IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Managing the cyber-physical security for unmanned aerial vehicles used in perimeter surveillance

Mahmod Al-Bkree

Department of Mechatronics, Institute of Mechatronics and Vehicle Engineering, Obuda University, Hungary.

(*Email:* albkriengineer@gmail.com)

Abstract

This paper discusses the vulnerabilities of perimeter surveillance unmanned aerial vehicles to cyber-physical security threats and discusses some approaches to manage them, as most cyber threats to the UAVs coming through their onboard wireless transceiver, we are suggesting an Antennas propagation type that limit the vector of the threat, also the importance of vulnerabilities scanner to evaluate the system risks. And addressing the limited energy and computation power resources onboard, a computation efficient onboard encryption method is proposed, and a sign cutting machine vision algorithm to provide warning of suspicious activity detected on interrupted surveillance imagery. The focus of this analysis is to manage the vulnerabilities of the system during both its operation time and its standby time, this is done by performing a checklist of computerized tests periodically and comparing two or more results to discover any unexpected changes. We showed that the onboard resources can be utilized more efficiently securing itself and the system from possible intrusion, however, some heavy calculation tasks still need to be performed on the ground control station which is causing some latency problem to such time sensitive operation. We have demonstrated that image registration techniques have produced useful results when applied to analyze the differences between two scene images.

Keywords: Cybersecurity, Image registration, Low power encryption, Perimeter surveillance network, Spoofing, Unmanned aerial vehicle, Vehicle positioning.

DOI: 10.53894/ijirss.v6i1.1173
Funding: This study received no specific financial support.
History: Received: 16 August 2022/**Revised:** 23 November 2022/**Accepted:** 8 December 2022/**Published:** 5 January 2023

Competing Interests: The author declares that there are no conflicts of interests regarding the publication of this paper.
Transparency: The author confirms that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained.
Ethical Statement: This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

Millions of new cyber malwares are detected every week. Unmanned aerial vehicles UAV have proliferated into many sectors ranging from low sensitive applications to higher sensitive ones such as surveillance. The vulnerabilities of UAVs to cyber threats are like those of any computer device, like a smartphone or a modern internet connected car. However, some special features of surveillance UAVs require management for their potential security flaws. Critical infrastructures often use perimeter surveillance UAVs with the following criteria,

- Flown a repeatable predetermined path around the perimeter.
- The path is usually long (e.g., international border, energy pipeline…).
- Surveillance is limited in time (e.g., one or few scans per day).
- Exposed physical space and cyberspace.

Many of the advanced tools that are used to counter cybersecurity threats are the same tools the malicious attacker uses, such as new methods for reconnaissance and delivering software to be installed, as well as command and control the system components.

In the literature, researchers have done good work identifying potential cyber-attacks, and highlighting the need for new designs that minimize cyber threats. The work on this paper is done to determine what are the main criteria of a UAV system that should affect the selection process from a cyber-security point of view, and how can we utilize the specificity of UAV tasks to manage cyber threats (e.g., flying predetermined path above well-known objects on the ground could allow navigation independent from major attack space of the Global Navigation Satellite System GNSS).

Another notable research gap is that many papers have been published on identifying suspicious activities in an active scene, while very few researches is done on analyzing passive scenes (e.g., sign cutting using passive scene).

Depending solely on a third-party providers could be on itself a vulnerability, in house development of strategy and customization is recommended to keep the uncertainty dynamic of the system and reduce the attacker knowledge of items, planning a unique operating system cryptography scheme, and cryptography, network security protocols, operating system mechanisms, database schemes to reduce the attacker's ability to exploit public available data and keep a moving target defense dynamic.

Factors of scalability, integration, and periodic upgrading affect the overall cost of buying a mass produced tool comparable to customizing special cybersecurity requirements, the three dimensional nature of UAV operation necessitate compromising certain methods to fit the onboard payload, computation power, memory and energy consumption, force the decision makers to find new ways to compensate the deficiency of onboard cyber defense hardware and software by redundancy in the ground control station GCS and achieve a cost efficient solution that satisfy standard security requirement. Figure 1 shows a block diagram of a UAV system.

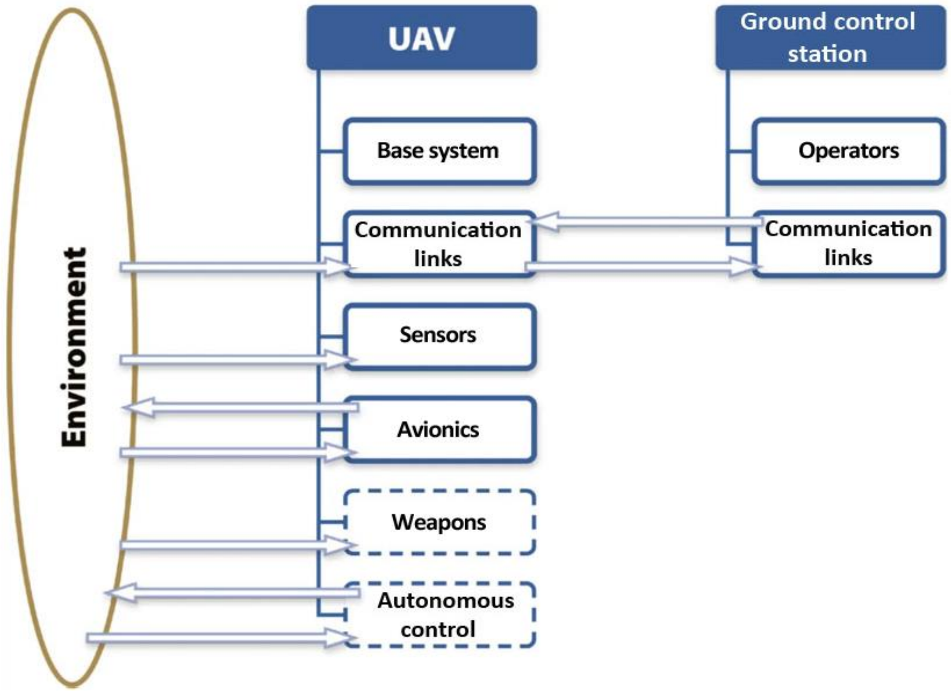


Figure 1.
Block diagram of a UAV system.
Source: Hartmann and Steup [1].

2. Related Works and Literature Review

Recently there are several different approaches about the meaning of the UAV systems. Szabolcsi [2] gave a main and robust framework for the Unmanned Aerial Systems (UAS) describing its main parts with further analysis. To get an UAV system with skills able to fly beyond line-of-sight (LoS) strong flight automation is required, which is thoroughly evaluated by Szabolcsi [3]. according to Nguyen and Nguyen [4] "most cybersecurity vulnerabilities are based on sensors, communication links, and privacy via photos".

It is well-known that any certification of the UAVs often bumps into a lack of existing and widely accepted regulations. In the scientific paper [2] firstly, gave a set of performances proper to use to evaluate UAVs air worthiness. Going into deep details, Szabolcsi [5] derived a set of dynamic performances of the UAV longitudinal motion, whilst Szabolcsi [6] derived a class of dynamic performances proposed to use to evaluate UAVs lateral/directional motion dynamic performances.

UAVs are suitable for perimeter surveillance tasks as they could cover long distances and reach difficult areas with relatively fast speed [7] a review of several known cybersecurity vulnerabilities and previous attacks shown in the work of Tang [8]. GNSS spoofing threats were evaluated in Schmidt, et al. [9] and concluded that even though spoofing currently might be hard to carry out in the field, the low-cost GNSS jammers indicate that eventually similarly low-cost GNSS spoofers will be developed. The need for balance between the security level of cryptography protocols and their requirement for computational power resources can be seen in Ralegankar, et al. [10].

The management starts from the manufacturing stage and the supply chain, regulating the main components as stated in Greer, et al. [11] "Internet of Things and cyber-physical systems comprise interacting logical, physical, transducer, and human components engineered for function through integrated logic and physics". Where it is important to design the infrastructure according to certain standards along the full supply chain "The virtual supply chain itself is a source of vulnerabilities and its resilience is only as good as the cyber-security infrastructure that it employs" [12] in their work Cheung, et al. [13] have identified a few key search gaps, and "has presented a systematic survey of the existing literature on cybersecurity in logistics and supply chain management. The key findings were as follows:
"1) They rarely use real cybersecurity data.
2) Studies focusing on cybersecurity in logistics are scarce although logistics plays an important role in supply chains.
3) There is only a limited number of papers adopting quantitative research approaches to study cybersecurity in logistics and supply chain management.
4) While a few studies focus on real-time recovery and aftermath measures, most studies focus on precautionary measures.
5) Blockchain technologies are still in their infancy in the transport and logistics sector.
6) Most studies use one-way encryption schemes that overlook the potential threats in a future dominated by quantum computing techniques.
7) Studies on information security and digital forensic investigation are scarce."

Cyber-security must be treated as important as the traditional quality, cost, functionality and availability of a UAV as the "Cyber-attacks on drones can pose significant safety risks to physical entities like large aircraft, airports, and human properties. If compromised, drones can cause a larger impact than a regular Information Technology (IT) device. As a result, UAVs demand highly reliable software and strict regulatory compliance like the vehicle industry" [14]. And a "Proactive prevention for public safety threats is one of the key areas with vast potential of surveillance and monitoring drones. Antennas play a vital role in such applications to establish reliable communication in these scenarios. This paper considers line-of-sight and non-line-of-sight threat scenarios with the perspective of antennas and electromagnetic wave propagation" [15]. The development of directional and other types of UAV antennas have been discussed in the literature as in Mohammadi, et al. [16]; Jacobsen and Marandi [17] and Semenov, et al. [18].

In their paper Hu, et al. [19] they have proposed "a cyberspace security situation prediction model based on MapReduce and Support Vector Machine SVM (MR-SVM)". A performance assessment of various vulnerability scanners is reported in Araújo, et al. [20] and several types of vulnerabilities have been found by analysis using Nessus Scanner [21].

"Global Positioning System (GPS)-dependent UAVs require accurate, trustworthy and uninterrupted position information for their safe operations. However, different research efforts have shown that GPS signals can be jammed or spoofed owing to its inherent vulnerabilities" [22]. An analysis of the spoofing signal effect on a UAV receiver in a navigation spoofing experiment has been done by Ma, et al. [23].

3. Method

The selection of optimum UAV to perform specific tasks is not trivial, Hamurcu and Eren [24] have suggested a model that identifies UAVs criteria and their weight using analytic hierarchy process, then rank each UAV using technique for order preference by similarity to ideal solution.

In this paper I have identified six main criteria that could enhance the cyber-physical security of perimeter UAVs so to be ranked based on their security level, the weight of each criterion will depend on the specifics of each task and its intersection with the other important consideration of performance level, cost level and the overall efficiency of the system. "The process of alternative evaluation is very complex and not well understood, and the information managed is incomplete, imprecise, and vague… A hybrid fuzzy-weighted average approach was proposed to offer an opportunity to carry out fuzzy analysis which takes full advantage of the information available to the decision maker" [25].

Considering the specific application of perimeter surveillance, the main criteria would differ from a general cyber security, allowing to optimize the selection process for how to design each hardware onboard within an acceptable trade-off with its functionality, while at the same time to use its functionality to support in detecting, identifying, classifying, managing and preventing cyber-physical security attacks.

4. Threat Spaces

A. Supply Chain

Some incidents of preinstalled malware during supply chain necessitate that managing the cybersecurity of UAV starts by studying each stage of the supply chain, the supply chain of UAV includes all entities who worked to make the product's hardware, software, or service. Typically, the supply chain is complex, and dynamic composed of tens of entities cooperated at some level to the final product, therefore, a due diligence of checklist steps should be taken in order to satisfy the triad of confidentiality, integrity and availability requirement. The testing includes an activity that might affect the final product regardless of the motive which could be due to.

- Malicious

- Negligence
- Accidental

The transparency of each entity of the supply chain about their security procedure to prevent flaws as well as their policy regarding reporting previous security incidents. The assessment of the UAV immunity to cyber supply chain threats should be a deciding factor when selecting and purchasing it.

B. Antennas Radiation

The majority of cyberthreats to the UAV come through its antennas (onboard wireless transceivers) while flying, the antenna is the main physical port for cybersecurity attack vector, threats either by sending a hacking code through it, or by receiving sensitive data transmitted by the antenna to the ground control station GCS, or by jamming it prohibiting it from any communication.

Limiting the propagation beam of the data link between the GCS and UAV to a narrow space can protect from these threats, and strengthen the antenna's gain, improving the signal range and minimizing the Fresnel zone radius. Using phased array antennas for the UAV, GCS, or both can create a safer line of communication, reducing the exposed space of attack to an order of magnitude.

When the data is transmitted omnidirectional it creates a sphere like propagation that allows an attacker to receive the data from any point in that sphere, while focusing the transmission direction into a very limited cone of space minimizes the attacker chances of receiving the signal outside, attacks such as the man in the middle, denial of service DoS. and data capture are examples for omni-directional antenna vulnerability. Figure 2 shows the propagation of Omni-directional and directional antennas.

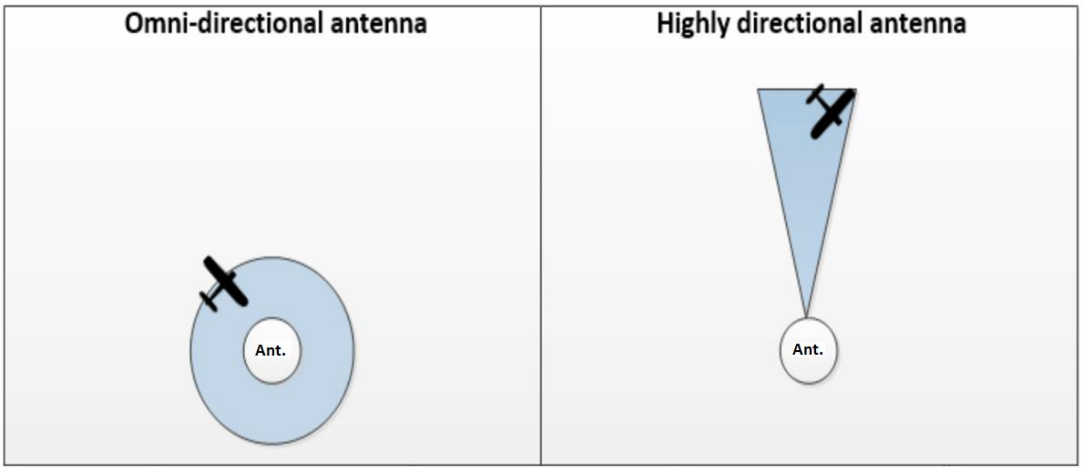


Figure 2.
Shows the propagation area for Omni-directional antenna (Left), and for directional antennas (Right).
Source: Alex [26].

The nature of operating surveillance UAV on a predetermined flying path facilitates steering both antennas propagation direction electronical, based on the planned flying path to ensure that the transmitted signal is only directed into the specific location of the targeted area, and the received signal is only possible to interfere from a specific location. Figure 3 shows patterns of directional antennas electronically steered, simulated at different phases.

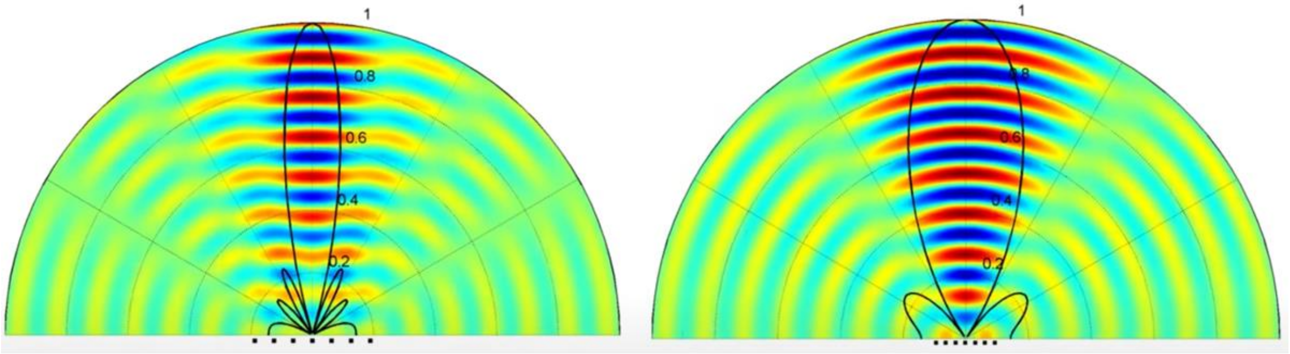


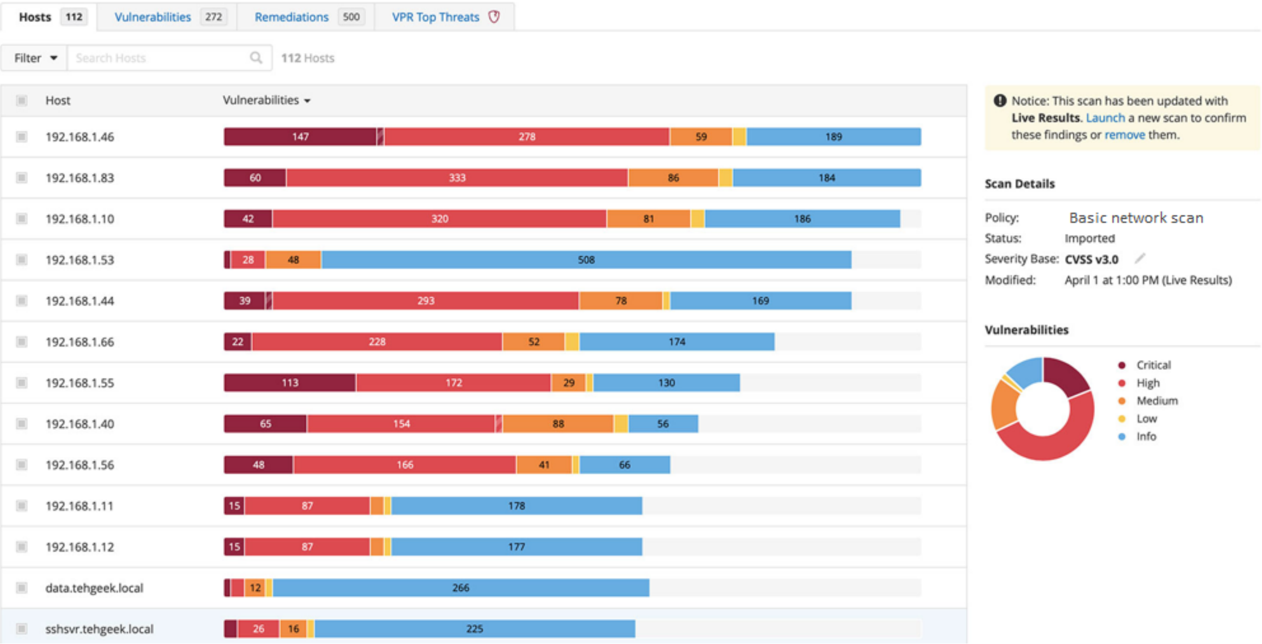
Figure 3.
Shows the propagation patterns of the directional antennas that are electronically controlled to produce narrower propagation area (Left), and a wider propagation area (Right), simulated at different phases.

C. Network Mapping

Knowing the network characteristics, all (used & unused) devices, hosts, ports, hops, operating systems, services and applications is essential for managing its security, therefore, a regular scanning for the network to ensure the hardware and software connected are benign and adequately secure would reduce the risk of attack. Scanning is the main tool that an attacker would use to find vulnerabilities, incidents of attackers getting access to the UAV control, WiFi connection, and to the GCS computers have been reported. Identifying the ports and their functions will help eliminate the unnecessary ones and adequately secure the rest of them.

A 5G network provides an extended wireless connection to the Internet, which exposes the UAV interconnectivity to a much wider range Beyond the Line of Sight BLoS of the GCS, with a fraction of a second latency and a data rate of multiple gigabytes per second, however, keeping the network private would reap the benefits of the technology without heavy cost on the cybersecurity, the proximity of surveillance UAV to the perimeter works will for the limited distance range of 5G, and the operational altitude would have few to none signal-impenetrable-obstacles.

An automated vulnerabilities scanner can highlight most of the critical attack points in the network, with a detailed description of the cyber issue comparable to the Common Vulnerabilities and Exposures CVE and suggest a variety of possible solutions and advisory to secure them. Figure 4 shows an overview of a vulnerability scan report.



Notice: This scan has been updated with **Live Results**. Launch a new scan to confirm these findings or remove them.

Scan Details

Policy: Basic network scan
Status: Imported
Severity Base: **CVSS v3.0**
Modified: April 1 at 1:00 PM (Live Results)

Figure 4.
An overview of Nessus vulnerability scan report.
Source: Daudelin [27].

D. Navigation System

Global positioning system GPS is the most widely used system for navigation, GPS spoofing is an attack that denies or distorts the GPS signal, although many countermeasures methods have been published for UAV navigation system spoofing attacks and many are implemented by manufacturers, this type of attack is still reported. A combination of multiple computing efficient methods could reduce susceptibility to spoofing. Onboard positioning of the UAV using multiple techniques and comparing them would help create a voting mechanism to determine the real position at any time.

- Positioning based on GPS.
- Positioning based on inertial measurement unit IMU.
- Positioning based machine vision.
- Implementing a geo-fence (restricting flying outside the surveillance path).

E. Encryption

Lack of adequate encryption is one of the most common vulnerability, Wi-Fi protected access® WPA is a common data encryption for wireless networks and can establish a secure wireless communication between the UAV and the GCS, the third version WPA3 could use 128-256 bit session key size with simultaneous authentication, it uses the advanced encryption standard AES method from an encryption point view it's sufficient for adequate security and is widely used in modern UAVs, however, for an onboard UAV the computation power and memory might in some cases require a lighter encryption methods such as Bleep64 which is a small, fast, and effective, consuming much less computations and memory, and require no special encryption hardware. Daudelin [27] has concluded that "general Information Technology (IT) cryptography cannot meet all UAS requirements".

F. Machine Learning (ML)

The big cybersecurity data and its complexity are beyond human manual ability to organize and act on, however, machine learning models thrive on big data. The use of ML could classify suspicious network activities and predict some threats giving an opportunity to change the reactive nature of cybersecurity and assist the available human resources.

Onboard the UAV machine learning models could instantly identify potential threats, models such as motion and event detection have a high accuracy to provide early warning of suspicious activity. For surveillance UAV where the perimeter is large the area will be periodically interrupted surveilled, leaving segments of the protected area non surveilled for an extended amount of time, using machine analytics model for man-tracking and sign cutting would help in terms of acquiring information about previous events, and it can identify if suspicious electronic devices have been planted near the perimeter, by comparing the current video stream with the stream from the previous days and highlight the differences in the two videos. The following figure shows an example of a surveillance sign identified by the model. Figure 5 shows a sign of a previous activity detected by a machine learning model.

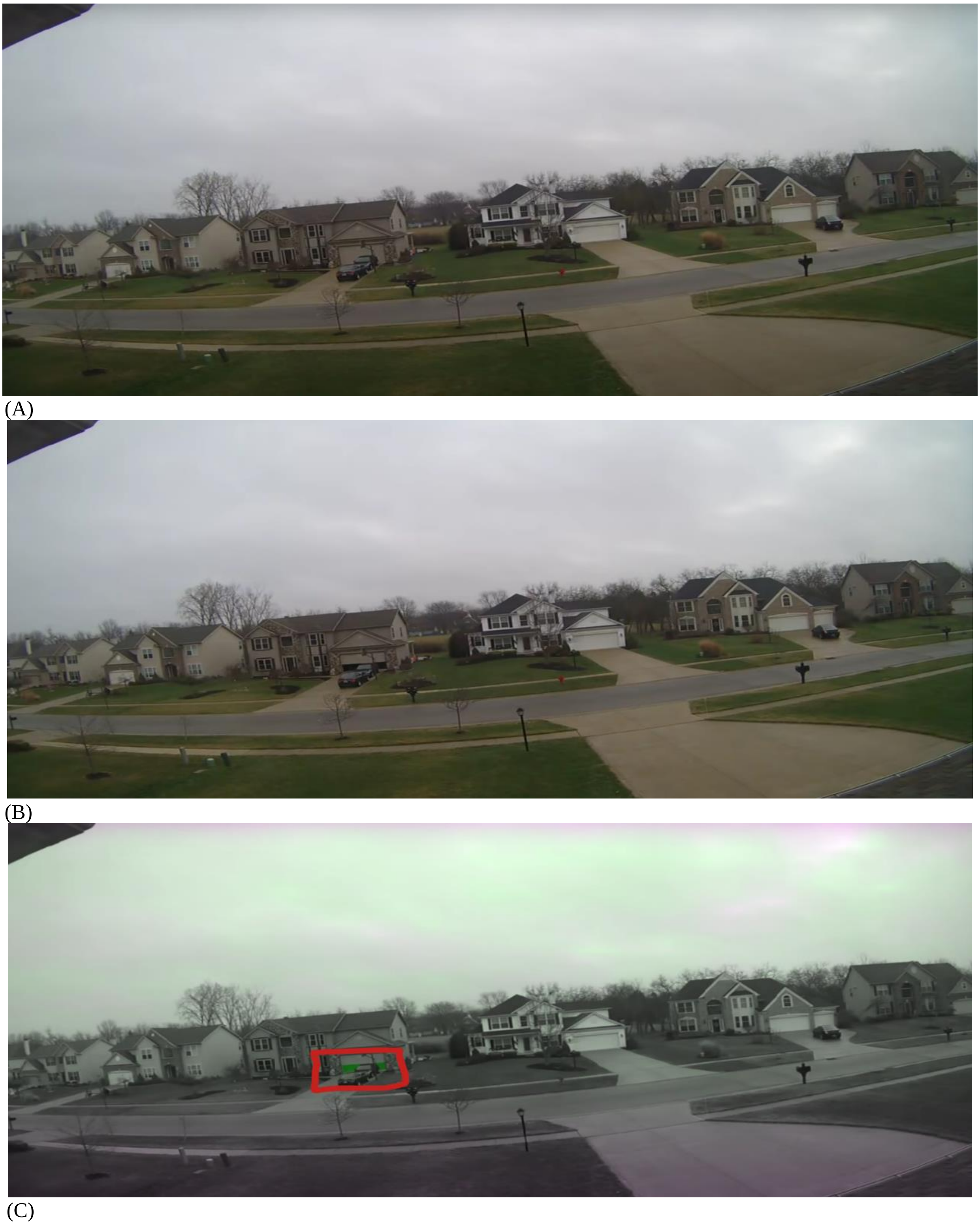


Figure 5. (A) shows the first surveilled scene, (B) shows the same location after time interruption, (C) shows the machine model identifying the highest difference between (A) & (B). highlighting a sign of a potential suspicious event, in this case the highlighted garage door was opened during the absence of the surveillance UAV. (A) & (B).

Source: Handa [28].

5. GPS\GNSS Spoofing

This section discusses the vulnerabilities of perimeter surveillance unmanned aerial vehicles to GPS spoofing threat and discusses some approaches to manage them, reviewing complementary positioning methods using onboard IMU and camera sensors, and local positioning system to increase the overall positioning accuracy and decrease the dependency on GPS. The vulnerable, weak and unauthenticated GPS signal necessitate techniques to handle the worst-case scenarios independent of GPS.

GPS spoofing is of a high interest in the UAV cyber-physical security community. Unmanned aerial vehicles UAV have proliferated into many sectors ranging from low sensitive applications to higher sensitive ones such as surveillance. The vulnerabilities of UAVs to cyber threats are like those of any computer device like a smartphone or a modern internet connected car. However, GPS spoofing could result of an attacker gaining access to the physical UAV, flying it to attack people, or damage physical equipment

GPS signals received near earth's surface are considered unauthenticated and weak (around –155dbW), an easily produced signals at similar frequency and higher power would overwrite them, exposing the UAV antenna to an intentional and unintentional interference from other signals, and enabling a low-cost attack point, especially on an exposed UAV by nature of operation.

The limited onboard capacity in terms of payload, computation power, memory and energy consumption, force the decision makers to find new ways to compensate for the deficiency of onboard cyber defense hardware and software by installing alternatives in the ground control station GCS and achieve a cost-efficient solution that satisfies standard security requirements. Figure 6 shows a spoofing attack illustration.

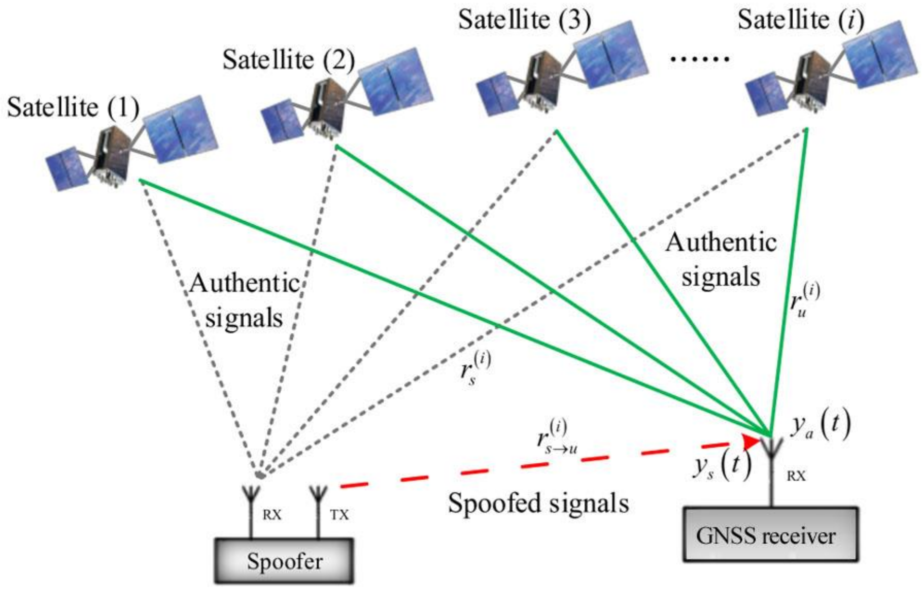


Figure 6.
Spoofing attack illustration.
Source: Liu, et al. [29].

The main three levels of securing the UAV against spoofing are prevention, detecting, and mitigation. A total dependency on one positioning method exposes the system to higher risk, the onboard receiver is the first line of defense, one or more differences between GPS and spoofed signal can be detected then acted upon by the receiver discrepancies such as the signals timing, direction, strength, and noise ratio are among the detectable anomalies identified in the literature.

One of the most cost-effective high-performance techniques is comparing Doppler residual which is resulted from the relative motion of satellites and the UAV, producing a spoofed signal that matches the Doppler residual of the legitimate signal is relatively complex. Detecting the spoofed signal is normally effective to reject their data, however, it has a low chance to isolate the legitimate data for a correct positioning. The consequences for failing to receive the legitimate GPS data by analyzing the signals, can be mitigated by integrating other positioning methods as described in the next section.

6. Complementary Positioning Methods

- *Positioning Based on Inertial Measurement Unit IMU*

This method is independent from wireless control signals, and requires no additional onboard hardware, the IMU an accelerometer that measures the linear acceleration of the UAV and a gyro sensor to measure its rotation in the 3-dimensional space, and many IMU units include a magnetometer. The processor can estimate the real-time position in reference to the launch platform by accumulating the summation of distances and directions data with relatively poor accuracy (meters), fusing other sensor data and software techniques such as the Kalman filter improves the accuracy. The main disadvantages of this method are the cumulative error, therefore, it’s mostly used simultaneously with other methods, its low requirement of computation power and no additional hardware attract the designer to include it with various positioning techniques, one example of an integration mechanism of two positioning methods is shown in Figure 7.

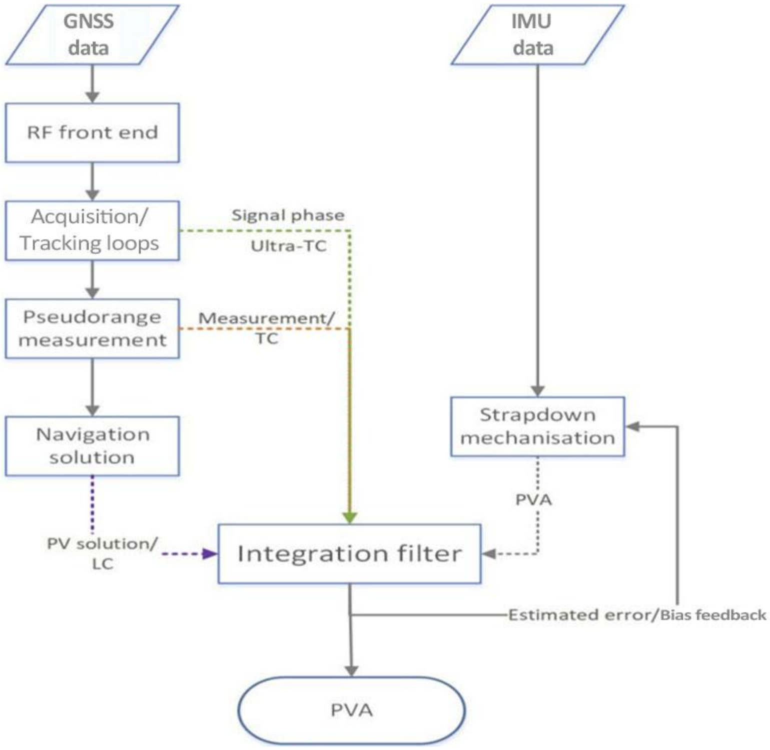


Figure 7.
The integration mechanism of two positioning methods to determine position, velocity, and attitude PVA.
Source: Jing, et al. [30].

- *Local Positioning System (LPS)*

The local positioning system uses 3 or more ground based radio signals instead of the GPS satellites, unlike GPS signals, LPS signals can be authenticated and encrypted reducing the probability of spoofing attack, however, this is a high cost complexity solution, and only suitable for a dedicated purpose infrastructure, the accuracy is relatively good especially when combined with other method, also it works in all-weather day and night conditions, the current rate improvement in electronics performance in parallel with reduction of cost have increased the feasibility and effectiveness of such method in some critical infrastructures. Different approaches have been suggested in the literature reviewed as the following,

- Measuring the signal attenuation to estimate the traveled distance from the transmission point.
- Measuring the angle of the received signal to estimate the orientation of the transmission point.
- Measuring the time delay of a clocked signal from different transmission points.

Figure 8 illustrates a local positioning system based on UltraWide-Band (UWB) radio technology, one UWB tag is installed on the UAV, and several UWB anchors installed on the ground to communicate the updated UAV coordinates.

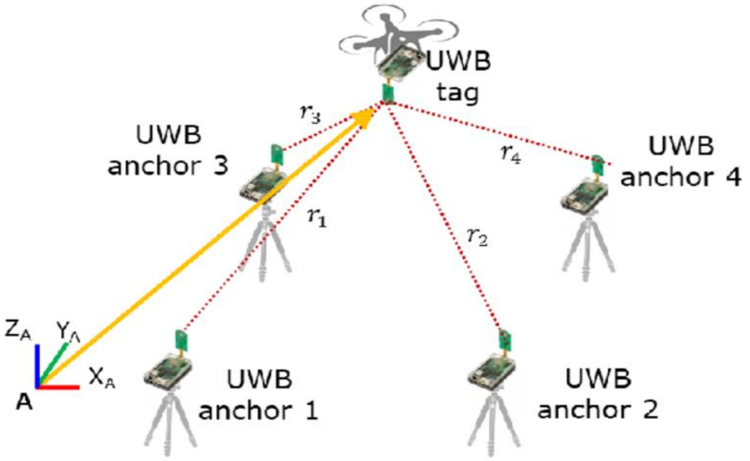


Figure 8.
Illustration of the Ultrawide-band (UWB) ranging positioning system, it shows four UWB ground anchors communicating the updated coordinates to the UWB tag mounted on the UAV.
Source: Park, et al. [31].

The inherited complexity of real-life application vs a controlled environment makes the risk of signal reflection a major drawback of the method and limits its usability in specific operation sites. The main advantage of this method is that the energy and computation consumption are mostly on the ground control stations, and not onboard the UAV.

- *Positioning Based on Vision*

This method use known ground visual cues to estimate the UAV position, and it achieve high positioning accuracy, the main disadvantages come from higher consumption of onboard computation power but still feasible, and low effectiveness when operating in low visibility environment, many algorithms for navigation aid and estimator of distance to approaching obstacles could be implemented, and the camera is a standard hardware on the UAV, to operate during low visibility thermal camera or a radar have been reviewed in the literature with effective performance.

Surveillance UAVs are mainly tasked to collect and analyze visual data, an onboard model that integrate imagery light intensity with accurate time and location of each image frame is an essential key performance of the system, although computational consuming, vision positioning by feature matching is an accurate, reliable, and cost-effective solution which has characteristics to override all other methods in an autonomous mode.

- *Positioning Based on Other Sensors*

Light Detection and Ranging (LiDAR) uses laser pulses to estimate distances to the ground objects by measuring the time for the reflected pulses to return to the receiver. In addition to all the vision limitations, LiDAR is limited in range, expensive (not a standard UAV sensor). The arguably higher accuracy has no added value over the vision method accuracy to countermeasure a spoofing attack. Acoustic sensors have similar limitations in range.

In practice the challenge arise for navigation priority in case of mismatching positioning, assigning a voting power is sufficient in one specific scenario, but should be abruptly changed according to the overall situation, an accurate collision avoidance and potential landing site detection still has many challenges in real life scenarios, computer vision is one domain that has the potential of satisfy multiple UAV system robustness requirement, it’s a cost effective in terms of hardware, software and onboard resources consumption.

The environment in which the UAV operates could affect the overall reliability, IMU is susceptible to a drift error, which can accumulate overtime, blurring and low visibility conditions impedes the vision performance. Any change in the operation environment dynamically changes the reliability of certain sensors, therefore human supervision is still needed.

Positioning is the cornerstone for autonomous navigation, GPS spoofing is a potential cyber-physical threat mostly for poorly designed systems, and many effective techniques could be implemented to mitigate the consequences of the attack, positioning based on multiple methods is feasible, and optimal to negate the disadvantage of individual methods, a combination of inertial and visual positioning can aid by improving accuracy and provide redundancy, autonomous flight system are not fully mature for the majority of locations.

7. Conclusion

The focus of this paper is to identify the main criteria to achieve adequate cyber-physical security level for surveillance UAV despite the exposed nature of operation and the limitation of onboard resources capacity, whenever possible the defensive tools should be installed in the ground stations. We found that using directional antennas could improve power consumption, increase the signal range, and reduce the attack space on the communication line to an order of magnitude. WPA3 encryption is effective for ground stations, lighter encryption for onboard such as Bleep64 would save onboard resources. Machine learning models have already achieved a high level of performance analyzing big data to predict and prevent cyber-attacks, as well as increase the performance efficiency of the system.

References

[1] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks-An approach to the risk assessment," presented at the 2013 5th International Conference on Cyber Conflict (CYCON 2013). IEEE, 2013.

[2] R. Szabolcsi, "A new approach of certification of the airworthiness of the UAV automatic flight control systems," *Land Forces Academy Review*, vol. 19, no. 4, pp. 423-431, 2014.

[3] R. Szabolcsi, "Conceptual design of unmanned aerial vehicle systems for non-military applications," in *Proceedings of the 11th Mini Conference on Vehicle System Dynamics, Identification and Anomalies VSDIA (pp. 637-644)*, 2008, pp. 637-644.

[4] H. P. D. Nguyen and D. D. Nguyen, "Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication," *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*, pp. 185-210, 2021. https://doi.org/10.1007/978-3-030-63339-4_7

[5] R. Szabolcsi, "Lateral/directional flying qualities applied in UAV airworthiness certification process," *Land Forces Academy Review*, vol. 19, no. 3, p. 336, 2014.

[6] R. Szabolcsi, "UAV longitudinal motion flying qualities applied in airworthiness certification procedure," *Land Forces Academy Review*, vol. 19, no. 2, p. 208, 2014.

[7] M. Khan, K. Heurtefeux, A. Mohamed, K. A. Harras, and M. M. Hassan, "Mobile target coverage and tracking on drone-be-gone UAV cyber-physical testbed," *IEEE Systems Journal*, vol. 12, no. 4, pp. 3485-3496, 2017. https://doi.org/10.1109/jsyst.2017.2777866

[8] A. C. Tang, "A review on cybersecurity vulnerabilities for urban air mobility. In AIAA Scitech 2021 Forum. Retrieved from https://studycrumb.com/alphabetizer," p. 0773, 2021.

[9] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Computing Surveys*, vol. 48, no. 4, pp. 1-31, 2016. https://doi.org/10.1145/2897166

[10] V. K. Ralegankar *et al.*, "Quantum cryptography-as-a-service for secure UAV communication: Applications, challenges, and case study," *IEEE Access,* vol. 10, pp. 1475-1492, 2021. https://doi.org/10.1109/access.2021.3138753

[11] C. Greer, M. Burns, D. Wollman, and E. Griffor, "Cyber-physical systems and internet of things. National Institute of Standards and Technology, US Department of Commerce. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf," 2019.

[12] N. Gupta, A. Tiwari, S. T. Bukkapatnam, and R. Karri, "Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks," *IEEE Access,* vol. 8, pp. 47322-47333, 2020. https://doi.org/10.1109/access.2020.2978815

[13] K.-F. Cheung, M. G. Bell, and J. Bhattacharjya, "Cybersecurity in logistics and supply chain management: An overview and future research directions," *Transportation Research Part E: Logistics and Transportation Review,* vol. 146, p. 102217, 2021. https://doi.org/10.1016/j.tre.2020.102217

[14] S. Iqbal, "A study on UAV operating system security and future research challenges," presented at the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2021.

[15] N. Zhao *et al.*, "Antenna and propagation considerations for amateur UAV monitoring," *IEEE Access,* vol. 6, pp. 28001-28007, 2018. https://doi.org/10.1109/access.2018.2838062

[16] A. Mohammadi, M. Rahmati, and H. Malik, "Location-aware beamforming for MIMO-enabled UAV communications: An unknown input observer approach," *IEEE Sensors Journal,* vol. 22, no. 8, pp. 8206-8215, 2022. https://doi.org/10.1109/jsen.2022.3157555

[17] R. H. Jacobsen and A. Marandi, "Security threats analysis of the unmanned aerial vehicle system," presented at the MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM). IEEE, 2021.

[18] S. Semenov, D. Voloshyn, V. Lymarenko, A. Semenova, and V. Davydov, "Method of UAVs Quasi-autonomous positioning in the external cyber attacks conditions," presented at the 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT). IEEE, 2019.

[19] J. Hu, D. Ma, C. Liu, Z. Shi, H. Yan, and C. Hu, "Network security situation prediction based on MR-SVM," *IEEE Access,* vol. 7, pp. 130937-130945, 2019. https://doi.org/10.1109/access.2019.2939490

[20] R. Araújo, A. Pinto, and P. Pinto, "A performance assessment of free-to-use vulnerability scanners-revisited," presented at the IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, Cham, 2021.

[21] M. A. Muin, K. Kapti, and T. Yusnanto, "Campus website security vulnerability analysis using nessus," *International Journal of Computer and Information System,* vol. 3, no. 2, pp. 79-82, 2022. https://doi.org/10.29040/ijcis.v3i2.72

[22] S. Z. Khan, M. Mohsin, and W. Iqbal, "On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions," *PeerJ Computer Science,* vol. 7, p. e507, 2021. https://doi.org/10.7717/peerj-cs.507

[23] C. Ma, J. Yang, J. Chen, Z. Qu, and C. Zhou, "Effects of a navigation spoofing signal on a receiver loop and a UAV spoofing approach," *GPS Solutions,* vol. 24, no. 3, pp. 1-13, 2020. https://doi.org/10.1007/s10291-020-00986-z

[24] M. Hamurcu and T. Eren, "Selection of unmanned aerial vehicles by using multicriteria decision-making for defence," *Journal of Mathematics,* vol. 2020, pp. 1-11, 2020. https://doi.org/10.1155/2020/4308756

[25] K.-P. Lin and K.-C. Hung, "An efficient fuzzy weighted average algorithm for the military UAV selecting under group decision-making," *Knowledge-Based Systems,* vol. 24, no. 6, pp. 877-889, 2011. https://doi.org/10.1016/j.knosys.2011.04.002

[26] A. Alex, "8 ways to increase your drone's range. Phantomangel. Retrieved from https://phantomangel.rocks/8-ways-to-increase-your-drones-range.html," 2022.

[27] M. Daudelin, "Nessus scan report. Tenable. Retrieved from https://www.tenable.com/sites/all/themes/tenablefourteen/img/nessus/live-results.jpg," 2022.

[28] M. Handa, "House fire 1-2-17 Recorded on the Nest Camera [Video]. YouTube. Retrieved from https://www.youtube.com/watch?v=yHfoMrge4Zg&t=236s," 2017.

[29] Y. Liu, S. Li, Q. Fu, and Z. Liu, "Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system," *Sensors,* vol. 18, no. 5, p. 1433, 2018. https://doi.org/10.3390/s18051433

[30] H. Jing, Y. Gao, S. Shahbeigi, and M. Dianati, "Integrity monitoring of GNSS/INS based positioning systems for autonomous vehicles: State-of-the-art and open challenges," *IEEE Transactions on Intelligent Transportation Systems,* vol. 23, no. 9, pp. 14166-14187, 2022. https://doi.org/10.1109/tits.2022.3149373

[31] K. Park, J. Kang, Z. Arjmandi, M. Shahbazi, and G. Sohn, "Multilateration under flip ambiguity for uav positioning using ultrawide-band," *ISPRS Annals of Photogrammetry, Remote Sensing and Spatial Information Sciences,* vol. 5, pp. 317-323, 2020. https://doi.org/10.5194/isprs-annals-v-1-2020-317-2020