IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 May 2023, accepted 24 May 2023, date of publication 31 May 2023, date of current version 8 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3281731

SURVEY

GPS Spoofing Attacks in FANETs: A Systematic Literature Review

ALA ALTAWEEL, (Member, IEEE), HENA MUKKATH, AND IBRAHIM KAMEL, (Senior Member, IEEE)

Department of Computer Engineering, Information and Network Security Research Group, College of Computing and Informatics, University of Sharjah, Sharjah, United Arab Emirates

Corresponding author: Ala Altaweel (aaltaweel@sharjah.ac.ae)

This work was supported by the University of Sharjah.

ABSTRACT Flying Ad-Hoc Networks (FANETs) are groups of UAVs connected in an Ad-Hoc manner to accomplish a common mission. The widespread acceptance of UAVs due to their low cost and high efficiency has attracted malicious security attacks against them. These attacks cannot be easily prevented due to UAVs' limited computational power, short battery life, and inability to execute complex algorithms. FANETs rely on the Global Positioning System (GPS) for localization. GPS Spoofing, an easy-to-launch attack, is one of the main challenges in FANETs. In which, the legitimate and not-encrypted civilian GPS signals are overridden by counterfeit signals to deceive the UAVs to collide or to be hijacked. Researchers proposed various countermeasures to address GPS Spoofing attacks in FANETs. To further assist future research, this paper provides a systematic literature review on GPS Spoofing attacks in FANETs and their defense mechanisms. After formulating eight research questions and applying well-defined inclusion/exclusion criteria and quality assessment tools, 70 research articles were extracted. The existing defense mechanisms were classified based on their objectives (i.e., detection, mitigation, and/or prevention) and according to their basis (i.e., relying on readings from various drones' devices/sensors, processing the signals received by various sensors, employing machine learning algorithms, relying on game theory, or leveraging cryptographic techniques to authenticate and protect the confidentiality of GPS signals). The defense mechanisms were also analyzed to identify the attacker models, impacts of the attack, and detection performance. This study found that most of the proposed methods are detection approaches, rather than mitigation or prevention. Also, almost all papers used simulation experiments rather than a proof-of-concept implementation, which does not demonstrate a convincing performance under realistic mobility and propagation models. Moreover, most solutions addressed GPS Spoofing for a single UAV. Only eight articles addressed multiple UAV scenarios and none of them provided a proof-of-concept evaluation.

INDEX TERMS Drones, unmanned ariel vehicle (UAV), Flying Ad-Hoc NETwork (FANET), GPS spoofing attack, wireless network security, systematic literature review.

I. INTRODUCTION

The advancements in technology have invaded almost every sphere of human life. Human intervention is been getting expelled from the aircraft industry as well. The development of autonomous drones or Unmanned Ariel Vehicles (UAVs), popularly known as 'drones', is a major indication of this fact. The drone market has put on huge investments since the beginning of this decade. As per a report from the Drone Industry Insights [1], the drone market worth ∼$30.6 billion in 2022 and is expected to reach ∼$55.8 billion by 2030. This is due to the widespread acceptance of UAVs for various military and civilian applications such as border surveillance [2], disaster monitoring [3], traffic monitoring [4], managing wildfire [5], relay for Ad-Hoc networks [6], wind estimation [7], emergency management and high-risk situations [8],

The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Mueen Uddin.

etc. The deployment of UAVs not only nullifies the risk for human operators but also minimizes the probability of human errors. Single large UAVs were recently used, yet, they are inadequate in terms of capability [9]. Thus, the technologists found it is advantageous to deploy small multiple UAVs that work in groups.

FANET is a self-organized UAV network, popularly known as UAV Swarm, in which UAVs operate together collaboratively to accomplish various missions. The UAVs in FANETs communicate with each other by establishing wireless Ad-Hoc UAV-to-UAV communication links [10]. That is, no pre-established infrastructure is required for FANET deployment. The capability of sharing information, not only with the ground station but also among the UAVs, makes FANETs less prone to the difficulties of short-range communications and network failures, which might occur when a single UAV is deployed. The deployment of multi-UAVs in groups is advantageous due to many reasons. The *cost* [11] of deploying and maintaining small UAVs instead of larger ones is more feasible. The *scalability* [11] of operation also enhances with small multi-UAVs. Also, since multiple UAVs work together, the chance of *Single-Point-of-Failure* [12] is minimized. Moreover, multiple UAVs can accomplish a task more *efficiently* [13]. On the other hand, FANETs confront various technical and security challenges [14].

The battery with limited capacity poses a major challenge in UAV operations by limiting their flight time. UAVs' computational power and storage are also limited. UAVs normally hover in 3-D space with a speed range of 30-460 km/h [15], leading to frequent variations in communication distances and topology changes. The drones should maintain connectivity within the network such that the area covered by individual drones and the swarm as a whole is maximized without causing network partitioning. The locational information provided by the GPS plays a vital role in this regard. The exchanged GPS information among the drones helps in relatively localizing each drone to other drones as well as within the swarm area. With the widespread acceptance of FANETs among public and private entities, they are also targeted by malicious attackers. The GPS sensors in drones are vulnerable to GPS Spoofing and Jamming attacks, which are the most popular and easy-to-launch attacks that can be instigated using low-cost Software Defined Radio (SDR) [16]. While Jamming intends to deny GPS services in the target area by transmitting stronger signals with the same frequency used by genuine GPS signals, spoofing attacks intend to redirect the UAVs from their actual path to the attacker's desired path. In December 2012, Iranian army engineers claimed that they hijacked a surveillance drone launched by U.S. Central Intelligence Agency (CIA) RQ170 Sentinel [17]. The first successful spoofing on GPS receivers of drones was demonstrated by a research team at the University of Texas [18], [19] as a part of a demonstration to raise concerns about civilian drone regulations. The U.S. Customs and Border Protection reported that some drug cartels spoofed their drones in 2015 and the attacks of the same kind increased afterward [20].

To address the aforesaid research challenge, a systematic literature review has been conducted with the aim of pinpointing the state-of-the-art of GPS Spoofing attacks in FANET, the attacker capabilities, and the detection and mitigation mechanisms. To the best of our knowledge, this is the first systematic review on GPS Spoofing attacks in FANETs that followed the review guidelines proposed by [21]. These guidelines are widely adopted by the research community to conduct unbiased and high-quality surveys. The articles published during the tenure from 2017 to 2022 are considered, as GPS Spoofing in FANETs is a recently developed research area. This survey was conducted in three phases. Specifically, planning, conducting, and reporting. In the planning phase, eight Research Questions were formulated. The articles for this survey have been collected from five databases, namely, **IEEE XPlore®, ACM Digital Library, ScienceDirect®, SpringerLink** and **Google Scholar** in the conducting phase. Afterward, 70 papers including 14 state-of-the-art survey papers and 56 technical papers relevant to the survey's topic were extracted. Among the 56 technical papers, 37 papers proposed various solutions to defend against GPS spoofing attacks in UAVs, nine papers discussed GPS Spoofing attack mechanisms, eight papers discussed how GPS spoofing can be used to deter malicious drones from sensitive areas, one article conducted an impact study on GPS Spoofing attack in UAVs, and one article portrayed the vulnerability of UAVs to GPS Spoofing attack.

The extracted technical papers were categorized into four groups. Specifically, GPS Spoofing attack mechanisms (that discussed the attacker models), GPS Spoofing defense mechanisms, GPS Spoofing as a defense mechanism (that leverages GPS Spoofing techniques to defend against other attacks), as well as GPS Spoofing impact and vulnerability, which studied the impact of and vulnerability to GPS Spoofing attack on drones. Then, a taxonomy of various defense mechanisms is redesigned based on their objectives and basis. For the objectives, the defense mechanisms are classified into three categories: 1) *detection mechanisms*, which sense or alert the presence of attack, 2) *mitigation mechanisms*, which help the drones to recover from the effects of the attack, 3) *prevention mechanisms*, which secure the drones from being attacked. For the basis, the defense mechanisms can also be classified into five categories: 1) *onboard sensor/devices*, which compare the readings from the devices on the drones like cameras, gyroscopes, accelerometers, barometers, etc. with the readings of GPS receivers, 2) *signal processing methods*, which analyze the received signal parameters like the Time of Arrival, Angle of Arrival, Signal Strength, etc., 3) *cryptographic techniques* such as encryption, decryption, authentication, digital signatures, etc., which are used to secure and verify the GPS signals received by the drones, 4) *game-theory based methods*, which depend on the strategic movements of the attacker and

the victim during the attack, and 5) *machine learning-based methods*, which leverage the training and learning models designed to defend against the attacks. The survey aims to enable the readers to gain insights into the directions of research in the field of GPS Spoofing attacks in FANETs. Also, the readers are aided to find the research gaps existing in the domain. The major contributions of this survey are as follows:

- Comprehensive guidelines for researchers in terms of FANETs' features, applications, mobility, propagation models, communication protocols, and security challenges (in Section II) are provided. GPS Spoofing attacks and their impacts are also discussed in detail.
- Following the guidelines of Kitechenham and Charters [21], this survey systematically extracted 70 articles that are relevant to GPS Spoofing attacks in UAVs, by applying the planning, conducting, and reporting phases recommended by [21] (in Section III). The extracted articles were classified into state-of-the-art articles and technical articles.
- A detailed analysis of the state-of-the-art articles in terms of the number of papers surveyed, the years of publications considered, and a brief description of the concepts discussed in these articles are provided (in Section IV). A summarized table of these articles is also provided in Table 11 in the Appendix.
- The technical articles on GPS Spoofing are classified (in Section V) into four main categories as follows:
  - *GPS Spoofing attack mechanisms*: the articles that discussed the attacker models. As a part of the attacker model, we discussed:
    - Spoofing tools such as simulators, repeaters, etc.
    - Spoofing techniques such as position denial and track break.
    - Spoofer location such as remote, onboard, and escort.
  - *Defense mechanisms against GPS Spoofing*: the research articles that discuss various mechanisms to defend against GPS Spoofing attacks in UAVs. These articles are further classified based on their objectives as follows:
    - Detection of GPS Spoofing attacks.
    - Mitigation the damage caused by GPS Spoofing attacks.
    - Prevention of GPS Spoofing.

    The defense mechanisms are also classified according to their basis as follows:
    - The use of devices/sensors on the drones.
    - Signal processing techniques applied on various signals received by various sensors on the drone.
    - Cryptographic techniques to protect the confidentiality of data collected by the drones.
    - Game-theory techniques that are used to defend against GPS Spoofing attacks.
    - Machine learning techniques that are used to defend against GPS Spoofing attacks.
  - *Use of GPS Spoofing* as a mechanism to deter malicious drones from sensitive infrastructure.
  - *Impact and Vulnerability*: the articles that discussed the impact of the GPS Spoofing attack and the vulnerability of drones to it.

  The above taxonomy is based on a systematic analysis of various approaches that deal with GPS Spoofing attacks in UAVs. The diversity in the existing research works and the lack of a proper taxonomy is the motivation behind the development of the above taxonomy. This survey aims to classify all the existing methods under various headers and conduct a comparative survey to identify the open issues for future research works.
- An extensive study of the 37 articles that dealt with defense mechanisms against GPS Spoofing attacks is conducted in Section V. The study focused on the proposed defense methodology in the existing works to extract the number of UAVs considered (i.e., FANET or single UAV environment), the detection performance evaluation methodologies (i.e., simulation or proof-of-concept implementation), and the performance metrics used. The limitations and open issues in the existing research are also identified.
- A detailed discussion and comparative analysis of the extracted results in terms of the datasets used in the experiments, the attacker models, the performance evaluation methods, and metrics from all covered articles are provided. This analysis is done in order to understand the current state of the defense mechanisms, identify the research gaps, and propose recommendations for future research works (in Section VI).

The rest of this paper is organized as follows: Section II briefly describes the technical background of FANETs, which includes a discussion of their mobility and propagation models, communication protocols, applications, performance evaluation methods and metrics, and security challenges. A special focus on GPS Spoofing attacks and their impacts on FANETs is also provided. Section III presents the systematic literature review methodology that was applied in this study. In Section IV, the state-of-the-art papers are discussed. The technical papers on GPS Spoofing attacks, the existing solutions, the application of GPS Spoofing attacks (as a defense mechanism), and the impact and vulnerability of the GPS Spoofing attack are elaborated in Section V. The results, discussions, and research gaps are portrayed in Section VI. The paper is concluded in Section VII.

II. FANETs: TECHNICAL BACKGROUND AND APPLICATIONS

In this section, the acronym 'FANET' is introduced in detail with a substantial description of the unique characteristics, mobility and propagation models, communication protocols, applications, and security issues in FANETs. Furthermore, various performance metrics that can be used to evalu-

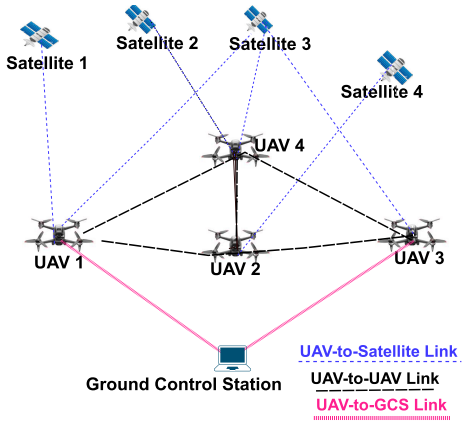

FIGURE 1. A typical FANET environment.

TABLE 1. Abbreviations related to FANET environment.

Abbreviation	Name
FANET	Flying Ad-Hoc Network
UAV	Unmanned Aerial Vehicle
GCS	Ground Control Station
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
INS	Inertial Navigation System
IMU	Inertial Measurement Unit

ate the performance of the FANET environment are also discussed.

A. FANETs: FLYING AD-HOC NETWORKS

FANETs comprise UAVs, connected together in an Ad-Hoc manner. The major components of an Unmanned Aerial System (UAS) include the UAV, the GCS, and the communication links. The communication links include the UAV-to-UAV links, UAV-to-Satellite links, and UAV-to-GCS links [11]. The UAVs in FANET utilize GPS and this locational information is exchanged within the network for maintaining the FANET topology. Fig. 1 depicts a typical FANET environment. The UAVs communicate with each other through Ad-Hoc UAV-to-UAV links. The UAVs have onboard GPS receivers and the locational information (via UAV-to-Satellite link) received from at least four satellites [22] is used to find the UAV position through the process of trilateration [23]. The radio waves from the satellite travel at the speed of light and the time of departure of the GPS signal from the satellite are obtained from this signal. The speed and time obtained are used by the GPS receivers to compute the distance between the satellite and the GPS receiver. One (or more) of the UAVs communicate with the GCS for exchanging control and other relevant information. Table 1 shows various abbreviations related to the FANET environment that are used throughout this paper. Some other common abbreviations used in this paper are shown in Table 2.

The UAVs constituting the FANETs are generally low-cost commercial off-the-shelf devices with limited computational power and storage. Thus, FANETs cannot rely on algorithms

TABLE 2. Abbreviations related to attacker models.

Abbreviation	Name
SDR	Software Defined Radio
RF	Radio Frequency
USRP	Universal Software Radio Peripheral

requiring complex computations for accomplishing their mission or incorporating security features. Due to the size and weight constraints of drones in FANETs, it is not possible to leverage powerful computation hardware. Also, since complex computations consume lots of energy, the battery gets drained faster. In Section II-B below, we provide a detailed discussion of the unique characteristic features of FANETs.

B. UNIQUE FEATURES OF FANET

The unique characteristics of FANET [24] are depicted in Fig. 2 and are elaborated in the subsequent lines:

- *Dynamic Network Topology*: The higher mobility and the failure or injection of drones in the FANET cause frequent topology changes. The movement of drones and the resultant variations in the distance between drones can lead to link outages [11].
- *Mobility Models*: The drones in FANET follow either a pre-defined trajectory or random paths [11]. A detailed discussion of the mobility models is provided in Section II-C.
- *Node Mobility*: The drones in FANET move at higher speeds than those in a MANET or VANET. Based on the type of flight and mission, this speed can range from 30 to 460 km/h. These variations in speed present various communication problems [11] such as network partitioning.
- *Node Density*: The UAVs in a FANET are generally distributed across the entire swarm area so that the coverage area of individual drones and the FANET itself are maximized. Thus, the node density (number of drones per unit area) is lesser when compared to the other networks such as MANET or VANET [11].
- *Propagation Models*: The communication between the UAVs (U2U) in the FANET is Line-of-Sight and those between UAV and GCSs are nLos (non-Line-of-Sight) [25]. A detailed discussion of the propagation models in FANET is provided in Section II-C.
- *Power Consumption*: FANETs, with battery-powered, drones are energy-limited devices. The power consumption varies with the size of the drones, distance to be covered, mission, communication hardware used, etc. [11]. Lowering the dependence on power-sensitive devices and complex computational algorithms in FANETs can enhance the network lifetime and reduce network outages.
- *3-D Space*: FANET flies in free space, mostly far above the ground without obstructions such as buildings, trees, etc. Thus, there is no significant path loss in the signals transmitted among the drones

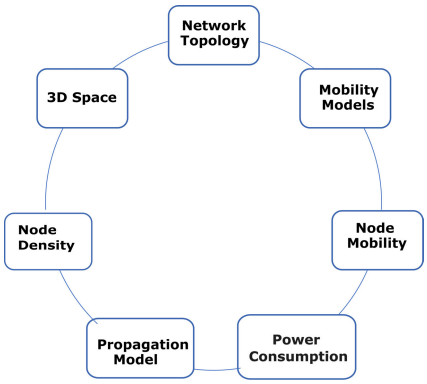

FIGURE 2. Unique features of FANET.

The frequent topology variations impact the communication and collaboration of the drones in a FANET. The movement pattern of the drones is represented (i.e., modeled) using various mobility patterns, which are discussed in Section II-C.

C. MOBILITY AND PROPAGATION MODELS IN FANETs

FANETs are unique in terms of their mobility, topology variations, propagation, and energy constraints [11]. In this section, some light is thrown on the mobility and propagation models in FANETs, which are also part of the Research Questions in this study (Section III-A: RQ6 and RQ7).

The UAVs in FANET move with higher velocity when compared to the ancestral networks, namely, MANETs and VANETs. Moreover, the UAVs hover in three-dimensional (3-D) space (roll, pitch, and yaw). Hence, more adequate mobility models are employed that simulate the motion of FANETs in real-world scenarios. Mobility models describe the motion pattern of the UAV including the velocity (speed change and direction) and acceleration. Different mobility models have been used in FANET environments such as random, group, time-dependant, and path-planned. A classification FANETs mobility models based on a study by Wheeb et al. [26] is illustrated in Fig. 3 and is briefly described below:

- **Random Mobility Model**: The drones in this mobility model move randomly and freely without any restrictions. Thus, this mobility model is not preferable for FANET scenarios as the drones in FANET should move in a coordinated manner without network partitioning. Random mobility model is further classified into the following four sub-types:
  - *Random Walk (RW)* in which the drones move in a random direction and speed for a fixed interval of time or distance, then new speed and direction are calculated. These are memory-less models.
  - *Random Waypoint (RWP)* in which halts are taken upon reaching each waypoint and then move to the random direction at a random speed.
  - *Random Direction (RD)* in which the destination is chosen towards the boundary of the simulation area; once it reaches the destination, it stops and new destinations are chosen again.
  - *Manhattan Grid (MG)* in which the UAVs follow a grid-structure path layout. These mobility models are used in scenarios where paths are well-defined. The UAV randomly chooses to move in the same direction or take turns at intersections of the grid.
- **Group Mobility Model**: This mobility model is deployed in scenarios where drones should move in groups, as is the case in FANETs, to accomplish a specific mission. This model can be further categorized into the following four sub-types:
  - *Column (CLMN)* in which a point of reference along a straight line will be defined; each node revolves around this point in a random direction and speed.
  - *Exponential Correlated Random (ECR)* in which a group of nodes exhibits correlated dynamic motion.
  - *Nomadic Community (NC)* in which every UAV node moves randomly around certain reference points following the same path leading to a collision.
  - *Pursue (PRS)* in which the UAV tracks a particular UAV that travels in a specific way.
- **Time-dependent**: The sudden changes in speed and direction are avoided in this model by considering various parameters like prior direction, current time, speed, etc. This model can be further categorized into the following three sub-types:
  - *Gauss Markov (GM)* in which sudden movement changes are minimized by adjusting randomness in direction and speed.
  - *Smooth Turn (ST)* in which the accelerations of UAVs are always maintained by adjusting the spatial and temporal variables.
  - *Enhanced Gauss Markov (EGM)* which is most widely used in FANETs. The direction deviations are used to reduce sharp turns and stops.
- **Path-Planned**: A pre-determined trajectory is generated and stored for each UAV. This model can be further classified into the following three sub-types:
  - *Flight Plan (FP)* in which UAV's flight plan is defined in a special file and time-dependent flight maps are designed accordingly.
  - *Semi Random Circular (SRCM)* in which UAVs move in curved paths around a central point.
  - *Paparazzi Model (PPRZM)*, a Probabilistic model based on state machines with five possible movements, namely, waypoint, scan, stay-at, eight, and oval.

Propagation models also occupy a relevant space in FANET communication. Propagation model refers to the mathematical modeling of the radio channel through which the waves are transmitted (i.e., to simulate the attenuation of the waves when propagated [27]). The FANET environment

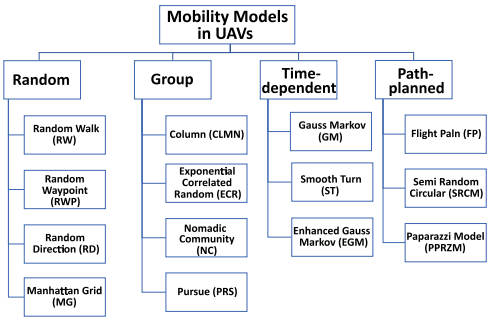

FIGURE 3. Classification of FANET mobility models.

TABLE 3. Classification of FANET propagation models.

Propagation Model	Brief Description
Free Space	The transmitter and receiver are assumed to be in free space
Two-Ray Ground	Two signal paths are assumed between transmitter and receiver: Line-of-Sight and Reflection from Ground
Shadowing	The fluctuations in the received signal power due to multi-path propagation or obstacles are considered

faces several challenges with regard to radio propagation. This is due to the frequent differences in communication distance between various nodes, the antenna pattern, shadowing from other UAVs, fluctuations in the link quality due to UAV attitude (yaw, pitch, and roll), and other environmental elements. The deployment of FANETs requires adequate knowledge of the radio channel characteristics. The communications between the UAVs (U2U) in the FANET are Line-of-Sight. Differently, they are nLos (non-Line-of-Sight) between UAV and GCSs. There are three major propagation models studied by Jun Peng [25] for UAV networks. Specifically, the free-space model, the two-ray model, and the shadowing model. A brief description of the propagation models is summarized in Table 3.

Another categorization by Antonio et al. [27] modeled the channel losses through which the electromagnetic waves (EM) are attenuated. The propagation models are divided into three classes. Specifically, theoretical, empirical, and semi-empirical models. The antenna structure also has an intense impact on the communication architecture of FANET. Directional and Omnidirectional antennas are used in FANET communications [15].

D. COMMUNICATION PROTOCOLS IN FANETs

The UAVs in a FANET communicate with each other through Ad-Hoc links established among each other without requiring any infrastructure. Setting up and maintaining such a network is challenging due to node mobility, high speed, operating environment, unstable communication links, and resource limitations. FANET requires efficient and secure wireless communication to be established with the ground stations as well as with other drones in the network.

Short-range unlicensed wireless technologies like Wi-Fi (IEEE 802.11), Bluetooth (IEEE 805.15.1), and Zigbee (IEEE 802.15.4) are most commonly used for drone communication [28]. LoRaWAN besides licensed and infrastructure-based technologies that rely on 5G, Beyond 5G, and 6G are also used in FANET for long-range communications (i.e., to enhance coverage and throughput demands). Table 4 showcases a summary of these technologies.

IEEE 802.11n and IEEE 802.15.4 protocols are mostly used for data exchanges in FANETs [29]. IEEE 802.11n ensures high data delivery no matter the number of UAVs in the network; however, it is costlier, consumes more power, and is more complex compared to IEEE 802.15.4. Also, due to the frequent fluctuations in the link quality, mesh topology (UAVs route messages to the GCS) is preferred over star topology (all drones directly communicate with the GCS) in a FANET scenario. Peer-to-peer communication is established for collaborative mission completion and collision avoidance. Various routing protocols [30] have been proposed to establish robust and reliable communications among the drones in FANET.

E. APPLICATIONS OF FANETs

Multiple UAVs cooperate to accomplish various applications in a collaborative manner. These include applications in remote sensing, the construction industry, drone delivery services, search and rescue operations, and monitoring and surveillance, as shown in Fig. 4. We present more details about these applications in the next paragraphs.

1) SEARCH AND RESCUE OPERATIONS

UAVs are widely considered nowadays for critical situations such as disaster management, rescue operations, and public safety. UAVs offer real-time visual (image/ video) data of intended locations. Consequently, a search and rescue team can timely detect and decide where accurately the assistance is urgently required. For instance, drones can be used to track people who were lost during any mission or to protect people lost in remote deserts or forests [31].

2) CONSTRUCTION INDUSTRY

UAVs can be deployed to monitor the progress and safety of construction and various equipment by providing a real-time visual view of the sites. Monitoring construction projects from beginning to end ensures the quality of work. The cracks in the buildings, pipelines, and other surfaces can also be accurately monitored using UAVs [32].

3) PRECISION AGRICULTURE

Drones are deployed in precision agriculture for sensing water quality, soil properties, pesticide spraying, disease and

TABLE 4. Communication technologies used in FANET.

Technology	Standard	Range	Features
Wi-Fi Ad-Hoc	IEEE 802.11 (a/b/g/ac/s/n/p)	∼100 m	Range can be extended using multi-hop networking; but this drains battery easily
Bluetooth	IEEE 802.15.1	10 - 200 m (Bluetooth 5)	Low cost, low power
Zigbee	IEEE 802.15.4	10 - 100 m	Low data rate, low cost & convenient, less energy consuming
LoRaWAN	IEEE 802.15g	5 - 15 km	Less energy consuming, wide connectivity
Sigfox	-	3 - 30 km	Low speed, low power, long range
NBIoT (Narrow Band IoT)	LTE Cat NB1 LTE Cat NB2	10 -35 km	Longer range; Telecommunication infrastructure required
5G	mmTC uRLLC emBB	Wide area	Longer range; Telecommunication infrastructure required
B5G	mmTC uRLLC emBB uRLLC + emBB	Wide area	Longer range; Telecommunication infrastructure required
6G	MBRLLC mURLLC HCS MPS	Wide area	Longer range; Telecommunication infrastructure required

weed detection, and irrigation scheduling. The incorporation of UAVs in precision agriculture saved a lot of time and cost, enhancing productivity and crop yields [33].

4) TRAFFIC MONITORING

Reliable and smart UAVs can aid in the automation of rescue teams, surveyors, and traffic police. UAVs can gather data about traffic conditions on highways as they can be deployed to get a vision of road accidents or vehicle thefts, to detect vehicle over-speeding, as well as to assist in avoiding traffic jams and mass congestion [34].

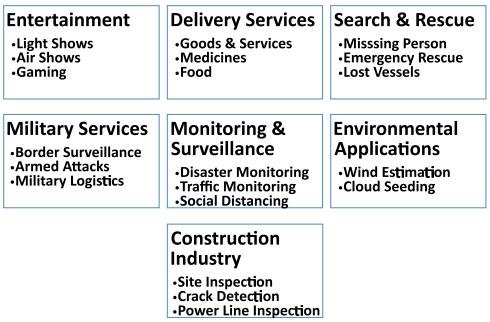

FIGURE 4. Applications of FANETs.

5) MILITARY SERVICES

UAVs play an integral role in military services. Most countries have added UAVs to their defense strategic plans to be used for enemy detection, border control, and maritime monitoring of critical sea lanes [35].

6) DISASTER MANAGEMENT

Drones play significant roles in the management of man-made or natural disasters such as terrorist attacks and floods. These disasters can severely destruct the telecommunication infrastructure, transportation, power, water, and other supplies. UAVs can be deployed to locate disasters and provide alerts. For instance, a swarm of drones can be deployed to extinguish fires in case of wild or domestic fires, so that human safety is not compromised [36].

7) DELIVERY DRONES

UAVs are also prominent nowadays for delivering various services including medicines, food, documents, and other services. Drones can be deployed to transport medicinal products (e.g., organs for transplantation, vaccines, pharmaceuticals, and medical samples) and prepared foods (e.g., pizzas and frozen beverages) [37].

8) ENTERTAINMENT PURPOSE

Apart from the above applications, drones are nowadays prominently used for various entertainment purposes such as light shows, airshows, photography, cinema, etc. [38].

F. PERFORMANCE METRICS

In this section, various performance metrics that were used to evaluate the performance of the proposed systems have been elaborated. Various symbols used in the equations to compute these metrics are listed in Table 5.

1) **False Positive** is the number of non-attack cases detected as attacks by the system/algorithm. The False Positive Rate (FPR), the ratio of false positives to total

TABLE 5. Symbols and meanings.

Symbol	Meaning	Symbol	Meaning
t_p	True Positive	P_i	i^{th} Predicted value
f_p	False Positive	A_i	i^{th} Actual value
t_n	True Negative	N	Total no. of observations
f_n	False Negative	avg	Average
TPR	True Positive Rate	FPR	False Positive Rate
TNR	True Negative Rate	FNR	False Negative Rate
RMSE	Root Mean Square Error	s	Seconds

non-attack cases, should be minimized to avoid the problem of Denial-of-Service (DoS) to legitimate users.

2) **True Positive** is the number of attack cases correctly detected by the system/algorithm. The True Positive Rate (TPR), which is the ratio of true positives to the total attack cases, should be maximized to discriminate and block the attackers.
3) **False Negative** is the number of attack cases not detected by the system/algorithm. In other words, it is the number of attack cases reported as legitimate cases. The False Negative Rate (FNR), the ratio of false negatives to total attack cases, should be minimized to discriminate against and block the attackers. True Positive Rate and False Negative Rate can be related using the following equation:

$$FNR = 1 - TPR \tag{1}$$

In relation to the above three metrics, systems can be also evaluated using Recall, Precision, and F1-score metrics as follows:

$$Recall = \frac{t_p}{t_p + f_n} \tag{2}$$

$$Precision = \frac{t_p}{t_p + f_p} \tag{3}$$

$$F1 - score = avg(Recall, Precision) \tag{4}$$

4) **Detection Latency** refers to the time delay between the instigation of attack and detection of attack by the system/algorithm. Detection latency is a crucial metric since it represents the time the attacker has to hijack the UAVs or cause mission failure before he/she gets detected.
5) **Position Drift** refers to the UAV displacement caused by spoofed signals from the original trajectory.
6) **Root Mean Square Error (RMSE)** indicates the differences between the values (e.g., position or velocity of UAV) predicted by a model and the actual or observed value.

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{N}(P_i - A_i)^2} \tag{5}$$

7) **Accuracy** refers to the ratio of correct predictions, both the true and attack signals, to the number of cases under consideration.

$$Accuracy = \frac{t_p + t_n}{t_p + f_p + t_n + f_n} \tag{6}$$

8) **UAV Capture Probability** is the probability that a drone gets captured or hijacked by an attacker in presence of the proposed algorithm.
9) **Power Consumption** refers to the energy consumed (battery) for the execution of the proposed algorithm. This metric should be minimized since drones are battery-limited entities.
10) **Memory Consumption** indicates the storage requirements of the proposed algorithms. The value of this metric should be low or negligible since the drones cannot carry large storage devices due to their light weightiness.

G. SECURITY ISSUES IN FANETs

FANETs are prone to various cyber-attacks, which are broadly classified into three categories by Mohsen et al. [39], namely, Data Interception attacks, Data Manipulation attacks, and Denial-of-Service attacks. Data interception attacks such as Eavesdropping and Key Logging mainly target the privacy of information transmitted between the UAV and the GCS. Data Manipulation attacks such as GPS Spoofing attacks, deauthentication, message injection, modification, and deletion mainly aim to hijack or take UAV control. Jamming are examples of Denial-of-Service attacks.

GPS Spoofing attack is one of the most dreadful attacks since it can capture, mislead and/or make the UAV collide with other UAVs or objects causing security and safety concerns. The ease of availability of low-cost Software Defined Radios (SDR) and the open nature of GPS signals have attracted the malicious attackers to exploit the UAV's vulnerabilities. In the following paragraphs, the GPS Spoofing attacks in UAVs and their impacts are briefly discussed.

GPS is a Global Navigation Satellite System (GNSS) that uses positional information broadcasted by satellite constellations. Different broadcast frequencies and modulation techniques are used by these satellites. The frequency of 1575.42 MHz is used for civilian GPS Signals and is popularly known as the L1 band. The Course Acquisition Code (C/A) is a Pseudo Random Number (PRN), which identifies the satellite of origin. Generally, a minimum of four satellite signals are needed to be identified by the receiver using PRNs

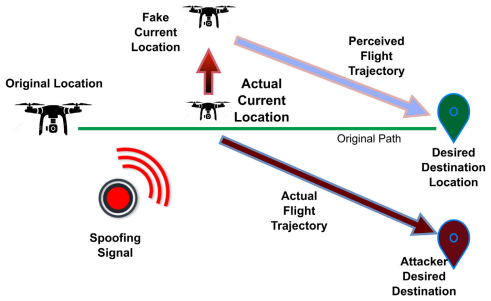

FIGURE 5. Illustration of GPS spoofing attack in UAV.

to calculate its position and time information by correlation. The GPS positioning systems apply the principle of three-sphere positioning. That is, the signal propagation delay to the GPS receiver is obtained from three satellites and it is multiplied with the speed of light. The pseudo-distance obtained from the three satellites gives three spherically connected equations. The readings from the fourth satellite are used for adjusting the clock differences.

GPS Spoofing attacks are launched in two ways: 1) The attacker locks the GPS receiver of the target by computing the pseudo-distance first. The received signal is jammed, delayed, and then forwarded. 2) The attacker generates counterfeit signals by analyzing the satellite signal characteristics to broadcast in the target located area. Both methods can mislead the target with erroneous locational information. As a consequence of GPS Spoofing, the entire network operation, and the existence of the network itself is severely affected. Fig. 5 illustrates a GPS Spoofing attack scenario in which the UAV at the 'Original Location' travels to the 'Desired Destination Location' through the 'Original Path' that is shown in green. The spoofer desires to redirect the UAV to the position labeled as 'Attacker Desired Destination'. The spoofer sends fake locational information to the UAV such that the UAV perceives that it is navigating in the wrong trajectory. However, it is located at the 'Actual Current Location', the spoofer deceives the UAV that it is located at the position labeled as 'Fake Current Location'. The UAV then follows the 'Perceived Flight Trajectory' shown as the blue arrow in Fig. 5. This movement makes the UAV travel in the 'Actual Flight Trajectory' shown in the dark red arrow, leading it to the 'Attacker Desired Destination'.

Location awareness of constituent nodes is required for better performance of FANETs or UAV swarms. The current UAV positions are exchanged within the network with other UAVs, GCS, and/or other centralized services for topology maintenance. Forging the GPS signals, which is the main source of localization in FANETs, and disseminating this information in the network has harsh impacts on FANETs missions as follows:

1) The absolute or relative locational information of UAVs is required for the successful completion of FANET's mission. So, falsifying this information can lead to mission failure.
2) Wrong locational information can cause two UAVs to collide.
3) False location information can cause the UAV to enter geofenced areas such as military bases, airports, etc.
4) Line-of-Sight (LoS) propagation is used by malicious UAVs to disseminate fake locational information. Hence, there is no chance of multi-path fading, which can be monitored otherwise using *SNR* (Signal-to-Noise Ratio) or *C/N0* (Carrier-to-Noise Power Density, *N0* represents the noise spectral density). *SNR* and *C/N0* are vital parameters to analyze the performance of GPS receivers.

In one aspect, GPS Spoofing in drones is relatively simple as multiple low-cost and simple drones are used. In another aspect, the spoofer has to counteract the swarm formation, i.e., the position of the FANET as a whole as well as the relative positions of UAVs within the swarm also has to be taken into account when spoofing attack is launched. A fake GPS signal relative to an individual drone will make obvious changes in the swarm formation and hence be detected easily.

Thus, it can be concluded that deeper investigations on the threat of GPS Spoofing attacks in FANETs need to be conducted. This paper conducts a systematic literature survey on this topic, so future researchers can conceive this survey as a comprehensive guide to propose various solutions to secure the FANET environment from the threat of GPS Spoofing attacks. In the following section, the methodology adopted for this survey has been detailed. Specifically, Research Questions, Search Strategy, Keywords, Databases, Selection Criteria, Quality Assessment Tools, Data Extraction, and Data Synthesis.

III. METHODOLOGY

The research methodology in this survey follows the guidelines of Kitchenham and Charters [21], which has three phases, namely, planning, conducting, and reporting. In the planning phase, a complete plan of how and why to conduct this survey is provided. The research questions are also identified; and the search strategy, keywords, and resources are determined. In the conducting phase, the search strategies are applied to select the research articles to be considered. Based on the Inclusion/Exclusion criteria (shown in Section III-E), irrelevant articles are filtered out. The selected articles are further refined by a quality assessment tool formulated for this survey. In the reporting phase, the synthesized data are compiled in the form of facts and figures. In the following sections, the aforementioned phases are detailed.

A. RESEARCH QUESTIONS (RQs)

The survey conducted in this paper aims to address the following Research Questions:

- **RQ1:** What is GPS Spoofing Attack and its impact in FANETs?
- **RQ2:** What are the GPS Spoofing Attacker Models in UAVs in terms of Spoofing Strategy, Spoofing

TABLE 6. Research questions and motivations.

RQs	Motivation
RQ1	Falsifying the location information in FANETs can lead to UAV capture, collision, or mission failure
RQ2	*Spoofing Strategy* - Mislead / Misreport *Spoofing Technique* - Position denial / track break *Spoofer Location* - On-board, Stand-off, Stand-in, Distributed *Spoofer System* - Simulator, Repeater, Hardware Injection
RQ3 & RQ8	Mechanisms are discussed, classified, and compared with other mechanisms in order to help researchers to understand the state-of-art and future scopes in securing FANET from GPS Spoofing attacks.
RQ4	Various simulations and/or proof-of-concept implementation that might be used in the experiments
RQ5	Various Performance metrics that might be used in the experiments
RQ6	Various mobility models that might be used in the experiments, namely, *Random Way Point, Pheromone Based Models, Gauss Markov Model, Mission Plan, Paparazzi Mobility Model, Semi Random Circular Models*
RQ7	Various propagation models that might be used in the experiments, namely, *Free Space, Two-ray Propagation Models, Shadowing Models*

Technique, Spoofer Location & Number, and Spoofer System?

- **RQ3:** What are the attack detection and prevention mechanisms presented in the existing literature?
- **RQ4:** What are the Performance Evaluation Mechanism(s) in terms of Simulation or Proof-of-Concept Implementation?
- **RQ5:** What are the Performance Metrics used in existing Literature?
- **RQ6:** What are the Mobility Models used in the detection and prevention mechanisms?
- **RQ7:** What are the Communication / Propagation Models used in the detection and prevention mechanisms?
- **RQ8:** What are the Future Directions and Open Issues that are unaddressed in GPS Spoofing Attack studies?

Table 6 lists the motivations that led to raising the above research questions.

B. SEARCH STRATEGY

The articles published on GPS Spoofing attacks in Unmanned Ariel Vehicles (UAVs) during the 2017-2022 period were searched in **IEEE XPlore®, ACM Digital Library, ScienceDirect®**, **Springer**, and **Google Scholar** databases to conduct this survey. The aim of the search is to locate papers that discussed GPS Spoofing attacks in FANETs and/or defense mechanisms. In the next section, we present the formulated search words, which are also associated with logical "AND" and "OR" operators.

C. SEARCH TERMS OR KEYWORDS

With the aim of identifying all scientific articles related to GPS Spoofing attacks in FANETs, the major search terms identified for this purpose are "Unmanned Ariel Vehicle" and its acronym "UAV", "Flying Ad-Hoc Network" and its acronym "FANET", "Drones" and "Global Positioning System Spoofing" and its acronym "GPS Spoofing". GPS being a subcategory of Global Navigation Satellite Systems, the term "Global Navigation Satellite System Spoofing" and its acronym "GNSS Spoofing" is also used. Below is the search query used in this survey: ("Unmanned Ariel Vehicles" OR "UAV" OR "Drones" OR "Flying Ad-Hoc Network" OR "FANET") AND ("Global Navigation Satellites Spoofing" OR "GNSS Spoofing" OR "Global Positioning System Spoofing" OR "GPS Spoofing").

The compiled query is pasted in the search text field of the resources discussed in the next section (III-D) and are searched in the "Title" and "Abstract" of the results.

D. RESOURCES

As mentioned before, this study explored publications listed in global databases. Specifically, **IEEE XPlore®, ACM Digital Library, ScienceDirect®**, **Springer**, and **Google Scholar** databases. Selected articles' bibliography sections are also analyzed for literature completion.

In the IEEE XPlore® and ACM Digital Library databases, the search was conducted for the above query, and a filter was applied to get results from the years 2017-2022. In IEEE XPlore®, an advanced search is conducted using the 'Command Search' option available under the 'Advanced Search' menu. The ScienceDirect® database, owned by Elsevier Publishers, is also queried in the same manner. In SpringerLink, in addition to the above filter, the results are further filtered to omit the result-bearing books' titles using the filtering tool in MS Excel (i.e., the results were exported to Excel Spreadsheets). Google Scholar database is also searched with the same search query and the year of search is selected as 2017-2022 from the options in the sidebar.

Recent survey papers on GPS Spoofing attacks were collected for reviewing the state-of-art in Section IV. The technical papers on GPS Spoofing attacks in existing literature are

TABLE 7. Database and search results (2017-2022) before & after inclusion/exclusion criteria.

Source	No. of Results	
	Before	After
IEEE XPlore®	46	33
ACM Digital Library	38	8
ScienceDirect®	78	7
SpringerLink	173	10
Google Scholar	87	16
From References	6	5
Total	**428**	**79**

presented in Section V. The following section presents the selection criteria applied in this survey.

E. SELECTION CRITERIA

Appropriate criteria have been applied for the inclusion/exclusion of identified publications into/from the final corpus. The published articles that meet all the inclusion criteria are included in this study. Oppositely, if the article has any exclusion criterion, it is omitted. The Exclusion Criteria (**EC**) and Inclusion Criteria (**IC**) employed in this survey are:

- **EC1:** The main focus of this study is GPS Spoofing attacks in UAVs and their impact on FANETs. So, this study doesn't consider publications that deal with any other security threats in UAVs or FANETs.
- **EC2:** The attacks on MANETs/ VANETs or any kind of networks other than FANETs are out of the scope of this work.
- **EC3:** All articles published in languages other than English are not considered.
- **IC1:** The publications that study GPS Spoofing attacks, which include Surveys and/or Detection and/or Prevention of GPS Spoofing attacks in FANETs.
- **IC2:** The year of publication should be 2017-2022.
- **IC3:** The publication should be well-structured and well presented in English writing.

The results obtained by applying these criteria have reduced the number of publications/articles to be considered in this survey to 79, which was 428 before. The summary of these results is tabulated in Table 7.

The articles/publications are then categorized into two groups: 1) State-of-the-art Papers and 2) Technical Papers. It is observed that out of 79, 14 papers were Survey or Review papers and are included in the category 'State-of-the-art Papers'. The 'Technical Papers' comprised 56 papers, which include various papers that present studies on or propose solutions for GPS Spoofing attacks in UAVs. Google Scholar has an overlap of nine papers from other databases. So, a total of 70 papers are considered in this study for further refinement. A year-wise analysis of this observation is illustrated in Fig. 6. The results are further refined based on Quality Assessment Tools, which are presented in the next section.

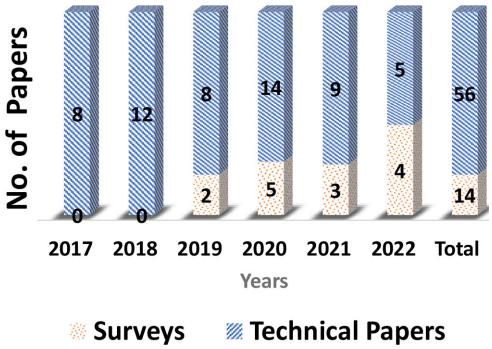

FIGURE 6. Year-wise analysis of research publications on GPS Spoofing attacks in UAVs.

F. QUALITY ASSESSMENT TOOLS

All papers resulted from the searches are subjected to a quality check using the tools that will be described in this section. This helps to select only the most relevant papers for consideration in this survey. "Quality instruments" [21] are used for this purpose, which are typically quality assessment questions. The numerical assessment of quality can be obtained if these instruments are mapped to numerical values.

The 'State-of-the-art' papers are evaluated using the following Quality Checklists (QCs):

- **QC1:** Does the study contain sufficient information about FANETs and GPS Spoofing attacks in FANETs?
- **QC2:** Does the survey adhere to any Survey Methodology or Searching Strategy?
- **QC3:** Does the survey clearly state its motivation?
- **QC4:** Does the survey review a sufficient number of papers?
- **QC5:** Does the survey identify the research gaps?

The 'Technical Papers' are evaluated using the following assessment questions:

- **QC6:** Does the study present the existing literature on GPS Spoofing attacks in FANETs before proposing the solution to defend the attack, if any solution is proposed by the authors?
- **QC7:** Does the study have clear problem(s) statement?
- **QC8:** Does the study portray implementation results?
- **QC9:** Does the study present a discussion on the results?
- **QC10:** Does the study clearly indicate the implementation tools used, i.e., simulation and/or proof-of-concept and/or datasets?
- **QC11:** Does the study make a comparison of the proposed system with existing ones and indicated how it outperformed them to fill the research gaps?
- **QC12:** Does the study addressed the research questions presented in Section III-A?

- **QC13:** Are the performance metrics used in the study valid and reliable?

Further, qualitative checklists were framed and applied to evaluate both the state-of-the-art papers and the technical papers, as follows:

- **QC14:** How clear are the links and flow between various sections in the paper?
- **QC15:** Are there any new insights delivered by the study?
- **QC16:** How well is the comprehensibility of the language and style used in the paper?

Each paper is assigned weights as '0', '0.5', or '1', based on the answers to the above **QCs**, that do not meet, partially meet, or clearly/fully meet the quality checklist, respectively. These weights are summed up to score the paper. A paper is included if its final score is ≥ 5 out of 8 (for state-of-the-art papers) and ≥ 8 out of 11 (for technical papers).

G. DATA EXTRACTION

The results refined after applying the criteria in Section III-E and III-F were processed to extract the information from the selected studies to answer the Research Questions (RQs) formulated in Section III-A. The following points were considered when processing state-of-the-art papers:

1) Authors' details, journal/publication details, year of publication, and the years or duration of studies considered in the survey.
2) Concepts or topics discussed in the study.
3) Open issues or future directions provided by the study.

The technical papers are processed with the following points in mind:

1) Authors' details, journal/publication details, year of publication.
2) The defense strategy applied for the proposed solution.
3) The proposed solution.
4) The implementation details.
5) The scenario where the proposed solution is deployed (whether it is FANET or Single UAV). If a single UAV, whether the solution is also applicable to FANETs.
6) The attacker model.
7) Whether the proposed solution is for detection, mitigation, and/or prevention.
8) The performance parameters (methods and metrics) considered in the evaluation.

H. DATA SYNTHESIS

The information extracted from the results is summarized, tabulated, and/or plotted graphically based on the nature of the information. Sections IV and V put light on the 'State-of-the-Art' and 'Technical' papers, respectively, that satisfied the criteria mentioned in Section III-E and passed the Quality Checks (QCs) in Section III-F.

IV. STATE-OF-THE-ART

In this section, a review of the state-of-the-art papers identified during this study is presented. A total of 12 out of 14 (that passed the Quality Checks) Survey/Review papers on GPS Spoofing attacks in FANETs were selected as a part of this study. However, it is found that most of the papers reviewed the security issues in Unmanned Ariel Vehicles (UAVs). The papers that have some special mention of the GPS Spoofing attacks in FANETs along with other attacks are discussed.

For instance, Mohsen et al. [39] reviewed ∼84 articles and presented a study on the cyber attacks on UAVs. The attacks on UAVs were analyzed and categorized. The authors also reviewed the recent defense mechanisms against various attacks on UAVs. Among these, ∼13 articles (from 2012 to 2019) were technical papers on GPS Spoofing attacks, which discussed GPS Spoofing attacks under the category of Data Manipulation attacks. They classified GPS Spoofing defense strategies into four categories, namely, Cryptography-based, Spatial Processing-based, Machine Learning-based, and Hybrid methods. However, only few of these studies addressed the security requirements of GPS Spoofing attacks in FANETs. Most of them are generalized defense mechanisms for GPS Spoofing attacks. The authors projected the need to develop efficient techniques in the future so that UAVs can navigate efficiently in GPS-denied environments.

Hamza et al. [40] reviewed ∼56 articles and discussed the UAV components, vulnerabilities, and defense methodologies. The authors created a taxonomy of attacks against UAVs based on the UAV components and the GPS Spoofing attacks were categorized under 'Attack against Communication Link'. Various defense techniques were also discussed by the authors in ∼8 articles (from 2014 to 2016). These include signal processing, encrypting GPS signals, and machine learning techniques. It also is observed that the GPS Spoofing strategies and defense mechanisms discussed in this paper are not specific to FANETs. The authors recommended the need for GPS-independent navigation solutions for UAVs so that the missions can be completed successfully during Jamming and spoofing attacks. As GPS signals are more prone to spoofing and Jamming attacks, the need for proposing effective navigation techniques that are less dependent on GPS is recommended as a future direction in this paper.

Yueyan et al. [41] studied ∼29 papers and analyzed the safety aspects of UAVs from three angles, namely, sensors, communications, and multi-UAVs. GPS Spoofing attacks were studied under the category 'attack on sensors'. Two types of spoofing threats (Repeater type and Generating type) in UAVs are also presented in this paper. The authors have cited only one technical paper (published in 2017) specific to GPS Spoofing attacks in which attack signals were broadcasted using USRP (Universal Software Radio Peripheral).

Fazal et al. [28] portrayed a review of communication perspectives of FANETs. They reviewed ∼73 papers with the goal of providing insights into communication technologies in FANETs, applications scenarios, challenges, and open issues in the area. Among these, ∼4 technical papers (from 2017 to 2019) discussed GPS Spoofing. This includes the GPS Spoofing vulnerability of 3-D Robotics

commercial drones and few solutions to GPS Spoofing attacks in FANETs. However, no detailed discussion of these solutions was provided.

Aicha et al. [42] presented a comprehensive survey (∼213 references) on UAV communication protocols, networking systems, architecture, and applications. The survey also discussed the technical challenges and open research issues. Among these, few technical papers (∼3 papers from 2020 to 2022) give a brief review of recent GPS Spoofing attack detection techniques in UAVs based on Visual Odometry, the fusion of GPS and optical flow raw data, and machine learning. No future direction related to GPS Spoofing attacks was discussed in this paper.

A review on GPS Spoofing vulnerability of UAVs was provided by Eshta et al. [43] after reviewing ∼41 articles. Among these, ∼29 technical papers were on GPS Spoofing attacks and only two papers (published in 2014) are specific to UAVs. The paper also discussed the spoofing problems, types, and various countermeasures in the existing literature. A detailed discussion on the different types of spoofing attacks, namely, Covert and Overt as well as based on the threat assessment, namely, Simplistic, Intermediate, and Sophisticated were also provided. Moreover, the authors discussed different countermeasures and categorized them into several groups - encryption-based, Receiver Autonomous Integrity Monitoring (RAIM), Navigation Message Authentication, differing spoofed signal and true GNSS signals in space, antenna motion or geometry, and signal power. The authors also stated that the studied solutions face a common pitfall in that they require specialized hardware, which increases the weight and cost of UAVs. This is because the solutions were not UAV specific and hence cannot address the GPS Spoofing issues in FANETs. As a future direction, the authors recommended conducting more research on improving the tools for counteracting GPS Spoofing attacks. They emphasized the adoption of cryptographic techniques to safeguard against GPS Spoofing attacks in UAVs. Also, the need for drone manufacturers to develop a minimal level of countermeasures against GPS Spoofing while manufacturing commercial drones is envisioned.

Hassija et al. [44] reviewed ∼ 165 articles and presented a comprehensive review on drone communication. The authors shed light on security-critical drone applications and security challenges. Furthermore, the authors discussed solution architectures for various attacks based on Blockchain, Software Defined Networks (SDNs), Machine Learning, and Fog/Edge Computing. Among various security issues discussed in this paper, GPS Spoofing attacks in drones also got a relevant space as discussed in ∼4 technical papers (from 2018 to 2019). An example of a GPS Spoofing attack on an American drone on December 5, 2011, was also showcased. The usage of BladeRFx40 SDR for generating falsified GPS Signals was also reviewed. Solutions to prevent GPS Spoofing attacks in drone environments based on Fog computing were discussed. The authors stated that Blockchain technology, SDNs, Fog computing, and machine learning techniques are new directions to consider while designing solutions for GPS Spoofing attacks in UAVs.

Vinay et al. [45] surveyed ∼144 articles to showcase a comprehensive review of UAV attacks and neutralization techniques. Among these, ∼7 papers are specific to GPS Spoofing attacks in UAV, which include spoofing tools, and solutions to GPS Spoofing attacks based on techniques like deep learning. These papers also discussed the misuse of UAVs for illegal surveillance and unmanned attacks. Discussion on GPS Spoofing being used as an anti-UAV tool to neutralize UAV attacks is also provided as well as the need for future research to address various security concerns in UAVs.

Faisal et al. [46] studied ∼20 recent articles to survey the Jamming and Spoofing attacks on UAVs. Among these, ∼4 papers (from 2019 to 2021) are specific to GPS Spoofing attacks in UAVs. The spoofing attacks that target the GPS, as well as Automatic Dependable Surveillance-Broadcast (ADS-B), are briefly illustrated. The authors observed the three ways of executing GPS Spoofing attacks, namely, falsified GPS signal or higher frequency signals, or spoofing the high gain antenna. The authors also observed that traditional defense mechanisms like GPS signal authentication are not suitable for resource constraint UAVs and recommended machine learning as an effective mechanism to defend against GPS Spoofing attacks.

Rugo et al. [47] collected ∼125 papers and presented a systematic literature review on drone security. Among these, ∼4 technical papers discussed GPS Spoofing attacks in UAVs. Along with other security issues studied, the authors dug into the history of GPS Spoofing attacks in UAVs. The countermeasures in the existing literature to mitigate GPS Spoofing were also discussed. The authors showcased sophisticated techniques like comparing the other sensors (such as onboard IMUs, signal amplitudes) measurements, vision-based techniques, and machine-learning-based methods. Their observation was that the attackers are becoming smarter as the defense mechanism are becoming stronger. Furthermore, the authors recommended the use of GPS authentication and encryption as the most effective tool to counteract the threat of GPS Spoofing in FANETs. The possibility of replay attacks using the previously sent signals exists though.

Syed et al. [48] surveyed ∼126 articles and showcased a comprehensive review of UAVs, types, classifications, security challenges, applications, and standardization. Apart from a pictorial illustration of a GPS Spoofing attack in UAV, there are no further discussions on GPS Spoofing attacks in this paper. The author concentrated more on other technical details like the types of UAVs, applications, etc.

Kai-Yun et al. [49] collected ∼200 papers and identified the cyber security threats and solutions when UAVs collaborate to form FANETs. A detailed study on UAV communication architecture, routing protocols, and UAV characteristics including the mobility models are also showcased.

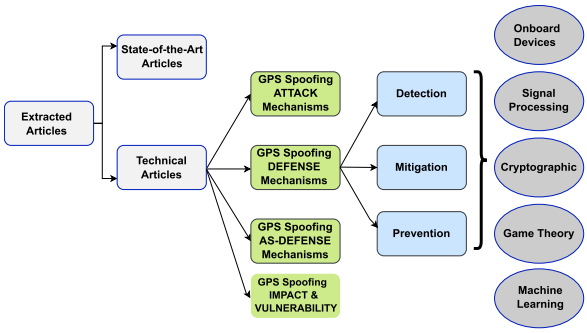

FIGURE 7. A taxonomy of GPS spoofing in FANETs.

Each paper studied in this survey is analyzed with an eye on security and non-security features addressed. A generic view of GPS Spoofing attacks and detection methods is given in this paper. The history of GPS spoofing attack is briefly explained through a pictorial illustration. As future directions, the authors recommended the use of techniques like lightweight encryption, reinforcement learning, and SDN to improve the security aspects of resource constraint UAV devices.

Table 11 in the Appendix shows a summary of the comparative analysis of the State-of-Art papers discussed in this study and presented how the survey conducted in this paper is different compared to them.

Conclusion. In this study, 12 out of 14 papers were selected after the quality assessment. The papers were considered relevant if they had some discussions on GPS Spoofing attacks in UAVs/FANETs. The discussion can be on the attacks and/or their impacts, the tools or algorithms for creating GPS Spoofing attacks, or the countermeasures. It is observed that most of the selected surveys studied the security issues in UAVs or FANETs in general and GPS Spoofing has been mentioned as one among many attacks. Some papers have elaborated on and viewed GPS Spoofing attacks in a broader sense. However, to the best of our knowledge, few studies have been conducted exclusively on GPS Spoofing attacks in FANETs. Though few studies exist on GPS Spoofing attacks on a single UAV scenario, none of the aforementioned followed any particular search/surveying methodology. Only one article followed systematic review guidelines, but that was also a generalized view of drone security. Accordingly, the survey presented in this paper on GPS Spoofing attacks in FANETs is the first of its kind to conduct a systematic literature review following the guidelines of Kitchenham [21]. An overview of this survey is shown in Figure 7.

V. GPS SPOOFING IN FANETs: A TAXONOMY

During this survey, it is observed that GPS Spoofing attack in FANETs is an issue of serious concern, and few research works that are specific to this topic have been undertaken. A total of 56 articles published between 2017 to 2022 has been considered, which can be classified into four categories, as shown in Figure 7. Articles that focus on GPS Spoofing attack mechanisms, articles that propose GPS Spoofing defense mechanisms, articles that have used GPS Spoofing as a defense mechanism (i.e., against other attacks), and articles that investigate the impact and vulnerability of GPS Spoofing attack. The following sections present a review of the articles in each category.

A. GPS SPOOFING ATTACK MECHANISMS IN UAVs

In this section, the articles that studied the GPS Spoofing attacker models are discussed in detail. The purpose of these articles is to provide guidelines to the research community and cyber experts to understand the attacker's capabilities and how they conduct the attack. Thus, to aid the development of novel solutions to defend against the threat of GPS Spoofing attack. As presented in Section II-G, the satellites transmit radio signals to UAV receivers to be processed in order to obtain the positional information. As these radio signals don't use any encryption or authentication mechanism, the positional information can be altered by a spoofer device. The attacker might project a mimicked route or trajectory to the GPS receiver in three possible ways:

- Generating fake GPS signals.
- Sending signals with higher frequency leading to a denial of GPS signals.
- Spoofing high gain antenna.

Bethi et al. [50] presented GPS Spoofing architecture layers, as shown in Fig. 8. The spoofing strategy and techniques are included in the application layer, whereas spoofer location, spoofer system, and user-spoofer understanding are placed under the device layer. The spoofing strategies adopted by the attackers are either to ''mislead'' the target or to ''misreport'' the positional information. While ''mislead'' guides the target UAV to a false destination, ''misreport'' reports false location information. The techniques used for implementing these two strategies are ''position denial'' and ''track break''. In ''position denial'' techniques (also called detection denial techniques), the receiver is denied from detecting legitimate GPS signals. In ''track break'', the targets are misled by sending false navigation signals. The spoofers can operate from different locations: ''stand-off'' (remote), ''escort'' (near but at a distance, also called stand-in), and ''onboard'' (resides along with the target). Distributed attackers deploy multiple spoofers at different locations. The spoofer systems include ''simulators'' (software codes to simulate GPS signals and radiate Radio Frequency (RF) signals with higher power), ''repeaters'' (the receiver module within the attacker captures the GPS signals, manipulates them, and re-transmits), and ''hardware injection'' systems, where the spoofed signals are combined with the receiver's hardware for intentional misreporting. The user-spoofer understanding is the relation between the receiver and the spoofer. It includes ''non-cooperative'' (the receiver is unaware of the spoofer's presence and always tries to avoid the attack) and ''cooperative'' (the user aims to get spoofed for misreporting its position to the base station).

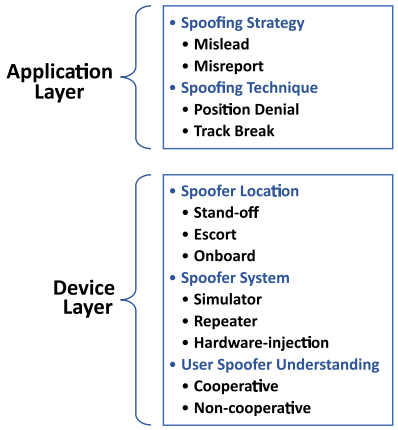

FIGURE 8. GPS spoofing attack layers.

In FANETs, the attacker manipulates UAV's GPS signals with two main objectives. Either to change the routing information leading to a collision of UAVs (or incomplete missions) or to capture the UAV. The attacker sends fake GPS signals with higher power to UAVs with two basic modes:

1) Covert Attack: the attacker avoids triggering any spoofing detection methods. This kind of attack is usually hard to detect.
2) Overt Attack: the attacker launches a severe attack without any caution being detected.

He et al. [51] studied the communication security of UAVs. Security vulnerabilities in UAV modules enable attackers to launch GPS Spoofing attacks. A low-cost implementation of GPS attacks is discussed in this paper. Since civilian GPS signals are not encrypted, they are more vulnerable to attacks. The spoofer system includes a repeater-based system. It is a low-cost GPS record-modify-and-replay system, which is hardware-based - Ettus USRP [52] radio family and software based on GNU Radio [53]. The spoofer location is remote and a track break spoofing technique is used in which the signal received from the satellite is recorded and sampled by USRP. The signal is then modified and reproduced to create spoofed GPS signals. The UAV's GCS receives different locational information under normal scenarios and spoofed scenarios when the UAV was located at the same place.

Eric et al. [16] developed a GPS Spoofing tool that can attack a DJI Matrice 100 Quadcopter. BladeRFx40 SDR is used to transmit the spoofed signals to the GPS receiver. The authors showcased the overall basics to details of the hardware and software of the DJI Matrice 100 Quadcopter. An open-source C-based software, GPS-SDR-SIM [54], is fed to the BladeRFx40 SDR to generate the spoofed signals. The authors aims to provide the research community with a general understanding of the GPS Spoofing concept in order to develop efficient defense mechanisms.

Guo et al. [55] proposed a covert GPS Spoofing tool that generates spoofed signals without being detected. The original trajectory of a UAV is first captured using some external devices such as radar and is then used to simulate similar counterfeit signals so that the UAV will not suffer from bigger shakes during this drift. For that purpose, the acceleration of the UAV is made adjusted so that it is moved to the deceptive trajectory. The authors have not put much focus on the simulator used and future directions.

The articles discussed so far have dealt with tools that can create GPS Spoofing attack on individual drones. However, the scenario in FANETs is different as swarms are formed with multiple drones working towards a common goal. These drones might be relatively of low cost and less complex and hence it is easier to instigate GPS Spoofing attacks. However, the concept of swarm formation plays a vital role in this case as transmitting a signal relative to any individual drone in the swarm might create obvious changes in the FANET's shape. This observation is considered by Ceccato et al. [56] in 2020 to design a spoofing tool against FANET to divert the routes of the entire swarm without disrupting the formation. This is called 'Spatial Spoofing', where FANETs move in the spoofed area in formation as if they are moving in their real target area. Multidimensional Linear Filters (e.g., Wiener Filter) are used for filtering the signals transmitted by the satellites in the target area and are further re-transmitted by multiple spoofing ground antennas. Ceccato et al. claimed that this releases the attacker from keeping track of each individual drone in the swarm.

Aru et al. [57] demonstrated the use of GPS-SDR-SIM, for generating spoofed signals to test the security vulnerability of DJI Phantom 3. GPS-SDR-SIM run by Attify 1.3 operating system, which is based on Ubuntu Linux and is built on a VirtualBox system. The GPS coordinates are input into the system. The tool then generates new coordinates and outputs into a `gpssim.bin` file. This is loaded to the BladeRF X40 device, which is then connected to the virtual machine. This system uses a track break mechanism and the attacker is operated from a remote position.

Wang et al. [58] proposed two spoofing trajectory planning algorithms, the extension line and the tangent line. Forward Spoofing Jamming technique is used, which generates the spoofed signal by adding a certain time delay to the original satellite signals. The authors considered the role of the Inertial Navigation System (INS) as well. In the extension line, the next spoofing position is the intersection of a circle with the center as the UAV's previous position and the direction vector of the Jamming signal. In the tangent line, the next spoofing position is the intersection of the tangent to the circle with the UAV position as the center from the actual destination of the UAV. MATLAB simulation experiments were conducted to evaluate the performance of the two algorithms. Even though both deflected the UAV from its original path, the tangent line algorithm was more powerful.

The various attacker models applied by GPS Spoofing attack mechanisms discussed in this section are summarized in Table 8.

B. GPS SPOOFING DEFENSE MECHANISMS IN UAVs

The proposed taxonomy of the GPS Spoofing defense mechanisms in UAVs is depicted in Fig. 7, which are

TABLE 8. Analysis of the attacker models.

Ref.	Location	Technique	Tool/Simulator
[51]	Remote	Track break	Ettus USRP
[59]	Remote	Position denial	LabSat3 GPS
[60]	Onboard	Track break	SITL
[16]	Remote	Track break	GPS-SDR-SIM, BladeRFx40 SDR
[56]	Remote	Track break (FANET)	Multi-dimensional antennas - Wiener Filter
[57]	Remote	Track break	GPS-SDR-SIM, BladeRF X40

classified under five major categories, based on the methodology adopted for or the basis of the defense. Specifically, onboard devices, signal processing, cryptographic, game theory-based, and machine or deep learning-based methods. The use of onboard navigation systems such as Inertial Measurement Units (IMUs) (e.g., Accelerometers, Gyroscopes) and cameras to compare with GPS measurements is the basis of defense using onboard devices. In signal processing methods, various characteristics of received signals like the Received Signal Strength (RSSI) are analyzed to check for any anomaly. Cryptography-based methods rely on encryption and authentication techniques. Strategic movements based on game theory are applied in game theory-based defense methods. The techniques of learning and training the network through various machine and deep learning concepts are employed in the machine or deep learning-based methods. In the following paragraphs, we discuss the details of the articles for each mechanism. A summarised table of these articles is shown in Table 13 in the Appendix.

Onboard devices or sensors techniques leverage various sensors onboard the drones for detecting GPS spoofing attack. The basic strategy is to employ the sensors to detect any anomalies or deviations from the expected GPS signals. There are several types of sensors that can be used onboard a UAV such as Inertial sensors (e.g., accelerometers and gyroscopes), Magnetic sensors (e.g., magnetometers), and Vision sensors (e.g., Cameras). Onboard sensors-based GPS spoofing detection approaches are advantageous as they can detect spoofing attacks in real-time and they are resistant to Jamming and interference. However, these approaches have some limitations and challenges like the need for accurate sensor calibration and the potential for false alarms due to other factors that might affect the sensor readings (e.g., environmental conditions or sensor noise). Fig. 9 depicts a high-level description of the methodology of these approaches. In the following paragraphs, we discuss the proposed defense solutions that are based on onboard devices or sensors.

In 2017, Qiao et al. [61] proposed a GPS Spoofing detection based on the vision of the UAV. The Monocular Camera,

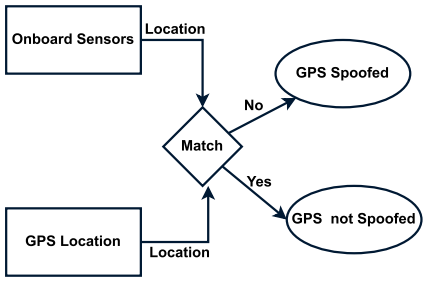

FIGURE 9. GPS spoofing detection using onboard devices or sensors.

using Lucas-Kanade (LK), and the IMU sensors were used to find the velocities of the UAVs. The velocity obtained via these two sensors is compared with the corresponding velocity obtained using the GPS. RMSE values are computed and spoofing is detected if the RMSE goes beyond a specific threshold value more than a pre-set number of times. The aforementioned process is performed during fixed time intervals. The proof-of-concept was implemented using DJI Phantom 4, which uses a rectangular trajectory. The GPS-spoofed signals are simulated at a UAV's speed of 5 m/s and the authors claimed that their method is efficient, as it does not require any additional hardware. The detection latency is used to evaluate the system. The experimental results show that the proposed methods detect GPS Spoofing in an average of 5 s. The authors plan to implement the proposed system in open-source platforms and outline the steps the UAVs must take upon detecting the attack.

The above work in [61] has been extended by Daojing et al. [62] in 2018 by proposing a method for the safe return of UAVs when spoofing is detected. The authors proposed to use the Oriented FAST and Rotated BRIEF (ORB) methods for feature detection, which are more precise and faster than their traditional counterparts like Scale Invariant Feature Transform (SIFT) and Speeded Up Robust Features (SURF). The UAV stores the image frames it captures during every prefixed time interval and if spoofing is detected, the UAV moves back in the same line. Then, after the same prefixed time interval, the UAV compares the captured image for that location with the stored one. If they match, it moves back from that location and repeats the same process until it reaches the starting location. The authors have not implemented their proposed method and therefore the performance is not evaluated. The authors recommended doing more research on decentralized approaches to control UAV clusters for decision-making and collision avoidance. However, continuous usage of the camera might rapidly drain the battery of the drones. Moreover, environmental factors like light, fog, and wind might affect the camera's performance.

Feng et al. [63] proposed a drone hijacking detection method in which the position of the drone detected by the Gyroscopes and Accelerometers sensors and the GPS receiver module are compared. The method avoids

accumulated errors when the INS is used. The performance of the proposed method is evaluated using proof-of-concept implementation with Quadrotor drone (equipped with L3GD20H gyroscopes and LSM303D accelerometers) using the PixhawkTMflight control system. The GPS system used in these drones is NEO-M8N. Hardware injection attack is conducted using an onboard micro-controller that generates fake GPS signals and a timer is set to trigger the hijacked mode. Position denial was used to prevents the GPS receivers from sensing the original signals. The ''Correctness Ratio'' (i.e., the ratio of the number of successful detection of hijacks to the total number of experiments) was calculated for the proposed method and it was 84% for non-hijacked cases and 100% for hijacked cases. At the same time, the systems that used GPS versus INS exhibited 0% and 100% correctness ratios, respectively. The authors recommend conducting future tests with other drones to generalize the results. The authors further improved their scheme in [64] to enhance the detection rate in non-hijacked cases. The GPS data (GPS angle) and gyroscope measurement (Yaw from the Angular Velocity) are the only factors used. This is because the readings from the accelerometers reduce the Accuracy of results in [63]. The authors claim that the correctness ratio of the system had become 100%, while it was 84% in [63] (DATE method) during non-hijacked *curved* trajectories. Yet, the method introduced subsequent degradation (still 92%) in the correctness ratio during non-hijacked line trajectories. Thus, in order to achieve 100% perfection in all scenarios, the authors recommended using [63] and [64] methods in fusion. In addition to the future direction in [63], the authors plan to extend their work to anti-hijacking flight control so that the drones can detect and stay resilient to fake or low-quality GPS signals.

Sun et al. [65] discuss the GPS Spoofing attack in UAVs that employ INS/GPS-integrated navigation systems. The authors state that in order to make the UAVs anti-spoof, the spurious GPS signals need to be identified first. For this, the system dynamics are based on the centroid motion model and attitude motion model. The measurements from INS and GPS are passed through two Extended Kalman Filters and are used to find relative estimation errors. Numerical Simulation experiments were conducted to evaluate the proposed model. The Estimation Error of centroid dynamics parameters Xc, Xy, and Xz with respect to time were used as performance parameters. The authors have not mentioned any future direction for their work.

Majidi et al. [66] proposed an approach to estimate the actual location of UAVs, which uses a fusion of INS/GPS data for navigational purposes. The spoofing is detected using the hypothesis method and the real trajectory to be followed during spoofed situations is estimated using particle filters. The authors used a Particle Swarm Optimization Filter (PSOF). The results obtained are compared with those of other particle filters such as the Sampling Importance Sampling Particle Filter (SIS-PF), Sampling Importance Re-sampling Particle Filter (SIR-PF), and Adaptive Unscented Particle File (AUPF). The PSOF is found to have a better performance, as it uses the experiences of each particle as well as neighbors for trajectory estimations. The performance of the system is evaluated using MATLAB simulations and the system has 97% Accuracy in positioning. Root Mean Square tests were conducted to validate the proposed method. No future directions were mentioned in this article.

Zhu et al. [67] proposed a method that involves a human operator supervisory control system. The image/video reels captured by onboard cameras are compared by a human operator with a pre-defined map. Any inconsistency in the correlation suspects a hacking attack and the operator can take control of the UAV for safe-return. The experiments to evaluate this concept was conducted on the Security-Aware Research Environment for Supervisory Control of Heterogeneous Unmanned Vehicles (RESCHU-SA) platform [68], [69]. The experimental results show 80% success rates. The data is analyzed using ANOVA tests and Pearson correlation. The authors recommended that Human Geo-location can be used as a potential tool to detect GPS Spoofing if the decision support systems are further enhanced. This work has been extended in 2019 using Hidden Markov Model (HMM) to reveal two hacking detection strategies (waypoint-oriented and target-oriented) [70]. The inefficiencies of these strategies were identified and recommended the need for a better decision support system as a future direction. The devices and systems that can provide real-time operational guidelines to the operators are other future directions. Yet, human operator is not a desirable feature for an autonomous environment.

Cheng et al. [71] proposed an approach that is based on the fusion of GPS and IMU information. The detection task is entrusted to the GCS and the GPS devices are relieved of any infrastructural changes. The authors have considered a FANET scenario where multiple UAVs interact and collaborate to accomplish a task. The locational information is also exchanged among the UAVs and they are compared with the locations obtained from GPS. Any mismatch indicates the probability of an attack. In case the number of drones in the system is not sufficient, the flight characteristics and other positional information from individual drones' onboard sensors are used to compare with GPS information. The Monte Carlo simulation [72] experiments claim that the system detects GPS Spoofing attacks within 8 s (and 28 s in the worst case) with a 98.6% detection rate. Communication Time Overhead, False Positive, and False Negative (miss detection) were the performance evaluation metrics used in this paper. No future directions are discussed in this paper. However, all drones in a FANET might not be always connected to GCS.

Ferrao et al. [73] proposed a GPS Spoofing detection mechanism that incorporates the security and safety of UAVs as a unified concept. A safety metric that indicates the health status of the UAV and the priority of a component for the overall system security is computed. Haversine Formula is applied to find the distance between two points. The readings

of the IMUs are also employed in the detection mechanism. The time data and distance are used to find the average speed of the drone. If the distance covered in the time range is acceptable (based on 80 Km/h speed), the drone is concluded to be in a stable state. Node Criticality Index (NCI) metric, which is the average of the health status index and priority, is applied to evaluate the performance of the proposed system. If the node is found to be unstable, the priority of UAV modules that can help the UAV to return to a safe state is increased. The experiments were conducted using 3DR solo drone. Fake GPS location Mobile App is employed to simulate spoofed GPS signals. The authors recommended conducting more research works on decision-making systems after the spoofing attack is detected.

Lianxiao et al. [74] proposed an approach that applied the fusion of the GPS and optical flow sensors to detect GPS Spoofing attacks in UAVs. The distance obtained by GPS coordinates of two positions traversed by a UAV and the pixel distance of images collected by optical flow sensors at these locations is compared. If the difference exceeds a preset threshold value, the UAV is considered to be spoofed. The proof-of-concept experiments have been conducted with a Quadrotor (PX4 Flight Control Software). It leverages PX4flow v1.3.1 as the optical flow model and HackRF SDR is operated to simulate the spoofed GPS signals. QGroundControl, which is a powerful and user-friendly GCS for UAVs, is employed for calibrating the sensors before the flight. Detection latency performance metric was measured. The method claims to have instantaneous detection of spoofing attacks. The future plan is to precisely locate the spoofed sensor and to investigate about the decision UAVs have to take after detecting the attack.

Varshosaz et al. [75] proposed an approach that can detect sophisticated GPS Spoofing attacks employing Visual Odometry. The trajectories determined by GPS and those by the onboard camera(s) are locally compared with the help of a moving window. The differences between these trajectories were estimated by computing the Euclidean Distances between corresponding points, Angle of Distance, and Taxicab Distance between Histogram of Oriented Displacements. The proof-of-concept evaluation of the proposed method is performed using images captured by DJI-FC6520 digital camera at Golgir village. The detection rate and latency performance metrics were measured. The method fails to detect the attack in certain scenarios like darkness, lack of features or texture in the images, etc. The changes in drone velocity might also affect the performance of the system.

Hacohen et al. [76] proposed a GNSS spoofing detection mechanism in UAV swarms that leverage the IMUs and the GNSS (GPS) receivers. Additionally, an onboard sensor that estimates the relative distance between the drones (like LoRa Sensor) is employed in this scheme. The drones in the swarm exchange their mutual distances among each other in the network and an Extended Kalman Filter is used for estimating the FANET distribution. The pool-testing method is applied to identify and isolate the malicious drones in the swarm. Experimental simulation experiments were conducted to evaluate the performance of the method. The method is found to have 90% Accuracy when there are at least 10 drones constituting the network.

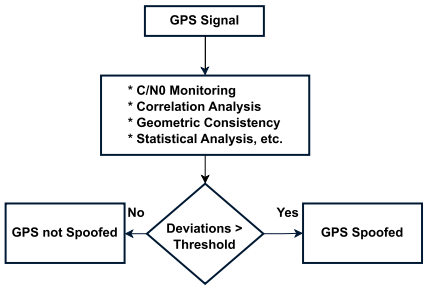

FIGURE 10. GPS spoofing detection using signal processing methods.

Signal Processing based methods can be deployed to detect GPS spoofing attacks in FANETs. GPS spoofing detection based on signal processing involves analyzing the received GPS signals to detect inconsistencies in the signal characteristics such as carrier-to-noise ratio (C/N0) Monitoring, Signal Correlation Analysis, Correlation Analysis, Geometric Consistency, Statistical Analysis, etc. If the deviations or inconsistencies exceed a prefixed threshold value, spoofing is detected. Figure 10 illustrates a high-level diagram of the process. Following paragraphs discuss various proposed solutions that leverage the signal processing methods to detect GPS Spoofing attacks in UAV environments.

Xiao et al. [77] proposed location authentication in drones against illegal hijacking by GPS Spoofing. The method named as ''WiDrone'' in which a WiFi Fingerprint location cross-check is performed. The Current WiFi Fingerprint (CWF) is compared with the Destination WiFi Fingerprint (DWF), which is already stored in the device. If there is any mismatch, spoofing is detected. The drone flies away from that location, gets a GPS signal, and then authenticates the destination again by employing the same procedure. The experimental evaluation is conducted using DJI Matrice 100. The system uses MT7601U wireless network card as the WiFi module to perform WiFi fingerprint collection. The drone and the Raspberry Pi were connected via UART cable. USRP N210 [78] simulates the GPS Spoofing signal, which is operated from a remote location. Track break technique was used to attack the drone. The WiFi Fingerprint similarity in different environments such as laboratory buildings, student dormitories, residential zones, and business districts are used for the performance evaluation. It is observed that the distance between CWF and DWF has a critical role in influencing the similarity. The authors judge that the distance of 50 m is suitable to perform the authentication. The authors recommended that instead of comparing RSSI of WiFi signals, other signal parameters can also be included, as WiFi works well only in urban/city areas. For mountainous areas without enough WiFi signal strength, this method fails. The authors project the possibility of introducing a ''No-Fly WiFi zone'' to overcome

the problem of bypassing the no-fly zone policies that can lead to terrorist attacks or illegal spying.

Javaid et al. [79] proposed a method to detect and mitigate GPS Spoofing attacks in UAVs leveraging Receiver Autonomous Integrity Monitoring (RAIM). The integrity of the signal packet received from the satellites is compared by computing the pseudo-range values from different satellites. If any discrepancy is found, the faulty satellites have to be isolated. The signals from five satellites are processed in three groups to detect the faulty host and the common host in all the groups is isolated to mitigate the effects. OMNeT++4.5 simulator [80] (with GPS module, called as UAVSim), which is a C++-based discrete event network simulator, is used to test the performance of the proposed concept.

Jansen et al. [81] proposed a method that leverages the periodic GPS position advertisements broadcasted by the aircraft for air traffic control purpose to detect GPS Spoofing attack and also to identify the location of the spoofer(s). The Time Difference of Arrival (TDoA) of the position advertisements at various globally distributed sensors at the OpenSky network [82] is used to estimate the position of the aircraft. The sensors are time-synchronized. The inconsistencies of these positions with those reported by the GPS receiver is used to detect the attack. The location of the spoofer is identified by employing the propagation delay in the advertisement traffic broadcasted by the receivers. The traffic is analyzed by dedicated infrastructure on the ground. USRP B200 from Ettus Research [52] and the software-defined GPS signal simulator, gps-sdr-sim [54], were applied to generate spoofed signals. Detection rate, delay, and coverage were the performance metrics measured. The detection rate is about 75% with a detection latency of fewer than two seconds. The attacker could be located within 15 minutes of monitoring.

Dang et al. [83] proposed a 5G-assisted method for monitoring the position of UAVs and hence live detection of GPS Spoofing attack. The method relies on the up-link Received Signal Strength (RSS) of signals received at the cellular base stations on the ground. The UAVs report their positional information to the Unmanned Ariel System Traffic Management (UTM), as per the Federal Aviation Administration (FAA) regulations. UAV residence areas and Adaptive Trustable Residence Areas (ATRAs) are computed using a trilateration approach. The UTM compares the location provided by the UAV with that of ATRA. If the UAV is located outside the ATRA, it is spoofed. The performance of the method, evaluated using Python, showed that more than 95% of the attacks are detected. True Positive, False Negative, and False Positive were used as performance evaluation metrics. The system applies the shadowing propagation model. For future works, the authors plan to work on LOS/NLOS Path Loss Models. Also, the proposed models would be extended to test the performance of the system under conditions where the UAV is not in the vicinity of fewer than three base stations. Additionally, the authors give directions to use machine learning techniques to access the channel quality.

Wan et al. [84] proposed a GPS Spoofing attack mitigation mechanism that tracks the attacker's location and estimates the effective range of the spoofing signals using an Extended Kalman Filter (EKF). This allows the UAV to move away from this range within the escape time and avoid sudden sensor drifts. The performance of the system is evaluated using numerical simulations with Julia Programming Language.

Tituona et al. [85] proposed a method to detect GPS Spoofing attacks in UAV networks leveraging the Bayesian Networks. The UAV system is modeled as a Bayesian Network and the GPS signals (Signal-to-Noise ratio, pseudo-range, Doppler shift, etc.) were analyzed to detect the spoofing attack. When a UAV receives a new GPS signal, the attack detector module embedded in the UAV checks the correctness of the signal by propagating signals in the network and estimating the conditional probability in the Bayesian Network. The performance of the proposed model was evaluated using MATLAB simulations and SatGrid datasets were used to generate GPS signals, which includes G22 (genuine GPS dataset collected from distributed locations) and S7 (spoofed dataset) [86]. The Precision, Recall, and FPR were the performance metrics measured. The method exhibited a Detection Accuracy of 96.2%. For future works, the authors plan to conduct experiments with more variables and compare the performance with other existing systems. The method does not work well if the trajectory is not pre-defined or if at least two neighbors do not follow the same trajectory.

In 2021, Bada et al. [87] proposed a trust-based method for detecting colluding GPS Spoofing attacks. The nodes in the FANET are classified as targets, active witnesses, and passive witnesses. The active witness can locate the spoofer using the angle of arrival and PRN code. The method is based on the free space loss factor in signal propagation. The free space loss factor is found to be negligible if the distance between the target and the satellite changes drastically in the case of authentic GPS signals, whereas a slight move can lead to a huge difference if the target is very close to the spoofer. The spoofer adjusts its transmission power such that the target receives it at almost the same power as received from the satellite. The neighboring UAVs (witnesses) can detect this signal with signal power greater than the detection threshold, making them aware of the attack. The UAVs in this model communicated using LrWPAN (Zigbee) protocol. The active witness detects this and communicates to all one-neighbor nodes in its vicinity. The passive witness, who can also witness the spoofed signal, confirms the attack and notifies the target. WEIBULL distribution is used to model the trust between nodes. The performance is evaluated using the NS3 simulator [88] with Random Mobility Model and ITU-R 1411 LOS propagation model. The detection rate (True Positives) and False Negatives were the performance metrics measured. The method detects 99.88% attacks with an Accuracy of 98.40%. For future works, the authors plan to integrate machine learning solutions with the proposed model,

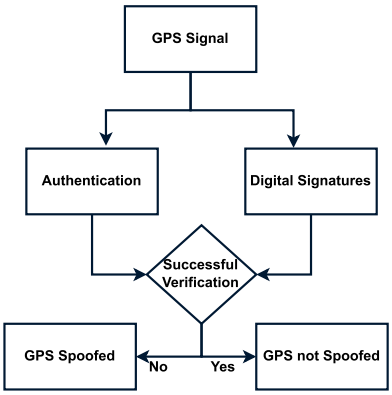

FIGURE 11. GPS spoofing detection using cryptographic methods.

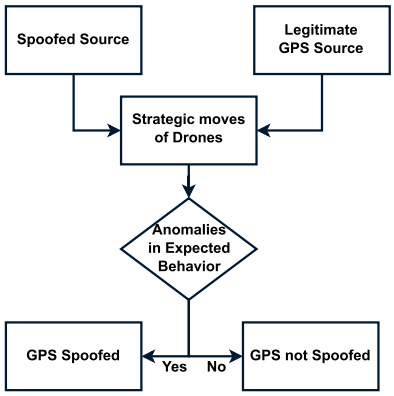

FIGURE 12. GPS spoofing detection using game-theory based methods.

alongside fusing the Byzantine Agreements to enhance and optimize the trust model.

In 2022, Pardhasaradhi et al. [89] proposed a method to detect and mitigate GPS Spoofing attacks in UAV Swarms using Distributed Radars. Multiple radars are deployed on the ground and the position, velocity, and time estimate of the signals from the targets are fused with GPS position estimate by the target in a central node. If both tracks are different, GPS Spoofing is detected. Then, the fused data from the radar are fed into the GPS receivers to mitigate the attack. Simulation experiments (simulation tool was not mentioned) were conducted to evaluate the performance of the system. Position Root Mean Square Error (PRMSE) has been used to detect the changes in the fusion node. Though the method does not require modifications in the existing GPS receiver infrastructure, it incurs high costs and computational overhead. Also, the deployment of multiple radars seems to be impractical. The security of the communication link between the radar and drones also needs to be ensured. For future works, the authors plan to deploy onboard radars instead of ground-based ones. Also, a fusion of IMU track, GPS tracking, and Radar track is to be considered.

Cryptographic methods are another approaches to detect GPS spoofing attacks in FANETs. These techniques involve employing cryptographic algorithms to authenticate and/or validate GPS signals. However, proper key management and computational overhead can be two hindering factors for the widespread adoption of these methods in resource-constrained drones. A high-level diagram of the process in these methods is depicted in Fig. 11. The following paragraphs discuss various proposed solutions that leverage cryptographic techniques.

In 2019, Han et al. [90] proposed a cooperative GNSS spoofing detection system for FANETs based on Blockchain technology. Blockchain is deployed as a layer on top of the UAVs, which upload their locational information from the GPS to the Blockchain. This updating is performed every second and the UAVs compare the locational information of the neighbors obtained through their Radio Direction Finding (RDF) unit. If any variation is detected, a spoofing attack is suspected and an alert is sent over the network to other nodes including the victim. The authors have not conducted any experimental study and no future direction was stated. This work has been included in this survey since it has given an orientation into GPS Spoofing attacks in FANETs whereas most other papers focused only on a single UAV.

Kara et al. [91] proposed a method to prevent/avoid GPS Spoofing attacks in FANETs. Their strategy aims to estimate the real position of UAV using a Leader-follower method. One of the UAVs in the FANET is elected as a leader using a consensus that is based on mission type, flight quality, etc. The leader gets its GPS position, which is then encrypted and sent to other drones. The follower drone decrypts the received message to get the leader's position, which is also appended with other parameters like propagation delay to compute its true position. In order to ensure the reachability of the leader drone by other drones, each drone sends the received message from the leader to all other connected drones. The leader is elected for a prefixed time period and then re-elected. The concept has yet to be implemented and its performance to be evaluated. The battery constraints of the drones for encryption and decryption also need to be considered.

Game-theory based methods are mathematical frameworks that model the interactions and decision-making of multiple entities in a strategic setting. The strategic movements of drones and attackers in this model are essential entities to be considered. A high-level diagram of the mechanism (or process) in these methods is illustrated in Fig. 12. The following paragraphs discuss various proposed solutions that are based on Game-theory.

In 2017, Tao et al. [92] envisioned the vulnerability of civilian UAVs to spoofing. After highlighting the impracticability of encrypting the GPS signals in civilian UAVs (due to cost, secrecy, and scalability requirements), the authors proposed a strategic defense against GPS Spoofing attacks in these UAVs. The receiver strategically infers a new location even if the attacker tries to mislead with false signals. A game-theoretic solution is proposed where the strategic interactions between UAV and the attacker are used to detect the attack. The game tries to attain Perfect Bayesian Equilibrium (PBE)

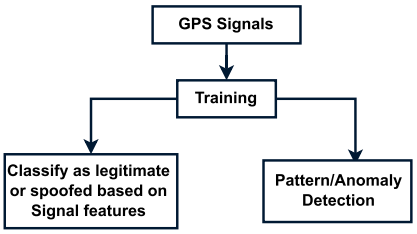

FIGURE 13. GPS spoofing detection using machine learning methods.

and it is observed that the equilibrium has a PLASH (Pooling in Low types And Separating in High types) structure. In case of a spoofing attack, the UAV infers its true position during the separating part and the strategic move of the UAV in the pooling portion makes it move such that the deviation from the true position is minimal. A continuous-kernel signaling game model analyzes the equilibrium of the game. Numerical experiments were conducted to evaluate the proposed scheme. The positions of UAVs under different scenarios were observed and employed as evaluation parameters. The remote spoofer captures the GPS signals and generates counterfeit ones for the UAV to track break and redirect the UAV to desired locations.

In 2020, Eldosouky et al. [93] proposed a GPS Spoofing defense mechanism that relies on the cooperative positioning of UAVs in the FANET to mitigate the effect of spoofing. A FANET scenario with five UAVs is studied in this paper. The authors aimed to capture the strengths of the Stackelberg Game Equilibrium to enhance their defense strategy. The optimal routes followed by UAVs during normal and attack scenarios were modeled using system dynamics. The performance of the proposed system is compared with other two systems that use random and deterministic strategies. The simulation results showed that the proposed system outperformed the other two systems in terms of UAV capture probability and UAV deflections from the planned routes. The authors direct future research to find solutions for the problem when more than five UAVs getting targeted by multiple simultaneous attackers. The reliability of other UAVs needs to be ensured in this scheme.

Machine Learning methods to defend against GPS Spoofing attacks in UAVs are used to analyze the GPS signals and detect any anomalies or deviations from the expected behavior. The system is trained to detect anomalies or classify them as legitimate or spoofed based on signal features. These approaches require diverse and realistic training datasets. A high-level diagram of the process in these methods is depicted in Fig. 13. The following paragraphs discuss the proposed solutions that employed machine learning approaches to detect GPS Spoofing in a UAV environment.

Panice et al. [94] discussed that the civilian GPS system does not guarantee authentication, integrity, and confidentiality, thus, it is vulnerable to GPS Spoofing attacks. The signal power is computed in many cases to detect the attack, however, this might not work for UAVs due to resource constraints. The authors proposed employing Support Vector Machines (SVM) to detect anomalies. The data fused from different navigation systems are analyzed using SVM. A decision boundary is constructed based on the knowledge of data during normal scenarios. The system is trained to detect deviation in order to indicate the attack. MATLAB simulations were used for performance evaluations. The attacker is considered to be located onboard as fake GPS data are injected into the simulation and used the track break strategy. FPR, TPR, and Accuracy were measured as the performance metrics. The system is found to detect the attacks within 30 *s*. The authors recommend conducting real-world experiments as a future direction for their work. However, the calibration of INS is done using GPS signals at the receiver.

Manesh et al. [95] proposed a machine learning-based approach that uses artificial intelligence to detect GPS Spoofing attacks in UAVs. The GPS signals are classified based on pseudo-range, Doppler Shift, and Signal-to-Noise ratio. The authors captured real GPS signals to create a meaconing (repeater-based) attack. RTL-SDR V.3 RTL2832U was used to receive the signals. RTKLIB [96] was deployed as a GNSS library. The experiments and training were only on the GPS data (i.e., without using any UAV). The detection rates, False Positives, and False Negatives were measured as performance metrics. The method exhibited an Accuracy of 98.2% and a detection rate of 99.4%. For future work, the authors recommended to use online learning to train the network when new data arrives.

In 2019, Xiao et al. [97] proposed a Recurrent Neural Network (RNN) based approach to identify behavioral anomalies in UAVs. Reliable normal behaviors are modeled using two scenarios and the UAVs are trained accordingly. The model Accuracy is enhanced by estimating the angle of arrival and Normalised Root Mean Square Error (NRMSE) that detects the deviation in a real position of the UAV and the position provided by the normal behavior models. If the NRMSE is greater than a prefixed threshold, abnormal behavior is detected. The experiments were simulated using Python and TensorFlow [98] and the Angle of Arrival is obtained by analyzing the real-time movement of the Dajiang Mavic Pro UAV and combining it with the national standards provided in the ITU-TY.IoT-UAS-Reqts [97]. The detection Accuracy of different RNNs in the deployed scenarios was measured and compared to the detection Accuracy of SVMs and Multi-Layer Perception (MLPs). The proposed method exhibited an Accuracy of 98.7% and a latency of 0.034 *s*. As a future direction, the authors projected the need of more optimized results that are in line with the real-world scenarios.

In 2020, Wang et al. [99] proposed a solution for UAVs with fixed routes like surveillance and delivery drones. The flight path of the UAV is predicted using the Long Short Term Memory (LSTM) algorithm, which relies on previous flight data. If the deviation between the predicted path and the GPS path exceeds a preset threshold, the path-based detection method is invoked. Path-based detection method uses the position estimated by integrating the velocity obtained from IMU. MATLAB simulations were used to evaluate the performance of the system using the detection latency and

the detection ratio metrics. The proposed method showed a detection ratio of 78% and a detection latency of 3 to 5 *s*.

Xue et al. [100] proposed a deep-learning-based approach that compares satellite images from Google Earth and images captured by their own UAV to detect GPS Spoofing attacks. The satellite images and aerial photos captured by UAV are fed into a deep learning model, which can be on-board or on-ground. The model compares the satellite and the UAV images. If a mismatch occurs, a spoofing alert is generated. The authors constructed a dataset, SatUAV [101], using images captured by DJI Phantom 4 with camera DJI FC631 and satellite images obtained from Google Earth. SatUAV dataset is further nourished with images obtained from the SenseFly website [102]. The performance of the model is evaluated using NVIDIA©Tesla®V100GPU (for deep learning), Raspberry Pi 3B+ and Python 3 with Pytorch [103]. Accuracy, precision, recall, F1-score (True Positive, False Positive, False Negative), Time Complexity, and Power Consumption were measured. The results exhibited a 95% success rate in detecting the attack within less than 100 ms. The authors suggested various future directions like exploring the probability of detecting the attack in featureless or feature-poor areas, parameter optimization or tuning for higher Accuracy, and overcoming challenges like detecting attacks at night and dealing with ephemeral objects, etc. Also, conducting more real-world experiments under various weather/air conditions (e.g., rain, snow, fog, haze, etc.) in more places for further evaluation. Fusion with other sensors like IMUs was also recommended. However, the proposed method relies on old images to detect the attack.

Jason et al. [104] proposed an intrusion detection system that detect GPS Spoofing attack in UAVs. The method is based on one-class classifiers, which used flight logs as a training dataset. A comparative analysis of various one-class classifiers, namely, One-Class Support Vector Machine (OC-SVM), Autoencoder Neural Network, and Local Outlier Factor (LOF) with the proposed system has been conducted. The authors used original flight log data, the UAV Attack Dataset [105], as a training set. The performance of the experiments is evaluated using SITL simulator and Gadgets HackRF software-defined radio with GPS-SDR-SIM tool for creating the spoofed signal. Keysight EXG N5172B signal generator has been used to provide the true coordinates as a location in Shanghai, China. Detection rate (precision, recall, and F1-score) and Accuracy performance metrics were measured. The system resulted in an average F1-score of 94.81% for the Autoencoder classifier, 81.17% for OC-SVM, and 58.93% for the LOF. As a future direction, the authors plan to develop classifiers for an onboard IDS using other sensors.

Feng et al. [106] proposed a machine learning-based method to train the UAV based on the GPS and IMU readings. The authors trained the UAVs off-board and on-board. XGBoost (XB) machine learning method is used for off-board training and the precision of the learning outcome is further fine-tuned using Genetic Algorithm (GA). Moreover, drones were trained onboard using real-time flight log data from the IMU and GPS receiver. The experiments were conducted using real-world Quadrotor drones. The spoofer is operated onboard triggering fake signals. The detection Accuracy and latency performance metrics were measured. The results show that the proposed method detects 93.3% and 100% of attacks in non-hijacked and hijacked cases, respectively, and the detection of the attack was within 1 *s*. For future works, the authors plan to conduct experiments in other drones with more complex trajectories and to investigate anti-hijacking flight control methods to make the drones resistant to low-quality GPS signals.

Dang et al. [107] proposed a method to detect GPS Spoofing in UAVs that leverages deep learning and statistical approaches. The statistical properties of path loss between UAV and nearby Base Station(s) are used to train the Multi-Layer Perceptron Model (MLP). Three statistical properties were considered (i.e., moment, quartile, and probability distribution difference) and three MLP-based models were designed. If the difference between the actual path loss (provided by the base station(s)) and the theoretical path loss (provided by UAV, which increases with distance) is greater than a threshold value, a spoofing is suspected. The accurate threshold values and selected base stations are given by MLP. The performance of the system was evaluated using Python and TensorFlow library. The Spoofer operated from a remote location with track break spoofing. The proposed method achieved a 93% detection rate if the UAV is in the vicinity of three base stations and an 80% detection rate if in the vicinity of one UAV. The future directions are to test the system using ensemble machine learning models and real data.

Richmond et al. [108] developed Deep Learning based models using UAV flight logs and telemetry data to detect GPS Spoofing attacks in real-time. The UAV log data for different models are generated and used for training. A classification-based training approach is adopted using two LSTM classifiers, namely, Binary Classifiers (BC) that use benign and spoofed data, and Autoencoder-based One-Class Classifiers (OCC) that use only benign data for training. Gazebo Simulator [109] was used for generating flight log datasets. PX4 Autopilot firmware with QGroundControl App (as GCS) was used to simulate UAVs. The performance and feasibility of the proposed model have been validated using Intel Neural Computing Stick (NCS2) [110]. The measured performance metrics were recall, precision, Accuracy, and F-1 score. UAV-specific and generalized evaluations were performed. UAV-generalized detectors are found to have a detection Accuracy of 97.79% using binary classifiers, whereas, 94.98% for one-class classifiers. The UAV-specific detectors exhibited a detection Accuracy of 99.56% using binary classifiers and $\sim$ 99.24% using one-class classifiers. The authors have evaluated the time overhead on the UAVs and found that the average time interference for the LSTM-based Autoencoder OCC is 4.32 ms and 3.986 ms for the binary classifier. For future works, the authors plan

to propose effective methods to address the attack after detecting it.

Aissou et al. [111] compared several tree-based machine learning models, Random Forest (RNF), Gradient Boost (GB), XB, and LightBM (LB), to detect GPS Spoofing attacks. The datasets were generated from real-time GPS signals using a USRP device and simulated spoofed GPS signals by manipulating various features of authentic signals (e.g., Carrier-to-Noise Ratio, Time of the Week, etc.). The models were trained and tested using the dataset and the performance of the models was evaluated. The probability of detection and misdetection, the probability of false alarm, and the Accuracy were measured. XB outperformed other algorithms in terms of Accuracy and probability of detection with an Accuracy of 95.52% (i.e., compared to 95.23%, 94.07%, and 91.45% for LB, RNF, and GB, respectively). RNF models outperformed others in terms of the probability of misdetection and false alarms. XB is faster with 2 ms latency compared to RNF: 21.01 ms, GB: 6.99 ms, and LB: 8.99 ms. XB is also less memory-consuming with 2.63 MB compared to RNF: 1.6 MB, GB: 3.19 MB, and LB: 2.0 MB. RNF outperformed in terms of memory consumption, however, it has the longest latency. From a UAS perspective, XB was the best algorithm.

Gasimova et al. [112] conducted a comparative study of three Ensemble based machine learning models. Namely, Bagging (Ba.), Boosting (Bo.), and Stacking (St.). The datasets were generated using the same approach in [111]. The performance of the models was evaluated in terms of Accuracy, probability of detection/misdetection, probability of false alarm, memory size, processing time, and prediction time per sample. The St. model outperformed others in terms of Accuracy with 95.43% (versus Ba.: 95.28%, Bo.: 94.61%), detection rate with 99.56% (versus Ba.: 95.28%, Bo.: 94.61%), FNR with 0.36% (versus Ba.: 0.64%, Bo: 2.95%), and FPR with 0.03% (versus Ba.: 1.07%, Bo.: 5.08%). However, the St. model showcased the worst performance in terms of memory consumption with 191.3 MB (versus Ba.: 190.4 MB, Bo.: 190.5 MB), processing time with 13.06 *s* (versus Ba.: 0.74 *s*, Bo.: 1.5 *s*), and prediction time with 0.24 *s* (versus Ba.: 0.02 *s*, Bo.: 0.01 *s*).

Tala et al. [113] proposed two techniques (Metric Optimized Dynamic selector and Weighted Metric Optimized Dynamic selector) to select the classifier for detecting GPS Spoofing attacks in UAVs. The authors compared ten machine learning algorithms and measured their performance in terms of Accuracy, detection probability, false alarm probability, misdetection probability, and detection latency. Thirteen GPS signal features from real-time experiments were used as datasets in MATLAB [114]. The proposed model showed an Accuracy of 99.6%, a detection probability of 98.9%, a false alarm probability of 1.56%, a misdetection probability of 1.09%, and a detection latency of 1.24 *s*.

C. GPS SPOOFING AS DEFENSE IN UAVs

Even though the technological innovation brought by UAVs is crucial, their problems are also critical. The illegal operations of UAVs make them difficult to manage. Anti-drone services that aim to disrupt or incapacitate non-cooperative drone operations are discussed in this section. That is, when GPS Spoofing is used as a tool to eliminate the security threats caused by UAVs.

Shijith et al. [115] proposed GPS Spoofing as a defense mechanism to counterfeit the GPS receiver on a drone that tries to enter restricted areas. The unencrypted nature of GPS signals is exploited to take over the drone to the desired location. The used tools are SatGen [116] simulator (as a GPS signal generator) and an SDR tool, USRP N210 [78], to transmit the signals. Specifically, to generate National Marine Electronics Association (NMEA) file that contains the locational information. This info is then converted to a text containing the coordinates of all intermediate locations. Python scripts were used to generate signals based on the location information. This signal is then transferred to the USRP N210 tool. The spoofer uses a track break technique and operates from a remote location, where false signals are generated and sent to the target. The targeted drone will be then directed to the desired location in the spoofed signal. The authors recommended a real-time implementation of their proposed system.

Gasper et al. [117], [118] recommended using GPS Spoofing vulnerability to divert unauthorized UAVs flying over unauthorized areas. The SDR, bladeGPS simulator, was used to generate fake GPS signals. The bladeGPS simulator uses NMEA messages that store GPS-related data. This field can be manipulated to make false signals. That is, to make the UAV recalculates its present position and moves out of the restricted area. The experiments were conducted in indoor and outdoor environments. The impact of spoofing in Smartphones, u-blox M8 GNSS evaluation kit, and u-blox MAX-7Q (GPS receiver used in most UAVs) were studied. The attacker is considered to operate from a remote location with a track breaking technique.

Li et al. [119] designed a miniature GPS spoofer that is based on Digital Signal Processing (DSP), Field-Programmable Gate Array (FPGA), and RF. Several experiments were conducted to spoof DJI Phantom Pro 4 using the mini spoofer and the results were studied. The DSP and FPGA are the core signal processing modules and the RF module up-converts the IF signals to resemble GPS L1 RF signals. The experimental results were successful in misleading the target by controlling its position and velocity. Also, the UAVs were made to land in the spoofed position. The authors claim that their spoofer can be used to control and manage low-altitude UAVs. They also recommended further study of the effectiveness of the spoofing strategy with real-time measurements from UAV target monitoring systems. Similarly, Sheng et al. [120] proposed a Reinforcement based Learning method to control UAVs that enter unauthorized areas. The authors suggested the use of GPS Spoofing as one example to expel the UAVs from the target estate.

Daojing et al. [121] proposed GNSS Spoofing as a method to counter non-cooperative UAVs that enter 'No-Fly Zone'

areas. The UAVs that entered the restricted area need to be sensed first (using some techniques like RADAR) and then jammed. When they convert to auto-pilot mode, they are spoofed with counterfeit signals that redirect them to far locations. The authors recommended, as a future direction, spoofing a cluster of non-cooperative drones.

Noh et al. [122] proposed hard spoofing techniques where the receiver is jammed with powerful signals for safe-hijacking the consumer drones. The proposed method aims to expel the drone safely from the protected area. The effect of GPS Spoofing and the behavior of the drones during and after the GPS failure and signal recovery were analyzed. Four safe-hijacking strategies have been introduced accordingly. Field studies were conducted using prominent consumer drones namely DJI (Phantom 3 and 4) drones, Parrot Bebop 2, and 3DR Solo. GSG-6 GNSS simulator [123] has been used in the experiments to generate spoofed signals and SITL (Software-in-the-Loop) [124] simulator was used to evaluate the results.

Hosam et al. [125] proposed a technique to land the unauthorized drones by transmitting manipulated GPS signals using RF-SDR. The technique also determines the launch location of the drones. The drones are forced to operate in rescue mode by the manipulated GPS signals and return to the launch location. The iterative guesses are made on the latitude and longitude of the launch locations using the current coordinate of the drone. As the drones return back to the launch location at a constant speed, the x and y components of the drone's speed become zero when it reaches the launch location. Experiments were conducted using HackRF SDR to launch spoofed GPS signals into Audrino chipset with GPS. Future works aims to minimize the number of guesses and evaluate the proposed algorithm on real drones.

D. GPS SPOOFING IMPACT AND VULNERABILITY

Vishal et al. [59] discussed the security vulnerabilities of drones such as the GPS Spoofing vulnerability of the DJI Phantom 4 Pro (P4P) drone. Afterwards, the architecture details of DJI P4P drones and the experimental studies (i.e., cracking the DJI SDK, reverse-engineering the firmware, and launching GPS Spoofing attacks) were discussed. The attacks were conducted using LabSat3 [126] GPS simulator. The u-blox NEO 8M GPS receiver of the DJI P4P defends jam-then-spoof attacks. However, the experiments were conducted using weak GPS signals. The active antenna RLACS198 of the LabSat Kit records the original GPS signals and the SatGen software was used to generate fake signals.

Mendes et al. [60] studied the impact of GPS Spoofing attacks on Quadcopters. The authors observed that increasing the duration of tampering will also increase the deviation. However, after short time, the UAV does not show any deviation. The spoofer system is a hardware injection system in which the ArduCopter flight controller (used for processing and calculations purposes) is instrumented with a GPS Spoofing module. This module triggers the attack by tampering GPS signal after 45 s of the starting time. The spoofer was onboard and used the track break technique. The experiments used SITL [124] simulator that simulates Quadcopter behavior (i.e., using a Navio2 control board developed by Emlid and Raspberry Pi with Raspbian OS). The deviation in UAVs' positions with respect to time was taken as a performance metric. As a future direction, the authors plan to conduct real-world experiments with Quadcopter.

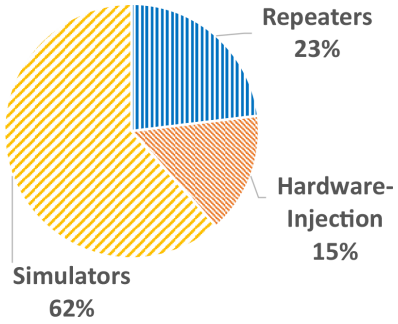

FIGURE 14. Comparative analysis of spoofer systems.

VI. RESULTS, DISCUSSIONS, AND RESEARCH GAPS

In this section, our observations, in terms of attacker models, defense mechanisms, performance measures, datasets, various research gaps, and open issues are discussed. This section aims to address **RQ2, RQ3, RQ4, RQ5,** and **RQ8** (raised in Section III-A).

A. ATTACKER MODELS

The study conducted in this paper has observed in Section V that the attacker uses different attacking strategies and tools that operate from different locations to conduct GPS Spoofing attacks. These attacker models are analyzed in this section, addressing **RQ2** of Section III-A. Table 12 in the Appendix shows a detailed analysis of the attacker model used in the articles studied in this survey. It is found that the majority (75%) of spoofers operate from remote locations in the existing literature and adopted track break spoofing techniques.

The spoofer system includes GPS simulators, repeater-based systems, and hardware injection methods. A percentage-wise analysis of the spoofer systems used in the proposed works is depicted in Fig. 14. It can be seen that the majority of the works (62%) relied on GPS simulators to generate spoofed signals. The low-cost and easy availability of the SDRs can be the main reason for this reliance. The repeaters, which capture the real signals, manipulate them, and then re-transmit them to the GPS receivers, are used by 23% of the works. Rest 15% used hardware injection systems, in which the spoofer device is embedded or installed on the GPS receiver.

The GPS simulator-based systems rely mostly on open-source GPS simulators like GPS-SDR-SIM [54] to generate fake GPS signals. These signals are converted to

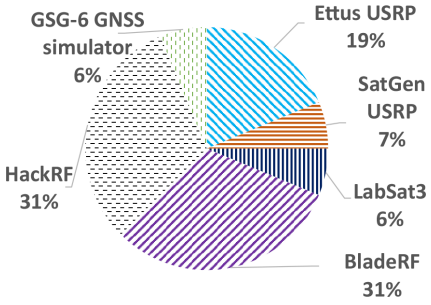

FIGURE 15. Comparative analysis of spoofing tools in simulators.

RF signals with the help of SDRs like HackRF, BladeRF, USRP, etc. A percentage-wise analysis of various spoofing tools used in the proposed works to spoof GPS signals is shown in Fig. 15. As is clear, BladeRF and HackRF were relied on by the majority (31% each) of the works. USRP tools, namely, Ettus USRP (19%) and SatGen USRP (7%) were used by some (26%) of the works. Other tools used are LabSat3 and GSC-6 GNSS (both by 6%).

To the best of our knowledge, and based on the covered articles, various research gaps exist related to attacker models, which are listed below:

- Other than mentioning the tools used for conducting the attack, most of the works failed to consider other attack parameters like the minimum distance from which the spoofer operates, the number of drones that can be victimized by a single malicious node, and the number of malicious nodes required to spoof the entire swarm area. These parameters can have a crucial impact on determining the attacker's capability. The distance from which the spoofer operates can affect the number of drones being spoofed. Even though the attacker might be targeting to spoof the GPS location information of one drone, other drones in its vicinity might also get locked into these spoofed signals. This will affect the FANET system itself, which relies on the locational information that gets exchanged among the drones. Moreover, any detection system that relies on the locational information shared by other drones will also get deceived by the wrong locational information provided by neighboring drones, which are also victims of the spoofing attack. For example, the solutions proposed in [71] and [87] leverage the GPS locational information shared by the neighboring drones. So, if these neighboring drones also fall in the spoofed area, the detection system fails. Thus, the effect of spoofer-to-target distance on successful GPS Spoofing attack instigation needs to be investigated. The possibility that the entire swarm area to be spoofed and the minimum number of malicious nodes required for such spoofing also needs to be investigated. It is anticipated that defensive mechanisms might fail in such scenarios. We recommend that future research works should assess these factors also so that a robust defense mechanism can be designed.
- A comparative evaluation of various tools in Fig. 15 can also be conducted. To the best of our knowledge, these tools are used to launch the spoofing attack in single UAV scenarios. None of the existing works performed an attack on FANET with these tools. So, the effectiveness of these tools in launching attacks in the FANET scenario needs to be investigated and analyzed in order to understand the attackers capabilities; hence, the effectiveness of the proposed detection or defense solutions can be accurately evaluated.
- The power capabilities of the attacker have not been much discussed in the covered articles. As per the authors in [87], the spoofer tries to adjust its transmission power such that targets that are at a distance 'D' from the spoofer will receive a signal of power -154 dBW. If the power received at the target is lesser than -157 dBW, the detection systems detect the presence of an attack. More studies need to be conducted in this direction considering the different power capabilities of the attacker and their impacts on the effectiveness of the proposed detection or defense mechanisms.
- None of the papers covered in this study has investigated the number and type of tools that can be used to simultaneously launch the attack. Future studies should thus investigate the number of tools that might be required to spoof the FANET. The impact of the collaboration of multiple attackers that are equipped with different tools (like HackRF and BladeRF) to launch the attacks from various locations also needs to be studied.

B. OBJECTIVE(S) AND TAXONOMY OF PROPOSED MECHANISMS

The study conducted in this paper has observed (as shown in Fig. 7 and detailed in Section V) that the proposed mechanisms can be classified into four main categories based on their objectives. Specifically, *GPS Spoofing Attack Mechanisms*, *GPS Spoofing Defense Mechanisms*, *GPS Spoofing as-Defense Mechanisms*, and *GPS Spoofing Impact and vulnerability*. Fig. 16 shows the statistical analysis of technical papers considered in this study. It can be seen that, out of 56 technical papers selected after various filtering, 37 papers addressed the detection, mitigation, and/or prevention of GPS Spoofing attacks in UAVs. Nine papers demonstrated how to instigate GPS Spoofing attacks in UAVs, eight papers proposed to use GPS Spoofing as a defense mechanism to deter malicious UAVs, and only two papers discussed the impacts and vulnerabilities of GPS Spoofing attacks in UAVs.

RQ3 in Section III-A is addressed by providing a taxonomy based on the approaches proposed to detect, mitigate and/or prevent GPS Spoofing attacks in UAVs. Following the basis or the technique leveraged to defend against GPS Spoofing attacks, the methodologies were categorized into *onboard devices or sensors, signal processing, cryptographic, game theory*, and *machine learning* mechanisms. A comparative analysis of the number of articles under various GPS Spoofing defense mechanisms is illustrated in Fig. 17. A major

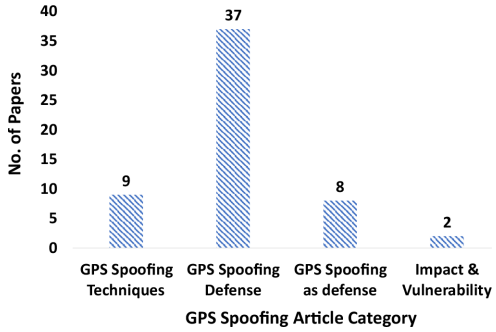

FIGURE 16. GPS spoofing paper categories.

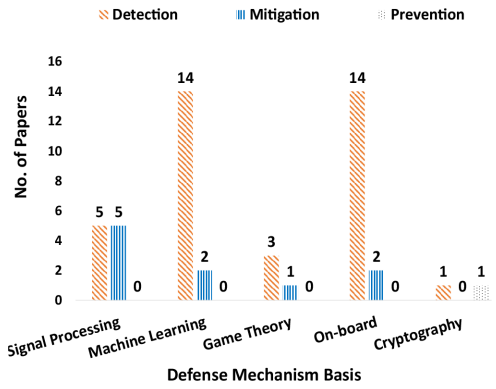

FIGURE 17. Number of papers based on attack defense mechanism's basis.

observation in Fig. 17 is the number of papers that aimed to prevent or mitigate the attack is lesser when compared to the total number of papers. Most of the papers aimed at the detection of the attack. Another observation is that 14 approaches leverage machine learning techniques and another 14 approaches leverage the onboard devices for the detection of GPS Spoofing attacks in UAVs. Signal processing approaches have been applied by five detection as well as mitigation approaches. Game theoretic solutions were proposed in three works to detect the attack and one work used it for mitigation. One approach used a cryptographic mechanism to detect and prevent the attack. A percentage-wise analysis of the articles according to their defense mechanisms is depicted in Fig. 18. Onboard devices and machine learning approaches have been adopted by 38% of the approaches, signal processing by 13%, and game theory by 8%. Cryptographic approaches were adopted by just 3% of the works. It is later seen that the approaches using cryptography were not implemented or not conceptually proved.

A percentage-wise analysis of the type of publication is shown in Fig. 19. Out of the 70 articles (14 state-of-the-art papers and 56 technical papers) considered in this survey, 40% of the articles were conference papers, 46% were articles published in journals, and 14% were published in magazines or book chapters. This is an indication that the research works on GPS Spoofing attacks in UAVs are still maturing.

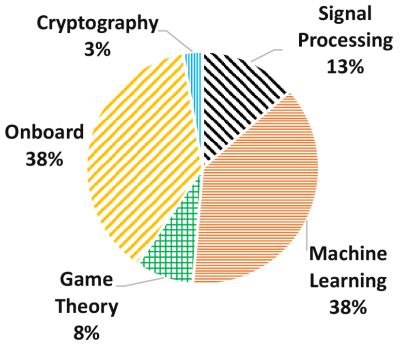

FIGURE 18. Percentage wise analysis of based on basis of defense.

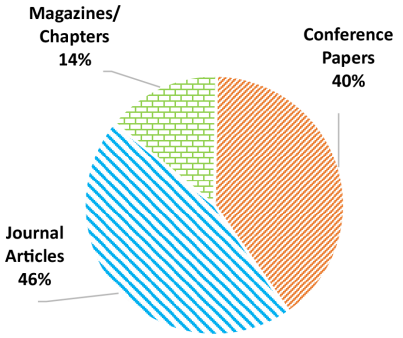

FIGURE 19. Comparative analysis of publication types.

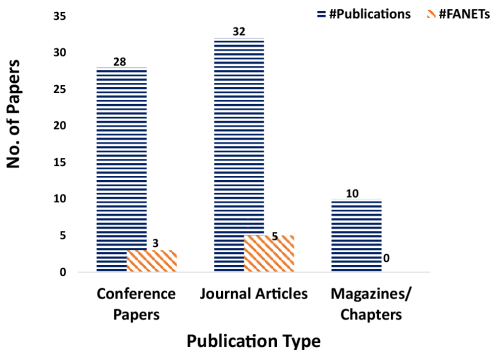

FIGURE 20. Papers on FANET scenario.

The number of papers that considered a FANET scenario, where multiple UAVs interact is also analyzed. Fig. 20 depicts that out of the 28 publications in conference proceedings, only three were addressing the GPS Spoofing attack problem in the FANET scenario. Also, among the 32 journal articles, only five dealt with FANET cases. None of the ten papers published in magazine/book chapters was on the FANET scenario. This again indicated that the area of research on GPS Spoofing attacks in FANET has obtained very little attention so far from the research community.

To the best of our knowledge, and based on the covered articles, various research gaps exist related to the objectives of the proposed mechanisms, which are listed below:

- From Fig. 16, it is noticed that only two articles [59] and [60], have studied the vulnerability and impact of

GPS Spoofing attacks in UAVs. Future research should analyze the vulnerability of various types of drones to GPS Spoofing attacks. The existing study was conducted for a particular type of drone only (i.e., DJI Phantom 4 Pro). The impact of GPS Spoofing attacks on FANETs with regard to different attack parameters such as the attack duration, and attack frequency should also be studied. Further to this, various position-based routing protocols such as Reactive-Greedy-Reactive protocol (RGR) [127] and Ad-Hoc Routing Protocol for Aeronautical MANETs (ARPAM) [128] rely on the knowledge of geographical positions that drones obtain through their GPS sensors. The geographical positions are leveraged in the data delivery to get the destination's location as well in cases of network disconnections to avoid network partitioning. The geographic positions of UAVs in the network are also exploited to select the shortest path between the source UAV and the destination UAV. Hence, when this locational information is manipulated, the packet delivery rate and routing capabilities are severely affected. Thus, it is recommended to conduct simulation experiments or proof-of-concept implementations to investigate the impacts of GPS Spoofing attacks on these protocols.

- Future research works should try to propose defense mechanisms that can not only detect, but mitigate, and prevent the attack.
- It is recommended that more research work might be conducted to investigate the effectiveness of:
  - Machine Learning-based or onboard devices-based defense mechanisms to mitigate or prevent the attacks as well rather than to detect the attack.
  - Game-theoretic approaches as well as Cryptographic-based approaches in dealing with GPS Spoofing attacks.
  - Hybrid-based approaches, which combine (i.e., employ) two or more of the above approaches together in dealing with GPS Spoofing attacks. For instance, signal processing approaches when combined with the onboard devices to defend against the attack since leveraging these methods don't require any infrastructural modification and hence can be cost-effective.
- Less than 50% of papers were published in journals, indicating the immature state-of-the-art of GPS Spoofing research works in FANETs, more research needs to be conducted and papers to be published in reputed journals. As per this study, out of the 46% journal papers covered, only five articles were on FANETs.

C. PERFORMANCE EVALUATION METHODS

In this section, various performance evaluation methods (i.e, simulation experiments and proof-of-concept implementations) of the papers covered in this study are analyzed, answering **RQ4**, which was formulated in Section III-A.

TABLE 9. List of Drones that can be used for FANET formation.

Name	Manufacturer	Communication
DJI Mavic 3 [132]	DJI (2023)	OcuSyn 2.0, WiFi
DJI Air 2S	DJI (2021)	WiFi, OcuSync 3.0
VOXL M500 [133]	ModalAI (2020)	WiFi, LTE, Microhard
Skydio 2/2+ [134]	Skydio (2021)	WiFi
Parrot Anafi USA [135]	Parrot (2020)	WiFi

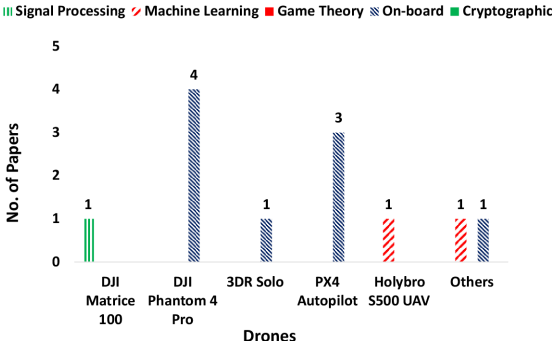

FIGURE 21. Papers evaluated using proof-of-concept implementation.

Fig. 21 illustrates the analysis of the number of papers evaluated using proof-of-concept implementation. DJI Matrice 100, DJI Phantom Pro, 3DR Solo, PX4 Autopilot (Flight Controller), and Holybro S 500 are the major drones used in articles considered in this study to evaluate various experiments in a single UAV scenario. However, most of these drones are no longer in production as newer versions were released recently. For instance, DJI Matrice 100 and Phantom 4 Pro drones are no longer in production nowadays and are replaced by DJI Matrice 300 [129] and DJI Phantom 4 Pro V2.0 [130] drones, respectively. The 3DR Solo has been discontinued and is replaced with Aurelia X4 Standard, which is an improved quadcopter drone [131]. Moreover, none of the papers that addressed GPS Spoofing attacks in FANETs have provided a proof-of-concept implementation. Hence, the upgraded drones that are presently available in the market, which are able to communicate with each other by forming an Ad-Hoc network, need to be considered and involved by future research. A list of the upgraded drones and their communication capabilities is shown in Table 9.

Some of the studied articles conducted simulation experiments. All the simulators that were used in the studied articles in this survey are analyzed in Fig. 22. Specifically, MATLAB [114], STIL (Software in The Loop) [124],

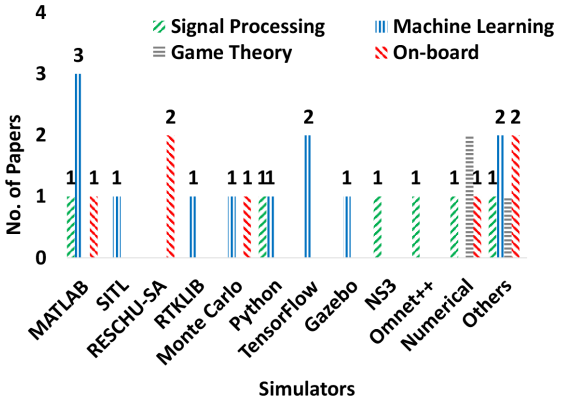

FIGURE 22. Papers evaluated using simulation experiments.

RESCHU-SA [69], RTKLIB [96], Monte Carlo [72], Python, TensorFlow [98], Gazebo [109], NS3 [88], and OMNeT++ [80] were used by the articles for performance evaluations. Some articles used numerical simulations and some others, categorized under 'Others' in Fig. 22, have not stated the names of simulators used for performance evaluations. It is observed that most of the machine learning-based schemes were evaluated using MATLAB [114] followed by TensorFlow [98], as both tools support various built-in machine learning libraries. Other simulators are used by one or a maximum of two experiments. Another observation is that the cryptography-based schemes were not evaluated even using the simulation experiments. Furthermore, Monte Carlo [72], NS3, OMNeT++ [80], and MATLAB [114] were used in experiments involving FANETs.

The mobility and propagation models of UAVs were neglected in most of the simulation experiments. A few articles have mentioned the random mobility model in the experimental details. This includes experiments conducted using OMNeT++ [80] and NS3 [88] simulators. One article that used NS3 [88] has mentioned the propagation model as ITU-R 1411 LOS (Line-of-sight). Thus, it is recommended to use either OMNeT++ [80] or NS3 [88] for future evaluations so that the mobility and propagation models can be easily employed and included in the evaluation. Also, this is an indication that **RQ6** and **RQ7** (Section III-A) have not been well addressed in the existing literature. Furthermore, since FANETs move in 3-D space, the mobility models that can simulate the 3-D movement of UAVs such as the Gauss Markov Model [136] can be used in future experiments. That is, the efficiency of the proposed approaches in terms of power requirements and/or storage and communication overhead when employing these mobility models must be considered.

A few methods have used some real and synthetic datasets in the experiments. Specifically, SatUAV [137], the senseFly drone dataset [102], UAV attack dataset (IEEE Dataports) [105], SatGrid [86], and OpenSky Network [82]. SatUAV Dataset is a synthetic dataset generated using a collection of images captured by a DJI Phantom 4 drone (with camera DJI FC631 and pixel resolution of 5472 × 3078),

TABLE 10. Overview of datasets.

Dataset	Data	Type
SatUAV [137]	967 Images	.jpg
senseFly [102]	362 Images	.jpg
UAV Attack [105]	UAV Log Files	.ulog, .csv
SatGrid [86]	GPS Signals	.dat, .mat
OpenSky [82]	Air Traffic	.csv, .avro, .json

which includes 967 SatUAV image pairs combined with the SenseFly dataset. SenseFly website has 362 photos available on the Internet [102] taken by eBee drones (with a camera resolution of 4608 × 3456 and 5472 × 3648 pixel resolution). It includes 160 photos (using a Canon IXUS125HS camera) of the Swiss village of Merlischachen at a flight height of 162 m (531.4 ft), 40 photos (using a Parrot Sequoia camera) outskirts of Renens, a municipality in Switzerland at a flight height of 100 m (328.1 ft), 113 images (using SenseFly S.O.D.A. camera) of Lausanne, Switzerland at a height of 100 m (328.1 ft), and 49 images (using Canon IXUS 125 HS) of Paris Le Bourget Airport at the height of 120 m (393.7 ft). UAV attack dataset (IEEE Dataports) [105] are flight log files saved by autopilot in ULog format having header (the file magic number, log version, and timestamp), definition (logged attributes and values), and data sections (contains informational, debug warning, and emergency information sent from the autopilot to the GCS) as the contents. It contains flight logs during both benign (i.e., normal) and attack (i.e., spoofed) scenarios. SatGrid dataset [86] includes SatGrid: G22 (Genuine GPS dataset) and SatGrid: S7 (spoofed dataset). These are real-time traces of GPS signals collected from different geo-locations, time, and environmental conditions. OpenSky [82] provides an Air Traffic Surveillance (ATS) dataset collected with the help of over 3000 sensors around the world. Table 10 presents a brief overview of these datasets.

To the best of our knowledge, and based on the covered articles, various research gaps exist in terms of performance evaluation methods, which are listed below:

- Some articles covered in this study have not clarified the method used for their performance evaluation experiments, which we stated as 'Others' in Fig. 21 and 22. Future research works should clearly mention the names of drones and GPS simulators used in proof-of-concept evaluations. Furthermore, the simulator, the mobility model, and the propagation model used in various simulation experiments.
- Simulated experiments generally don't reflect real-world scenarios. For example, environmental factors like wind, light, and fog have a crucial impact on the movement and performance of drones, might not be addressed by simulators. However, the majority of the experiments in the covered articles in this survey are evaluated using simulated experiments. Thus, we recommend that future research works rely on real-world experiments or proof-of-concept implementations.

D. PERFORMANCE METRICS

In this section, various metrics that were used in the performance evaluation experiments, discussed in Section VI-C, are analyzed to answer **RQ5** (raised in Section III-A). Specifically, FPR, TPR, FNR, Detection Latency (Delay), Position Drift, Precision, F1-Score, Accuracy, RMSE, UAV Capture Probability, Power Consumption, and Memory Overhead. Fig. 23 illustrates the number of articles that used these metrics in their evaluations. As shown in this figure, TPR, Accuracy, Detection Latency, and FPR are most commonly used in the articles covered in this study. To the best of our knowledge, and based on the covered articles, various research gaps exist in terms of performance metrics, which are listed below:

- The FPR, which is a major factor that hinders the service delivery to legitimate users of any system, has not been extensively evaluated in the existing works. Indeed, the detection of the attack is the major goal of the proposed approaches, however, higher false alarms can unintentionally lead to Denial-of-Service attack as it might prohibit legitimate drones or disable their services.
- Detection time (latency) was not evaluated in some articles that were covered in this study. Also, the articles that reported the detection latency haven't studied the impact of varying different attack parameters on it such as the number of victim drones and the number of malicious nodes that launch the attack (discussed in Section VI-A). The detection latency is a crucial measure that reflects the time taken by the proposed algorithms to detect the attack after it is launched by the malicious attackers. This metric must be evaluated by future research works as longer detection time might cause the UAVs to be hijacked or collide and as a result causes a mission failure (i.e., long detection time allows the malicious attackers to cause more damage into the system before the detection approach issue warnings/alarms).
- Only few articles of the existing works evaluated the power/energy consumption and memory of the proposed algorithms. Since drones are devices with constraints on the resources such as low battery power, less memory storage, and limited processing capabilities, these resource constraints factors should be considered when designing the defensive schemes.
- Other metrics such as the victim-to-attacker ratio (i.e., the number of drones that can be spoofed by malicious drones), communication overhead (i.e., the number and size of messages that are used by the proposed approaches), *Big O* notation (i.e., that represents the worst-case complexity of the proposed algorithms) also need to be considered and evaluated by future research works.

E. COMPARATIVE ANALYSIS

A detailed comparative analysis of the articles covered in this study that proposed solutions to defend against GPS Spoofing attacks in UAV environments is depicted in Table 14

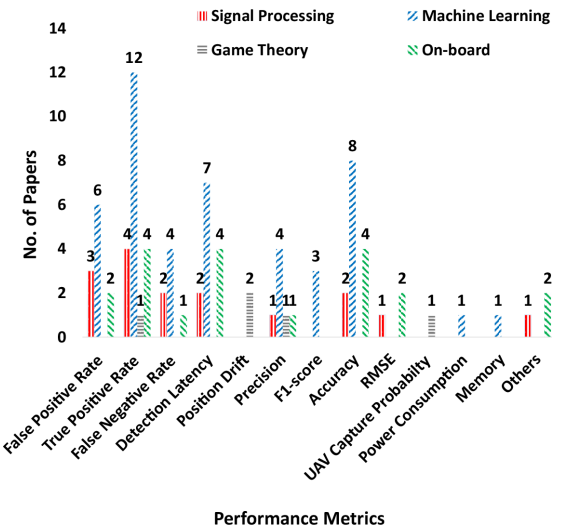

FIGURE 23. Papers evaluated using performance metrics.

in the Appendix. The performance evaluations of the proposed systems were compared in terms of the performance metrics used by the majority of the articles, which were also observed to be crucial in determining the performance of any detection mechanism. Specifically, TPR, FPR, Accuracy, and Latency. The prerequisites of the aforementioned articles were also analyzed in terms of any additional requirements on hardware devices or sensors, storage, battery, and any other specific requirements such as datasets, as shown in Table 14. It can be seen that the defensive approaches that are based on Machine Learning algorithms outperformed other detection mechanisms in terms of their performance. However, it is well known that Machine Learning algorithms require a high amount of computation and processing power, which in turn demands battery and storage. Apart from these, the requirement for a sufficient amount of diverse and realistic training datasets also hinders the acceptance of machine learning algorithms in securing resource-constrained drone networks. Signal processing-based methods such as [87] and [83] exhibited detection rates of 99.98% and 95% followed by methods that leverage onboard sensors [71], which exhibited 98.6% [67], [70]. In terms of Accuracy, signal processing-based methods [85], [87] also show relatively high results of 98.4% and 96.2%, respectively. The methods that rely on onboard sensors such as [66] and [76] showcased greater Accuracy of 97% and 90%, respectively. The methods that rely on signal processing and onboard sensors were efficient in terms of detection time (latency) as well, which was less than two seconds in [81]. However, the main problems with methods that used onboard cameras are the additional storage, battery, and weight requirements. Furthermore, these methods require favorable atmospheric conditions such as ambient light, fog, wind, and rain free environments. The main limitation of the signal processing method, which we suggest to be evaluated and mitigated in future works, is the communication overhead with the ground (GCS, Radars, etc.) [81].

TABLE 11. Comparative analysis of the state-of-art articles.

Ref.	Title	Description	Difference(s) from this Survey
[39]	Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions	- Attacks on UAVs were analyzed and categorized - Reviewed the recent defense mechanisms against various attacks in UAVs - GPS Spoofing attacks discussed under the data manipulation attacks - Classified GPS Spoofing defense strategies into four categories: Cryptography-based, Spatial Processing-based, Machine Learning-based, and Hybrid methods	- Does not addressed GPS Spoofing attacks in FANETs - Discussed generalized defense mechanisms for GPS Spoofing attacks - Not systematic literature survey
[40]	Unmanned Aerial Vehicles Threats and Defence Solutions	- Discussed UAV components, vulnerabilities and defense methodologies - Created a taxonomy of attacks against UAVs based on the UAV components - GPS Spoofing attacks were categorized under 'Attack against Communication Link' - Various defense techniques based on: signal processing, encrypting the GPS signals, and machine learning techniques	- Does not addressed GPS Spoofing attacks in FANETs - Not systematic literature survey
[41]	Security and privacy issues of UAV: A survey	- Analyzed the safety aspects of UAVs from three perspectives: sensors, communications, and multi-UAVs - GPS Spoofing attacks studied under the category 'Attack on sensors' - Presented two types of spoofing threats (Repeater type and Generating type) in UAVs	- Does not addressed GPS Spoofing attacks in FANETs - Not systematic literature survey
[28]	A Review on Communications Perspective of Flying Ad-Hoc Networks: Key Enabling Wireless Technologies, Applications, Challenges, and Open Research Topics	- Provides insights into communication technologies in FANETs, application scenarios, challenges, and open issues - Discussed GPS Spoofing vulnerability of 3D Robotics commercial drones - Few solutions to GPS Spoofing attacks in FANETs	- No detailed discussions on the solutions were provided - Not systematic literature survey
[42]	Comprehensive survey of UAVs communication networks	- Presented a comprehensive survey on UAV communication protocols, networking systems, architecture, and applications - Discussed the technical challenges and open research issues - Brief review on recent GPS Spoofing attack detection techniques in UAVs based on Visual Odometry, a fusion of GPS and optical flow raw data, and machine learning	- No future directions related to GPS Spoofing attacks - Not systematic literature survey

TABLE 11. *(Continued.)* **Comparative analysis of the state-of-art articles.**

Ref.	Title	Description	Difference(s) from this Survey
[43]	Unmanned Aerial Vehicle's vulnerability to GPS Spoofing a review	- Discussed the spoofing problems, types, and various countermeasures in existing literature - Provided detailed discussion on Covert and Overt attacks; Simplistic, Intermediate, and Sophisticated attacks - Discussed countermeasures and categorized them into several groups - encryption-based, Receiver Autonomous Integrity Monitoring (RAIM), Navigation Message Authentication, differing spoofed signal and true GNSS signals in space, antenna motion or geometry, and signal power	- Technical papers were on GPS Spoofing attacks and only two papers are specific to UAVs - Not systematic literature survey
[44]	Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey	- Presented a comprehensive review on drone communication - Lights are thrown on security-critical drone applications, security challenges, and solution architectures for various attacks based on Blockchain, SDNs, Machine Learning and Fog/Edge Computing - Discussed solutions to prevent GPS Spoofing attacks in drone environment based on Fog computing	- Not specific on GPS Spoofing attack - Not systematic literature survey
[45]	A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques	- Discussed UAV attacks and neutralization techniques - Discussed the misuse of UAVs for illegal surveillance and unmanned attacks - Provided a discussion on using GPS Spoofing as an anti-UAV tool to neutralize the UAV attacks	- Not on GPS Spoofing in FANETs - Not systematic literature survey
[46]	A Survey on the Jamming and Spoofing attacks on the Unmanned Aerial Vehicle Networks	- Illustrated spoofing attacks that target the GPS and ADS-B - Three ways of executing GPS Spoofing attack: falsified GPS signal, higher frequency signals, and spoofing the high gain antenna	- Not on GPS Spoofing in FANETs - Not systematic literature survey
[47]	A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis	- Studied the GPS Spoofing attacks in UAV, countermeasures techniques like comparing with the measurements of onboard IMUs sensor and signal amplitudes sensor, vision-based techniques, and machine-learning based methods	- Not specific on GPS Spoofing attack
[48]	Towards the Unmanned Aerial Vehicles (UAVs): A Comprehensive Review	- Showcased a comprehensive review on UAVs, types, classifications, security challenges, applications, and standardization - Concentrated on technical details like the types of UAVs, applications, etc.	- No detailed discussions on GPS Spoofing attacks - Not systematic literature survey
[49]	A survey of cyber security threats and solutions for UAV communications and flying Ad-Hoc networks	- Detailed study on UAV communication architecture, routing protocols, and UAV characteristics including the mobility models - Generic view on GPS Spoofing attacks and detection methods are given	- Not specific to GPS Spoofing problem - Not systematic literature survey
*****End of Table XI*****			

TABLE 12. Detailed analysis of the attacker models.

Ref.	Spoofer System	Spoofer Location	Spoofing Technique	Ref.	Spoofer System	Spoofer Location	Spoofing Technique
[51]	Repeater (Ettus USRP)	Remote	Track break	[121]	Simulator (HackRF/ BladeRF/ USR)	Not Available	Track break
[115]	Simulator (SatGen, USRP N210)	Remote	Track break	[122]	Simulator (Spectracom GSG-6 GNSS)	Remote	Track break
[63]	Hardware injection	Onboard	Position denial	[99]	Repeater	Remote	Track break
[77]	Simulator (USRP N210)	Remote	Track break	[73]	Simulator (Fake GPS Location Mobile App)	Remote	Track break
[92]	Repeater	Remote	Track break	[57]	Simulator (BladeRF X40)	Remote	Track break
[59]	Simulator (LabSat3)	Remote	Track break	[104]	Simulator (HackRF)	Remote	Track break
[118]	Simulator (bladeGPS simulator)	Remote	Track break	[74]	Simulator (HackRF)	Remote	Track break
[60]	Hardware Injection	Onboard	Track break	[106]	Hardware Injection	Onboard	Track break
[64]	Hardware Injection	Onboard	Track break	[125]	Simulator HackRF	Onboard	Position denial
[16]	Simulator (BladeRF)	Remote	Track break	[138]	Simulator (BladeRF)	Remote	Position denial
[95]	Repeater	Remote	Position denial	[55]	Repeater	Remote	Position denial
[89]	Repeater	Escort	Track break	[81]	Simulator (Ettus USRP B200)	Remote	Track break
*****End of Table XII*****							

TABLE 13. Summary of defense mechanisms (NA: Not Available).

Ref.	Defense	Description	FANET	Performance Evaluation	Performance Metrics	Open Issues
Onboard Devices: Accelerometers, Gyroscopes, Camera, etc.						
[61]	Detection	Monocular Camera and IMU sensors used to find the velocities of the UAVs and then compared with the velocity obtained using GPS; RMSE values are computed and spoofing is detected if the RMSE goes beyond a specific threshold value.	No	DJI Phantom 4	Latency (5 s)	Continuous camera usage drains battery sooner
[62]	Mitigation	Extension of [61]. UAV stores the image frames it captures during every prefixed time interval and if spoofing is detected, it moves back in the same line. Then, after the same prefixed time interval, it compares the captured image with the stored one for that location. If they match, it moves back from that location and repeats the same process until it reaches the starting location.	No	Not implemented	Not evaluated	- Storage overhead of images - Camera drains battery
[63]	Detection	Compares GPS measurement with Accelerometer and Gyroscope readings.	No	Quadrotor drone, PixhawkTMflight control system	Accuracy (82%)	Accumulative error of Accelerometer and Gyroscope
[64]	Detection	Extension of [63]. GPS data (GPS angle) and gyroscope measurement (Yaw from the Angular Velocity) are used.	No	Quadrotor drone, PixhawkTMflight control system	Accuracy (92%)	Measurement and calculation error problems cause lower Accuracy
[65]	Detection	Measurements from INS and GPS are passed to two Extended Kalman Filters and are used to find relative estimation errors.	No	Numerical Simulation	Precision, Accuracy	Accumulative error of INS lessens Accuracy
[66]	Detection & Mitigation	Works in two phases: 1) the spoofing detection phase using hypothesis test and 2) the trajectory estimation during the spoofing phase using Particle Swarm Optimization Filter (PSOF).	Yes	MATLAB	Accuracy (97%)	Memory Overhead, requires careful consideration of the computational resources and communication bandwidth

TABLE 13. *(Continued.)* **Summary of defense mechanisms (NA: Not Available).**

Ref.	Defense	Description	FANET	Performance Evaluation	Performance Metrics	Open Issues
[67], [70]	Detection	Image/video reels captured by drone camera compared with a pre-defined map by human operator.	No	Simulation: Security-Aware Research Environment for Supervisory Control of Heterogeneous Unmanned Vehicles (RESCHU-SA) experiment platform	Detection rate (80%), False Positive (22%)	Availability of Human Operator is not always possible
[71]	Detection	GPS and IMU fusion for Single UAV and data exchange among other UAVs for FANET scenario with the involvement of GCS.	Yes	Monte Carlo simulations	Time Overhead, Detection Time (8 s), True Positive (98.6%), False Positive, False Negative (miss detection)	GCS might not be always reachable
[73]	Detection	A safety metric that indicates the health status of the UAV and the priority of a component for the overall system security is computed. If the distance covered in the time range is acceptable (based on 80 Km/h speed), it is concluded that the drone is in a stable state.	No	3DR Solo Quadcopter	Node Criticality Index	If there is no noticeable velocity change, the system fails. Also, environmental factors like wind might affect the system
[74]	Detection	Used fusion of the GPS and Optical flow sensors to detect GPS spoofing attacks in UAV. The distance obtained by GPS coordinates of two positions traversed by UAV and the pixel distance of images collected by optical flow sensors at these locations is compared. If the difference exceeds a preset threshold value, the UAV is considered to be spoofed.	No	PX4 open source code for flight control	Latency	Drains battery sooner

TABLE 13. *(Continued.)* **Summary of defense mechanisms (NA: Not Available).**

Ref.	Defense	Description	FANET	Performance Evaluation	Performance Metrics	Open Issues
[75]	Detection	Visual Odometry: the trajectories determined by GPS and those by the onboard camera(s) are locally compared using a moving window. The differences between these trajectories were estimated using the Euclidean Distances between corresponding points, Angle of Distance, and Taxicab Distance between Histogram of Oriented Displacements.	No	DJI Phantom 4 digital camera	Detection Rate, Latency	The method fails to detect in scenarios like darkness, lack of features or texture in the images, etc. Changes in drone velocity might affect the system's performance
[76]	Detection	A GNSS spoofing detection mechanism in UAV swarms using the IMUs and the GNSS (GPS) receivers. Also, an onboard sensor to estimate the relative distance between the drones (like LoRa Sensor) is used.	Yes	Monte Carlo simulations	Accuracy (90%)	The distance between two UAVs are measured by LoRa sensors; however, it is not specified how to be achieved in real-world scenarios
Signal Processing Methods						
[77]	Detection & Mitigation	WiDrone: WiFi Fingerprint location cross-checking technique. Current WiFi Fingerprint is compared with the Destination WiFi Fingerprint, which is already stored in the device. In case of any mismatch, spoofing is detected. The drone flies away from that location and gets a GPS signal and authenticates the destination again using the same procedure.	No	DJI Matrice 100	NA	Do not work well in remote or Mountainous areas, where WiFi signal strength is low
[79]	Detection & Mitigation	The integrity of the signal packet received from the satellites are compared by computing the pseudo-range using the values from different satellites. The discrepancy is found and the faulty satellites are isolated. The signals from five satellites are processed in three groups to detect the faulty host and the common host in all the groups was isolated to mitigate the effects.	No	OMNet++ (UAVSim)	Receiver Autonomous Integrity Monitoring (RAIM) duration (90 s)	Pseudo-range measurement can be affected by atmospheric interference, signal blockage, and receiver errors, which can reduce the Accuracy of the position estimation. So, it is better to be integrated with other means

TABLE 13. *(Continued.)* **Summary of defense mechanisms (NA: Not Available).**

Ref.	Defense	Description	FANET	Performance Evaluation	Performance Metrics	Open Issues
[81]	Detection & Mitigation	Based on the contents and time of arrival traffic advertisements broadcasted by the aircraft for traffic control purpose. An independent infrastructure on the ground analyzes the traffic.	No	Real-world data (OpenSky Network) and simulation	Latency (<2 s), Detection rate (75%), Attacker Localisation (15 minutes)	Communication Overhead with ground
[83]	Detection	5G-assisted method for monitoring the UAVs' positions and live detection of GPS Spoofing attack. The method relies on the Up-link Received Signal Strength (RSS) of signals received at the Cellular base stations on the ground.	No	Python	Detection Rate (95%), False Negative, False Positive	Communication Overhead with ground
[84]	Mitigation	GPS Spoofing attack mitigation mechanism, which tracks the attacker's location and estimate the effective range of the spoofing signals using Extended Kalman Filter (EKF). This allows the UAV to move away from this range within the escape time and avoid sudden sensor drifts.	No	Numerical simulations with Julia Programming Language	NA	To report different performance measures
[85]	Detection	The UAV system is modeled as a Bayesian Network and the GPS signals (Signal-to-Noise ratio, pseudo-range, Doppler shift, etc.) were analyzed to detect the spoofing attack. When a UAV receives a new GPS signal, the attack detector module embedded in the UAV(s) checks the correctness of the signal by propagating signals in the network and estimating the conditional probability in the Bayesian Network.	Yes	MATLAB simulations and SatGrid datasets	Precision, Recall, FPR, Detection Accuracy (96.2%)	The trajectory should be pre-defined; at least two neighbors do follow the same trajectory
[87]	Detection & Mitigation	A trust-based method for detecting colluding GPS Spoofing attacks. The active witness detects and communicates to all one-neighbor nodes in its vicinity. The passive witness, who can also witness the spoofed signal, confirms the attack and notifies the target.	Yes	NS3 simulator	Detection rate 99.88% , False Negative, Detection Accuracy (98.40%)	Method fails if the witness(s) falls in a spoofed location
[89]	Detection & Mitigation	Multiple radars are deployed on the ground and the position, velocity, and time estimate of the signals from the targets are fused with GPS position estimate by the target in a central node. If both tracks are different, GPS Spoofing is detected. Then, the fused data from the radar are fed into the GPS receivers to mitigate the attack.	Yes	Simulation (simulation tool was not mentioned)	RMSE, Detection Accuracy	Deployment of multiple radars across the globe is challenging. Communication Overhead and Security of communication links

TABLE 13. *(Continued.)* **Summary of defense mechanisms (NA: Not Available).**

Ref.	Defense	Description	FANET	Performance Evaluation	Performance Metrics	Open Issues
Cryptographic Methods						
[90]	Detection	Employ Blockchain technology for detecting GNSS spoofing. The Blockchain is maintained as a layer on top of the FANET and the UAVs upload their location information to it. The locational information obtained by the Radio Direction Finding (RDF) antennas of the UAV is compared with the one stored in the Blockchain.	Yes	NA	NA	Byzantine Failure (if one-third or more UAVs spoofed). Computational cost of Blockchain and cryptographic operation
[91]	Prevention	One UAV in the FANET is elected as a leader using some consensus process (based on mission type, flight quality, etc.). The leader gets its GPS position, encrypts it, and then sends it to other drones. The follower(s) drone(s) decrypts the received message and gets the leader's position. The message is appended with additional parameters like propagation delay to compute its true position.	Yes	NA	NA	The battery constraints of the drones for encryption and decryption processes. Additional communication is required among the drones that can affect the performance. Leader can be Single-Point-of-Failure
Game Theory based Methods						
[92]	Detection	Strategic interactions between UAV and the attacker are used to detect GPS spoofing. Kernal Signaling Game model - by analyzing the equilibrium of the game. Perfect Bayesian Equilibrium is attained.	No	Numerical Simulation	Detection Rate, Position drift	Computational Complexity is high
[93]	Detection & Mitigation	Detection: Game Theory (Stackelberg game) - the optimal routes followed by UAV during normal and attack scenarios are modeled using system dynamics. Mitigation: cooperative localization to enable a UAV to determine its location using nearby UAVs instead of the possibly spoofed GPS locations.	Yes	Numerical Simulation	UAV Capture Probability, UAV deflections from the planned routes	Reliability of other UAVs

TABLE 13. *(Continued.)* **Summary of defense mechanisms (NA: Not Available).**

Ref.	Defense	Description	FANET	Performance Evaluation	Performance Metrics	Open Issues
Machine Learning based Methods						
[94]	Detection	SVM is used to detect anomalies. The data fused from different navigation systems are analyzed using SVM and a decision boundary is constructed based on the knowledge of data during normal scenarios (Support Vector Data Description). The system is trained to detect any deviation to detect the attack.	No	MATLAB	False Positive Rates, True Positive Rates, Accuracy, Latency (30 s)	Performance degradation in long attacks with Micro Electro-Mechanical System (MEMS) sensors. The system fails if the attacker knows the actual trajectory by inducing large position errors
[95]	Detection	Supervised machine learning method based on Artificial Neural Network. Different features such as pseudo-range, Doppler shift, and signal-to-noise ratio (SNR) were used to perform the classification of GPS signals.	No	RTKLIB Simulation: Real GPS Signals were used to collect data using SDR RTL-SDR V.3 RTL2832U	False Positive Rates (2.6%), Detection Rates (99.4%), False Negative Rates (0.8%), Accuracy (98.2%)	Not online/real-time detection
[97]	Detection	Recurrent Neural Network (RNN) based approach to identify the behavioral anomaly in UAVs. Reliable normal behaviors are modeled using two scenarios and the UAVs are trained using these models. The Accuracy of the model is enhanced by estimating the angle of arrival and Normalised Root Mean Square Error (NRMSE) that detects the deviation in a real position of the UAV and the position provided by the normal behavior models. If the NRMSE is greater than a prefixed threshold, abnormal behavior is detected.	No	Python and TensorFlow	Accuracy (98.7%), Latency (0.034 s)	Results can be optimized to be inline with real-world scenarios
[99]	Detection & Mitigation	The flight path of the UAV is predicted using the LSTM algorithm, which uses previous flight data. If the deviation between the predicted path and the GPS path exceeds a preset threshold, the path-based detection method is invoked. Path-based detection method uses the position estimated by integrating the velocity obtained from IMU.	No	MATLAB	Detection Latency (3 to 5 s), Detection Ratio (78%)	Works for UAVs with fixed routes only

TABLE 13. *(Continued.)* **Summary of defense mechanisms (NA: Not Available).**

Ref.	Defense	Description	FANET	Performance Evaluation	Performance Metrics	Open Issues
[100]	Detection	Deep learning-based approach that uses satellite images and images captured by UAV cameras to detect spoofing. The satellite images and aerial photos captured by UAV are fed into a deep learning model, which can be onboard or on the ground. The model compares the images and if a mismatch occurs, a spoofing alert is generated.	No	For training and graphics processing NVIDIA® Tesla® V100 GPU with 16GB GPU memory Created SatUAV dataset that combines satellite images (like Google Earth) and those captured using UAV camera	Accuracy, Precision, Recall, F1 score, Time Complexity, and Power Consumption	Cameras drain battery; the images used for comparison might be old/historical images (Google Earth) leading to false alarms
[104]	Detection	An Intrusion Detection System (IDS) that detects GPS Spoofing in UAVs. The method is based on one-class classifiers, which used flight logs as a training dataset. A comparative analysis has been conducted with OC-SVM, Autoencoder Neural Network, and LOF one-class classifiers. The authors used original flight log data as a training dataset.	No	SITL Simulator; UAV Attack Dataset	Accuracy, Detection rate (precision, recall, and F1 score)	One-class classifiers might fail to detect new or previously unseen/untrained GPS spoofing attacks
[106]	Detection	Train the UAVs (both off-board and on-board) based on the GPS and IMU readings. XGBoost machine learning method is used for off-board training and the precision of the learning outcome is further fine-tuned using Genetic Algorithm (GA). The drones were trained onboard using real-time flight log data from the IMU and GPS receiver.	No	Quadrotor drones	Accuracy (93.3%), Latency (1 s)	Computational & Memory Overhead for training two algorithms
[107]	Detection	The statistical properties of the path loss between UAV and nearby Base Station(s) are used to train the Multi-Layer Perceptron (MLP) Model. Three statistical properties were considered (i.e., moment, quartile, and probability distribution difference) and three MLP-based models were designed. If the difference between the actual path loss (provided by the Base Station(s)) and the theoretical path loss (provided by UAV) is greater than a specific threshold value, a spoofing is suspected.	No	Python and TensorFlow	Detection Rate (93%)	MLP models are computationally expensive to be trained on large datasets

TABLE 13. *(Continued.)* **Summary of defense mechanisms (NA: Not Available).**

Ref.	Defense	Description	FANET	Performance Evaluation	Performance Metrics	Open Issues
[108]	Detection	Deep Learning based models using UAV flight logs and telemetry data to detect GPS Spoofing attacks in real-time. The UAV log data for different models are generated and used for training. A classification-based training approach is adopted using Binary Classifiers (BC) that use benign and spoofed data, and Autoencoder-based One-Class Classifiers (OCC) that use only benign data for training.	No	Gazebo Simulator (flight log datasets), PX4 Autopilot firmware with QGroundControl App (UAVs), Intel Neural Computing Stick (NCS2)	Recall, Precision, Accuracy (99.56% with binary classifiers; 99.24% with one-class classifiers), F-1 score	LSTM models are computationally expensive to be trained on large datasets
[111]	Detection	Compared Random Forest (RNF), Gradient Boost (GB), XB, and LightBM (LB) machine learning models to detect GPS Spoofing attacks in UAV.	No	Simulation using Real and Synthesized GPS Signals	Detection Rate, False Positive, False Negative, Accuracy, Latency, Memory Consumption	Availability of labeled dataset, Difficulty of handling new attacker/adversary models
[112]	Detection	A comparative study of three Ensemble based machine learning models - Bagging, Boosting, and Stocking.	No	Simulation with same datasets as in [111]	Detection Rate, False Positive, False Negative, Accuracy, Latency, Memory Consumption	Computational complexity, training time, the models need to be optimized
[113]	Detection	Two techniques (Metric Optimized Dynamic selector and Weighted Metric Optimized Dynamic selector) for selecting the classifier for detecting GPS Spoofing attacks in UAVs. Tested and compared ten machine learning algorithms.	No	MATLAB with 13 GPS signal features from real-time experiments	Accuracy, Detection Rate, False alarm Rate, False Negative Rate, Latency	Computational complexity, training time, the models need to be optimized
		*****End of Table XIII*****				

TABLE 14. Comparative analysis of performance evaluations & additional requirements for proposed solutions. (NA: Not Available).

Ref.	Performance Metrics				Additional Requirements on			
	True Positive	False Positive	Accuracy	Latency	Hardware	Storage	Battery	Other Requirements
Onboard								
[61]	NA	NA	NA	5 s	No	No	High	Favourable atmospheric conditions such as light, wind, fog, etc.
[62]	NA	NA	NA	NA	No	Yes	High	Favourable atmospheric conditions such as light, wind, fog, etc.
[63]	NA	NA	82%	NA	No	No	No	No
[64]	NA	NA	92%	NA	No	No	No	No
[65]	NA	NA	NA	NA	NA	NA	NA	NA
[66]	NA	NA	97%	NA	No	Yes	No	No
[67]	80%	22%	NA	NA	No	No	High	Human intervention; Favourable atmospheric conditions such as light, wind, fog, etc.
[71]	98.6%	NA	NA	8 s	No	No	No	GCS should be always reachable.
[73]	NA	NA	NA	NA	NA	NA	NA	NA
[74]	NA	NA	NA	~ 0 s	No	No	No	No
[75]	NA	NA	NA	NA	NA	NA	NA	NA

TABLE 14. *(Continued.)* Comparative analysis of performance evaluations & additional requirements for proposed solutions. (NA: Not Available).

Ref.	Performance Metrics				Additional Requirements on			
	True Positive	False Positive	Accuracy	Latency	Hardware	Storage	Battery	Other Requirements
[76]	NA	NA	90%	NA	Sensors to find the relative distance between drones (e.g., LoRa).	No	No	No
Signal Processing								
[77]	NA	NA	NA	NA	Yes	NA	NA	WiFi Signal Strength.
[79]	NA	NA	NA	90 s	No	No	No	No
[81]	75%	NA	NA	< 2 s	On ground to analyse signal.	No	No	Communication Overhead with ground.
[83]	$> 95\%$	NA	NA	NA	On ground to analyse signal.	No	No	Communication Overhead with ground.
[84]	NA	NA	NA	NA	NA	NA	NA	NA
[85]	NA	NA	96.2%	NA	No	No	No	No
[87]	99.98%	NA	98.4%	NA	No	No	No	No
[89]	NA	NA	NA	NA	Multiple Radars on ground.	No	No	Secure Communication links between drone and Radars; Communication Overhead.
Cryptographic Methods								
[90]	NA	NA	NA	NA	No	Yes	High	Blockchain Maintenance and communication overhead.
[91]	NA	NA	NA	NA	No	Yes	High	Communication overhead.
Game Theory based Methods								
[92]	NA	NA	NA	NA	No	Yes	No	Attacker and drone controller should have complete information about each other, which might not be always the case.
[93]	NA	NA	NA	NA	No	Yes	No	Attacker and drone controller should have complete information about each other.
Machine Learning based Methods								
[94]	NA	NA	NA	30 s	Computation and Processing Power.	Yes	High	Sufficient amount of diverse and realistic training data.

TABLE 14. *(Continued.)* Comparative analysis of performance evaluations & additional requirements for proposed solutions. (NA: Not Available).

Ref.	Performance Metrics				Additional Requirements on			
	True Positive	False Positive	Accuracy	Latency	Hardware	Storage	Battery	Other Requirements
[95]	99.4%	2.6%	98.2%	NA	Computation and Processing Power.	Yes	High	Sufficient amount of diverse and realistic training data.
[97]	NA	NA	98.7%	0.034 s	Computation and Processing Power.	Yes	High	Sufficient amount of diverse and realistic training data.
[99]	78.8%	NA	NA	3 to 5 s	Computation and Processing Power.	Yes	High	Sufficient amount of diverse and realistic training data.
[100]	95%	NA	NA	$<$ 100 ms	Computation and Processing Power.	Yes	High	Sufficient amount of diverse and realistic training data.
[104]	94.81% (AE) 81.71% (SVM) 58.93% (LOF)	NA	NA	NA	Computation and Processing Power.	Yes	High	Sufficient amount of diverse and realistic training data.
[106]	NA	NA	93.3%	1 s	Computation and Processing Power.	Yes	High	Sufficient amount of diverse and realistic training data.
[107]	93%	NA	NA	NA	Computation and Processing Power.	Yes	High	Sufficient amount of diverse and realistic training data.
[108]	NA	NA	97.79% (BC) 94.98% (OCC)	Time Overhead: BC: 3.986 ms OCC: 4.32 ms	Computation and Processing Power.	Yes	High	Sufficient amount of diverse and realistic training data.
[111]	RNF: 96.23% GB: 95.52% XB: 95.38% LB: 95.38%	RNF: 8.53% GB: 9. 84% XB: 4.30% LB: 4.96%	RNF: 94.07% GB: 91.45% XB: 95.52% LB: 95.23%	RNF: 21.01 ms GB: 6.99 ms XB: 2.00 ms LB: 8.99 ms	Computation and Processing Power.	(In MB) RNF: 1.6 GB: 3.19 XB: 2.63 LB: 2.01	High	Sufficient amount of diverse and realistic training data.
[112]	Ba.: 99.24% Bo.: 99.55% St.: 99.56%	Ba.: 1.07% Bo.: 5.08% St.: 0.03%	Ba.: 95.28% Bo.: 94.61% St.: 95.43%	Ba.: 0.02 ms Bo.: 0.01 ms% St.: 0.24 ms	Computation and Processing Power.	(In MB) Ba.: 190.4 Bo.: 190.5 St.: 191.3%	High	Sufficient amount of diverse and realistic training data.
[113]	98.9%	1.56%	99.6%	1.24 s	Computation and Processing Power.	Yes	High	Sufficient amount of diverse and realistic training data.
*****End of Table XIV*****								

F. SUMMARY

To summarize, the following were the research gaps identified as a result of this study:

- The minimum spoofer-to-target distance, the count of victims as well as the number of malicious nodes that are required to launch the attack were not well addressed in the existing works. These parameters should be taken into account when designing future research solutions.
- Defense approaches to mitigate and prevent GPS Spoofing attacks in FANETs needs more attention. So far, the approaches to detect the attacks have been the main focus and proposed most.
- From Fig. 17, it can be observed that machine learning and onboard devices were mostly relied on by the existing approaches to address the problem of GPS Spoofing attacks in UAVs, which is then followed by signal processing approaches. Since the machine-learning approaches impose high computational overhead on drones, they are not desirable for real-time applications; where FANET cannot invest considerable resources for complex computations due to its limited computational power and battery constraints. Thus, it is recommended that future research should focus on onboard devices and signal processing approaches to address the problem of GPS Spoofing attacks in FANETs without imposing any additional overhead. Leveraging onboard devices is promising as it does not require any infrastructural changes in the drones.
- Researchers should consider publishing more comprehensive and thorough articles in reputed journals, that address the threat of GPS Spoofing in FANETs.
- From Fig. 20, it is evident that the research works, which considered a FANET environment where multiple UAVs collaborate and exchange information, is not well addressed. Thus, future research works should focus on addressing GPS Spoofing attacks in the FANET environment by leveraging the unique characteristics of FANET such as high mobility, limited battery life, frequent topology change, and the information exchanged among the drones.
- The latest drones that are capable of forming Ad-Hoc wireless networks (the list is shown in Table 9) need to be investigated to conduct proof-of-concept implementation of future solutions. Existing literature lacks such works that used proof-of-concept evaluation in the FANET scenario. The defense mechanisms against GPS Spoofing attacks on single drones only are evaluated using proof-of-concept implementation. Some articles have conducted simulation experiments, however, their simulation experimental setup don't reflect the real-world environment where the drones operate. The names and specs of the drones and/or simulators used in the proof-of-concept implementation or simulation experiments should be clearly identified and justified.
- The mobility models and communication propagation models that are followed or used by drones are not well considered in the proposed solutions. The simulation platforms that can employ the mobility and propagation models of drones in FANETs need to be investigated.
- From Fig. 23, TPR, FPR, detection latency, and Accuracy are most widely used in the experiments of the proposed solutions. Apart from these, considering the unique characteristics of FANET, future works should report as many metrics as possible. For example, the ratio of the number of victimized UAVs to the total number of UAVs can be one metric to be considered.

VII. CONCLUSION

In this paper, a systematic literature survey of the articles that addressed GPS Spoofing attacks in FANETs has been conducted. This survey aims to enhance the understanding of the existing works and propose future scopes in securing FANETs against GPS Spoofing attacks. The GPS Spoofing attacks in FANETs have been viewed from four perspectives, namely, GPS Spoofing techniques, GPS Spoofing defense mechanisms, GPS Spoofing as-defense mechanisms, and GPS Spoofing Impact and Vulnerability. A taxonomy of the mechanisms that addressed the threat of GPS Spoofing attacks in the existing literature has been portrayed. Based on the adopted survey methodology, eight research questions were formulated. Moreover, 37 research articles on detection, mitigation, and prevention of GPS Spoofing attacks in UAVs that were published between 2017 and 2022 were extracted for deep investigation. Specifically, in terms of the basis of the defense approach, the attacker models, and the performance evaluation mechanisms and metrics. The research gaps in the proposed methods were identified and future directions for the researchers have been recommended. For future works, we aim to address some of the research gap(s) identified in this study and propose robust solutions to defend against the threat of GPS Spoofing attacks in FANETs.

APPENDIX: DETAILED TABLES FOR ARTICLES

See Tables 11–14.

REFERENCES

[1] B. O'Connell. *U.S. News & World Report: 7 Drone Stocks to Watch for 2023*. Accessed: Dec. 29, 2022. [Online]. Available: https://money.usnews.com/investing/stock-market-news/slideshows/drone-stocks-to-consider-as-the-technology-soars
[2] S. J. Kim and G. J. Lim, "Drone-aided border surveillance with an electrification line battery charging system," *J. Intell. Robotic Syst.*, vol. 92, nos. 3–4, pp. 657–670, Dec. 2018.
[3] B. Rabta, C. Wankmüller, and G. Reiner, "A drone fleet model for last-mile distribution in disaster relief operations," *Int. J. Disaster Risk Reduction*, vol. 28, pp. 107–112, Jun. 2018.
[4] I. Bisio, C. Garibotto, H. Haleem, F. Lavagetto, and A. Sciarrone, "A systematic review of drone based road traffic monitoring system," *IEEE Access*, vol. 10, pp. 101537–101555, 2022.
[5] L. Tang and G. Shao, "Drone remote sensing for forestry research and practices," *J. Forestry Res.*, vol. 26, no. 4, pp. 791–797, Dec. 2015.
[6] E. Yanmaz, "Positioning aerial relays to maintain connectivity during drone team missions," *Ad Hoc Netw.*, vol. 128, Apr. 2022, Art. no. 102800.
[7] M. Simma, H. Mjøen, and T. Boström, "Measuring wind speed using the internal stabilization system of a quadrotor drone," *Drones*, vol. 4, no. 2, p. 23, Jun. 2020.

[8] C. Kyrkou and T. Theocharides, "EmergencyNet: Efficient aerial image classification for drone-based emergency monitoring using atrous convolutional feature fusion," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 13, pp. 1687–1699, 2020.

[9] G. Skorobogatov, C. Barrado, and E. Salamí, "Multiple UAV systems: A survey," *Unmanned Syst.*, vol. 8, no. 2, pp. 149–169, Apr. 2020.

[10] W. Zafar and B. M. Khan, "Flying ad-hoc networks: Technological and social implications," *IEEE Technol. Soc. Mag.*, vol. 35, no. 2, pp. 67–74, Jun. 2016.

[11] A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, "FANET: Communication, mobility models and security issues," *Comput. Netw.*, vol. 163, Nov. 2019, Art. no. 106877.

[12] A. Nadeem, T. Alghamdi, A. Yawar, A. Mehmood, and M. Siddiqui, "A review and classification of flying ad-hoc network (FANET) routing strategies," *J. Basic Appl. Sci. Res.*, vol. 8, no. 3, pp. 1–8, 2018.

[13] M. Campion, P. Ranganathan, and S. Faruque, "Notice of removal: A review and future directions of UAV swarm communication architectures," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, May 2018, pp. 903–908.

[14] M. I. B. Azevedo, C. Coutinho, E. M. Toda, T. C. Carvalho, and J. Jailton, "Wireless communications challenges to flying ad hoc networks (FANET)," in *Mobile Computing*, J. H. Ortiz, Ed. Rijeka, Croatia: IntechOpen, 2019, ch. 1, doi: 10.5772/intechopen.86544.

[15] M. A. Khan, A. Safi, I. M. Qureshi, and I. U. Khan, "Flying ad-hoc networks (FANETs): A review of communication architectures, and routing protocols," in *Proc. 1st Int. Conf. Latest trends Electr. Eng. Comput. Technol. (INTELLECT)*, Nov. 2017, pp. 1–9.

[16] E. Horton and P. Ranganathan, "Development of a GPS spoofing apparatus to attack a DJI Matrice 100 quadcopter," *J. Global Positioning Syst.*, vol. 16, no. 1, pp. 1–11, Dec. 2018.

[17] D. Shepard, J. A. Bhatti, and T. E. Humphreys. (2012). *Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle*. Accessed: Dec. 29, 2022. [Online]. Available: https://www.gpsworld.com/drone-hack/

[18] D. P. Shepard, J. Bhatti, and T. Humphreys, "Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle," *GPS World*, vol. 23, pp. 30–33, Aug. 2012.

[19] T. Humphreys, *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing*. Austin, TX, USA: Univ. Texas Austin, Jul. 2012, pp. 1–16.

[20] D. Goward. *GPS Spoofing Incident Points to Fragility of Navigation Satellites*. Accessed: Aug. 2017. [Online]. Available: https://www.nationaldefensemagazine.org/articles/2017/8/22/viewpoint-gps-spoofing-incident-points-to-fragility-of-navigation-satellites

[21] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," *EBSE Tech. Rep.*, vol. 2, pp. 1–56, Jan. 2007.

[22] N. Cast. (Dec. 2022). *How Drone GPS Navigation Works*. [Online]. Available: https://www.remoteflyer.com/how-drone-gps-navigation-works/

[23] *Gps.Gov, Official U.S. Government Information About the Global Positioning System (GPS) and Related Topics Trilateration Exercise*. Accessed: Nov. 25, 2022. [Online]. Available: https://www.gps.gov/multimedia/tutorials/trilateration/

[24] F. Pasandideh, J. P. J. da Costa, R. Kunst, N. Islam, W. Hardjawana, and E. Pignaton de Freitas, "A review of flying ad hoc networks: Key characteristics, applications, and wireless technologies," *Remote Sens.*, vol. 14, no. 18, p. 4459, Sep. 2022.

[25] J. Peng, "Radio propagation models in wireless networks of unmanned aerial vehicles," *Int. J. Comput. Netw. Commun.*, vol. 7, no. 3, pp. 119–126, May 2015.

[26] A. H. Wheeb, R. Nordin, A. A. Samah, M. H. Alsharif, and M. A. Khan, "Topology-based routing protocols and mobility models for flying ad hoc networks: A contemporary review and future research directions," *Drones*, vol. 6, no. 1, p. 9, Dec. 2021.

[27] A. Guillen-Perez and M.-D. Cano, "Flying ad hoc networks: A new domain for network communications," *Sensors*, vol. 18, no. 10, p. 3571, Oct. 2018.

[28] F. Noor, M. A. Khan, A. Al-Zahrani, I. Ullah, and K. A. Al-Dhlan, "A review on communications perspective of flying ad-hoc networks: Key enabling wireless technologies, applications, challenges and open research topics," *Drones*, vol. 4, no. 4, p. 65, Sep. 2020.

[29] E. A. Marconato, J. A. Maxa, D. F. Pigatto, A. S. R. Pinto, N. Larrieu, and K. R. L. J. C. Branco, "IEEE 802.11n vs. IEEE 802.15.4: A study on communication QoS to provide safe FANETs," in *Proc. 46th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshop (DSN-W)*, Jun. 2016, pp. 184–191.

[30] I. Bekmezci, O. K. Sahingoz, and S. Temel, "Flying ad-hoc networks (FANETs): A survey," *Ad Hoc Netw.*, vol. 11, no. 3, pp. 1254–1270, May 2013.

[31] Y.-H. Ho and Y.-J. Tsai, "Open collaborative platform for multi-drones to support search and rescue operations," *Drones*, vol. 6, no. 5, p. 132, May 2022.

[32] Y. Li and C. Liu, "Applications of multirotor drone technologies in construction management," *Int. J. Construction Manage.*, vol. 19, no. 5, pp. 401–412, Sep. 2019.

[33] P. Radoglou-Grammatikis, P. Sarigiannidis, T. Lagkas, and I. Moscholios, "A compilation of UAV applications for precision agriculture," *Comput. Netw.*, vol. 172, May 2020, Art. no. 107148.

[34] E. Barmpounakis and N. Geroliminis, "On the new era of urban traffic monitoring with massive drone data: The pNEUMA large-scale field experiment," *Transp. Res. C, Emerg. Technol.*, vol. 111, pp. 50–71, Feb. 2020.

[35] C. Paucar, L. Morales, K. Pinto, M. Sánchez, R. Rodríguez, M. Gutierrez, and L. Palacios, "Use of drones for surveillance and reconnaissance of military areas," in *Proc. Int. Conf. Res. Appl. Defense Secur.* Cham, Switzerland: Springer, 2018, pp. 119–132.

[36] S. M. S. M. Daud, M. Y. P. M. Yusof, C. C. Heo, L. S. Khoo, M. K. C. Singh, M. S. Mahmood, and H. Nawawi, "Applications of drone in disaster management: A scoping review," *Sci. Justice*, vol. 62, no. 1, pp. 30–42, Jan. 2022.

[37] H. Chen, Z. Hu, and S. Solak, "Improved delivery policies for future drone-based delivery systems," *Eur. J. Oper. Res.*, vol. 294, no. 3, pp. 1181–1201, Nov. 2021.

[38] S. J. Kim, Y. Jeong, S. Park, K. Ryu, and G. Oh, "A survey of drone use for entertainment and AVR (augmented and virtual reality)," in *Augmented Reality and Virtual Reality: Empowering Human, Place and Business*, T. Jung and M. C. tom Dieck, Eds. Cham, Switzerland: Springer, 2018, pp. 339–352, doi: 10.1007/978-3-319-64027-3_23.

[39] M. R. Manesh and N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions," *Comput. Secur.*, vol. 85, pp. 386–401, Aug. 2019.

[40] A. Hamza, U. Akram, A. Samad, S. N. Khosa, R. Fatima, and M. F. Mushtaq, "Unmaned aerial vehicles threats and defence solutions," in *Proc. IEEE 23rd Int. Multitopic Conf. (INMIC)*, Nov. 2020, pp. 1–6.

[41] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: A survey," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 95–101, Feb. 2020.

[42] A. I. Hentati and L. C. Fourati, "Comprehensive survey of UAVs communication networks," *Comput. Standards Interface*, vol. 72, Oct. 2020, Art. no. 103451.

[43] E. Ranyal and K. Jain, "Unmanned aerial vehicle's vulnerability to GPS spoofing a review," *J. Indian Soc. Remote Sens.*, vol. 49, no. 3, pp. 585–591, 2020.

[44] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, N. C. Luong, D. Niyato, F. R. Yu, and M. Guizani, "Fast, reliable, and secure drone communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2802–2832, 4th Quart., 2021.

[45] V. Chamola, P. Kotesh, A. Agarwal, N. Gupta, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad Hoc Netw.*, vol. 111, Feb. 2021, Art. no. 102324.

[46] F. Alrefaei, A. Alzahrani, H. Song, and S. Alrefaei, "A survey on the jamming and spoofing attacks on the unmanned aerial vehicle networks," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Jun. 2022, pp. 1–7.

[47] A. Rugo, C. A. Ardagna, and N. E. Ioini, "A security review in the UAVNet era: Threats, countermeasures, and gap analysis," *ACM Comput. Surv.*, vol. 55, no. 1, pp. 1–35, Jan. 2022.

[48] S. A. H. Mohsan, M. A. Khan, F. Noor, I. Ullah, and M. H. Alsharif, "Towards the unmanned aerial vehicles (UAVs): A comprehensive review," *Drones*, vol. 6, no. 6, p. 147, Jun. 2022.

[49] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," *Ad Hoc Netw.*, vol. 133, Aug. 2022, Art. no. 102894.

[50] P. Bethi, S. Pathipati, and P. Aparna, "Stealthy GPS spoofing: Spoofer systems, spoofing techniques and strategies," in *Proc. IEEE 17th India Council Int. Conf. (INDICON)*, Dec. 2020, pp. 1–7.

[51] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 134–139, Aug. 2017.
[52] *Ettus Research*. Accessed: Dec. 29, 2022. [Online]. Available: https://www.ettus.com/
[53] *Gnu Radio: Free & Open Source Radio Ecosystem*. Accessed: Dec. 29, 2022. [Online]. Available: https://www.gnuradio.org/
[54] *Software-Defined GPS Signal Simulator*. Accessed: Dec. 29, 2022. [Online]. Available: https://github.com/osqzss/gps-sdr-sim
[55] Y. Guo, M. Wu, K. Tang, J. Tie, and X. Li, "Covert spoofing algorithm of UAV based on GPS/INS-integrated navigation," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6557–6564, Jul. 2019.
[56] M. Ceccato, F. Formaggio, and S. Tomasin, "Spatial GNSS spoofing against drone swarms with multiple antennas and Wiener filter," *IEEE Trans. Signal Process.*, vol. 68, pp. 5782–5794, 2020.
[57] J. Aru Saputro, E. Egistian Hartadi, and M. Syahral, "Implementation of GPS attacks on DJI phantom 3 standard drone as a security vulnerability test," in *Proc. 1st Int. Conf. Inf. Technol., Adv. Mech. Electr. Eng. (ICITAMEE)*, Oct. 2020, pp. 95–100.
[58] Z. Wang, H. Wang, and N. Cao, "Research on spoofing jamming of integrated navigation system on UAV," in *Artificial Intelligence and Security*, X. Sun, X. Zhang, Z. Xia, and E. Bertino, Eds. Cham, Switzerland: Springer, 2021, pp. 3–13.
[59] V. Dey, V. Pudi, A. Chattopadhyay, and Y. Elovici, "Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study," in *Proc. 31st Int. Conf. VLSI Design 17th Int. Conf. Embedded Syst. (VLSID)*, Jan. 2018, pp. 398–403.
[60] D. Mendes, N. Ivaki, and H. Madeira, "Effects of GPS spoofing on unmanned aerial vehicles," in *Proc. IEEE 23rd Pacific Rim Int. Symp. Depend. Comput. (PRDC)*, Dec. 2018, pp. 155–160.
[61] Y. Qiao, Y. Zhang, and X. Du, "A vision-based GPS-spoofing detection method for small UAVs," in *Proc. 13th Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2017, pp. 312–316.
[62] D. He, Y. Qiao, S. Chan, and N. Guizani, "Flight security and safety of drones in airborne fog computing systems," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 66–71, May 2018.
[63] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, "Efficient drone hijacking detection using onboard motion sensors," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2017, pp. 1414–1419.
[64] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, "An efficient UAV hijacking detection method using onboard inertial measurement unit," *ACM Trans. Embedded Comput. Syst.*, vol. 17, no. 6, pp. 1–19, Nov. 2018.
[65] S. Leyuan, H. Wende, Z. Yifan, W. Yueke, and Y. Jun, "GPS spoofing detection of unmanned aerial vehicles by dynamics identification," in *Proc. IEEE CSAA Guid., Navigat. Control Conf. (CGNCC)*, Aug. 2018, pp. 1–6.
[66] M. Majidi, A. Erfanian, and H. Khaloozadeh, "A new approach to estimate true position of unmanned aerial vehicles in an INS/GPS integration system in GPS spoofing attack conditions," *Int. J. Autom. Comput.*, vol. 15, no. 6, pp. 747–760, Dec. 2018.
[67] H. Zhu, M. Elfar, M. Pajic, Z. Wang, and M. L. Cummings, "Human augmentation of UAV cyber-attack detection," in *Augmented Cognition: Users Contexts*, D. D. Schmorrow and C. M. Fidopiastis, Eds. Cham, Switzerland: Springer, 2018, pp. 154–167.
[68] M. Elfar, H. Zhu, A. Raghunathan, Y. Y. Tay, J. Wubbenhorst, M. L. Cummings, and M. Pajic, "WiP abstract: Platform for security-aware design of human-on-the-loop cyber-physical systems," in *Proc. ACM/IEEE 8th Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Apr. 2017, pp. 93–94.
[69] M. Pajic. *RESCHU-SA*. Accessed: Dec. 29, 2022. [Online]. Available: https://cpsl.pratt.duke.edu/research/securityaware-human-loop-cps
[70] H. Zhu, M. L. Cummings, M. Elfar, Z. Wang, and M. Pajic, "Operator strategy model development in UAV hacking detection," *IEEE Trans. Human-Mach. Syst.*, vol. 49, no. 6, pp. 540–549, Dec. 2019.
[71] C. Liang, M. Miao, J. Ma, H. Yan, Q. Zhang, and X. Li, "Detection of global positioning system spoofing attack on unmanned aerial vehicle system," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 7, pp. 123–139, Mar. 2022.
[72] *Monte Carlo Method*. Accessed: Sep. 22, 2022. [Online]. Available: https://en.wikipedia.org/wiki/Monte_Carlo_method
[73] I. G. Ferrão, S. A. da Silva, D. F. Pigatto, and K. R. L. J. C. Branco, "GPS spoofing: Detecting GPS fraud in unmanned aerial vehicles," in *Proc. Latin Amer. Robot. Symp. (LARS), Brazilian Symp. Robot. (SBR) Workshop Robot. Educ. (WRE)*, Nov. 2020, pp. 1–6.
[74] L. Meng, S. Ren, G. Tang, C. Yang, and W. Yang, "UAV sensor spoofing detection algorithm based on GPS and optical flow fusion," in *Proc. 4th Int. Conf. Cryptogr., Secur. Privacy*, Jan. 2020, pp. 146–151.
[75] M. Varshosaz, A. Afary, B. Mojaradi, M. Saadatseresht, and E. G. Parmehr, "Spoofing detection of civilian UAVs using visual odometry," *ISPRS Int. J. Geo-Inf.*, vol. 9, no. 1, p. 6, Dec. 2019.
[76] S. Hacohen, O. Medina, T. Grinshpoun, and N. Shvalb, "Improved GNSS localization and Byzantine detection in UAV swarms," *Sensors*, vol. 20, no. 24, p. 7239, Dec. 2020.
[77] F. Xiao, M. Zhou, Y. Liye, J. Yang, and Q. Wang, "Poster: Enabling secure location authentication in drone," in *Proc. 23rd Annu. Int. Conf. Mobile Comput. Netw.*, Oct. 2017, pp. 600–602.
[78] *USRP n210*. Accessed: Dec. 29, 2022. [Online]. Available: https://www.ettus.com/all-products/un210-kit/
[79] A. Javaid, F. Jahan, and W. Sun, "Analysis of global positioning system-based attacks and a novel global positioning system spoofing detection/mitigation algorithm for unmanned aerial vehicle simulation," *Simulation*, vol. 93, pp. 427–441, May 2017.
[80] *OMNeT++: Discrete Event Simulator*. Accessed: Dec. 29, 2022. [Online]. Available: https://omnetpp.org/
[81] K. Jansen, M. Schäfer, D. Moser, V. Lenders, C. Pöpper, and J. Schmitt, "Crowd-GPS-sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 1018–1031.
[82] *Opensky Network : Open Air Traffic Data for Research*. Accessed: Dec. 29, 2022. [Online]. Available: https://opensky-network.org
[83] Y. Dang, C. Benzaíd, Y. Shen, and T. Taleb, "GPS spoofing detector with adaptive trustable residence area for cellular based-UAVs," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.
[84] W. Wan, H. Kim, N. Hovakimyan, L. Sha, and P. G. Voulgaris, "A safety constrained control framework for UAVs in GPS denied environment," in *Proc. 59th IEEE Conf. Decis. Control (CDC)*, Dec. 2020, pp. 214–219.
[85] C. Titouna and F. Naït-Abdesselam, "A lightweight security technique for unmanned aerial vehicles against GPS spoofing attack," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2021, pp. 819–824.
[86] M. Foruhandeh, R. G. A. Zubair Mohammed, G. Kildow, and P. Berges. *SatGrid Dataset, Realtime Genuine and Spoofing Traces of GPS Signals Collected at Different Geographical Locations, Times and Environmental Conditions*. Accessed: Sep. 22, 2022. [Online]. Available: https://figshare.com/articles/dataset/SatGrid
[87] M. Bada, D. E. Boubiche, N. Lagraa, C. A. Kerrache, M. Imran, and M. Shoaib, "A policy-based solution for the detection of colluding GPS-spoofing attacks in FANETs," *Transp. Res. A, Policy Pract.*, vol. 149, pp. 300–318, Jul. 2021.
[88] *Network Simulator-3 (NS-3)*. Accessed: Dec. 29, 2022. [Online]. Available: https://www.nsnam.org/
[89] B. Pardhasaradhi and L. R. Cenkeramaddi, "GPS spoofing detection and mitigation for drones using distributed radar tracking and fusion," *IEEE Sensors J.*, vol. 22, no. 11, pp. 11122–11134, Jun. 2022.
[90] R. Han, L. Bai, J. Liu, and P. Chen, "Blockchain-based GNSS spoofing detection for multiple UAV systems," *J. Commun. Inf. Netw.*, vol. 4, no. 2, pp. 81–88, Jun. 2019.
[91] M. Kara, A. Laouid, A. Bounceur, M. Hammoudeh, M. Alshaikh, and R. Kebache, "Semi-decentralized model for drone collaboration on secure measurement of positions," in *Proc. 5th Int. Conf. Future Netw. Distrib. Syst.*, Dec. 2021, pp. 64–69.
[92] T. Zhang and Q. Zhu, "Strategic defense against deceptive civilian GPS spoofing of unmanned aerial vehicles," in *Decision and Game Theory for Security*, S. Rass, B. An, C. Kiekintveld, F. Fang, and S. Schauer, Eds. Cham, Switzerland: Springer, 2017, pp. 213–233.
[93] A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2840–2854, Apr. 2020.
[94] G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, and A. Pescapè, "A SVM-based detection approach for GPS spoofing attacks to UAV," in *Proc. 23rd Int. Conf. Autom. Comput. (ICAC)*, Sep. 2017, pp. 1–11.

[95] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of GPS spoofing attacks on unmanned aerial systems," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–6.

[96] T. Takasu. *RTKLIB: An Open Source Program Package for GNSS Positioning*. Accessed: Dec. 29, 2022. [Online]. Available: https://rtklib.com/rtklib.html

[97] K. Xiao, J. Zhao, Y. He, C. Li, and W. Cheng, "Abnormal behavior detection scheme of UAV using recurrent neural networks," *IEEE Access*, vol. 7, pp. 110293–110305, 2019.

[98] *Tensorflow*. Accessed: Dec. 29, 2022. [Online]. Available: https://www.tensorflow.org/

[99] S. Wang, J. Wang, C. Su, and X. Ma, "Intelligent detection algorithm against UAVs' GPS spoofing attack," in *Proc. IEEE 26th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2020, pp. 382–389.

[100] N. Xue, L. Niu, X. Hong, Z. Li, L. Hoffaeller, and C. Pöpper, "DeepSIM: GPS spoofing detection on UAVs using satellite imagery matching," in *Proc. Annu. Comput. Secur. Appl. Conf.*, Dec. 2020, pp. 304–319.

[101] Wangxiaodiu. *Wangxiaodiu/Deepsim: Source Code for Acsac Paper. Deepsim: GPS Spoofing Detection on UAVs Using Satellite Imagery Matching*. Accessed: Dec. 29, 2022. [Online]. Available: https://github.com/wangxiaodiu/DeepSim

[102] *Sensefly Drone Dataset*. Accessed: Dec. 29, 2022. [Online]. Available: https://www.sensefly.com/education/datasets/

[103] A. Paszke, S. Gross, S. Chintala, G. Chanan, E. Yang, Z. DeVito, Z. Lin, A. Desmaison, L. Antiga, and A. Lerer, "Automatic differentiation in PyTorch," in *Proc. NIPS Workshop Autodiff*, 2017, pp. 1–4.

[104] J. Whelan, T. Sangarapillai, O. Minawi, A. Almehmadi, and K. El-Khatib, "Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles," in *Proc. 16th ACM Symp. QoS Secur. Wireless Mobile Netw.*, Nov. 2020, pp. 23–28.

[105] J. Whelan, T. Sangarapillai, O. Minawi, A. Almehmadi, and K. El-Khatib, "UAV attack dataset," IEEE Dataport, 2020, doi: 10.21227/00dg-0d12.

[106] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, "Efficient drone hijacking detection using two-step GA-XGBoost," *J. Syst. Archit.*, vol. 103, Feb. 2020, Art. no. 101694.

[107] Y. Dang, C. Benzaïd, B. Yang, and T. Taleb, "Deep learning for GPS spoofing detection in cellular-enabled UAV systems," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Oct. 2021, pp. 501–506.

[108] R. A. Agyapong, M. Nabil, A. Nuhu, M. I. Rasul, and A. Homaifar, "Efficient detection of GPS spoofing attacks on unmanned aerial vehicles using deep learning," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Dec. 2021, pp. 01–08.

[109] O. Robotics. *Gazebo*. Accessed: Dec. 29, 2022. [Online]. Available: https://gazebosim.org

[110] Intel. *Intel Neural Compute Stick 2*. Accessed: Dec. 29, 2022. [Online]. Available: https://www.intel.com/content/dam/support/us/en/documents/boardsandkits/neural-compute-sticks

[111] G. Aissou, H. O. Slimane, S. Benouadah, and N. Kaabouch, "Tree-based supervised machine learning models for detecting GPS spoofing attacks on UAS," in *Proc. IEEE 12th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Dec. 2021, pp. 0649–0653.

[112] A. Gasimova, T. T. Khoei, and N. Kaabouch, "A comparative analysis of the ensemble models for detecting GPS spoofing attacks on UAVs," in *Proc. IEEE 12th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2022, pp. 310–315.

[113] T. T. Khoei, S. Ismail, and N. Kaabouch, "Dynamic selection techniques for detecting GPS spoofing attacks on UAVs," *Sensors*, vol. 22, no. 2, p. 662, Jan. 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/2/662

[114] MathWorks. *MATLAB*. Accessed: Dec. 29, 2022. [Online]. Available: https://www.mathworks.com/products/MATLAB.html

[115] N. Shijith, P. Poornachandran, V. G. Sujadevi, and M. M. Dharmana, "Spoofing technique to counterfeit the GPS receiver on a drone," in *Proc. Int. Conf. Technol. Advancements Power Energy (TAP Energy)*, Dec. 2017, pp. 1–3.

[116] *Satgen Software*. Accessed: Dec. 29, 2022. [Online]. Available: https://www.labsat.co.uk/index.php/en/products/satgen-simulator-software

[117] J. Gaspar, R. Ferreira, P. Sebastião, and N. Souto, "Capture of UAVs through GPS spoofing," in *Proc. Global Wireless Summit (GWS)*, Nov. 2018, pp. 21–26.

[118] J. Gaspar, R. Ferreira, P. Sebastião, and N. Souto, "Capture of UAVs through GPS spoofing using low-cost SDR platforms," *Wireless Pers. Commun.*, vol. 115, no. 4, pp. 2729–2754, Dec. 2020.

[119] M. Li, Y. Kou, Y. Xu, and Y. Liu, "Design and field test of a GPS spoofer for UAV trajectory manipulation," in *Proc. China Satell. Navigat. Conf. (CSNC)*, J. Sun, C. Yang, and S. Guo, Eds. Singapore: Springer, 2018, pp. 161–173.

[120] G. Sheng, M. Min, L. Xiao, and S. Liu, "Reinforcement learning-based control for unmanned aerial vehicles," *J. Commun. Inf. Netw.*, vol. 3, no. 3, pp. 39–48, Sep. 2018.

[121] D. He, H. Liu, S. Chan, and M. Guizani, "How to govern the non-cooperative amateur drones?" *IEEE Netw.*, vol. 33, no. 3, pp. 184–189, May 2019.

[122] J. Noh, Y. Kwon, Y. Son, H. Shin, D. Kim, J. Choi, and Y. Kim, "Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing," *ACM Trans. Privacy Secur.*, vol. 22, no. 2, pp. 1–26, Apr. 2019.

[123] *GSG 5/6 Series GPS/GNSS Simulators*. Accessed: Sep. 22, 2022. [Online]. Available: https://www.orolia.com/product/gsg-5-6-series-gps-gnss-simulators/

[124] A. D. Team. *SITL Simulator (Software in the Loop)*. Accessed: Dec. 29, 2022. [Online]. Available: https://ardupilot.org/dev/docs/sitl-simulator-software-in-the-loop.html

[125] H. Alamleh and N. Roy, "Manipulating GPS signals to determine the launch location of drones in rescue mode," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Apr. 2021, pp. 1–5.

[126] *Labsat 3*. Accessed: Dec. 29, 2022. [Online]. Available: https://www.labsat.co.uk/index.php/en/products/labsat-3

[127] R. Shirani, M. St-Hilaire, T. Kunz, Y. Zhou, J. Li, and L. Lamont, "On the delay of reactive-greedy-reactive routing in unmanned aeronautical ad-hoc networks," *Proc. Comput. Sci.*, vol. 10, pp. 535–542, Jan. 2012.

[128] M. Iordanakis, D. Yannis, K. Karras, G. Bogdos, G. Dilintas, M. Amirfeiz, G. Colangelo, and S. Baiotti, "Ad-hoc routing protocol for aeronautical mobile ad-hoc networks," in *Proc. 5th Int. Symp. Commun. Syst., Netw. Digit. signal Process. (CSNDSP)*, 2006, pp. 1–5.

[129] *DJI Matrice 100*. Accessed: Apr. 18, 2023. [Online]. Available: https://www.dji.com/ae/matrice100/info

[130] *DJI Phantom 4 Pro 100*. Accessed: Apr. 18, 2023. [Online]. Available: https://www.dji.com/ae/phantom-4-pro

[131] U. S. International. *3DR Solo*. Accessed: Apr. 18, 2023. [Online]. Available: https://uavsystemsinternational.com/products/3dr-solo-drone

[132] *DJI Mavic 3*. Accessed: Apr. 18, 2023. [Online]. Available: https://www.dji.com/ae/mavic-3

[133] ModalAI. *Modalai VOXL*. Accessed: Apr. 18, 2023. [Online]. Available: https://www.modalai.com/products/voxl-m500?variant=41019913764915

[134] Skydio. *Skdio 2+*. Accessed: Apr. 18, 2023. [Online]. Available: https://www.skydio.com/skydio-2-plus

[135] Parrot. *Parrot Anafi USA*. Accessed: Apr. 18, 2023. [Online]. Available: https://www.parrot.com/en/drones/anafi-usa

[136] D. Broyles, A. Jabbar, and J. Sterbenz, "Design and analysis of a 3–D Gauss–Markov mobility model for highly-dynamic airborne networks," Jan. 2010, pp. 1–10.

[137] *SATUAV*. Accessed: Dec. 29, 2022. [Online]. Available: https://github.com/wangxiaodiu/DeepSim

[138] S. P. Arteaga, L. A. M. Hernández, G. S. Pérez, A. L. S. Orozco, and L. J. G. Villalba, "Analysis of the GPS spoofing vulnerability in the drone 3DR solo," *IEEE Access*, vol. 7, pp. 51782–51789, 2019.

ALA ALTAWEEL (Member, IEEE) received the B.Sc. degree in computer engineering from the Jordan University of Science and Technology, Jordan, in 2006, the M.S. degree in information technology from the University of Stuttgart, Germany, in 2009, and the Ph.D. degree in computer engineering from Texas A&M University, USA, in 2019. He is currently an Assistant Professor with the Computer Engineering Department, University of Sharjah. His research interests include cybersecurity, wireless networks and computer security, distributed systems, and edge computing. Before joining the University of Sharjah, he was a Postdoctoral Researcher with the Laboratory for Embedded & Networked Sensor Systems, Texas A&M University. He was a recipient of the Best Paper Award

of the 19th IEEE International Conference on Mobile Ad-Hoc and Smart Systems (IEEE MASS 2022), the Junior Researcher Travel Grant of the IEEE Conference on Communications and Network Security (CNS 2019), the Jordanian Royal Academic Sponsorship, the King Abdullah University of Science and Technology's Fellowship (declined), and the Irbid Secondary School's Outstanding Student Award.

HENA MUKKATH received the B.Tech. degree in computer science and engineering from the Cochin University of Science and Technology, Kerala, India, in 2011, and the M.Tech. degree in software technology and the Ph.D. degree in information technology and engineering from VIT Vellore, Tamil Nadu, India, in 2013 and 2023, respectively. Since 2022, she has been a Research Assistant with the University of Sharjah, United Arab Emirates. She was an Assistant Professor in computer science and engineering with Eranad Knowledge City Technical Campus, Kerala, India, and a Lecturer in computer science with the University of Kerala, India. She has published ∼16 papers in various peer-reviewed international journals and conferences. Her research interests include network and information security issues in FANET, big data, and cloud computing environments. She has been awarded merit-cum-means scholarship by the Central Government of India (Prime Minister's Fund) for her outstanding performance in the higher secondary examinations, in 2007.

IBRAHIM KAMEL (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Maryland, College Park. He was an Adjunct Professor with Concordia University, Canada, Rutgers University, NJ, USA, New York University, Brooklyn, NY, USA, and Strayer University, VA, USA. He was the Chairperson of the Department of Computer Engineering. He was the Director of the Institute for Leadership in Higher Education, University of Sharjah, where he was also the Chairperson of the Department of Electrical and Computer Engineering. He also worked for eight years in industrial research as a Lead Scientist in USA. He is currently a professor in computer engineering. He has published 23 patents and more than 170 refereed papers published in international conferences and journals (H-index=37; citations=5800). His research interests include spatial indexing, databases, cybersecurity, multimedia systems, and social networks. He is serving in the editorial boards for several international journals and chaired several international conferences.