sensors

MDPI

Article

A Self-Diagnosis Method for Detecting UAV Cyber Attacks Based on Analysis of Parameter Changes

Elena Basan [1,*], Alexandr Basan [1], Alexey Nekrasov [1], Colin Fidge [2], Ján Gamec [3] and Mária Gamcová [3]

[1] Institute for Computer Technologies and Information Security, Southern Federal University, Chekhova 2, 347922 Taganrog, Russia; basanalex@gmail.com (A.B.); alexei-nekrassov@mail.ru (A.N.)
[2] Science and Engineering Faculty, Gardens Point Campus, Queensland University of Technology (QUT), Brisbane City QLD 4001, Australia; c.fidge@qut.edu.au
[3] Faculty of Electrical Engineering and Informatics, Technical University of Košice, Letná 9, 042 00 Košice, Slovakia; jan.gamec@tuke.sk (J.G.); maria.gamcova@tuke.sk (M.G.)
* Correspondence: ele-barannik@yandex.ru; Tel.: +7-951-20-5488

Abstract: We consider how to protect Unmanned Aerial Vehicles (UAVs) from Global Positioning System (GPS) spoofing attacks to provide safe navigation. The Global Navigation Satellite System (GNSS) is widely used for locating drones and is by far the most popular navigation solution. This is because of the simplicity and relatively low cost of this technology, as well as the accuracy of the transmitted coordinates. Nevertheless, there are many security threats to GPS navigation. These are primarily related to the nature of the GPS signal, as an intruder can jam and spoof the GPS signal. We discuss methods of protection against this type of attack and have developed an experimental stand and conducted scenarios of attacks on a drone's GPS system. Data from the UAV's flight log were collected and analyzed in order to see the attack's impact on sensor readings. From this we identify a new method for detecting UAV anomalies by analyzing changes in internal parameters of the UAV. This self-diagnosis method allows a UAV to independently assess the presence of changes in its own subsystems indicative of cyber attacks.

Keywords: UAV; GPS; cyber threats; anomalies; spoofing; entropy; cyber attacks

check for updates

Citation: Basan, E.; Basan, A.; Nekrasov, A.; Fidge, C.; Gamec, J.; Gamcová, M. A Self-Diagnosis Method for Detecting UAV Cyber Attacks Based on Analysis of Parameter Changes. *Sensors* **2021**, *21*, 509. https://doi.org/10.3390/s21020509

Received: 13 December 2020
Accepted: 9 January 2021
Published: 13 January 2021

1. Introduction

A drone or Unmanned Aerial Vehicle (UAV) is a cyber-physical system combining physical processes, computation, and networking. If an attack on the Global Positioning System (GPS) is executed well, it can lead to serious consequences for a single UAV or a UAV group [1]. In addition to the natural errors and inaccuracies in sensor readings, GPS vulnerabilities also affect the flight controller. These vulnerabilities include the possibility of signal jamming or a signal distortion that disrupts the availability of the GPS signal. GPS vulnerabilities go beyond the natural properties of the transmitted signal. In GPS spoofing attacks, satellites transmitting a GPS signal are tampered with to manipulate the UAV's navigation system by transmission of fake coordinates [2,3]. Although the GPS signal's waveform can be implemented in a secure design, thanks to authentication and encryption mechanisms [4], for military applications, civilian GPS variants, which do not have protection mechanisms, are frequently used. Consequently, civilian GPS is highly vulnerable to spoofing attacks [3].

A GPS spoofing attack entails consequences associated with the fall (crash) of the UAV or its interception and redirection along a different flight path. In both cases, these problems are related to cyber security. A targeted attack that takes control of a UAV or destroys it can harm everyone in the UAV's flight area or damage other vehicles [5]. One of the main security concerns of UAVs is GPS spoofing attacks [6]. The civil GPS specification is publicly available [7], which makes the signal highly predictable and increases the potential risk of tampering. Therefore, GPS spoofing has become an important research topic since an attacker could hijack a UAV, use it to eavesdrop, or attack people or objects remotely.

Currently, many different methods of detecting GPS spoofing attacks are known [8–12]. Some of these methods allow the UAV's GPS receiver to detect spoofing attacks [8]. These techniques include the ability of the GPS receiver to analyze the received signal strength and to compare it to the normal signal strength over time. UAVs can monitor GPS satellite identification codes or continually check the time intervals to ensure their constancy. These methods can be efficient in detecting attackers with weak capabilities. However, such methods may be ineffective against complex attacks, in which an attacker can falsify the coordinates of the victim with great accuracy [9]. O'Hanlon et al. proposed a method for detecting GPS spoofing attacks based on the use of two GPS receivers to check their cross-correlation [10]. This method has been tested for multiple attack scenarios and the authors have proven that it successfully detects attacks, although the method is unable to distinguish spoofing signals from genuine GPS signals and cannot detect spoofing when the signals are weak [13]. Other methods to prevent GPS spoofing, such as autonomous monitoring of receiver integrity, signal-to-noise ratio measurements, and Doppler shift detection, have been discussed [6,14]. For instance, Shepard et al. proposed a method allowing the UAV to detect the source of GPS spoofing using a ground station that continuously analyzes the content and time of arrival of information about the estimated location of the UAV [2]. It has been shown that their method is efficient and detects spoofing attacks in less than 2 s and determines a counterfeit's source location after monitoring for 15 up to 150 m. Solove uses the automatic GPS signal gain control in a GPS receiver to detect and alert potential spoofing attacks within the method [15].

The ability to use multiple receivers to detect GPS spoofing attacks has been presented in several previous works [16–18]. Jansen et al. [17] used several independent GPS receivers to detect GPS spoofing attacks. Their proposed method depends on the distance between the receivers and then measuring the distance between the specified locations of the receivers. With the same GPS signals, the measured distances are the same as the previously recorded distances. However, in a GPS spoofing attack, the distances obtained will be very close to zero, since all receivers transmit information where the same location is indicated. Montgomery et al. demonstrated the possibility of using a receiver with two antennas for detecting GPS spoofing attacks [16]. Their proposed method is based on fixing the difference in carrier frequencies between different antennas tied to the same generator. In their configuration, the attacker must use an additional transmit antenna for each additional receiver antenna, which complicates the attacker's task. Heng et al. [18] use multiple receivers to confirm the authenticity of GPS signals based on correlation with the military GPS signal without the need to decode it. This uses cross-validation receivers to authenticate the GPS signals. It has been shown that the proposed technique is efficient even when cross validation receivers are tampered with. This method has been tested on fixed and moving GPS receivers and shown to be effective in detecting spoofing attacks.

Panice et al. [19] presented an approach to detecting a GPS spoofing attack for a UAV, based on state analysis using a Support Vector Machine (SVM), which is used as an anomaly detection tool. They present solutions for detecting anomalies and a simulation environment for GPS attacks to assess the functionality and performance of the method. Their approach does not require additional equipment, and so it can be implemented on a small UAV. On the other hand, if the intruder has absolute knowledge of the positioning and trajectory of the UAV, he can go unnoticed by the system, causing significant false operations. Nonetheless, since usually the intruder does not know the actual trajectory of the UAV, the risk of a false alarm is small. Thus, the system can detect any spoofing attack.

Eldosouky et al. [20] suggested a protective mechanism based on the concept of co-localization [21]. Their mechanism is a methodology that allows a UAV to determine its real position in a two-dimensional coordinate system using the location of three other UAVs. It is assumed that each UAV has a device for measuring the relative distances to other neighboring UAVs. The co-localization of the UAV selects any three adjacent UAV to update their location, assuming that the selected UAVs do not lie on a straight line. The UAV can then pinpoint its 2D position accurately. With a covert GPS spoofing attack, the UAV cannot trust its GPS location or the location of other UAVs. However, the choice of a nearby UAV for the co-localization mechanism is fraught with risk since the UAV itself may be compromised. To overcome this limitation, the authors propose a protection mechanism based on the assumption that an attacker using GPS spoofing can attack only one UAV [20]. In their proposed mechanism, the UAV will use the location of four adjacent UAVs, instead of three, to determine its real location by identifying the UAV under attack and excluding it from calculations. This mechanism has the same cooperative localization requirements (i.e., the UAVs are non-collinear), UAVs can query the location of other UAVs through communication between them, and each UAV must be able to measure distances to neighboring UAVs. Thus, it should be noted that their method has many restrictions on its applicability.

Qiao et al. presented a method of counteracting GPS attacks based on the use of a technical vision system, which additionally allows calculation of the UAV's speed and some other indicators and correlates them with the data received from the GPS [22]. Thus, the main methods of protecting UAVs from attacks related to GPS signal spoofing are based on the analysis of the state change in comparison with the reference of one sensor or on the correlation of data obtained from several GPS sensors. In some methods, in addition to GPS, other sensory mechanisms such as an accelerometer magnetometer and others are used to improve the quality of flight [23]. In this case, the correlation can take place both between devices of one UAV and between devices of a group of UAVs [24].

Semanjski et al. presented a method for determining the authenticity of a GPS signal based on the correlation between true and incoming signals using C-Support Vector Machine (C-SVM) classification [25]. Application of their method is suggested at the signal receiver level to avoid changes that may occur during signal processing. To train their classifier the authors used both data obtained under laboratory conditions and in real cases of attacks. They believe that the supervised machine learning-based approach (C-SVM) has great prospects since they managed to achieve positive results. The model they presented has achieved high detection rates compared to previously existing ones. In addition, by including a real meaconing event, the complexity of the model was improved. Thus, supplementing training datasets with real-world scenarios appears to be a valuable contribution to safety-critical models such as the detection of attempts to manipulate Global Navigation Satellite System (GNSS) signals. However, a disadvantage of this approach is the significant time and effort required for preparation and elaboration of the data set for training.

Kwon and Shim proposed a method for direct detection of GPS spoofing attacks using a positioning system based on an accelerometer [26]. They conducted a performance analysis using probability density functions. The difference between the measurements obtained by the accelerometer and a GPS receiver is used to detect an attack. The value of the error is used to obtain decision variables indicating the presence of an attack. The performance of two decision variables was compared by calculating the spoofing detection probability and the detectable minimum spoofing acceleration, considering the predetermined false alarm probability and the predetermined detection probability. The decision variables represent the change in the horizontal and vertical acceleration, both of which must be used together. Then the authors add another variable for the solution of the northern acceleration. The GPS spoofing detection method suggested in their paper is thus influenced by the acceleration error. Flying or driving conditions can affect GPS spoofing detection performance. For instance, if a ground vehicle encounters obstacles in the road, such as potholes, bumps, etc., its accelerometers can show large changes and degrade the ability to detect GPS spoofing.

Guo et al. presented a method for detecting and countering spoofing [27]. They used an algorithm based on Maximum Likelihood (ML) to solve the problem of multipath reduction to anti-spoofing. The authors presented tracking channels using multi-correlators and proposed a set of actions to detect and remove fake signals, to ensure that the receiver blocks the signals during a spoofing attack. Due to the complexity and variety of interference implemented by an attacker, using one anti-spoofing method may not prevent all types of spoofing. For example, an anti-spoofing method based on a multi-correlator structure can help block the signal. However, if spoofing started during data collection, this method will not be able to distinguish the genuine and fake recipient signals. Experimental results show that their proposed anti-spoofing method allows estimating the time delay, amplitude, and phase of the carrier of a fake signal with a small delay, and then eliminating it by adding the opposite fake signal. In addition, this method can perform a self-test, so that it can directly distinguish the phase of the genuine signal when the fake signal has a long delay. Finally, their proposed method can ensure that the receiver keeps the authenticated signal blocked when the correlation peak of the fake signal overlaps or moves away from the correlation peak of the authenticated signal and can further ensure that the receiver is positioned correctly in the presence of spoofing.

However, many authors say these previous methods are prone to false positives. Instead we present a method for detecting anomalies and attacks on UAVs based on the analysis of data collected and analyzed from the UAV's own sensors only. The analysis compares normalized readings of the sensors at different points in time and identifies the degree of difference between them.

This offers a new method for detecting anomalies and attacks on UAVs based on the analysis of changes in the UAV's state. The main difference of our method from the methods discussed above is that, to detect an attack, we do not need reference values or need to correlate the collected data with additional GPS receivers or other external systems. Our "self-diagnosis" method is based on the UAV's ability to detect critical changes in its own behavior over time. The analysis is based on the collection and processing of data received from various parts of the UAV's sensor system. Any sensors that produce numerical readings can be used. At the same time, as experimentally confirmed, our method makes it possible to detect accurately the presence of anomalous behavior and identify an attack.

The main purpose of this article is to present our method for detecting UAV sensor anomalies under the influence of a GPS attack. Therefore, the following tasks should be solved:

- To develop and implement a stand for carrying out an attack on a UAV;
- To carry out flight tests with a UAV in normal mode and during an attack;
- To collect the results in the form of UAV logs;
- To analyze the logs and identify the parameters that are susceptible to attack;
- To get raw data for testing the method;
- To develop a method for detecting anomalies for a UAV and to prove its effectiveness.

2. Materials and Methods

As a result of theoretical and experimental analysis, we identified a set of the most informative parameters that may indicate a cyber attack. These parameters are: CPU workload, UAV flight altitude (h_a), satellite fix status (G_n), GPS uncertainty (G_u), and GPS noise (G_{noi}) when detecting a GPS spoofing attack. To analyze changes in these parameters, it is necessary to choose an appropriate type of probability distribution. The choice is based on the fact that these parameters are discrete. Let us consider the most common distribution laws and assess whether they are suitable for the given parameters presented above or not. If the number of occurrences of a random event per unit of time is available, when the fact of the occurrence of this event in each experiment does not depend on how many times and at what points in time it happened in the past, and does not affect the future, and tests are carried out under stationary conditions, then Poisson's law is usually used to describe such a quantity. Poisson's law is also called the law of rare events. Thus we used the Poisson distribution law because, when analyzing the parameters in this study, it is necessary to assess the occurrence of unexpected peak values, which are rare events during the total number of operations of the UAV [28]. The Poisson model $P()$ is typically used to describe a rare events scheme [29]. Under some assumptions on the nature of random events (the changes observed are random, independent, and discrete events), their number occurring over a specified time interval or a space area often obeys the Poisson distribution:

$$P(K_n) = \frac{\lambda^{K_n}}{K_n!}e^{-\lambda}, \tag{1}$$

$$P(Gn) = \frac{\lambda^{Gn}}{Gn!}e^{-\lambda}, \tag{2}$$

$$P(h_a) = \frac{\lambda^{h_a}}{h_a!}e^{-\lambda}, \tag{3}$$

$$P(G_u) = \frac{\lambda^{G_u}}{G_u!}e^{-\lambda}, \tag{4}$$

$$P(G_{noi}) = \frac{\lambda^{G_{noi}}}{G_{noi}!}e^{-\lambda}, \tag{5}$$

where P is the probability function of the distribution of a random variable according to Poisson's law; K_n is the percentage of the total amount of processor time in the interval between n and $n-1$ that the processor spent on processing tasks when running in the kernel mode; h_a is the UAV's flight altitude; G_n is the state of fixation by satellites (i.e., the number of satellites from which the UAV receives position information); G_u is the GPS's uncertainty; G_{noi} is the GPS's noise (these parameters are discrete); λ is the mathematical expectation (the average number of events of interest per unit of time); and e is Euler's number.

To obtain the distribution, ten random variables are used. Then the sliding window concept is used to update the distribution information. Six previous values and four new ones are taken and a new distribution is constructed. This concept allows fixing a sharp increase in values. Further, to determine the presence of an anomaly or a state change, it is necessary to determine to what extent the distributions differ from each other. Comparison of distributions rather than raw data gives a more accurate result. Raw data can vary dramatically. At the same time, the changes and observations obtained based on raw data will not indicate an anomaly or attack. Normalizing the raw data and bringing it to a suitable distribution will capture the change in the system. If the entropy values are used (i.e., differences between distributions), an anomaly can be detected. The Kullback-Leibler divergence can be used to calculate the entropy value, for example as in Afgani et al.'s work [30]. In this case, it is necessary to use not an integral value, but a sum, since we are talking about discrete quantities:

$$D(P_n(\lambda_n)\Delta t||P_n(\lambda_n)(\Delta t-1)) = \sum_{n_i \in N} P_n(\lambda_n)\Delta t * \ln\frac{P_n(\lambda_n)\Delta t}{P_n(\lambda_n)(\Delta t-1)}, \tag{6}$$

where $P_n(\lambda_n)\Delta t$ is the Poisson distribution for a given exponent n for the current period Δt; $P_n(\lambda_n)(\Delta t-1)$ is the Poisson distribution for a given exponent n for the previous period of time; and ln is the natural logarithm.

Then, our algorithm for detecting anomalies is as follows:

1. Fixation of the raw values of the analyzed parameters for a certain period of time.
2. Plotting a suitable distribution type for the collected parameters.
3. Selection of the previous values and supplementing them with those collected at a new point in time, to build a time series of values using a sliding window.
4. Construction of a new distribution for new values according to the same distribution law.
5. Calculation of the Kullback-Leibler divergence between the two distributions.
6. The higher the obtained value of the Kullback-Leibler divergence, the more likely it is that the system has been influenced in the form of an attack or external destructive influence. Typically, this value should be greater than or equal to two. This value was

chosen with the condition that the divergence should tend to zero and not exceed one. But to avoid unnecessary false alarms, the threshold was increased to two, which was confirmed experimentally.

7. Repeat the algorithm for subsequent values, starting from step 3.

Therefore, the higher the entropy, the more likely it is that abnormal behavior is observed. Abnormal behavior can occur not only due to the attack but also due to environmental conditions. Thus, for example, changes in the engine speed and flight altitude may not be related to an attack. To unambiguously identify an attack, it is necessary to analyze several indicators at once and determine the degree of their deviation. Figure 1 shows the calculation of the entropy value for the UAV flight altitude during an attack.

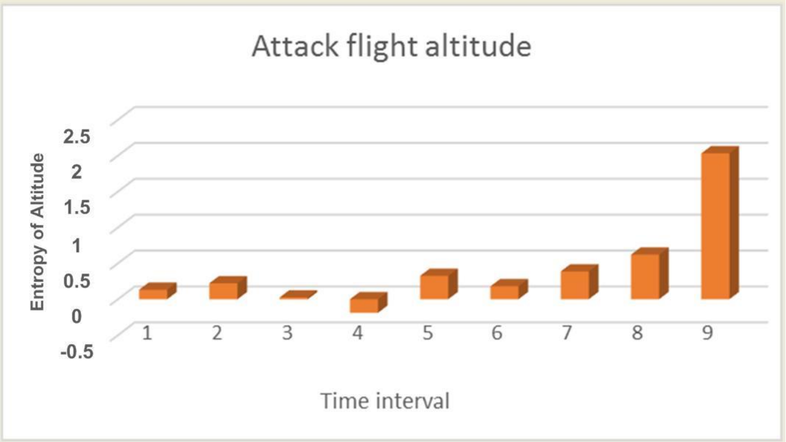


Figure 1. The result of calculating the Kullback-Leibler divergence of the deviation of the flight altitude indicator during an attack.

Since the attack on the UAV did not begin immediately, the first few values in Figure 1 are quite low, and so we can see an increase in value only in the last three calculations. This is because the UAV under attack may crash and has already begun to descend sharply, but as a result of operator intervention in the crash process, it was prevented. But as mentioned earlier, a lowering of the flight altitude can only indirectly confirm an attack. The most indicative parameter is the number of GPS satellites. The parameter for this calculation is shown in Figure 2.

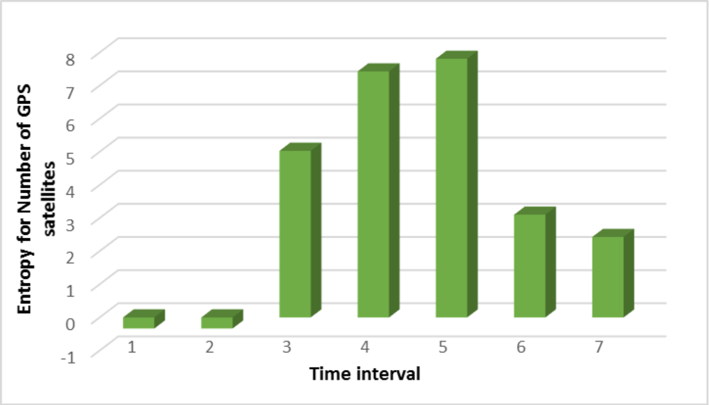
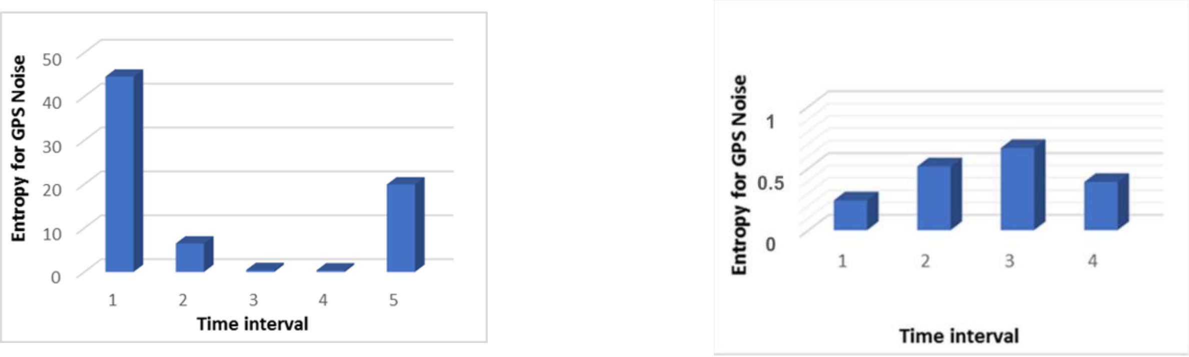


Figure 2. The result of calculating the Kullback-Leibler divergence for the indicator “number of GPS satellites” at the time of the attack.

Figure 2 shows that high values begin in interval 3. This does not mean that the number of satellites has increased as it also could have decreased. The main thing is that the type of distribution between intervals 2 and 3 does not coincide, and this indicates that significant changes have occurred when the number of satellites should be approximately the same. It should be noted that the comparison did not take place with the data obtained in a normal situation. Namely, the data obtained from the different time intervals in the same overall period of the UAV's flight was compared. For example, let us compare the results of searching for anomalies when analyzing the noise level with and without an attack, as shown in Figure 3.



(**a**) (**b**)

Figure 3. The result of measuring the Kullback-Leibler divergence of the GPS noise index: (**a**) During the attack; and (**b**) under normal conditions.

Figure 3 shows that during the attack, an increase in the entropy value is observed three times. In other words, we can say that it took place throughout the entire flight. During the normal flight, the entropy value remained at the minimum level. This does not mean that there were no deviations during normal flight. They were simply insignificant and did not affect the quality of the flight.

3. Results and Discussion

For the experimental study of our method, a quadcopter UAV whose architecture was developed for testing attacks and analyzing security threats was used. Table 1 presents the main characteristics of the experimental stand.

Table 1. Experimental stand characteristics.

Part Name	Model
Flight controller	Pix Hawk 4 (STable 10.1 firmware)
Frame	S500
Speed controllers	XT-XINTE 30A
Telemetry	3DR Radio Telemetry 915 MHz 100 mW Aerial Ground Data Transmission Module for Pixhawk 4
Receiver	FS-I6B
Battery	ZOP Power 3S 11.1V 4200 mAh 40C Lipo Battery XT60 Plug

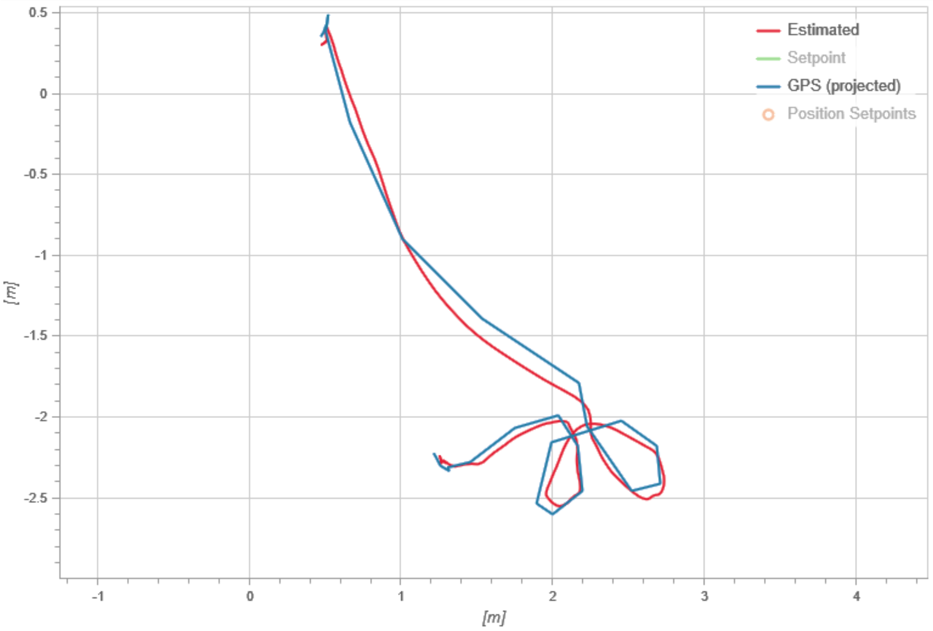
One of the scenarios is that the quadcopter, having determined its current position, receives the static coordinates of its target. A copter-type UAV moves to a given point and fixes its position in space, while maintaining its altitude. In the case of an external physical impact, for example, a natural factor or impact from another object, the UAV's autopilot system increases the engine speed and sets it in the opposite direction to maintain a given position. When the UAV is displaced from its preset position, the position hold system increases the engine's RPM power depending on the distance between the preset point and the actual location of the UAV. When the UAV returns to a given point, the autopilot enters the normal altitude control mode. In the scenario of maintaining a position with fixed coordinates, an attacker could influence the direction and speed of movement. After the start of the attack, the quadcopter navigation system perceives the broadcast signal as real, thus the actual location of the UAV differs from that determined by the navigation system. After the autopilot system detects the displacement, the UAV starts moving in the opposite direction. Thus, by indicating a fake offset on the circle, where the center will be the fixation point of the UAV, you can set the direction of movement. The attacker's task is to smoothly shift the fake geo position from the center, that is, the place where the quadcopter is fixed, to the point of the circle. By adjusting the radius of this circle, the attacker can influence the speed of the quadcopter. By adjusting the speed and motion vector, the attacker can control the location of the UAV. An important factor is that when broadcasting a fake position, the attacker must independently consider the physical impact on the UAV. To counteract external factors, it is important to determine the real position of the quadcopter.

During our experimental study, an attack was carried out on the UAV five times, while the positive effect took place every time. Let us consider the data collected from the logbook during the attack and normal UAV flight. Figure 4 shows the result of fixing the UAV's flight trajectory.

In Figure 4, the red line shows the estimated trajectory (Estimated) which is the flight path calculated by the on-board computer according to the accelerometer. The blue line shows the GPS trajectory (GPS projected) which is a trajectory built based on GPS module data.

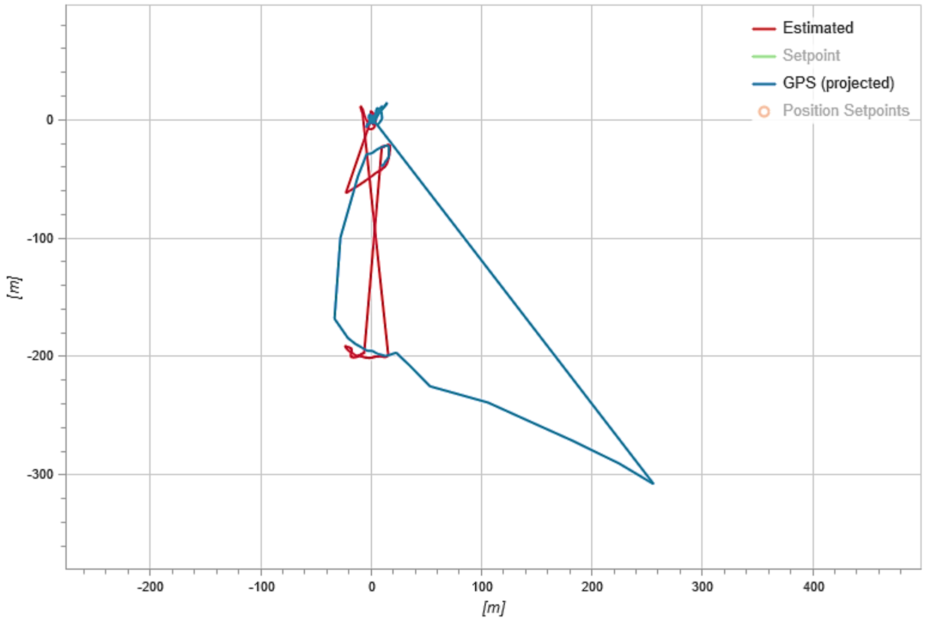
As we can see from Figure 4a, both trajectories coincide during the normal flight and this indicates the normal operation of the UAV. Figure 4b shows that during an attack, the GPS trajectory differs from the UAV trajectory recorded by the internal sensor. Since the attack was aimed at spoofing GPS data, it led to the difference in trajectories, because many GPS systems are only updated once a second (and high-performance GNSS devices are updated five to 10 times a second) and often have an accuracy of ±1 m only in good conditions. The condition evaluator uses other sensors to fill in the gaps between 1 s GPS updates and thus improves accuracy.

Next, it is necessary to analyze the UAV's flight altitude in the normal mode and during an attack since this parameter affects the detection of an attack. Figure 5 shows the result of changing the UAV's flight altitude in the normal mode and during an attack.



(**a**)

Figure 4. *Cont.*



(**b**)

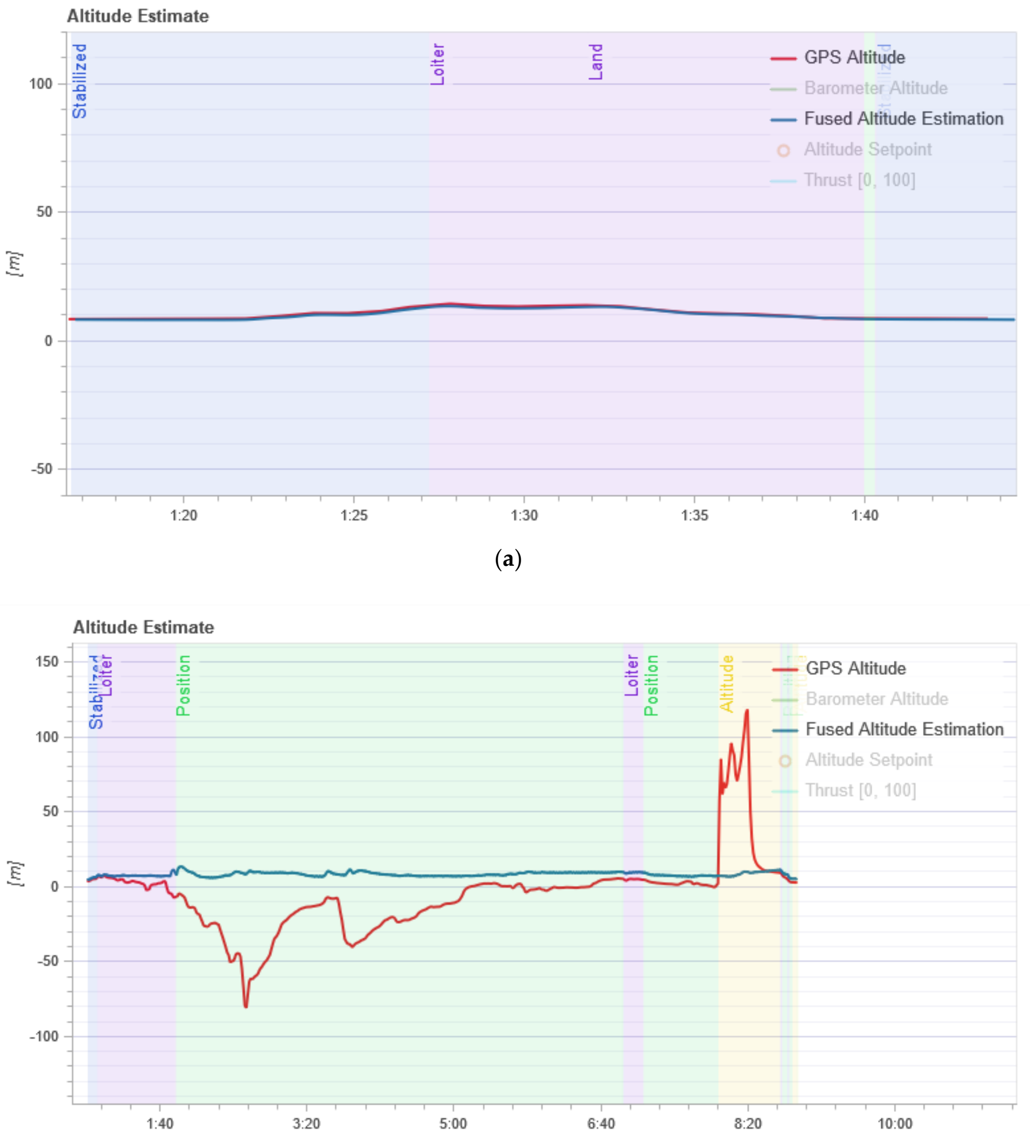
Figure 4. UAV flight trajectories: (**a**) In the normal mode; and (**b**) during a GPS attack.

In Figure 5, the red line (GPS Altitude) is the UAV flight altitude according to the GPS module, and the blue line (Fused Altitude Estimation) is the estimate of the change in altitude. Fused Altitude Estimation is the result of the state estimator, and so it uses not only the raw GPS data but also the accelerometer. As shown in Figure 5a, the GPS altitude and the final altitude coincide during normal UAV flight. Figure 5b shows that the altitude changes and the GPS altitude graph and the final altitude graph do not coincide during an attack on the GPS.

Next, we analyzed the data on the number of satellites that the UAV captures during regular flight and under the influence of an attack, as shown in Figure 6. In Figure 6, the gray line (Num Satellites used) is the number of satellites used. The blue line (GPS Fix) is the state of fixation by satellites. The GPS uncertainty graph shows information from the GPS device. The number of satellites used must be about 12 or higher.

Figure 6 shows that the GPS fix (blue line) is constant during normal flight. It means that the drone does not lose communication with satellites and always knows where it is. The average number of satellites used is 18 (gray line). During the attack (Figure 6), communication with satellites is not stable and the number of satellites is constantly changing. You can also see when the UAV loses its GPS fix, the number of satellites used to determine the location is 0.

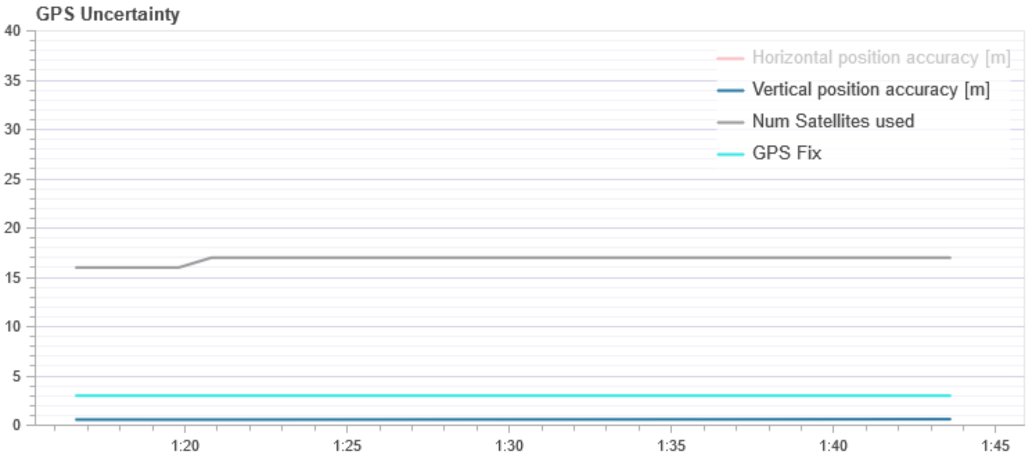
The GPS noise sensor readings are shown in Figure 7. In Figure 7, the red line (Noise per msec) is the GPS noise. The GPS noise and interference graph is useful for checking for GPS signal interference. The GPS signal is very weak and; therefore, can be easily disturbed/jammed by components transmitting (via cable) or transmitting at the frequency used by the GPS. The interference indicator should be around or below 40. Values around 80 or above are too high. Signal interference results in reduced accuracy and less satellite usage. Figure 7 shows that during normal flight the noise does not exceed 105 per ms, but during an attack, this indicator is not stable and at the peak has a value of 300 per ms. So we can conclude that during the attack a high noise level is in the GPS channel.



(**a**)

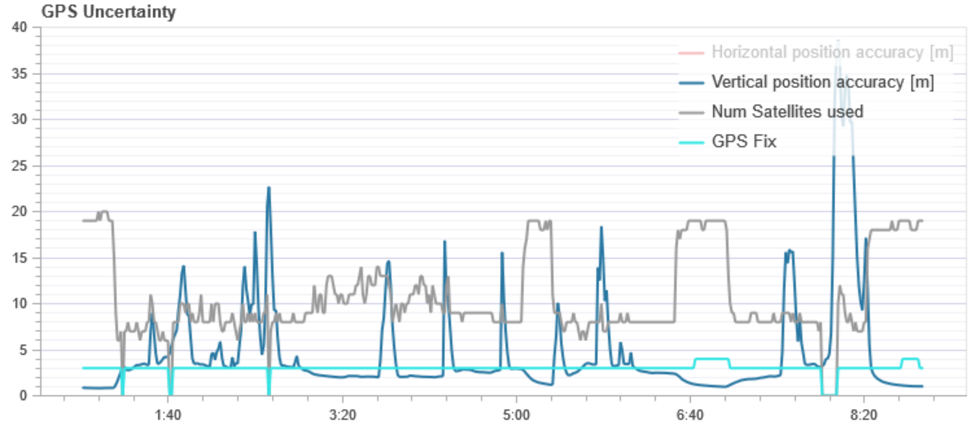
(**b**)

Figure 5. Readings of flight altitude sensors: (**a**) In the normal mode; and (**b**) during a GPS attack.



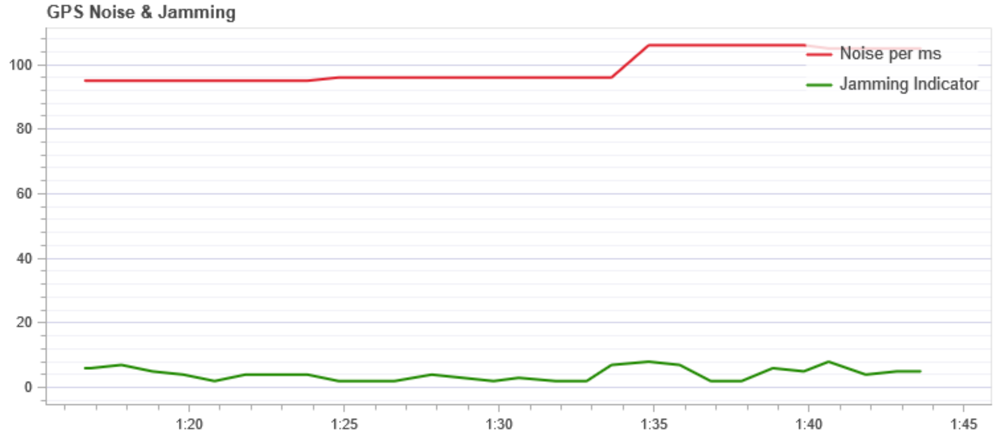
(**a**)

Figure 6. *Cont.*

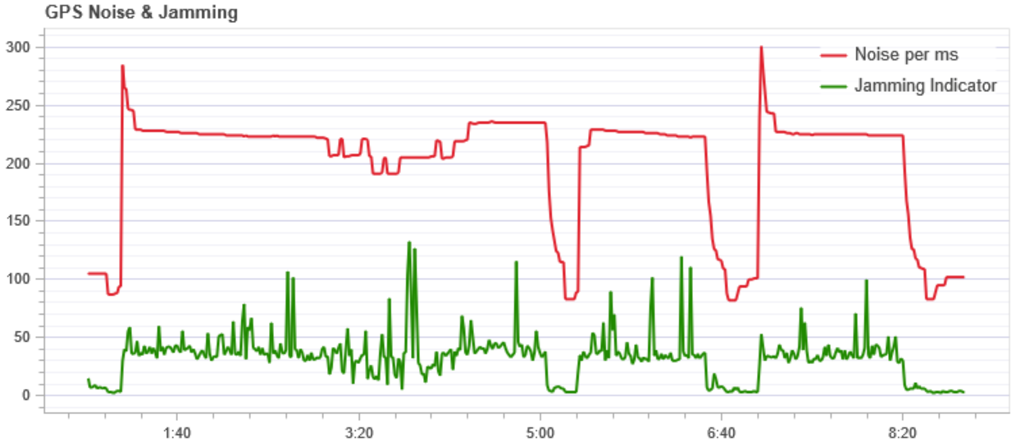


(**b**)

Figure 6. The state of the parameter indicating the number of GPS satellites: (**a**) In normal UAV flight mode; and (**b**) during a GPS attack.



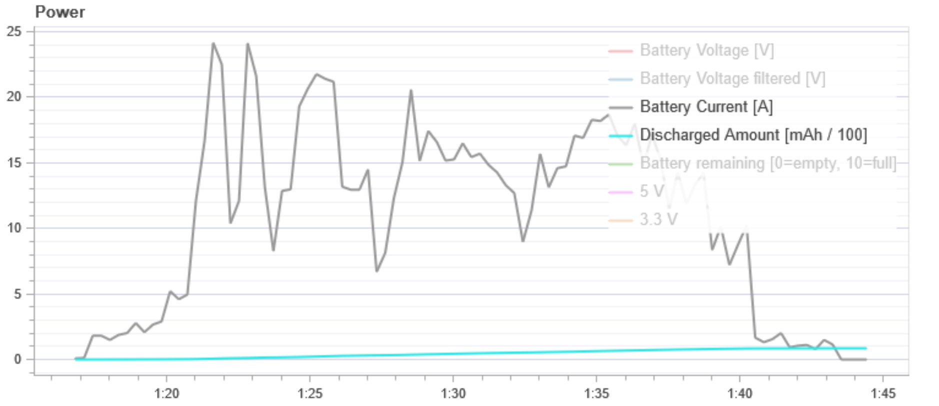
(**a**)



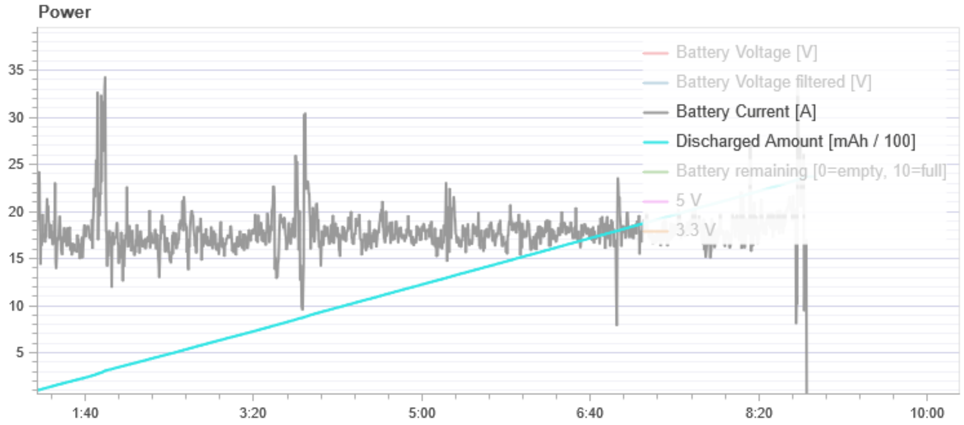
(**b**)

Figure 7. Indication of the level of noise affecting GPS: (**a**) In the normal mode; and (**b**) during a GPS attack.

Figure 8 shows energy consumption. In the normal flight mode, the UAV has an average power consumption of 500 to 1000 mAh. During the attack, we see a strong power consumption of 10,000 to 40,000 mAh. Thus, we can conclude that the UAV spends much more energy to maintain its flight when it is under attack.



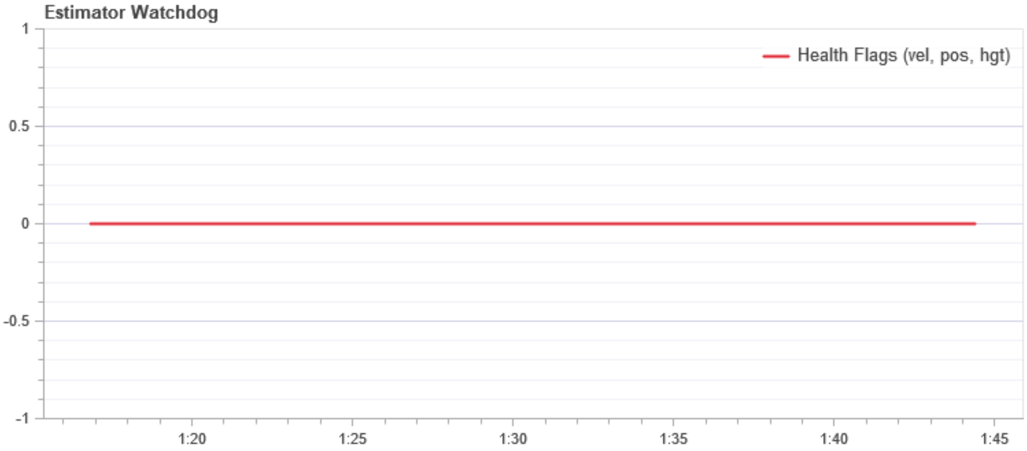
(**a**)



(**b**)

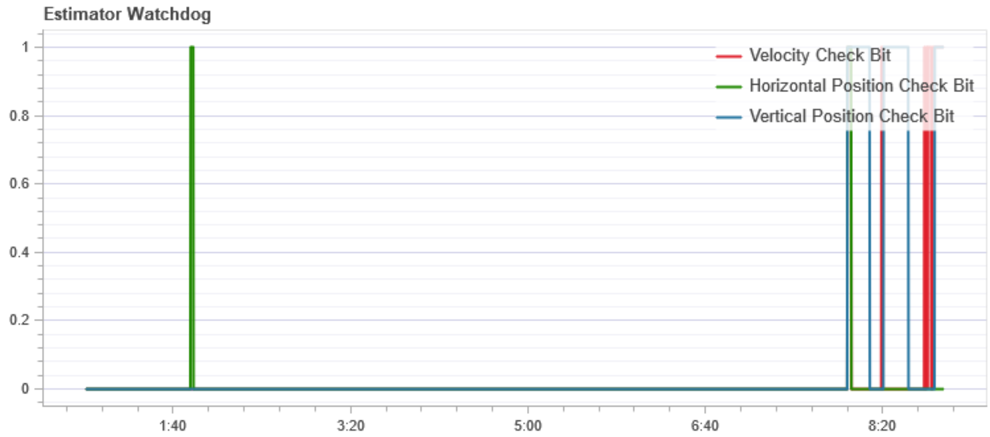
Figure 8. Energy consumption curves: (**a**) In the normal mode; and (**b**) during a GPS attack.

Figure 9 shows the measurement result of the condition evaluator. It should be a constant zero. If one of the flags is nonzero, the evaluator has encountered a problem that requires further investigation. In most cases, this is a problem with the sensor, for example, magnetometer interference.



(**a**)

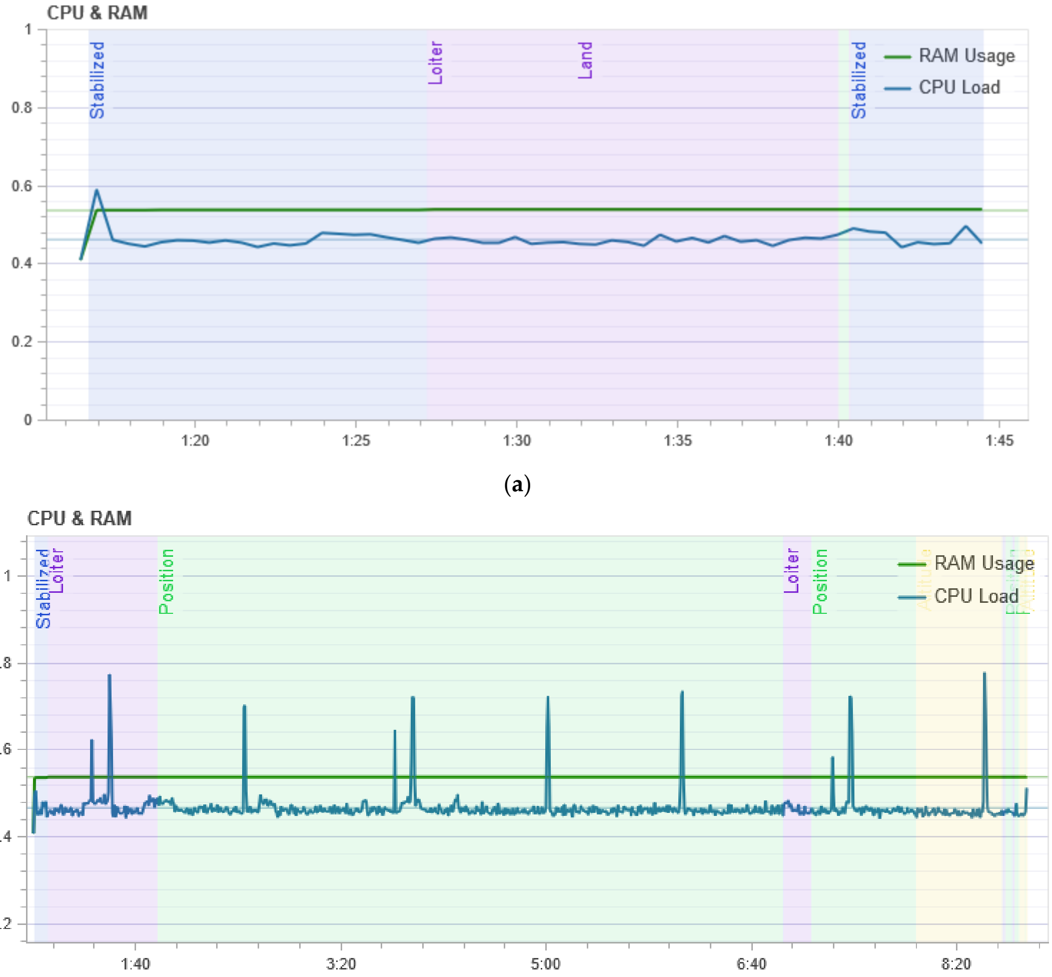
Figure 9. *Cont.*



(**b**)

Figure 9. The state of the system performance evaluator: (**a**) In the normal mode; and (**b**) during a GPS attack.

Figure 10 shows the result of measuring the processor load. It shows that in the normal mode of UAV flight, the central processor of the flight controller is loaded at its peak by 45%, and during the attack, the load is not stable and reaches 80% at its peak, which means that the drone requires more computation during the attack to maintain its flight stability.



(**a**)

(**b**)

Figure 10. Loading the UAV processor: (**a**) In the normal mode; and (**b**) during a GPS attack.

From Figure 5b we can see that the flight altitude is rather uneven during the attack, especially in the last time intervals when there is a sharp rise. This change in altitude is correlated with the calculation of entropy which is shown in Figure 1. The figure shows an increase in the entropy for the flight altitude indicator, which indicates the presence of an anomaly. The parameter number of GPS satellites constantly changes during an attack, and this is clearly seen from Figure 6b. If there is no attack, this graph looks like a straight line. At the same time, it can be seen from Figure 2 that in the second time interval the level of divergence has already grown significantly. This indicates the presence of serious changes in the system and may indicate an anomaly. At the same time, we draw attention to the fact that the numbers with a change in the altitude and the number of satellites have different orders, but for our method, this turns out to be not important. Due to the use of the probability distribution, we can recognize that the value of the divergence has increased by more than two and this is enough to detect the anomaly.

Unlike previous work [23–26], we do not need to know which behavior is considered normal, or to compose many training datasets. It is enough for the UAV system to obtain one value and it does not need to be compared with a normal value, as in other approaches [8–12]. Our solution compares observable variables only using their own value in the previous and current periods of time.

From Figure 7a, which shows the result of measuring the GPS noise level, it can be seen that even during normal operation the graph is not a straight line and some noise is evident with changes in its level. At the same time, as shown in Figure 3b, the Kullback-Leibler divergence is at a low level, that is, the system does not consider this behavior an anomaly. This is due to several factors. Firstly, the change in the noise level with normal behavior is not significant. Secondly, due to the algorithm for processing incoming data, which is presented in Section 2, during data processing, the series are constructed in such a way that the probability distribution does not change its form too much with small changes.

This cannot be said about the situation with the GPS noise during an attack. In this situation it changes significantly, as can be seen from Figure 7b. As a result, the divergence value during the attack is quite high immediately after the first interval, as can be seen in Figure 3a.

Even though the attack is directed at the GPS system, it ultimately affects several parameters at once. These are both the flight altitude and GPS noise and the number of GPS satellites and the level of CPU utilization and energy consumption. For other attacks, such as the eavesdropping attack presented by Wang et al. [31], other sets of parameters can be analyzed and applied. An attack can be detected precisely by a combination of factors. In future papers, a decision-making system will be presented to determine both the attack and, by analyzing several parameters and the degree of their changes, the type of attack. It is difficult to do this using just one parameter, since weather conditions and noise attacks, etc. can also be the cause of changes. In this paper, we focused on GPS spoofing attacks only and studied in detail what parameters are affected and to what extent.

Thus, our presented method, based on the analysis of changes in the internal state of the UAV, makes it possible to accurately detect the presence of anomalous behavior and diagnose a possible spoofing attack. The novelty and advantages of our method are as follows.

- It is versatile and can be applied to various data sets obtainable from the particular UAV's sensor system.
- It determines only that a change has occurred in the system and does so quite accurately; it is then up to the decision-making system to determine whether the change is an attack or not.
- It does not require information about reference and normal values, or inputs from external sources. The UAV independently analyzes the changes in indicators and compares its own state at different intervals. If the state is stable or quickly becomes stable, it means that there are no anomalies.

4. Conclusions

Although a large number of methods have been published for countering UAV navigation system spoofing attacks, this topic is still relevant. To date, a number of successful attacks on the navigation system of UAVs have been demonstrated. Our new self-diagnosis method for analyzing and detecting system anomalies has several advantages that distinguish it from other methods.

First of all, the method is universal and can be used for any UAV subsystems from which numerical readings can be taken. The main thing is to determine the correct type of probability distribution for the analyzed parameter. Secondly, the method is lightweight and energy efficient. The software implementation of the method has little impact on CPU load and the UAV's energy consumption. Thirdly, since the method allows analyzing any parameters, it does not matter what configuration the UAV has, and so the approach can work with whatever data is available. Fourthly, using our method, it is possible not only to detect anomalies but also to determine a change in the patterns of UAV behavior and a change in its states. If the values of entropy are not too high, and a single increase takes place, then this may indicate a change in flight mode. Correlation of the analyzed parameters can unambiguously reveal an attack and determine its type. Each attack affects a certain number of subsystems so the type of attack can be characterized by which parameters are affected. The data collected in the form of time series can be used in the future to train a neural network, which can be trained on these sets and help to decide about the presence of an attack.

This method can be implemented and applied to detect attacks on the GPS system installed on a UAV to ensure its safe navigation. The method can be integrated into any type of UAV. In addition, the method can be used for the analysis of other sets of parameters and applied not only to UAVs, but to any cyber-physical system.

Author Contributions: Conceptualization, E.B. and A.B.; methodology, E.B., A.B. and A.N.; software, E.B. and M.G.; validation, E.B., A.B., A.N., C.F., J.G. and M.G.; formal analysis, E.B. and A.B.; investigation, E.B., A.B., A.N., C.F., J.G. and M.G.; resources, E.B., and A.N.; data curation, E.B., A.B., A.N. and J.G.; writing-original draft preparation, E.B., A.B., A.N. and C.F.; writing-review and editing, E.B., A.B., A.N. and C.F.; visualization, E.B., and J.G.; supervision, E.B., A.N. and C.F.; project administration, E.B. and J.G.; funding acquisition, A.B. and M.G. All authors have read and agreed to the published version of the manuscript.

Funding: The work of Russian authors E.B., A.B., A.N. and Australian author C.F. was supported by the Southern Federal University. The work of Slovak author J.G. was supported by the Slovak Research and Development Agency under Contract APVV-18-0373. The work of Slovak author M.G. was supported by the Scientific Grant Agency (VEGA) under Contract 1/0584/20.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Li, C.; Wang, X. Jamming research of the UAV GPS/INS integrated navigation system based on trajectory cheating. In Proceedings of the 2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), Datong, China, 15–17 October 2016; pp. 1113–1117. [CrossRef]
2. Shepard, D.; Humphreys, T.; Fansler, A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *Int. J. Crit. Infr. Prot.* **2012**, *5*, 146–153. [CrossRef]
3. Warner, J.; Johnston, R. A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. *J. Secur. Adm.* **2003**, 1–9. Available online: https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-2384 (accessed on 8 January 2021).
4. Lester, E.T. Military position source challenges for worldwide ADS-B out compliance. In Proceedings of the 2013 Integrated Communications Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, 22–25 April 2013. [CrossRef]

5. Ericson II, C.A. Software Safety in a Nutshell. Available online: http://www.dcs.gla.ac.uk/~{}johnson/teaching/safety/reports/Clif_Ericson1.htm (accessed on 8 January 2021).
6. Seo, S.-H.; Lee, B.-H.; Im, S.-H.; Jee, G.-I. Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal. *J. Positioning, Navig. Timing* **2015**, *4*, 57–65. [CrossRef]
7. Navstar GPS Space Segment/Navigation User Interfaces. Interface Specification IS-GPS-200G. 2012. Available online: https://navcen.uscg.gov/pdf/gps/IS-GPS-200G.pdf (accessed on 8 January 2021).
8. Warner, J.S.; Johnston, R.G. GPS Spoofing Countermeasures. LAUR-03-6163. Available online: http://lewisperdue.com/DieByWire/GPS-Vulnerability-LosAlamos.pdf (accessed on 8 January 2021).
9. Iqbal, M.U.; Lim, S. Legal and Ethical Implications of GPS Vulnerabilities. *J. Int. Commercial Law Technol.* **2008**, *3*, 178–187. Available online: https://media.neliti.com/media/publications/28794-EN-legal-and-ethical-implications-of-gps-vulnerabilities.pdf (accessed on 8 January 2021).
10. O'Hanlon, B.W.; Psiaki, M.L.; Humphreys, T.E.; Bhatti, J.A. Real-Time Spoofing Detection Using Correlation between Two Civil GPS Receiver. In Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012), Nashville, TN, USA, 17–21 September 2012; pp. 3584–3590. Available online: https://gps.mae.cornell.edu/ohanlon_ION_C6_7_preprint.pdf (accessed on 8 January 2021).
11. Schmidt, D.; Radke, K.; Camtepe, S.; Foo, E.; Ren, M. A survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Comput. Surv.* **2016**, *48*, 1–31. [CrossRef]
12. Jansen, K.; Schäfer, M.; Moser, D.; Lenders, V.; Pöpper, C.; Schmitt, J. Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–24 May 2018; pp. 1018–1031. [CrossRef]
13. Humphreys, T. Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing, Austin, USA. 2012. Available online: https://radionavlab.ae.utexas.edu/images/stories/files/papers/Testimony-Humphreys.pdf (accessed on 8 January 2021).
14. Cenciotti, D.; Captured, U.S. Stealthy Drone Was Hijacked Exploiting GPS Vulnerability. But Hack Description Does Not Solve the Mystery. *The Aviationist*. 15 December 2011. Available online: https://theaviationist.com/2011/12/15/gps-spoofing/ (accessed on 8 January 2021).
15. Solove, D.J. *The Digital Person: Technology and Privacy in the Information Age*; New York University Press: New York, NY, USA, 2004; p. 296. Available online: https://poseidon01.ssrn.com/delivery.php?ID=104119098102027015118064085010107007042068069003049020126091029087121115103007094028042013055035009000054124064101068095067065102052026003014068087077107027081088068076064113026084018000121065088105092074069017117069066108110083120095008098079106031&EXT=pdf (accessed on 8 January 2021).
16. Montgomery, P.Y.; Humphreys, T.E.; Ledvina, B.M. Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense Against a Portable Civil GPS Spoofer. In Proceedings of the ION 2009 International Technical Meeting, Anaheim, CA, USA, 26–28 January 2009; pp. 124–130. Available online: https://core.ac.uk/download/pdf/211337540.pdf (accessed on 8 January 2021).
17. Jansen, K.; Tippenhauer, N.O.; Pöpper, C. Multi-receiver GPS spoofing detection: Error models and realization. In Proceedings of the 32nd Annual Conference on Computer Security Applications, Los Angeles, CA, USA, 5–9 December 2016; pp. 237–250. [CrossRef]
18. Heng, L.; Work, D.B.; Gao, G.X. GPS signal authentication from cooperative peers. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 1794–1805. [CrossRef]
19. Panice, G.; Luongo, S.; Gigante, G.; Pascarella, D.; Di Benedetto, C.; Vozella, A.; Pescapè, A. A SVM-based detection approach for GPS spoofing attacks to UAV. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 1–11. [CrossRef]
20. Eldosouky, A.; Ferdowsi, A.; Saad, W. Drones in Distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing. *IEEE Internet Things J.* **2020**, *7*, 2840–2854. [CrossRef]
21. Qu, Y.; Zhang, Y. Cooperative localization against GPS signal loss in multiple UAVs flight. *J. Syst. Eng. Electron.* **2011**, *22*, 103–112. [CrossRef]
22. Qiao, Y.; Zhang, Y.; Du, X. A vision-based GPS-spoofing detection method for small UAVs. In Proceedings of the 2017 13th International Conference on Computational Intelligence and Security (CIS), Hong Kong, China, 15–18 December 2017; pp. 312–316. [CrossRef]
23. Youn, W.; Rhudy, M.B.; Cho, A.; Myung, H. Fuzzy adaptive attitude estimation for a fixed-wing UAV with a virtual SSA sensor during a GPS outage. *IEEE Sens. J.* **2020**, *20*, 1456–1472. [CrossRef]
24. Basan, E.; Basan, A.; Nekrasov, A. Method for detecting abnormal activity in a group of mobile robots. *Sensors* **2019**, *19*, 4007. [CrossRef] [PubMed]
25. Semanjski, S.; Semanjski, I.; Wilde, W.D.; Gautama, S. Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—Part II. *Sensors* **2020**, *20*, 1806. [CrossRef] [PubMed]
26. Kwon, K.-C.; Shim, D.-S. Performance analysis of direct GPS spoofing detection method with AHRS/Accelerometer. *Sensors* **2020**, *20*, 954. [CrossRef] [PubMed]

27. Guo, Y.; Miao, L.; Zhang, X. Spoofing detection and mitigation in a multi-correlator GPS receiver based on the maximum likelihood principle. *Sensors* **2019**, *19*, 37. [CrossRef] [PubMed]
28. Harremoës, P. Poisson's law and information theory. In Proceedings of the 2001 IEEE International Symposium on Information Theory (IEEE Cat. No.01CH37252), Washington, DC, USA, 24–29 June 2001; p. 46. [CrossRef]
29. Deon, A.F.; Menyaev, Y.A. Poisson twister generator by cumulative frequency technology. *Algorithms* **2019**, *12*, 114. [CrossRef]
30. Afgani, M.; Sinanovic, S.; Haas, H. Anomaly detection using the Kullback-Leibler divergence metric. In Proceedings of the 2008 First International Symposium on Applied Sciences on Biomedical and Communication Technologies, Aalborg, Denmark, 25–28 October 2008; pp. 1–5. [CrossRef]
31. Wang, Q.; Dai, H.-N.; Li, X.; Shukla, M.K.; Imran, M. Artificial noise aided scheme to secure UAV-assisted Internet of Things with wireless power transfer. *Comput. Commun.* **2020**, *164*, 1–12. [CrossRef]