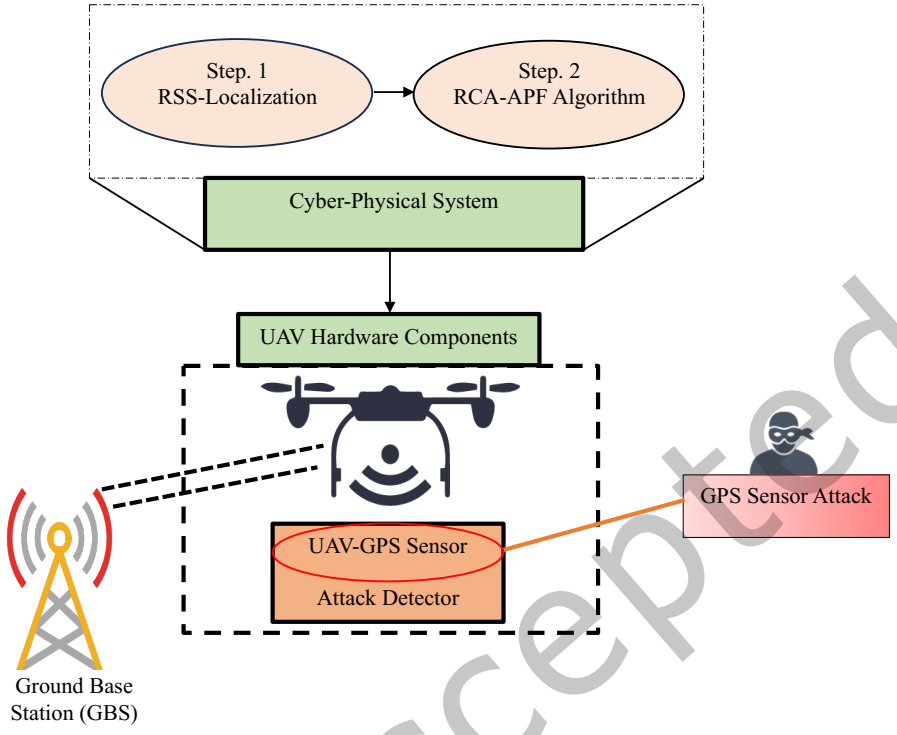

Fig. 2. Cyber-physical system architecture.

Threat Model. In this work, our attention is centered on the physical mechanisms of Unmanned Aerial Vehicles (UAVs). Specifically, we explore the strategies for path planning in scenarios where UAVs encounter persistent GPS sensor malfunctions. In addition, false GPS data alters the real data by compromising the integrity and availability of the GPS sensor measurements. The wrong readings modify the GPS sensor data and feed it into the system, making it unreliable, and thus the estimated state based on the sensor measurements becomes corrupted and untrustworthy.

For example, the value $\mathbf{r(t)}$ can be set to be $\tilde{\mathbf{r}}(\mathbf{t}) \pm \mathbf{e}$ by an attack, where $\mathbf{e}$ is the perturbation/modification value. Another attack scenario can be realized by the attacker through delay of the data sent to the GPS sensor, i.e., $\mathbf{r(t)} = \tilde{\mathbf{r}}(\mathbf{t_0})$ for a time period of $\mathbf{T}$ where $\mathbf{t_0}$ is the start time of the attack, and then $\mathbf{r(t)} = \tilde{\mathbf{r}}(\mathbf{t - T})$ for $\mathbf{t \geq t_0 + T}$.

GPS Sensor Spoofing/Jamming. The UAV depends on the GPS signals received and processed by the onboard GPS receiver. GPS spoofing attack is the most common attack form where the attackers take control of the UAV by transmitting signals from the satellites to the target UAV. Compared with the spoofing attacks, GPS jamming is more implemented GPS sensor spoofing attacks are directed toward onboard sensors that depend on the outside environment. The goal of this attack is to destabilize UAVs by compromising the sensor by injecting false data. Some attacks try to steal information through security holes of communication links in the system while others aim to spoof sensors, such as GPS spoofing. Therefore, successful attacks will lead to serious consequences [8].

Just Accepted

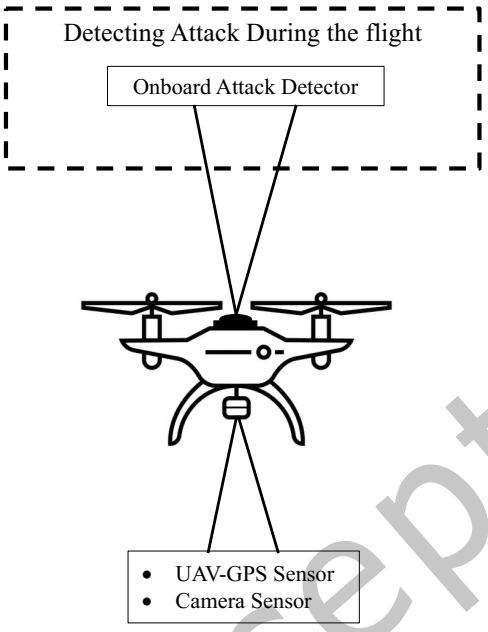

Fig. 3. The hardware components of the UAV.

Just Accepted

Another example that can be related to the spoofing attack, is to develop acoustic injection attacks on MEMS accelerometers [35].

False GPS Sensor Data Injection The UAV can be forced to respond to false signals as a result of the GPS sensor attack, and it can completely disrupt its navigation system and mislead the UAV from achieving its goal [14]. Fake GPS sensor data injection targets onboard GPS sensing components such as accelerometers and actuators that are dependent on sensing external environment conditions. Authors in [16] took the UAVs navigation as the example and modeled it as a stochastic liner CPS system with the Gaussian noise. The purpose of these permanent faults is to destabilize UAVs by compromising a collection of sensors such as GPS and introducing falsified readings into the flight controller, hence jeopardizing the control system and the flight mission of the UAV [25].

4 UAV CYBER-PHYSICAL SYSTEM

The physical state of the UAV path planning under GPS permanent faults is addressed in this section. It contains physical and cyber components including computation, communication, and on-board sensors. Figure 2 depicts the data flows that begin with the UAV-GPS sensor, which communicates the original data from the UAV to the nearest GBS. Computation modules, analyze and make decisions based on all the acquired information. In our case, the onboard UAV-GPS sensor records all the decisions that the UAV makes. For example, the UAV flies from an initial location following the path plan and at a specific time, the GPS sensor starts being disabled and compromised due to faults. After a short delay, as shown in Figure 4.

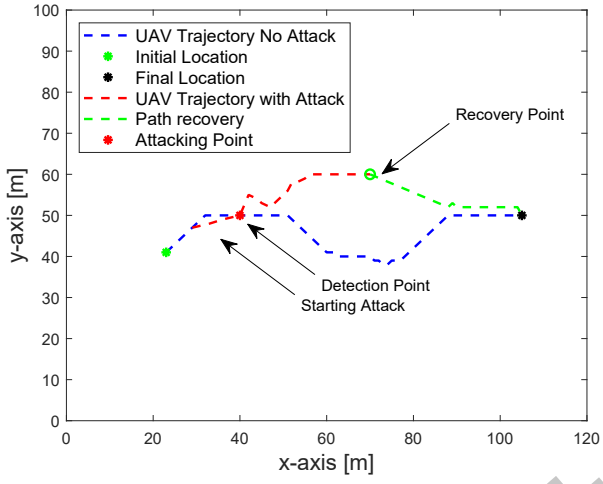

Fig. 4. The Path planning framework of the UAV at different scenarios.

The system architecture of the UAV includes the GPS procedure based on two main steps. Firstly, the UAV localization method was introduced using the received signal strength trilateration approach, and then we implemented the resilience to GPS permanent fault artificial potential field algorithm (RCA-APF). In other words, the UAV generates the path plan in the environment with randomly distributed obstacles, where the UAV flies from an initial position to the final destination while it communicates with the GBSs. Due to the GPS false readings, the UAV loses its connectivity with the GBSs. Therefore, location estimation for the UAV is obtained using the received signal strength trilateration.

4.1 Received Signal Strength Based Trilateration

To estimate the location of the UAV under the GPS attack, we use a geolocation approach based on the received signal strength (RSS). Essentially, the UAV flies along a trajectory and receives signals from the surrounding ground base stations (GBSs). The RSS traditional model [40] has been implemented to collect those measurements. Using the long-distance path loss propagation model [20], [12], the location-related information measurements are obtained from the RSS, which is generally affected by multi-path effects and NLoS propagation. Furthermore, the location of the UAV can be ideally determined in 2D space with the use of the three GBSs. In general, the average received power P_k associated with the kth GBS can be modeled in dB form as

$$P_k = P_0 - 10\alpha_k log_{10} d_k + e_{RSS,k}, k = 1, 2, ..., N, \tag{4}$$

where P_0 is the reference received average power at a reference distance of 1 meter, α_n denotes the path loss exponent, and $e_{RSS,n}$ represents the error of the RSS measurements. Assuming that P_0 and $\alpha_k, k = 1, 2, ..., K$ are given, the distance between the UAV and each of the GBSs can be estimated. Therefore, the RSS measurement model that comes from the kth GBS and received by the UAV can be derived as follows

$$r_{RSS,k} = P_k - P_0, \tag{5}$$

$$q_{RSS}(\mathbf{p}_k, \mathbf{w}) = -10\alpha_k log_{10} d_k, \tag{6}$$

$$r_{RSS,k} = q_{RSS}(\mathbf{p}_k, \mathbf{w}) + e_{RSS,k}, k = 1, 2, ..., N. \tag{7}$$

Just Accepted

where $r_{RSS,k}$ denotes the RSS measurement associated with the k^{th} GBS, $q_{RSS}(\mathbf{p}_k, \mathbf{w})$ is a nonlinear function which contains all necessary information to calculate the location of the UAV, and $e_{RSS,k}$ represents the measurement error. The main task of RSS-localization is to estimate $\mathbf{w}$ based on the obtained $\{r_{RSS,k}\}_{k=1}^{K}$ in (7).

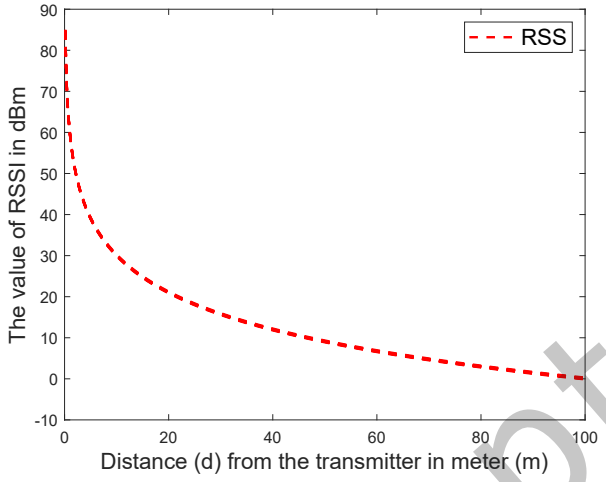

Fig. 5. RSS values from UAV to GBS.

In Figure 5, we show the RSS measurements from K GBSs at different locations received by the UAV. Typically, solving nonlinear equations requires the application of nonlinear estimators, which include the nonlinear least squares (NLS), weighted nonlinear least squares (WNLS), and maximum likelihood (ML) estimators [48]. Based on the RSS model (7), the cost function of the NLS estimator can be expressed as [9]

$$\begin{aligned} Q_{NLS}(\mathbf{w}) &= \sum_{k=1}^{K} (r_{RSS,k} - q_{RSS}(\mathbf{p}_k, \mathbf{w}))^2 \\ &= (\mathbf{r} - \mathbf{q}(\mathbf{w}))^T (\mathbf{r} - \mathbf{q}(\mathbf{w})), \end{aligned} \tag{8}$$

where $\mathbf{r} = [r_{RSS,1}, ..., r_{RSS,K}]^T$ and $\mathbf{q}(\mathbf{w}) = [q(\mathbf{p_1}, \mathbf{w}), ..., q(\mathbf{p_K}, \mathbf{w})]^T$. The solution of NLS estimator corresponds to the estimated location $\widehat{\mathbf{w}}$ that minimizes the cost function (8), i.e.,

$$\widehat{\mathbf{w}} = \arg\min_{w} Q_{NLS}(\mathbf{w}). \tag{9}$$

The NLS estimator does not rely on any assumption about the error statistics. However, when the covariance of the error vector $\mathbf{w} = [e_1, ..., e_K]^T$ is available, we can obtain the WNLS estimator, which can be expressed as [28]

$$\begin{aligned} \widehat{\mathbf{w}} &= \arg\min_{w} Q_{WNLS}(\mathbf{w}) \\ &= \arg\min_{w} (\mathbf{r} - \mathbf{q}(\mathbf{w}))^T \mathbf{C}^{-1}(\mathbf{e}) (\mathbf{r} - \mathbf{q}(\mathbf{w})), \end{aligned} \tag{10}$$

where $\mathbf{C}(\mathbf{e}) = \mathbb{E}[\mathbf{e}\mathbf{e}^\mathbf{T}]$ represents the covariance of $\mathbf{e}$, and $\mathbb{E}[.]$ denotes the expectation operation. In addition, when error probability distribution $P_e(\mathbf{e})$ is known, the ML estimator can be used for location estimation [4],[5]

$$\begin{aligned} \widehat{\mathbf{w}} &= \arg\min_{w} Q_{ML}(\mathbf{w}) \\ &= \arg\min_{w} \log P_e(\mathbf{e}) (\mathbf{r} - \mathbf{q}(\mathbf{w})). \end{aligned} \tag{11}$$

Just Accepted

The errors follow the zero-mean Gaussian distribution, and the WNLS and ML estimators have the same performance. To solve the optimization problems in (9), (10), (11), several approaches exist. For instance, grid search is a reliable method to find the point $\widehat{\mathbf{w}}$ that minimizes the objective function Q.

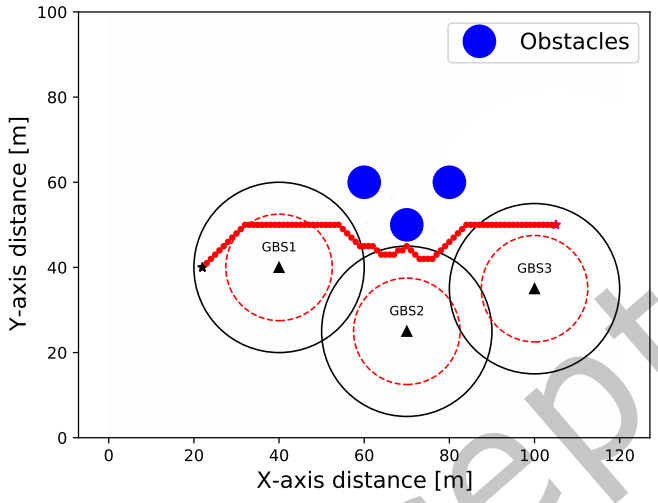

Fig. 6. The map elements of the system.

Moreover, the main advantage of RSS-based localization lies in that time synchronization among different GBSs is not required and RSS measurements are readily available in almost all practical wireless systems. On the other hand, the main drawback of RSS-based approaches is the poor localization accuracy. Also, RSS-based distance estimation can be challenged due to the unpredictable variations of the channel behavior. However, due to inaccuracy in the RSS localization, we consider a larger obstacle to covering the issue, as shown in Figure 6.

RSS-based Trilateration.

Trilateration determines the location of the UAV under attack using distance-related signal measurements for multiple GBSs. In other words, the UAV would be located at the intersection of the three circles with the centers being the locations of the GBSs and radii equal to the distances from the UAV to each of the GBSs. The locations of the GBSs are known and their distances to the UAV can be determined based on the RSS measurements [15, 43–45]. Furthermore, the RSS measurements from all GBSs are calculated and then converted into distances. Based on this distance, the system trilaterates the UAV location as illustrated in Figure 7. The trilateration method uses RSS measurement values to calculate the distance between the UAV and GBSs. The location of the UAV $[x_u, y_u]$ needs to be computed, then the formulated circles are calculated using mathematical computations. Assuming $z = 0$ and to simplify the calculations, the equations are formulated so that the intersection of circles occurs at the Cartesian plane. The equation for each circle can be expressed as [27]

$$(x_u - x_k)^2 + (y_u - y_k)^2 = d_k^2. \tag{12}$$

where (x_k, y_k) denotes the location of the kth GBS.

The intersection of three circles is obtained by solving systems of linear equations for two variables simultaneously. Hence, by solving the linear systems, the location of $[x_u, y_u]$ can be determined. The accuracy of coordinate $[x_u, y_u]$ depends on the measurement of RSS values.

Just Accepted

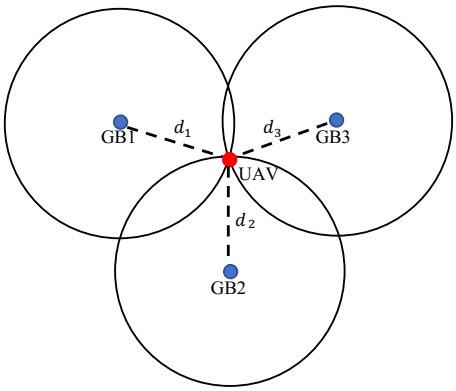

Fig. 7. RSS-based localization, where d_k, $k = 1, 2, 3$, denote the actual distances from the UAV to each of the GBS.

4.2 UAV Estimated Location Based On Three GBSs

Given the three GBSs coordinates $W_1 = [x_1, y_1]$, $W_2 = [x_2, y_2]$, $W_3 = [x_3, y_3]$ and the distance measurements d_1, d_2, and d_3 as shown in Figure 7. The UAV coordinates $L_u = [x_u, y_u]$ can be calculated by finding the solution to the following system of quadratic equations: [23]

$$(x_u - x_1)^2 + (y_u - y_1)^2 = d_1^2 \tag{13}$$

$$(x_u - x_2)^2 + (y_u - y_2)^2 = d_2^2 \tag{14}$$

$$(x_u - x_3)^2 + (y_u - y_3)^2 = d_3^2 \tag{15}$$

Equations (13), (14), and (15) can be rearranged and represented in matrix as:

$$\begin{bmatrix} 1 & -2x_1 & -2y_1 \\ 1 & -2x_2 & -2y_2 \\ 1 & -2x_3 & -2y_3 \end{bmatrix} \begin{bmatrix} x^2 + y^2 \\ x \\ y \end{bmatrix} = \begin{bmatrix} d_1^2 - x_1^2 - y_1^2 \\ d_2^2 - x_2^2 - y_2^2 \\ d_3^2 - x_3^2 - y_3^2 \end{bmatrix} \tag{16}$$

Thus, (16) is the matrix equation and which can be written as:

$$\mathbf{A_0}.\mathbf{x} = \mathbf{b_0}; \quad \mathbf{x} \in E = \{(x_0, x_1, x_2, x_3)^T \in \mathbb{R}^4 : x_0 = x_1^2 + x_2^2 + x_3^2\} \tag{17}$$

The UAV flies each time step updating its coordinate at different locations. Therefore, equation (17) does not lie on a straight line and the solution can be given by:

$$\mathbf{x_1} = \mathbf{x_k} + t_1\mathbf{x_i} \tag{18}$$

$$\mathbf{x_2} = \mathbf{x_k} + t_2\mathbf{x_i} \tag{19}$$

where t_1 and t_2 are real parameters that can be calculated using a quadratic equation $t_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. x_k and x_i are the particular and homogeneous solutions, respectively. The solution for the trilateration estimation values for the UAV based on three GBSs locations is given by

$$UAV_1 = \mathbf{x_1}.I \quad UAV_2 = \mathbf{x_2}.I. \qquad where \;\; I = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{20}$$

Just Accepted

4.3 RCA-APF Algorithm

Artificial Field Algorithm. The Artificial Potential Field (APF) method offers a straightforward yet efficient technique for the motion planning of unmanned vehicles. The APF algorithm is capable of encapsulating comprehensive environmental data, including obstacles, the destination, and other entities within the vicinity. Our focus is on a solitary UAV navigating towards a target point within a three-dimensional space, assuming a relatively uncomplicated setting characterized by a singular objective and several obstacles. To address the issue of local minima, we employ the strategy outlined in [46], incorporating extra terms for the attractive potential field and adjusting the potential field configuration to ensure the UAV circumvents any halt between obstacles and the target. The UAV navigates along the horizontal plane, maintaining a 2D position denoted as $\mathbf{L}_u = [x_u(t), y_u(t)]^T$ at any time t. The destination is stationary, located at $\mathbf{L}_g = [x_g, y_g]^T$. Consequently, the attractive potential function for a single UAV is defined as per [30].

$$J_{att}(\mathbf{L}_u) = q_{att}\frac{(\mathbf{L}_u - \mathbf{L_g})^2}{2}. \tag{21}$$

The single UAV case is similar to the attractive potential function of the traditional APF. The attractive force of the UAV $F_{att}(\mathbf{L}_u)$ is the negative gradient of the attractive potential function given as

$$F_{att}(\mathbf{L}_u) = -\nabla J_{att}(\mathbf{L}_u) = -q_{att}(\mathbf{L}_u - \mathbf{L_g}). \tag{22}$$

The additional field function helps the UAV to avoid the local minimum point by pulling it toward the target. The additional field force $J_{add}(\mathbf{L}_u)$ is given by [46]

$$J_{add}(\mathbf{L}_u) = \begin{cases} \frac{q_{add}}{2}\left[(\mathbf{L_u} - \mathbf{L_g}) - \mathbf{p_{add}}\right]^2 & , \parallel \mathbf{L_u} - \mathbf{L_g} \parallel \leq \mathbf{p_{add}}\,, \\ 0 & , \parallel \mathbf{L_u} - \mathbf{L_g} \parallel > \mathbf{p_{add}}\,. \end{cases} \tag{23}$$

where q_{add} is the additional field coefficient, $\parallel \mathbf{L_u} - \mathbf{L_g} \parallel$ is the distance between the UAV and the goal, $\mathbf{p_{add}}$ is the impact of the field on the distance between the UAV and the goal.

The additional field force $F_{add}(\mathbf{L}_u)$ is represented as follows:

$$F_{add}(\mathbf{L_u}) = -\nabla[J_{add}(\mathbf{L_u})] = \begin{cases} q_{add}\left[(\mathbf{L_u} - \mathbf{L_g}) - \mathbf{p_{add}}\right] & , \parallel \mathbf{L_u} - \mathbf{L_g} \parallel \leq \mathbf{p_{add}}\,, \\ 0 & , \parallel \mathbf{L_u} - \mathbf{L_g} \parallel > \mathbf{p_{add}}\,. \end{cases} \tag{24}$$

The modified repulsive potential function, which takes the relative distance between the UAV and the target into consideration is given as

$$J_{rep}(\mathbf{L_u}) = \begin{cases} \frac{q_{rep}}{2}\left(\frac{1}{\mathbf{L_u} - \mathbf{L_0}} - \frac{1}{\mathbf{p_0}}\right)^2 & , \parallel \mathbf{L_u} - \mathbf{L_0} \parallel \leq \mathbf{p_0}\,, \\ 0 & , \parallel \mathbf{L_u} - \mathbf{L_0} \parallel > \mathbf{p_0}\,. \end{cases} \tag{25}$$

The repulsion force function $F_{rep}(\mathbf{L_u})$ for the single UAV is given by

$$F_{rep}(\mathbf{L_u}) = -\nabla[J_{rep}(\mathbf{L_u})] = \begin{cases} q_{rep}(\frac{1}{\mathbf{L_u} - \mathbf{L_0}} - \frac{1}{\mathbf{p_0}})\frac{1}{(\mathbf{L_u} - \mathbf{L_0})^2} & , \parallel \mathbf{L_u} - \mathbf{L_0} \parallel \leq \mathbf{p_0}\,, \\ 0 & , \parallel \mathbf{L_u} - \mathbf{L_0} \parallel > \mathbf{p_0}\,. \end{cases} \tag{26}$$

Just Accepted

As demonstrated in equations (25) and (26), the formulations closely mirror the original APF. The pivotal modification lies in the introduction of an extra force, ensuring the UAV's evasion of local minimum points. The complete potential field encountered by the UAV at each step can be expressed as follows:

$$J_{\mathrm{L_u}} = \sum_{r=1}^{i} J_{rep}(r) + \sum_{l=1}^{t} [J_{att}(l) + J_{add}(l)] \tag{27}$$

where i is the number of obstacles, and t is the number of the goals. Similarly, the total force that affects the UAV and applies to multiple targets and obstacles is given as follows:

$$F_{\mathrm{L_u}} = \sum_{r=1}^{i} F_{rep}(r) + \sum_{l=1}^{t} [F_{att}(l) + F_{add}(l)]. \tag{28}$$

There are other factors that can affect the performance of the RCA-APF algorithm.

Drawing from the equations outlined in the preceding section, we have devised an iterative algorithm to determine the optimal UAV trajectory using the RCA-APF method. At each iteration, the UAV computes the attractive and repulsive potential field functions, thereby gathering essential data regarding the location of the target, obstacles, and Ground-Based Stations (GBS). Within a compact grid of size $[s \times s]$, the UAV deliberates its subsequent maneuver. The operational geographic expanse of our system is demarcated as $[M \times Z]$.

The UAV is equipped with a repertoire of eight possible movements to navigate from its starting point to the intended target. The matrix's rows and columns correspond to the UAV's x_u and y_u coordinates, respectively. The intricacies of the algorithm are encapsulated in Algorithm 1. It is important to note that this algorithm evolves from the conventional APF algorithm.

4.4 Algorithm Description

Based on the equations in the previous sections, we construct an iterative RCA-APF algorithm for the best UAV path planning. Initially, we calculate the UAV path planning using a modified version of the traditional artificial potential field algorithm. Specifically, at every move of its journey, the UAV actively computes the attractive and repulsive potential field functions. This process enables the UAV to assimilate critical data regarding the positions of the target, any obstacles in the vicinity, and Ground-Based Stations (GBSs). Operating within a confined grid space measured at $[q \times q]$, the UAV assesses and selects its forthcoming course of action. The system's operational terrain is designated as $[M \times Z]$. From the onset of its mission, the UAV is presented with a selection of eight directional choices to navigate towards its ultimate goal. At this point of the RCA-APF algorithm, the UAV coordinates (x_u, y_u) will get calculated and updated for the next iterative loop. The UAV coordinates will be constructed as a matrix representing x_u values for the rows and y_u values for the column, respectively. We calculat the UAV positions at each time step and we use the trilateration estimation localization technique to estimate the location of the UAV. The implementation of the trilateration algorithm is combined with the RCA-APF algorithm. For the fixed coordinate values of each of the GBSs, we calculated the distances from the UAV at each time step to the GBSs. In addition, we computed the received signal strength between UAV and GBSs. From the measured distances for each GBS, the algorithm finds the coordinates that minimize the error function and returns the most optimal solution of the estimated location coordinates (x_{ues}, y_{ues}) of the UAV. The specifics of the algorithm are concisely explained in Algorithm 1. It is noteworthy to mention that this algorithm evolves from the conventional Artificial Potential Field (APF) algorithm. The path planning is computed to be used as a reference to the UAV simulator. In the final iteration of the RCA-APF algorithm, we applied both calculated and estimated coordinates of the UAV as input to an open-source UAV simulator implementing UAV path planning scenarios. The UAV simulator is based on Python Dynamics, which is a toolkit made to enable the study of multibody dynamics. The

Just Accepted

Algorithm 1: RCA-APF Algorithm for single UAV

Input: For given position of initial location $\mathbf{L_s}$, position of final location $\mathbf{L_g}$, position of GBS W_k, position of obstacles $\mathbf{L_o}$, the attraction gain coefficient q_{att}, the repulsive gain coefficient q_{rep}, additional field coefficient q_{add}, the UAV height H_u, RSS-based Trilateration measurement values

Output: path planning of the UAV P

```
for j = 1 : J do
    for s = 1 : S do
        calculate equation (21), (23) and (25) for given input
        calculate the total force potential field (28)
        while d_k(t), d_j(t) ≥ [q × q] do
            for each UAV step do
                Update x_u(t) and y_u(t)
                if x_u(t), y_u(t) < 0 or x_u(t), y_u(t) > [M × Z] then
                    Break;
                Update UAV coordinate x_u(t) and y_u(t) ;
            end
        end
        if the UAV have reached the final location Z_g then
            Break ;
    end
    return x_u, y_u;
    for i = 1 : I do
        each UAV (x_u, y_u) step; calculate distances using equations (13), (14), and (15)
        calculate the RSS values (7)
        for each UAV RSS value do
            calculate UAV estimated value (x_ues, y_ues) equation (11)
        end
    end
    return x_ues, y_ues
    for calculated inputs (x_u, y_u) and (x_ues, y_ues) start to implement the path planning using an
      open-source simulator
end
return P
```

Just Accepted

simulator is built on multiple packages. The main functionality of the UAV simulator is to initialize the UAV with various parameters and conditions. Also, the simulator includes a control algorithm that is strongly inspired by the PX4 multicopter control algorithm. It is a cascade controller, where the position error (difference between the desired position and the current position) generates a velocity setpoint, the velocity error then creates a desired thrust magnitude and orientation, which is then interpreted as a desired rotation (expressed as a quaternion). Figure 8, depicts the workflow of the proposed RCA-APF algorithm.

5 SIMULATION RESULTS AND ANALYSIS

In this section, we show the UAV's behavior with GPS permanent faults and the effectiveness of the proposed algorithm by conducting experiments and simulations on different path planning of the UVA at different

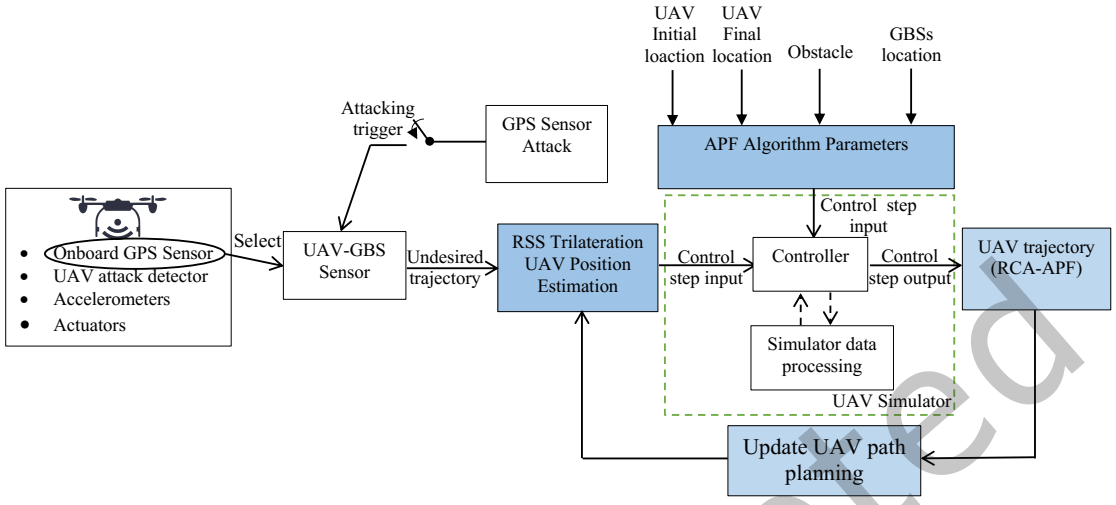

Fig. 8. Architecture of the proposed approach.

environment setups. Also, we consider the UAV communicates with the nearest GBS to receive all the information about the current location of the UAV at each time step.

To illustrate the concepts and the algorithm discussed in this paper, we present and show simulation results to demonstrate how the RCA-APF algorithm operates. We conduct multiple experiments and set up the appropriate values for the parameters. To facilitate the simulation, the UAV is set to fly at a known altitude, which is fixed throughout the entire simulation. We run the simulation using an open-source UAV simulator. Also, we provide 2D plan implementation of the UAV path planning. In the simulations, the UAV path is generated based on an input to the UAV simulator, $\mathbf{v} \leq 5m/s$, and flight altitude is $60m$. In addition, the time flying off the UAV varies based on the path planning time delay. We have further explained the robustness of our UAV path-planning algorithm, particularly focusing on its obstacle avoidance capabilities, which, alongside permanent fault detection and recovery, stands as one of its primary functionalities. To this end, we have designed and executed several additional experiments under a variety of environmental conditions. The outcomes of these experiments are comprehensively detailed in Table 1.

Table 1 shows the success rates of UAV missions conducted across various scenarios, each uniquely characterized by a varying number of obstacles while maintaining a constant configuration of three Ground Base Stations (GBSs). The presence of three GBSs across all scenarios is a strategic choice, reflecting a realistic density of navigational aids that a UAV might typically have access to. Moreover, we define the success rate as the proportion of missions in which the UAV successfully navigates to its intended destination without incurring collisions or deviating significantly from its planned trajectory. To ensure the reliability and accuracy of our success rate, we ran our algorithm to a rigorous testing protocol, executing the experiment a total of 100 times for each obstacle scenario. Upon analyzing the data, we observed a clear trend: as the number of obstacles increased, the success rate tended to decrease. This was expected, as more obstacles present a greater navigational challenge.

In Figure 9, we demonstrate a 2D path planning design of a single UAV. The UAV flies from an initial location to its final destination with obstacle collision avoidance integrated into the system. The obstacles are generated in a way that fits with the setup framework. Furthermore, the framework includes the GBSs located at fixed

Just Accepted

Number of obstacles	Number of GBSs	Number of Iteration	Success Rate
10	3	100	98%
25	3	100	85%
50	3	100	74.5%
75	3	100	60%
100	3	100	50%

Table 1. Success/Failure Rates of the UAV.

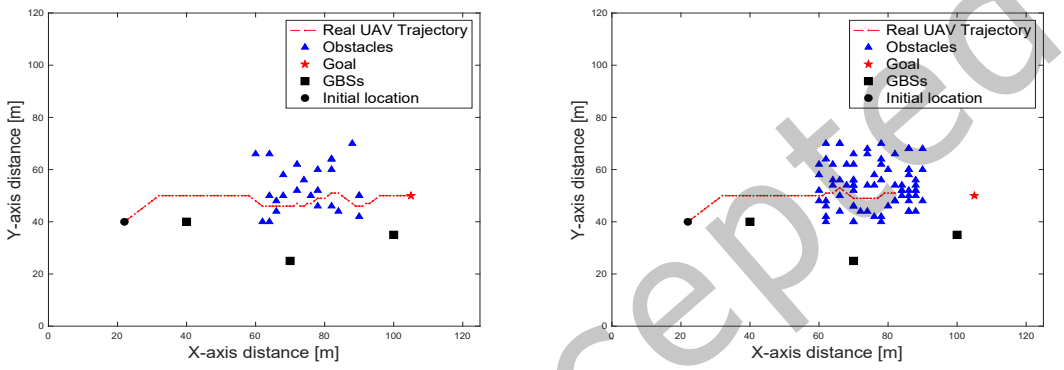

Fig. 9. The path planning of the UAV with a different number of obstacles.

positions to maintain connectivity with the UAV during the mission. The figures show a different number of obstacles. Indeed, the obstacles are randomly distributed with mean and variance. We run the experiment with 25 and 75 obstacles. In an environment with more obstacles, the UAV has failed to reach the final location. Indeed, the obstacles are randomly distributed with mean $\mu = 0$and variance $\sigma = 0.01$.

In Figure 10, we illustrate two distinct scenarios of UAV path-planning. These scenarios compare the actual UAV path planning with a trajectory estimated using the RSS-trilateration method. Specifically, Figure 10 (a) depicts the intended UAV trajectory in blue, while the estimated trajectory derived from RSS-trilateration is shown in red. The comparison demonstrates the efficacy of the RSS-trilateration estimation algorithm, as it closely mirrors the desired trajectory.

Extending this analysis to Figure 10 (b), we observe a scenario where, despite the UAV's inability to reach its final destination, the RSS-trilateration estimation remains accurate and reliable. This is evidenced by the red trajectory, which is based on RSS-trilateration, closely following the actual path taken by the UAV until its early termination. The consistency of the RSS-trilateration algorithm's performance in both scenarios underscores its robustness and potential applicability in real-world UAV navigation systems.

5.1 UAV Simulator

To validate our results, we used an open-source Quadcopter simulator. In that simulator, we implemented a simple scenario with a single UAV flying from the initial location to the final destination. The Quadcopter simulator provides a simple working simulation of the quadcopter's dynamics and a simple controller that can handle position control and supports minimum snap (but also minimum velocity, acceleration, and jerk) trajectory

Just Accepted

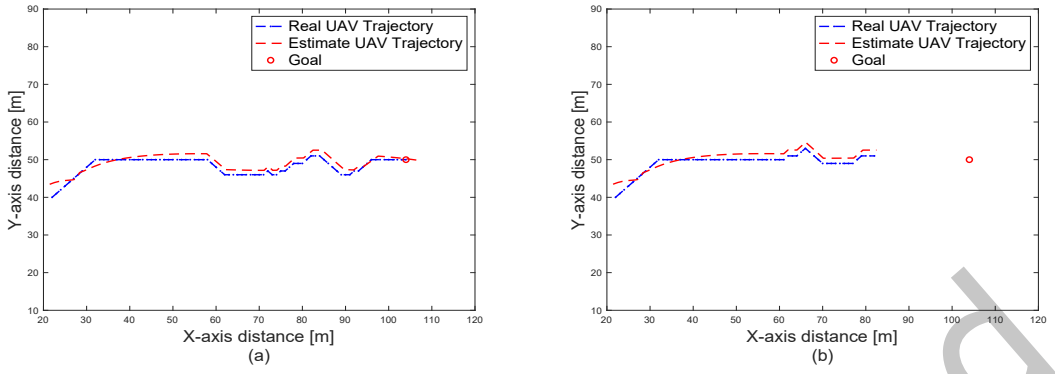

Fig. 10. The path planning of the UAV with the estimated path planning.

generation. The UAV's orientation is based on two frames: the first one is the X direction North, Y East, and Z Down. The second frame is the X direction East, Y North, and Z Up. Also, the simulator uses the quaternion for the UAV's rotation. Different trajectories can be selected, for both position and heading. Using the simulator, we can set the desired position and heading waypoints, and the time for each waypoint. We can select to use each waypoint as a step, interpolate between waypoints, or generate a minimum velocity, acceleration, jerk, or snap trajectory. The controller of the Quadcopter simulator is the most critical part. There are three controllers: one to control XYZ positions, one to control XY velocities and Z position, and one to control XYZ velocities. In all 3 current controllers, it is also possible to set a Yaw angle (heading) setpoint. The control algorithm is strongly inspired by the PX4 multicopter control algorithm. It is a cascade controller, where the position error (difference between the desired position and the current position) generates a velocity setpoint, the velocity error then creates a desired thrust magnitude and orientation, which is then interpreted as a desired rotation (expressed as a quaternion). The source code is available at https://github.com/bobzwik/Quadcopter_SimCon.

It should be noted that the UAV encounters a certain delay in detecting attacks, a critical metric that is essential for assessing the effectiveness of our system. We have conducted additional experiments to measure this delay, which is the time duration from the initial data point of an attack being observed to the point where our system successfully identifies the attack. Particularly, we utilized an open-source simulation tool to implement and test the attack/recovery scenario. It is important to note that the delay in attack detection observed in these simulations is influenced by the performance capabilities of the computing device, particularly the GPU and CPU specifications. To provide a more thorough insight into this aspect, for each system, we executed the simulation 10 times to ensure statistical reliability and to mitigate any anomalies or outliers in the data. After each run, we meticulously recorded the time taken by the attack detection mechanism to identify the breach. This process involved measuring the interval from the initial indication of an attack to the point where our system successfully recognized and flagged the anomaly. Below, Table 2 summarizes the results of these experiments:

Processor	GPU Specs	CPU Specs	Average attack detection delay
Intel Core i9	Intel UHD Graphics 630	2.4 GHz 8-core	16.32 sec
Apple M1 Max	Integrated Apple GPU	10-core CPU	10.45 sec

Table 2. Attack delay table.

Just Accepted

The modeling of our attack detector is intricately designed around the RCA-APF algorithm. This setup encompasses a comprehensive environment configuration, precise parameter tuning, and a realistic representation of potential obstacles. Utilizing an open-source simulator, we have meticulously adapted and fine-tuned various parameters to accurately replicate scenarios where a UAV deviates from its intended flight path due to an external attack. In these simulated scenarios, the attack detector is integrated into the UAV's system. Its primary role is to promptly identify any form of attack that causes trajectory deviation. The moment an attack-induced diversion is detected, our RCA-APF algorithm is triggered to initiate an immediate recovery process. This process is designed to swiftly reorient the UAV back to its original course, thereby mitigating the impact of the attack. Our modifications to the simulator parameters include adjustments to the UAV's response sensitivity to external disruptions, the threshold levels for attack detection, and the dynamic recalibration of the UAV's pathfinding algorithms post-attack detection. These enhancements enable us to simulate with high fidelity the UAV's behavior under attack conditions and to rigorously test the efficacy of our attack detection and recovery mechanism. This comprehensive setup not only demonstrates the robustness of our attack detector in identifying and responding to trajectory deviations but also underscores the effectiveness of the RCA-APF algorithm in ensuring the UAV's swift return to its intended path post-attack.

In our experiments, the implementation of the attack detector, based on the RCA-APF algorithm, was conducted in a controlled simulation environment designed to mimic real-world UAV operational scenarios. We utilized a sophisticated open-source UAV simulator that allowed us to create the attack scenario. This includes a GPS attack, which could potentially divert the UAV from its intended path. In addition, the attack detector was integrated into the UAV's onboard system within the simulator. This integration was crucial to ensure that the detector had access to real-time flight data, including the UAV coordinates, flight speed, and trajectory information. Also, we configured specific parameters within the simulator to define the attack detection threshold. This involved setting up conditions under which the UAV would be considered under attack, such as sudden deviations from the planned path. Following the detection of an attack, our RCA-APF algorithm was automatically activated. This algorithm then recalculated the optimal path to ensure the UAV returned to its original trajectory. Throughout the experiments, data was collected on the response time of the attack detector, the accuracy of attack detection, and the effectiveness of the recovery path. This data was crucial for evaluating the performance of our system under various parameters. The experiments were conducted iteratively, allowing us to refine the attack detection parameters and recovery algorithms based on the outcomes of each test. This iterative process was key to enhancing the robustness and reliability of our system.

In Figure 11, we present an overhead view of a 3D path planning simulation for a UAV navigating in an environment with obstacles. This simulation is derived from an enhanced version of the original Quadcopter Simulation and Control program, to which we have integrated a reference UAV path planning algorithm with no attack. The modifications enable the simulator to generate a realistic depiction of the UAV's trajectory based on the provided input parameters.

Specifically, Figure 11 demonstrates the UAV's path planning capabilities in an attack-free scenario. This allows us to observe the UAV's trajectory as it smoothly progresses from its initial location to the intended destination, strictly adhering to the pre-calculated trajectory determined by our algorithm. The simulation, conducted in such an idealized setting, serves as a benchmark for evaluating the UAV's navigational proficiency and the path planning algorithm's efficacy under optimal conditions. In addition, the simulation results depicted in Figure 11 not only demonstrate the UAV's adherence to the predefined trajectory but also underscore the precision and robustness of our path planning algorithm. It is evident from the UAV's flight pattern that the trajectory is followed with remarkable accuracy, highlighting the algorithm's capability to navigate with minimal deviation from the set course. This fidelity to the planned route is indicative of the algorithm's sophisticated design, which accounts for various flight dynamics and environmental factors to ensure a seamless navigation experience.

Just Accepted

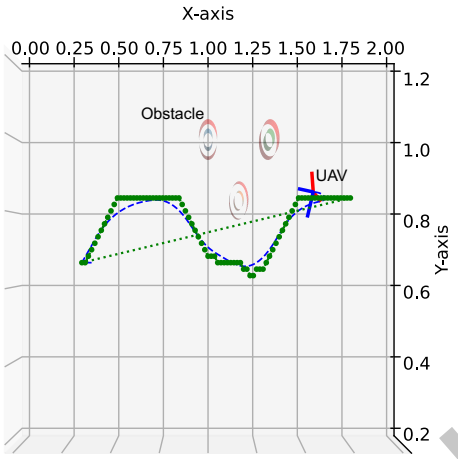

Fig. 11. UAV Path planning simulation with no attack.

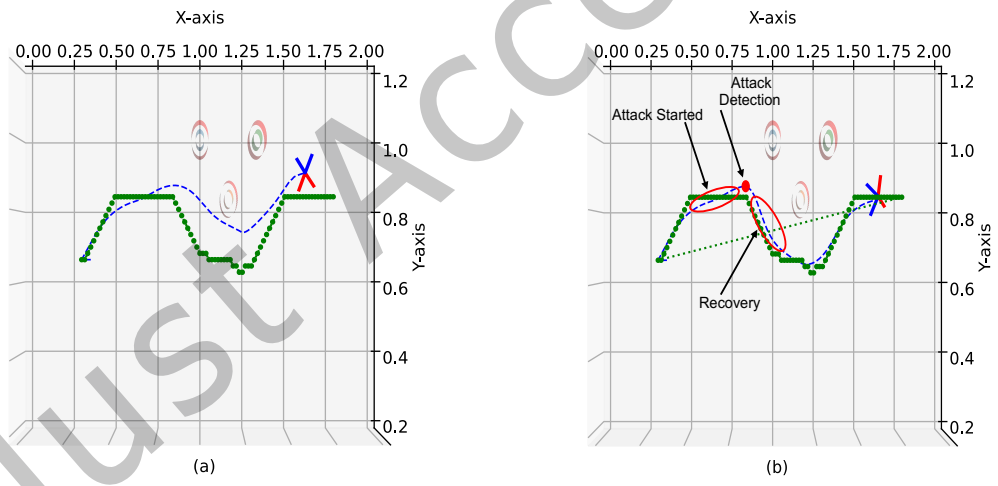

Fig. 12. UAV Path planning simulation with (a) attack and no recovery, (b) attack and recovery.

In Figure 12, we show a comparative visual analysis of two scenarios that highlight the resilience and adaptability of our algorithm in UAV path planning simulations. Figure 12 (a) depicts the UAV's path when it encounters a hostile attack and lacks any recovery protocols. This particular depiction serves to illustrate the vulnerability of the UAV's trajectory to external disruptions, which can lead to significant deviations from the intended path or, in some cases, result in the failure to complete the mission. The trajectory shown reveals the extent to which adversarial interference can compromise the UAV's operational integrity and underscores the necessity for

Just Accepted

robust countermeasures within the path planning framework. In contrast, Figure 12 (b) illustrates the UAV's trajectory under the condition of an external attack, which is initiated at a specific time and location during the flight. The system is designed to detect such an attack within a brief time frame, triggering the activation of the recovery protocol embedded within our algorithm. This sequence of events sets the stage for a critical evaluation of the recovery mechanism's robustness. The subsequent path of the UAV, as shown in Figure 12 (b), serves as a testament to the resilience of the recovery protocol. Despite the initial disruption, the UAV is not only able to detect and respond to the attack but also to recalibrate its course effectively. This realignment with the pre-planned route is a crucial demonstration of the algorithm's dynamic response capabilities. The UAV's successful navigation back to its intended trajectory and ultimate arrival at the target destination.

Moreover, the UAV's successful completion of its mission, as shown in the simulation, is proof of the algorithm's operational effectiveness. The algorithm's ability to guide the UAV through its journey with or without interference showcases its potential for real-world applications where reliability and precision are paramount. The UAV's performance, in this case, reflects a well-synchronized harmony between the algorithm's theoretical underpinnings and practical execution, paving the way for its deployment in more complex and dynamic environments.

6 CONCLUSIONS AND FUTURE WORK

As shown in this work, the cyber-physical nature of UAVs demands an extension to the scope of ordinary vulnerability analysis for such systems. In addition to threats in the computational components such as the GPS sensor and detectors, a largely overlooked class of vulnerabilities is fostered by the interactions between the computational systems and electrical and mechanical components. Pondering the list of UAV attacks, we started to investigate some of these computational threats where we have determined strategies and policies for path planning of the UAV under GPS performant faults. In the considered setting, we have developed a path planning procedure based on three stages: firstly, we use the modified artificial potential field algorithm to find the best path planning of the UAV, which flies in a complex environment with obstacles and GBSs. Secondly, we used the RSS trilateration localization approach to estimate the location of the UAV under GPS permanent faults. The RSS trilateration localization measurements helped us to estimate the location of the UAV at every step. Finally, combining the first two steps, we implemented the RCA-APF algorithm considering a single UAV. Simulation and experiment results have demonstrated the path-planning conditions under which the UAV can reach its final destination. Finally, we validate the feasibility of our design using a path-planning UAV simulator. Future work will show more complex environments including multiple path planning for several UAVs.

ACKNOWLEDGEMENT

This work was supported in part by NSF CNS-2333980 and NSF CNS- 2221875. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the National Science Foundation (NSF).

REFERENCES

[1] N Adam. 2010. Workshop on future directions in cyber-physical systems security. *U.S. Department of Homeland Security* October 2014 (2010), 1–61. https://reeves.ee.washington.edu/people/faculty/radha/dhs{_}cps.pdf

[2] Akram Al-Hourani, Sithamparanathan Kandeepan, and Abbas Jamalipour. 2014. Modeling air-to-ground path loss for low altitude platforms in urban environments. In *2014 IEEE Global Communications Conference, GLOBECOM 2014*. Institute of Electrical and Electronics Engineers Inc., 2898–2904. https://doi.org/10.1109/GLOCOM.2014.7037248

[3] Alvaro A. Cárdenas, Saurabh Amin, and Shankar Sastry. 2008. Secure control: Towards survivable cyber-physical systems. *Proceedings - International Conference on Distributed Computing Systems* (2008), 495–500. https://doi.org/10.1109/ICDCS.WORKSHOPS.2008.40

[4] Yiu Tong Chan, Herman Yau Chin Hang, and Pak Chung Ching. 2006. Exact and approximate maximum likelihood localization algorithms. *IEEE Transactions on Vehicular Technology* 55, 1 (jan 2006), 10–16. https://doi.org/10.1109/TVT.2005.861162

Just Accepted

[5] Cheng Chang and Anant Sahai. 2004. Estimation bounds for localization. In *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, IEEE SECON 2004*. 415–424. https://doi.org/10.1109/sahcn.2004.1381943

[6] Isadora G. Ferrao, Sherlon A. Da Silva, Daniel F. Pigatto, and Kalinka R.L.J.C. Branco. 2020. GPS Spoofing: Detecting GPS Fraud in Unmanned Aerial Vehicles. *2020 Latin American Robotics Symposium, 2020 Brazilian Symposium on Robotics and 2020 Workshop on Robotics in Education, LARS-SBR-WRE 2020* (nov 2020). https://doi.org/10.1109/LARS/SBR/WRE51543.2020.9307036

[7] Rong Xiao Guo, Ji Wei Tian, Bu Hong Wang, and Fu Te Shang. 2020. Cyber-Physical Attack Threats Analysis for UAVs from CPS Perspective. *Proceedings - 2020 International Conference on Computer Engineering and Application, ICCEA 2020* (mar 2020), 259–263. https://doi.org/10.1109/ICCEA50009.2020.00063

[8] Rong Xiao Guo, Ji Wei Tian, Bu Hong Wang, and Fu Te Shang. 2020. Cyber-Physical Attack Threats Analysis for UAVs from CPS Perspective. In *Proceedings - 2020 International Conference on Computer Engineering and Application, ICCEA 2020*. Institute of Electrical and Electronics Engineers Inc., 259–263. https://doi.org/10.1109/ICCEA50009.2020.00063

[9] Ismail Güvenç and Chia Chin Chong. 2009. A survey on TOA based wireless localization and NLOS mitigation techniques. *IEEE Communications Surveys and Tutorials* 11, 3 (2009), 107–124. https://doi.org/10.1109/SURV.2009.090308

[10] Majumder Haider, Imtiaz Ahmed, and Danda B. Rawat. 2022. Cyber Threats and Cybersecurity Reassessed in UAV-assisted Cyber Physical Systems. In *International Conference on Ubiquitous and Future Networks, ICUFN*, Vol. 2022-July. IEEE Computer Society, 222–227. https://doi.org/10.1109/ICUFN55119.2022.9829584

[11] Yoshiyuki Harada, Yoriyuki Yamagata, Osamu Mizuno, and Eun-Hye Choi. 2017. Log-based anomaly detection of CPS using a statistical method. In *2017 8th International Workshop on Empirical Software Engineering in Practice (IWESEP)*. IEEE, 1–6.

[12] Di Jin, Feng Yin, Carsten Fritsche, Fredrik Gustafsson, and Abdelhak M. Zoubir. 2020. Bayesian cooperative localization using received signal strength with unknown path loss exponent: Message passing approaches. *IEEE Transactions on Signal Processing* 68 (2020), 1120–1135. https://doi.org/10.1109/TSP.2020.2969048 arXiv:1904.00715

[13] O. Khatib. 1985. Real-time obstacle avoidance for manipulators and mobile robots. In *Proceedings - IEEE International Conference on Robotics and Automation*. 500–505. https://doi.org/10.1109/ROBOT.1985.1087247

[14] Tng T. Kim and H. Vincent Poor. 2011. Strategic protection against data injection attacks on power grids. *IEEE Transactions on Smart Grid* 2, 2 (2011), 326–333. https://doi.org/10.1109/TSG.2011.2119336

[15] Praveen Kumar, Lohith Reddy, and Shirshu Varma. 2009. Distance measurement and error estimation scheme for RSSI based localization in wireless sensor networks. In *5th International Conference on Wireless Communication and Sensor Networks, WCSN-2009*. 80–83. https://doi.org/10.1109/WCSN.2009.5434802

[16] Cheolhyeon Kwon, Weiyi Liu, and Inseok Hwang. 2013. Security analysis for Cyber-Physical Systems against stealthy deception attacks. In *Proceedings of the American Control Conference*. 3344–3349. https://doi.org/10.1109/acc.2013.6580348

[17] Mengyu Liu, Lin Zhang, Pengyuan Lu, Kaustubh Sridhar, Fanxin Kong, Oleg Sokolsky, and Insup Lee. 2022. Fail-safe: Securing cyber-physical systems against hidden sensor attacks. In *2022 IEEE Real-Time Systems Symposium (RTSS)*. IEEE, 240–252.

[18] Yuan Luo, Ya Xiao, Long Cheng, Guojun Peng, and Danfeng Yao. 2021. Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. *ACM Computing Surveys (CSUR)* 54, 5 (2021), 1–36.

[19] Cheng Ma, Jinglei Li, Ying Shang, Shuai Zhang, and Qinghai Yang. 2022. A Dynamic Obstacle Avoidance Control Algorithm for Distributed Multi-UAV Formation System. In *2022 IEEE International Conference on Mechatronics and Automation, ICMA 2022*. Institute of Electrical and Electronics Engineers Inc., 876–881. https://doi.org/10.1109/ICMA54519.2022.9856064

[20] Richard K. Martin, Amanda Sue King, Jason R. Pennington, Ryan W. Thomas, Russell Lenahan, and Cody Lawyer. 2012. Modeling and mitigating noise and nuisance parameters in received signal strength positioning. *IEEE Transactions on Signal Processing* 60, 10 (2012), 5451–5463. https://doi.org/10.1109/TSP.2012.2207118

[21] Daniel Mendes, Naghmeh Ivaki, and Henrique Madeira. 2019. Effects of GPS spoofing on unmanned aerial vehicles. In *Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC*, Vol. 2018-Decem. IEEE Computer Society, 155–160. https://doi.org/10.1109/PRDC.2018.00026

[22] Mohammad Mozaffari, Walid Saad, Mehdi Bennis, and Mérouane Debbah. 2016. Unmanned Aerial Vehicle with Underlaid Device-to-Device Communications: Performance and Tradeoffs. *IEEE Transactions on Wireless Communications* 15, 6 (jun 2016), 3949–3963. https://doi.org/10.1109/TWC.2016.2531652 arXiv:1509.01187

[23] Abdelmoumen Norrdine. 2012. An algebraic solution to the multilateration problem. In *Proceedings of the 15th international conference on indoor positioning and indoor navigation, Sydney, Australia*, Vol. 1315.

[24] Miroslav Pajic, James Weimer, Nicola Bezzo, Paulo Tabuada, Oleg Sokolsky, Insup Lee, and George J. Pappas. 2014. Robustness of attack-resilient state estimators. *2014 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS 2014* (2014), 163–174. https://doi.org/10.1109/ICCPS.2014.6843720

[25] Junkil Park, Radoslav Ivanov, James Weimer, Miroslav Pajic, Sang Hyuk Son, and Insup Lee. 2017. Security of Cyber-Physical Systems in the Presence of Transient Sensor Faults. *ACM Trans. Cyber-Phys. Syst.* 1, 3, Article 15 (may 2017), 23 pages. https://doi.org/10.1145/3064809

[26] Shamsur Rahman and You Ze Cho. 2018. UAV positioning for throughput maximization. *Eurasip Journal on Wireless Communications and Networking* 2018, 1 (dec 2018), 1–15. https://doi.org/10.1186/s13638-018-1038-0

Just Accepted

[27] Mohd Ezanee Rusli, Mohammad Ali, Norziana Jamil, and Marina Md Din. 2016. An Improved Indoor Positioning Algorithm Based on RSSI-Trilateration Technique for Internet of Things (IOT). In *Proceedings - 6th International Conference on Computer and Communication Engineering: Innovative Technologies to Serve Humanity, ICCCE 2016*. Institute of Electrical and Electronics Engineers Inc., 12–77. https://doi.org/10.1109/ICCCE.2016.28

[28] Fernando Seco, Antonio R. Jiménez, Carlos Prieto, Javier Roa, and Katerina Koutsou. 2009. A survey of mathematical methods for indoor localization. In *WISP 2009 - 6th IEEE International Symposium on Intelligent Signal Processing - Proceedings*. 9–14. https://doi.org/10.1109/WISP.2009.5286582

[29] Bingbing Song, Haiyang Chen, Jiashun Suo, and Wei Zhou. 2022. Low-power Robustness Learning Framework for Adversarial Attack on Edges. *2022 18th International Conference on Mobility, Sensing and Networking (MSN)* (dec 2022), 821–828. https://doi.org/10.1109/MSN57253.2022.00133

[30] M. Hani Sulieman, M. Cenk Gursoy, and Fanxin Kong. 2021. Antenna Pattern Aware UAV Trajectory Planning Using Artificial Potential Field. In *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, Vol. 2021-Octob. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/DASC52595.2021.9594394

[31] Jiayi Sun, Jun Tang, and Songyang Lao. 2017. Collision Avoidance for Cooperative UAVs with Optimized Artificial Potential Field Algorithm. *IEEE Access* (2017). https://doi.org/10.1109/ACCESS.2017.2746752

[32] Jiwei Tian, Buhong Wang, Rongxiao Guo, Zhen Wang, Kunrui Cao, and Xiaodong Wang. 2021. Adversarial Attacks and Defenses for Deep Learning-based Unmanned Aerial Vehicles. *IEEE Internet of Things Journal* (2021). https://doi.org/10.1109/JIOT.2021.3111024

[33] Jiwei Tian, Buhong Wang, Rongxiao Guo, Zhen Wang, Kunrui Cao, and Xiaodong Wang. 2022. Adversarial Attacks and Defenses for Deep-Learning-Based Unmanned Aerial Vehicles. *IEEE Internet of Things Journal* 9, 22 (nov 2022), 22399–22409. https://doi.org/10.1109/JIOT.2021.3111024

[34] Chafiq Titouna and Farid Naït-Abdesselam. 2021. A Lightweight Security Technique For Unmanned Aerial Vehicles Against GPS Spoofing Attack. In *2021 International Wireless Communications and Mobile Computing, IWCMC 2021*. Institute of Electrical and Electronics Engineers Inc., 819–824. https://doi.org/10.1109/IWCMC51323.2021.9498734

[35] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. 2017. WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks. In *Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017*. Institute of Electrical and Electronics Engineers Inc., 3–18. https://doi.org/10.1109/EuroSP.2017.42

[36] Haichao Wang, Jin Chen, Guoru Ding, and Jiachen Sun. 2018. Trajectory Planning in UAV Communication with Jamming. In *2018 10th International Conference on Wireless Communications and Signal Processing, WCSP 2018*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/WCSP.2018.8555700

[37] Haichao Wang, Guochun Ren, Jin Chen, Guoru Ding, and Yijun Yang. 2018. Unmanned Aerial Vehicle-Aided Communications: Joint Transmit Power and Trajectory Optimization. *IEEE Wireless Communications Letters* 7, 4 (2018), 522–525. https://doi.org/10.1109/LWC.2018.2792435 arXiv:1801.05351

[38] Shenqing Wang, Jiang Wang, Chunhua Su, and Xinshu Ma. 2020. Intelligent detection algorithm against Uavs' GPS spoofing attack. *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS* 2020-December (dec 2020), 382–389. https://doi.org/10.1109/ICPADS51040.2020.00058

[39] Xueyuan Wang and M. Cenk Gursoy. 2022. Resilient UAV Path Planning for Data Collection under Adversarial Attacks. In *IEEE International Conference on Communications*, Vol. 2022-May. Institute of Electrical and Electronics Engineers Inc., 625–630. https://doi.org/10.1109/ICC45855.2022.9838325

[40] Anthony J. Weiss. 2003. On the Accuracy of a Cellular Location System Based on RSS Measurements. *IEEE Transactions on Vehicular Technology* 52, 6 (nov 2003), 1508–1518. https://doi.org/10.1109/TVT.2003.819613

[41] Qingqing Wu, Yong Zeng, and Rui Zhang. 2018. Joint trajectory and communication design for multi-UAV enabled wireless networks. *IEEE Transactions on Wireless Communications* 17, 3 (mar 2018), 2109–2121. https://doi.org/10.1109/TWC.2017.2789293 arXiv:1705.02723

[42] Jiaping Xiao and Mir Feroskhan. 2022. Cyber Attack Detection and Isolation for a Quadrotor UAV With Modified Sliding Innovation Sequences. *IEEE Transactions on Vehicular Technology* 71, 7 (jul 2022), 7202–7214. https://doi.org/10.1109/TVT.2022.3170725

[43] Zhiqiang Xiao and Yong Zeng. 2022. An overview on integrated localization and communication towards 6G. https://doi.org/10.1007/s11432-020-3218-8 arXiv:2006.01535

[44] Jie Yang and Yingying Chen. 2009. Indoor localization using improved rss-based lateration methods. In *GLOBECOM - IEEE Global Telecommunications Conference*. https://doi.org/10.1109/GLOCOM.2009.5425237

[45] Zheng Yang, Zimu Zhou, and Yunhao Liu. 2013. From RSSI to CSI: Indoor localization via channel response. *Comput. Surveys* 46, 2 (dec 2013). https://doi.org/10.1145/2543581.2543592

[46] Qingfeng Yao, Zeyu Zheng, Liang Qi, Haitao Yuan, Xiwang Guo, Ming Zhao, Zhi Liu, and Tianji Yang. 2020. Path Planning Method With Improved Artificial Potential Field—A Reinforcement Learning Perspective. *IEEE Access* 8 (2020), 135513–135523. https://doi.org/10.1109/ACCESS.2020.3011211

Just Accepted

[47] Esen Yel and Nicola Bezzo. 2020. GP-based Runtime Planning, Learning, and Recovery for Safe UAV Operations under Unforeseen Disturbances. In *IEEE International Conference on Intelligent Robots and Systems*. Institute of Electrical and Electronics Engineers Inc., 2173–2180. https://doi.org/10.1109/IROS45743.2020.9341641

[48] Seyed A.Reza Zekavat and Michael Buehrer. 2011. *Handbook of Position Location: Theory, Practice, and Advances*. https://doi.org/10.1002/9781118104750

[49] Yong Zeng and Rui Zhang. 2017. Energy-Efficient UAV Communication with Trajectory Optimization. *IEEE Transactions on Wireless Communications* 16, 6 (jun 2017), 3747–3760. https://doi.org/10.1109/TWC.2017.2688328 arXiv:1608.01828

[50] Hang Zhang and Fei Luo. 2022. An improved UAV path planning method based on APSOvnp-APF algorithm. In *Proceedings of the 34th Chinese Control and Decision Conference, CCDC 2022*. Institute of Electrical and Electronics Engineers Inc., 5458–5463. https://doi.org/10.1109/CCDC55256.2022.10034025

[51] Lin Zhang, Zifan Wang, Mengyu Liu, and Fanxin Kong. 2022. Adaptive window-based sensor attack detection for cyber-physical systems. In *59th ACM/IEEE Design Automation Conference, DAC 2022*. Institute of Electrical and Electronics Engineers Inc., 919–924.

[52] Long Zhang, Hui Zhao, Shuai Hou, Zhen Zhao, Haitao Xu, Xiaobo Wu, Qiwu Wu, and Ronghui Zhang. 2019. A Survey on 5G Millimeter Wave Communications for UAV-Assisted Wireless Networks. *IEEE Access* 7 (jul 2019), 117460–117504. https://doi.org/10.1109/access.2019.2929241

Received 19 April 2023; revised 22 January 2024; accepted 29 February 2024

Just Accepted