IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) | 978-1-6654-9427-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/INFOCOMWKSHPS57453.2023.10225980

GPS Spoofing on UAV: A Survey

Ryan D Restivo[1], Laurel C. Dodson[2], Jian Wang[3], Wenkai Tan[2], Yongxin Liu[2],
Huihui Wang[1], and Houbing Song[4]
[1]St. Bonaventure University, St. Bonaventure, NY, USA
[2]Embry-riddle Aeronautical University, Daytona Beach, FL, USA
[3]The University of Tennessee at Martin, TN, USA; [4]University of Maryland, Baltimore County, MD, USA
[1]restivrd19@bonaventure.edu, hwang@sbu.edu
[2]{dodsonl1, tanw1}@my.erau.edu, liuy11@erau.edu
[3]jwang186@utm.edu; [4]songh@umbc.edu

***Abstract*—With the development of the Internet of Things (IoT) and Cyber-Physical System (CPS), Unmanned Aerial Vehicles (UAVs) are deployed in various implementations which improve the performance of the IoT and reduce labor consumption significantly. As the core of UAV, Global Positioning System (GPS) is essential to provide the navigation information for UAVs to finish missions. GPS receives satellite signals and calculated localization so UAVs can recognize their positions. However, malicious attackers leverage the mechanism to generate forged GPS signals that can spoof UAV that has wrong positions. The wrong positions can lead to missions' failure and threaten public safety and private security. In this paper, we investigated the overview of GPS spoofing and explored the development of GPS spoofing on UAVs. This work can provide researchers with state-of-the-art GPS spoofing development on UAVs and inspiration for new directions in this field.**

I. INTRODUCTION

With the development of Artificial Intelligence (AI), Machine Learning (ML), and the continuous evolution of wireless communication, the Internet of Things (IoT) and Cyber-physical Systems (CPS) are playing essential roles in different fields like industry [1], healthcare [2], [3], agriculture [4], disaster rescue [5], and smart cities [6]. With the massive deployment of IoT and CPS, human beings can extend their operation to extreme and dangerous environments with mobile communication relays which enable the operators can achieve their missions remotely and safely. The operators can leverage advanced wireless communication like 5G New Radio (5G NR) [7] and 6G cellular network [8] to control sensors to acquire information remotely, control the parameters of the environments accurately, and manage the processing of each device precisely. With the enhancement of AI and ML, IoT and CPS can be deployed in space, air, and ground scenarios which can have a Space-Air-Ground Communication (SAGC) system and provide different services for various applications.

As the core of IoT and CPS, Unmanned Aerial Vehicles (UAVs) are significant to the processing of massive deployment of IoT and CPS which is also an implacable part of SAGC development [9]. Due to flexibility and flight dynamics, UAVs with sensors can acquire ground and aerial information and transmit the information to help Ground Control Station (GCS) to achieve comprehensive surveillance for the target areas which extends the sensing scale of IoT and CPS [10]. Also, UAVs with wireless devices can provide network services for the target areas like disaster areas. In flight missions, there are many sensors of UAV providing fundamental services for UAV to finish missions. Among the sensors, Global Positioning System (GPS) module acquires the signal generated from satellites and calculates the localization of UAV simultaneously [11]. With localization, UAV controls its motion to follow the trajectory to reach the destinations and finish missions. The accuracy and correctness of the signal generated from satellites are serious to UAVs' flight and safety [12] which also affects the success rate of mission compliment.

However, hackers can leverage the mechanism of GPS localization to play spoof attacks on UAVs and interfere with the normal functions of UAVs. The hackers acquire real satellite signals and imitate the signal patterns and re-generate the forged signal that contains incorrect time tags and satellite information to mislead the GPS module to generate a wrong position [13]. The wrong position can navigate UAV to unsafe or sensitive areas and make threats to public safety and private security.

In this paper, we investigated state-of-the-art GPS spoofing on UAV and obtain a survey on this topic. We

978-1-6654-9427-4/23/$31.00 ©2023 IEEE

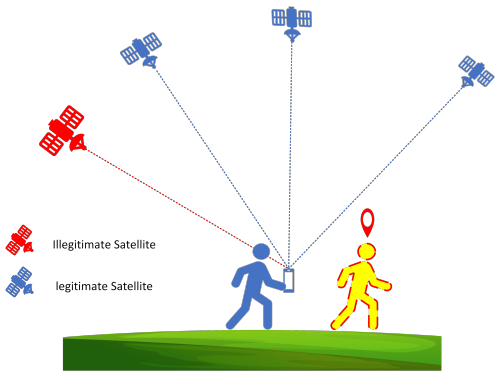

Fig. 1. GPS spoofing attack.

explore the mechanism of GPS spoofing and category different technologies in this topic. Under each category, we have summaries for the technology development that will help other researchers to have a quick overview of the attacks in each category. We believe our contributions can affect the development of the research on this topic and more exploration will be made with our insights.

The rest of the paper is organized as the following. Sec. II demonstrates the overview of GPS spoofing attacks. Sec. III investigates the detection of GPS spoofing attacks. Sec. IV discussed the safeguards against GPS spoofing attacks. Sec. V discussed current challenges and future directions of GPS spoofing on UAV. Sec. VI concludes our investigation results.

II. Overview of GPS spoofing

GPS spoofing can be a huge public safety concern since it allows attackers to take control of UAVs. GPS spoofing fundamentally exploits the nature of the GPS system. Therefore, in order to explain GPS spoofing, we must explain GPS. This section will describe GPS as well as how GPS spoofing works.

GPS is a Global Navigation Satellite Systems (GNSS) used to determine a receiver's location. If someone wished to manipulate the perceived location of a device, they could forge or modify GPS signals. As demonstrated in Fig. 1, the receiver (blue phone at center right) locks on to four GPS signals (top). More prominent than the more powerful spoofer signals overpower the authentic ones. The victim's perceived location moves away from the victim's actual location (outlined man on the right).

[14] explains that each GPS satellite transmits ephemeris data containing their precise location and a timestamp of the transmission used to calculate the distance between themselves and the satellites. GPS receivers use these distances to triangulate their position [15]. Because of this, it is necessary to spoof multiple satellites to completely fool a receiver.

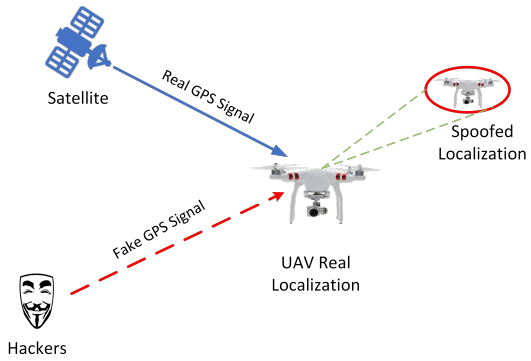

Fig. 2. GPS spoofing on UAV

During a GPS spoofing attack, (shown in Fig. 2), satellite (top left) broadcasts authentic GPS signals to the UAV (center). Hacker (bottom left) broadcasts fraudulent GPS signals to the UAV. UAV picks up on both GPS signals and calculates its position. The UAV calculates an incorrect location for itself (top right) due to the hacker's spoofer signal.

With UAVs, the goal of GPS spoofing is to alter the self-perceived location of the victim so it travels in the wrong direction while trying to reach its destination [16]. This can be used for no-fly zones, to set incorrect return points, to cause confusion, or to hijack UAVs [17]. GPS spoofing is used in [18] to navigate UAVs along the shortest possible path around a no-fly zone.

In Fig. 3, a malicious UAV (center) navigates using authentic GPS signals (top right). The malicious UAV attempts to fly into a sensitive area (bottom right). A legitimate defender (bottom left) conducts a GPS spoofing attack against the malicious UAV. As a result, the UAV is successfully navigated around the sensitive area.

Research on GPS spoofing has a wide range of effects both good and bad. On one hand, research into GPS spoofing helps the creation of no-fly zones where UAVs could be hazardous. On the other hand, UAVs used for delivery or emergency services could be at an increased risk of hijacking.

III. Detection of GPS spoofing attacks

GPS spoofing has can cause a lot of damage. This is especially true with UAVs. While countermeasures against GPS spoofing do exist, to use them, the victim needs to know an attack is occurring. Because of

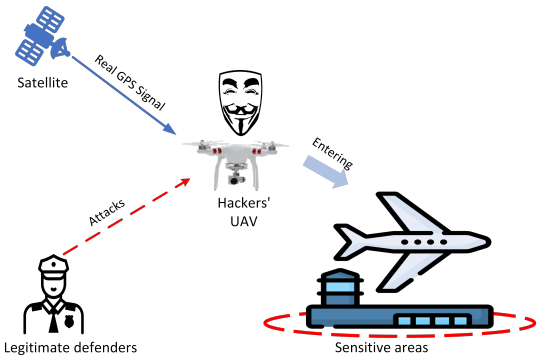

Fig. 3. Enforcement of a no-fly zone using GPS spoofing

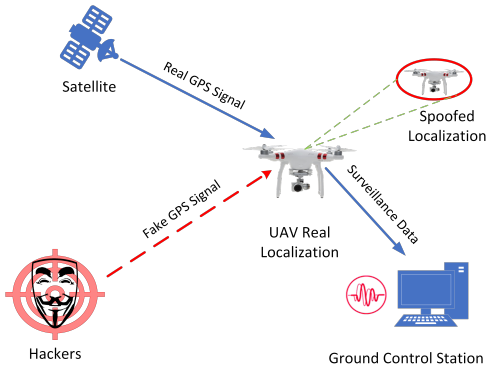

Fig. 4. GPS spoofing detection on UAV

this, detecting GPS spoofing is as important as having safeguards against it. This section focuses on currently established methods for detecting GPS spoofing attacks.

In Fig. 4, we see a GPS spoofing attack causing the UAV (center) to perceive itself at an incorrect location (top right). In this method, surveillance data is sent to the ground control station (bottom right). Ground control determines based on surveillance data that GPS spoofing is occurring. With this knowledge, safeguards against GPS spoofing are triggered.

Multiple papers on GPS spoofing classify attacks into simple, intermediate, and sophisticated attacks [19]. Simplistic spoofing uses low-cost hardware to perform the most basic easiest to detect attack [19]. Intermediate spoofing uses knowledge of the receiver to avoid detection [20]. Sophisticated spoofing attacks use with multiple spoofers at different locations that are synchronized to be even more effective [20].

[21] uses a technique involving the camera feed and Inertial Measurement Unit (IMU) to determine the UAV's velocity and compare it with the velocity calculated with GPS signals. Even just the IMU and GPS suggested velocities show a discrepancy that can be used to detect spoofing [22]. [23] proposes checking the consistency of GPS signals with other technologies like WiFi or other GNSS.

Authentic GPS signals are often weaker than spoofing signals making it possible to approximate the transmission origin. This can be used to determine if a signal is fraudulent [24]. [23] outlines methods where the GPS signal strength is observed in relation to the UAV's movement and where the signal strength and delay of L1 and L2 code coming from the GPS signal. [25] explains how since background noise is often present in authentic signals, its absence is a sign of GPS spoofing. [16] uses authentication in GNSS signals through encryption methods. [26] discusses the use of Angle of Arrival (AOA), Time of Arrival (TOA), and a number of satellite signals received to determine the direction from which the signal came. [27] Proposes the use of HAMSTER (HeAlthy, Mobility and Security based data communication archiTEctuRe) that communicates data from the UAV to ground control station for verification. [28] proposed radar ground stations with local trackers that receive a UAV's perceived position information and sift through to find outliers.

In [29], three ensemble models of machine learning (Bagging, Stacking, and Boosting) were tasked with detecting fraudulent GPS signals. Stacking yielded the best results, but required the most processing power. Support Vector Machines (SVMs) can be used in perfecting already existing methods of detection using no extra hardware [30].

Long-Term and Short-Term Memory systems have been used both to determine the difference between an attack and natural phenomenon, and to approximate flight paths prior to takeoff to be compared to actual trajectory information [31] [17]. [32] demonstrates the use of neural networks with different combinations of information from GPS signals showing that neural networks with two hidden layers improved performance but increased complexity. In [33] a Bayesian network took characteristics of GPS signals and compared them with older GPS information from both the same and a neighboring UAV yielding promising results. [34] conducted a comparison of different supervised and unsupervised machine learning models. Of the unsupervised models, Autoencoder had the highest performance and K-means had the worst performance. For supervised models, CART seemed to yield the best results. Overall, the Gaussian Naïve Bayes model showed the worst results.

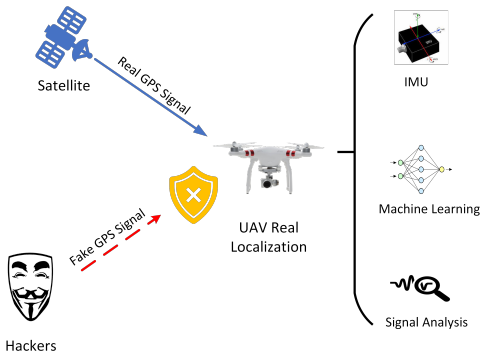

Fig. 5. Safeguards against GPS spoofing attacks

In [35], a multitude of machine learning models are used with both a Metric Optimized Dynamic Selector and Weighted Metric Optimized Dynamic Selector to choose the best model out of all of them dynamically to get the most accurate detection.

Much like GPS spoofing, research on detection has both good and bad potential. Learning to attack UAVs is beneficial if they are behaving maliciously. The same is true for defending UAVs. We want UAVs that provide services to be protected from outside interference. However, defensive techniques could hypothetically be used to protect malicious UAVs. Advances in detection techniques, while more advanced than our safeguards, should remain a focus in future research to combat new GPS spoofing methods.

IV. Safeguards against GPS spoofing attacks

Once an attack is detected, the UAV must counteract the attack. Many safeguards are now placed on commercial drones for this purpose. This section will cover the techniques used by UAVs in order to defend against GPS spoofing.

Fig. 5 shows a hacker (bottom left) attempting to spoof a UAV (center). The UAV has defenses to help with detection and mitigation of GPS spoofing attacks (right). These are used to protect the UAV from the false signals broadcast by the attacker. This prevents the UAV from going off course.

Since the IMU can be used to maintain a steady position, some drones already rely on it when they detect GPS signals that are stronger than a certain threshold [36]. In [37], it was shown that some UAVs are able to utilize other GNSS like GLONASS. The paper also displays the simplest form of GPS spoofing in which the UAV will hover in place until a signal is received from ground control to continue.

Other safeguards, like that in [38], involve predicting the most advantageous time for an attacker and using a Stackelberg game which involves two parties reacting to each other repeatedly with the most favorable possible decision. [39] used a Stackelberg game to test their method which uses linear regression to predict a route and an LSTM network to compare said prediction with the actual path.

[26] proposes broadcasting an opposing version of the spoofing signal (phase-shifted 180 degrees) to cancel out the spoofing signal. AOA information can mitigate GPS spoofing through the directional broadcast of null signals that mitigate spoofed signals and through directional filtering of signals [23][23]. [40] designs a method to find differences in background noise and the delay between authentic and spoofed signals to prevent a loss of authentic signals. In [41], the position of the attacker is calculated and the ideal path to take to avoid the attacker is generated and followed by the UAV to escape the range of the attack so GPS navigation can resume.

[28] suggests using ground radar stations and local trackers where positioning information is transmitted back to the target UAVs to be used in place of GPS. [42] proposes the use of Crowd-GPS-Sec to communicate with aircraft about their received GPS signals to triangulate the origin of GPS spoofers.

The creation of safeguards against GPS spoofing allows drones resist attack. Good safeguards have both positive and negative effects depending on their implementation. Because of the difficulty of a loss of direction, safeguards currently vary in effectiveness. Although multiple strategies exist to combat attacks, safeguards need more research.

V. Discussion and Future Research

With such a wide variety of techniques for GPS spoofing detection and remediation, it can be difficult to see where each should be used. Each one has its own benefits and drawbacks that make them more suitable under certain conditions. Most of the time, these drawbacks manifest as increases in the implementation cost and overhead of that system. Different UAV manufacturers might choose to implement certain detection and remediation techniques based on these limitations.

Of the detection methods discussed in this paper, those that can use the hardware already installed in the UAV are among the easiest to implement. This includes the method that uses the onboard camera and the Lucas-Kanade method, detection methods that use discrepancies in the IMU's readings, and methods that check other sources for accuracy purposes. These methods

require little overhead to implement because each utilizes hardware that is already possessed by the UAV. However, easier methods to implement are typically easier for attackers to bypass. For example, if the attacker can accurately mimic authentic GPS signals for a time, the first two methods of detection may be bypassed. And, with the last method, other sources of info could be easily blocked through jamming.

Some of the more effective GPS spoofing detection techniques require much more overhead by way of hardware but are much more difficult to avoid. Take, for example, the methods discussed that analyze the angle-of-arrival of satellite signals. These methods require that the receiver have multiple antennas so that the angle by which the signal is received can be determined. This requires more work to implement but would require attackers to spread out their attacks across multiple locations. Other methods discussed, like the use of ground radar stations or the implementation of authentication and encryption in the GNSS prove very effective but come at a higher cost.

Other methods of detection could require more computational power. The prime example of this is methods that utilize machine learning techniques to detect spoofing. While these methods are generally effective, some UAVs built today may have trouble implementing them due to extra computational requirements. The methods discussed that use machine learning are incredibly effective at precisely determining when GPS spoofing is occurring based on a variety of factors. Machine learning could be paired with other, more hardware-oriented detection techniques to improve their effectiveness too.

As previously discussed, the most common currently used GPS spoofing safeguards involve using the UAV's autopilot to hold still until authentic signals are reestablished or switching to other GNSS if one is compromised. However, holding a steady position doesn't always ensure the safety of the drone and with jamming, other GNSS can be blocked out. Thus, more effective safeguards need to be implemented.

Most of the more effective safeguards currently proposed will require extra overhead either on the UAV or on the ground. The previously discussed anti-spoofer signals require the UAV to pinpoint the direction the spoofer signals are coming from, which would require extra hardware and also requires the ability to broadcast a signal to counteract it. The use of radar trackers and Crowd-GPS-Sec require more infrastructure on the ground to find discrepancies and track down spoofers respectively.

VI. Conclusion

As one implacable part of IoT and CPS, UAV is significant to the processing of massive deployment of IoT and CPS which is fundamental to SAGC development. However, GPS is critical to UAVs which helps remote operators to finish missions precisely and effectively. In this paper, we investigated state-of-the-art GPS spoofing on UAVs and obtain a survey on this topic. We explore the mechanism of GPS spoofing and category different technologies. For each category, we have summaries that present an overview of the attacks in each category. We believe our contributions can affect the development of this topic and more exploration will be made with our work.

VII. Acknowledgement

This work was supported by the U.S. National Science Foundation under Grant No. 2317117.

References

[1] S. Priyadarshy, "Iot revolution in oil and gas industry," *Internet of Things and Data Analytics Handbook*, pp. 513–520, 2017.

[2] H. K. Sharma, A. Kumar, S. Pant, and M. Ram, *Artificial Intelligence, Blockchain and IoT for Smart Healthcare*. CRC Press, 2022.

[3] H. Abie, "Cognitive cybersecurity for cps-iot enabled healthcare ecosystems," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, 2019, pp. 1–6.

[4] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, "An overview of internet of things (iot) and data analytics in agriculture: Benefits and challenges," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3758–3773, 2018.

[5] T. Khan, S. Ghosh, M. Iqbal, G. Ubakanma, and T. Dagiuklas, "Rescue: A resilient cloud based iot system for emergency and disaster recovery," in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2018, pp. 1043–1047.

[6] H. Kim and J. Ben-Othman, "Toward integrated virtual emotion system with ai applicability for secure cps-enabled smart cities: Ai-based research challenges and security issues," *IEEE Network*, vol. 34, no. 3, pp. 30–36, 2020.

[7] J. Wang, Y. Liu, S. Niu, and H. Song, "Optimal routing for beamforming-constrained swarm uas networking," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 2897–2908, 2021.

[8] R. Liu, A. Liu, Z. Qu, and N. N. Xiong, "An uav-enabled intelligent connected transportation system with 6g communications for internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–15, 2021.

[9] J. Wang, Y. Liu, S. Niu, and H. Song, "Reinforcement learning based scheduling for heterogeneous uav networking," in *2021 17th International Conference on Mobility, Sensing and Networking (MSN)*, 2021, pp. 420–427.

[10] J. Wang, Y. Liu, S. Niu, W. Jing, and H. Song, "Throughput optimization in heterogeneous swarms of unmanned aircraft systems for advanced aerial mobility," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2752–2761, 2022.

[11] H. Qin, Z. Meng, W. Meng, X. Chen, H. Sun, F. Lin, and M. H. Ang, "Autonomous exploration and mapping system using heterogeneous uavs and ugvs in gps-denied environments," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1339–1350, 2019.

[12] J. S. Russell, M. Ye, B. D. O. Anderson, H. Hmam, and P. Sarunic, "Cooperative localization of a gps-denied uav using direction-of-arrival measurements," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 3, pp. 1966–1978, 2020.

[13] B. Van den Bergh and S. Pollin, "Keeping uavs under control during gps jamming," *IEEE Systems Journal*, vol. 13, no. 2, pp. 2010–2021, 2019.

[14] R. V. Karpe and S. Kulkarni, "Software defined radio based global positioning system jamming and spoofing for vulnerability analysis," in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 2020, pp. 881–888.

[15] N. Shijith, P. Poornachandran, V. G. Sujadevi, and M. M. Dharmana, "Spoofing technique to counterfeit the gps receiver on a drone," in *2017 International Conference on Technological Advancements in Power and Energy (TAP Energy)*, 2017, pp. 1–3.

[16] E. Ranyal and K. Jain, "Unmanned aerial vehicle's vulnerability to gps spoofing a review," *Journal of the Indian Society of Remote Sensing*, vol. 49, no. 3, pp. 585–591, 2020.

[17] S. Wang, J. Wang, C. Su, and X. Ma, "Intelligent detection algorithm against uavs' gps spoofing attack," in *2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS)*, 2020, pp. 382–389.

[18] P. Ortner, R. Steinhöfler, P. Hödl, E. Leitgeb, and H. Flühr, "Geospatial guidance of unmanned aerial vehicles around no-fly-zones by global positioning system spoofing," in *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, 2021, pp. 1–7.

[19] J. Gaspar, R. Ferreira, P. Sebastião, and N. Souto, "Capture of uavs through gps spoofing using low-cost sdr platforms," *Wireless Personal Communications*, vol. 115, no. 4, pp. 2729–2754, 2020.

[20] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, P. M. Kintner *et al.*, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, 2008, pp. 2314–2325.

[21] Y. Qiao, Y. Zhang, and X. Du, "A vision-based gps-spoofing detection method for small uavs," in *2017 13th International Conference on Computational Intelligence and Security (CIS)*, 2017, pp. 312–316.

[22] Q. Zou, S. Huang, F. Lin, and M. Cong, "Detection of gps spoofing based on uav model estimation," in *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, 2016, pp. 6097–6102.

[23] M. Ahmad, M. A. Farid, S. Ahmed, K. Saeed, M. Asharf, and U. Akhtar, "Impact and detection of gps spoofing and countermeasures against spoofing," in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2019, pp. 1–8.

[24] J. NIELSEN, A. BROUMANDAN, and G. LACHAPELLE, "Gnss spoofing detection for single antenna handheld receivers," *Navigation (Washington)*, vol. 58, no. 4, pp. 335–344, 2011.

[25] L. He, W. Li, C. Guo, and R. Niu, "Civilian unmanned aerial vehicle vulnerability to gps spoofing attacks," in *2014 Seventh International Symposium on Computational Intelligence and Design*, vol. 2, 2014, pp. 212–215.

[26] T.-H. Kim, C. S. Sin, S. Lee, and J. H. Kim, "Analysis of effect of anti-spoofing signal for mitigating to spoofing in gps l1 signal," in *2013 13th International Conference on Control, Automation and Systems (ICCAS 2013)*, 2013, pp. 523–526.

[27] 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 *2020 Latin American Robotics Symposium (LARS), 2020 Brazilian Symposium on Robotics (SBR) and 2020 Workshop on Robotics in Education (WRE)*, 2020, pp. 1–6.

[28] B. Pardhasaradhi and L. R. Cenkeramaddi, "Gps spoofing detection and mitigation for drones using distributed radar tracking and fusion," *IEEE Sensors Journal*, vol. 22, no. 11, pp. 11 122–11 134, 2022.

[29] A. Gasimova, T. T. Khoei, and N. Kaabouch, "A comparative analysis of the ensemble models for detecting gps spoofing attacks on uavs," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 2022, pp. 0310–0315.

[30] 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 *2017 23rd International Conference on Automation and Computing (ICAC)*, 2017, pp. 1–11.

[31] R. A. Agyapong, "Efficient detection of gps spoofing attacks on unmanned aerial vehicles using deep learning," 2021.

[32] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of gps spoofing attacks on unmanned aerial systems," in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2019, pp. 1–6.

[33] C. Titouna and F. Naït-Abdesselam, "A lightweight security technique for unmanned aerial vehicles against gps spoofing attack," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, 2021, pp. 819–824.

[34] T. T. Khoei, A. Gasimova, M. A. Ahajjam, K. A. Shamaileh, V. Devabhaktuni, and N. Kaabouch, "A comparative analysis of supervised and unsupervised models for detecting gps spoofing attack on uavs," in *2022 IEEE International Conference on Electro Information Technology (eIT)*, 2022, pp. 279–284.

[35] T. Talaei Khoei, S. Ismail, and N. Kaabouch, "Dynamic selection techniques for detecting gps spoofing attacks on uavs," *Sensors*, vol. 22, no. 2, p. 662, 2022.

[36] V. Dey, V. Pudi, A. Chattopadhyay, and Y. Elovici, "Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study," in *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*, 2018, pp. 398–403.

[37] 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. Priv. Secur.*, vol. 22, no. 2, apr 2019. [Online]. Available: https://doi-org.ezproxy.libproxy.db.erau.edu/10.1145/3309735

[38] A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: A game-theoretic countermeasure for protecting uavs against gps spoofing," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2840–2854, 2020.

[39] L. Meng, L. Yang, S. Ren, G. Tang, L. Zhang, F. Yang, and W. Yang, "An approach of linear regression-based uav gps spoofing detection," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.

[40] Y. Hu, S. Bian, B. Li, and L. Zhou, "A novel array-based spoofing and jamming suppression method for gnss receiver," *IEEE Sensors Journal*, vol. 18, no. 7, pp. 2952–2958, 2018.

[41] W. Wan, H. Kim, N. Hovakimyan, L. Sha, and P. G. Voulgaris, "A safety constrained control framework for uavs in gps denied environment," in *2020 59th IEEE Conference on Decision and Control (CDC)*, 2020, pp. 214–219.

[42] 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 *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 1018–1031.