Analysis of the Impact of a GPS Spoofing Attack on a UAV

Elena Basan [1], Oleg Makarevich [1], Maria Lapina [2] and Massimo Mecella [3]

[1] *Southern Federal University, Chekhov St. 2, Taganrog, 347922, Russia*
[2] *North-Caucasus Federal University, Prospect Kulakova 2, 355000, Stavropol, Russia*
[3] *SAPIENZA Università di Roma, via Ariosto 25, I-00185 Roma, Italy*

Abstract

The paper discusses scenarios of GPS spoofing attacks on UAVs. Three scenarios are proposed: when the attack is not carried out, when a low-intensity attack is carried out, and when an intense attack is carried out. After that, logs from the UAV are collected and the result of the attack is analyzed in relation to its impact on the cyber-physical parameters of the UAV. This analysis is carried out with the aim of further developing an intrusion detection and response system. It is necessary to understand which parameters change to what extent and under the influence of which attack scenario.

Keywords

GPS, Spoofing Attack, UAV, Kalman filters, attack scenario

1. Introduction

Today, an attack on the global navigation system GPS, if properly executed, can lead to serious consequences for a UAV or a group of UAVs [1]. The flight controller, in addition to the natural error present in the sensor readings, is also affected by natural GPS vulnerabilities such as signal blocking or jamming that compromise the availability of the GPS signal. In the GPS Spoofing Attack, satellites transmitting a GPS signal are forged to manipulate the UAV's navigation system by transmitting fake coordinates created by an attacker with a higher power than the original signal [2], [3]. However, civil GPS does not have the protection mechanisms used to transmit the signal. Consequently, civilian GPS is highly vulnerable to spoofing attacks [4,5]. A targeted attack that takes control of the UAV or simply destroys it can easily harm everyone in the UAV's flight area or damage other vehicles [6-8]. Therefore, GPS spoofing has become an important research topic, since an attacker can hijack a UAV, use it to eavesdrop or attack people or objects without the need to stay close to the target. Thus, the topic related to the analysis of the impact of the GPS spoofing attack on the UAV navigation system is very relevant. Before developing a protection system against such attacks, it is necessary to understand how the attack affects the UAV and its subsystems to further analyze this influence and detect the attack. The main purpose of this paper is to analyze the possibility of detecting an attack on the UAV navigation system by analyzing changes in the readings of the flight controller sensors. It is necessary to determine which cyber-physical parameters change the readings because of a GPS spoofing attack. Once the sets of parameters that are susceptible to attack are determined, you can develop a system for detecting and preventing attacks and intrusions.

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia
EMAIL: ebasan@sfedu.ru (Elena Basan), obmakarevich@sfedu.ru (Oleg Makarevich), mlapina@ncfu.ru (Maria Lapina), mecella@diag.uniroma1.it (Massimo Mecella)
ORCID: 0000-0001-6127-4484 (Elena Basan), 0000-0003-0066-8564 (Oleg Makarevich), 0000-0001-8117-9142 (Maria Lapina), 0000-0002-9730-8882 (Massimo Mecella)

2. Analysis of methods of protection against spoofing attacks on UAVS GPS system

Today there are many methods for detecting an attack on a UAV navigation system. Let us analyze the parameters for detecting attacks on which various methods are based. Today there are many methods for detecting an attack on a UAV navigation system. Let us analyze the parameters for detecting attacks on which various methods are based. In [9], a method for detecting a GPS spoofing attack based on the use of neural networks is presented. Let us determine the parameters that the authors take to generate data for training a neural network.

Satellite Number: Used to identify the various satellites orbiting the Earth. This number can be read from the content of the decoded received GPS signals.

Signal-to-Noise Ratio: SNR is an indicator of the strength of the GPS signal after being mixed with noise and interference. It can be measured and calculated from the received signals using special algorithms [10].

Pseudo range: Each GPS satellite has a unique Gold code; its autocorrelation function is in the shape of an equilateral triangle, which peaks with perfect correlation. This characteristic can be used to determine the transmission time signal from the satellite to the receiver by cross correlating the Gold code with its copy generated by the receiver.

Doppler shift: The GPS carrier signal is multiplied by the reference signal at the receiver.

Carrier Phase Offset: Referring to [11], the carrier phase offset observed at a time can be captured.

In paper [12], the impact of GPS spoofing on UAVs is analyzed using a series of tests in a simulation environment. The results are presented as a deviation from the original UAV trajectory during flight. The authors emulated GPS spoofing attacks by changing the readings of the parameters of the GPS receiver. For each flight, after 45 seconds from the start of the mission, the GPS readings were distorted. The duration of each attack ranged from 1 second to 20 seconds in 1 second increments.

The attack type is determined based on how the attack affected the GPS parameters and is defined as follows.

- Random Longitude: Changes longitude readings randomly from a valid range of values (-180 to 180);
- Random Latitude: Changes the latitude reading at random from the valid range of values (-90 to 90);
- Random Position: Changes the position reading randomly along three axes (latitude, longitude, and altitude);
- Delayed message: does not change the message information but delivers it with a certain delay;
- Force Landing: Changes elevation values higher than the actual value while attempting to force an unplanned landing. Secondary drone capture distorts the position readings randomly from the trajectory of another drone along three axes (latitude, longitude, and altitude);
- Capture from the Attacker's Position: Changes the position readings at random from a static position, set by the attacker, along three axes (latitude, longitude, and altitude).

Thus, in the context of changing the parameters that are affected by the attack, this study analyzes only the position of the UAV and the delay of transmitted messages.

The paper [13] presents the following detection method. The GPS spoofing detection system has been developed using dynamic identification. A centroid motion model and an orientation motion model were created. Measurement information from inertial measurement units (IMU) and position information from GPS are visualized responses to the dynamic laws of motion of a UAV. These two types of measurement information were used to estimate the dynamic parameters of the UAV online using two extended Kalman filters (EKF). The detection of GPS false signals has been efficiently implemented by monitoring the relative errors estimations. Numerical modeling has shown that dynamics parameters can be estimated online using combined filters. In this work, the following parameters were investigated: Position error, Speed error, Attitude error, Attitude angle error, Accelerometer, Gyroscope, GPS positioning.

The method proposed in [14] is based on the use of a support vector machine for data analysis of a hybrid navigation system. The inertial system (IS) gives an error in free fall, which increases over time.

The deviation from the error becomes worse when the UAV is equipped with a microelectromechanical (MEMS) inertial navigation system. GPS is the fundamental mechanism for calibrating the inertial system for correct navigation. Evaluating errors over time can help detect spoofing attacks. Indeed, from the experimental data, the authors found that in normal conditions, the error between the GPS and inertial navigation system has a certain distribution, and that at the time of the error of attack grows abnormally. The anomaly disappears over time, because the action of the GPS in the inertial unit hides the effect of the attack. In this case, the error is determined for the following parameters: position determined by GPS, speed determined by GPS rotation speed, acceleration position determined by IS, speed determined by IS.

In paper [15], the authors develop and implement a new intrusion detection and response scheme that operates on UAVs and ground stations to detect anomalies that threaten network performance. This paper proposes a set of methods for detecting and responding to anomaly based on tracking UAV behavior and categorizing them (normal, abnormal, suspicious, and malicious) according to the cyberattack that was detected. The authors focused on the most dangerous cyberattacks that can target a UAV network: spreading false information, spoofing GPS, jamming, and attacks using black and gray holes. Numerous experiments confirm that the proposed scheme is effective for detecting attacks even with many UAVs and intruders. It demonstrates high detection rate, low false alarm rate and fast detection with low communication overhead.

A set of rules is proposed for modeling the normal behavior of nodes based on the characteristics of GPS spoofing attacks [16, 17]:

1) a GPS spoofing attack generates a signal strength intensity (SSI) to gain control of the drone, and this SSI is higher than satellites, as shown by Shepard et al. [18] and Kim et al [19].

2) an attacker transmits multiple signals from one antenna; therefore, they have almost the same power level [20].

The detection process is carried out as follows: The detection system collects SSI information from transmitters (satellites and intruders) and then estimates the distribution of the SSI random variable using a normal distribution. Moreover, SSIs will be correctly distributed (ie have almost the same value) if they are within the mean [21]. However, SSIs that are in this range are identified as being generated by the same transmitter. Therefore, the transmitter is suspected in the implementation of GPS spoofing attacks. In addition, a reasonable maximum SSI can be set to limit the spurious signal power, since according to Wen et al. [22] An attacker can increase the signal strength by at least 3 dB.

Thus, we can conclude that the reviewed works focus on the parameters related to UAV positioning and GPS signal characteristics. Moreover, most of the results were obtained by the authors using modeling methods, and not on real attacks on UAVs. Of course, conducting a real attack on a UAV can be dangerous, as it will lead to unforeseen consequences. Nevertheless, to expand the range of indicators for detecting an attack, it is proposed to investigate the results of an experiment that included a full-scale model of a UAV for carrying out an attack.

The purpose of this article is to analyze the results of an attack on a UAV and to identify sets of features that change under the influence of a GPS spoofing attack [7].

3. Experimental stand and attack scenario

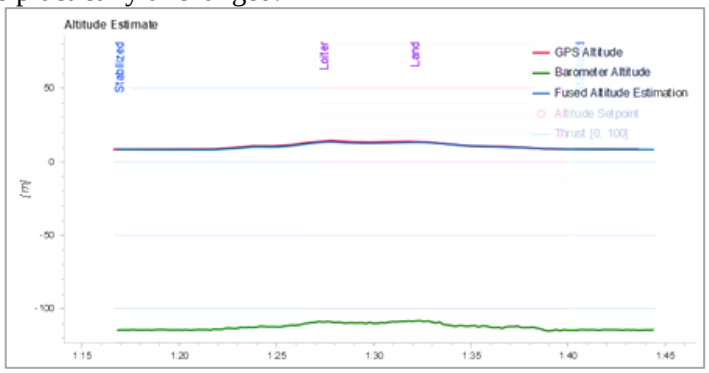
To carry out the attack, a UAV was developed, the design of which uses the Pixhawk 4 flight controller. This flight controller is the most popular and modern solution on the market for flight controllers for drone-type UAVs [23]. The attack scenario is that the UAV should hover over one fixed point and keep over it all the time. Attacker use HackRF. This device allows you to create a fake signal and create false satellites with higher power so that the UAV picks up the signal from them, and not from the true satellites [24]. In this case, the attacker transmits fake coordinates in order to smoothly move the UAV to another point and fix it there. The aim of the attacker is to intercept control of the UAV using a GPS spoofing attack [25]. Thus, the UAV, after determining its current location, receives the static coordinates of the target. A drone-type UAV moves to a given target and fixes its position in space while maintaining altitude. In case of external physical impact, for example, the impact of natural factors or the physical impact of another object, the UAV autopilot system increases engine speed and sets the opposite direction to maintain a given position. When the UAV is displaced from the set

position, the position hold system increases the engine speed depending on the distance between the set point and the actual location of the UAV. Upon returning to the set point, the operation of the engines goes into the normal mode of maintaining the altitude.

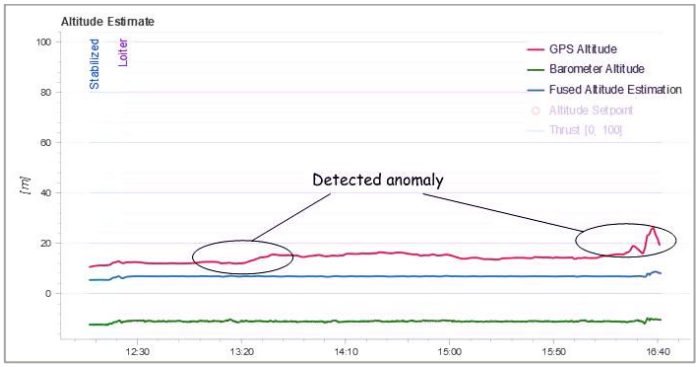
You can set the direction vector and speed of the attacked device by broadcasting a fake geo position. Using the fact that the UAV is trying to counteract the displacement, starting to move towards the initial position, it is possible to set the direction of movement necessary for the attacker. By changing the distance from the fake geolocation to the specified one, you can increase or decrease the speed of movement, for a more accurate direction and control of the attacked UAV.

4. Analysis of the UAV logbook after the attack

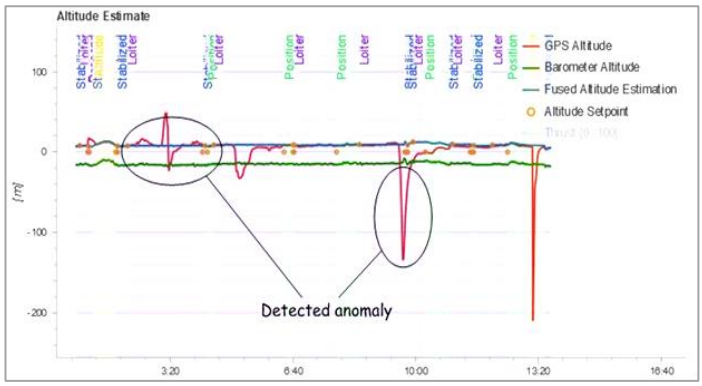
Figure 1 shows the readings of the drone's flight altitude during the attack and normal flight, respectively. Comparing the two upper graphs, we can say that during an attack, the altitude readings obtained from the GPS system change slightly, no global changes are observed, during normal flight the altitude remains practically unchanged.



(a)



(b)

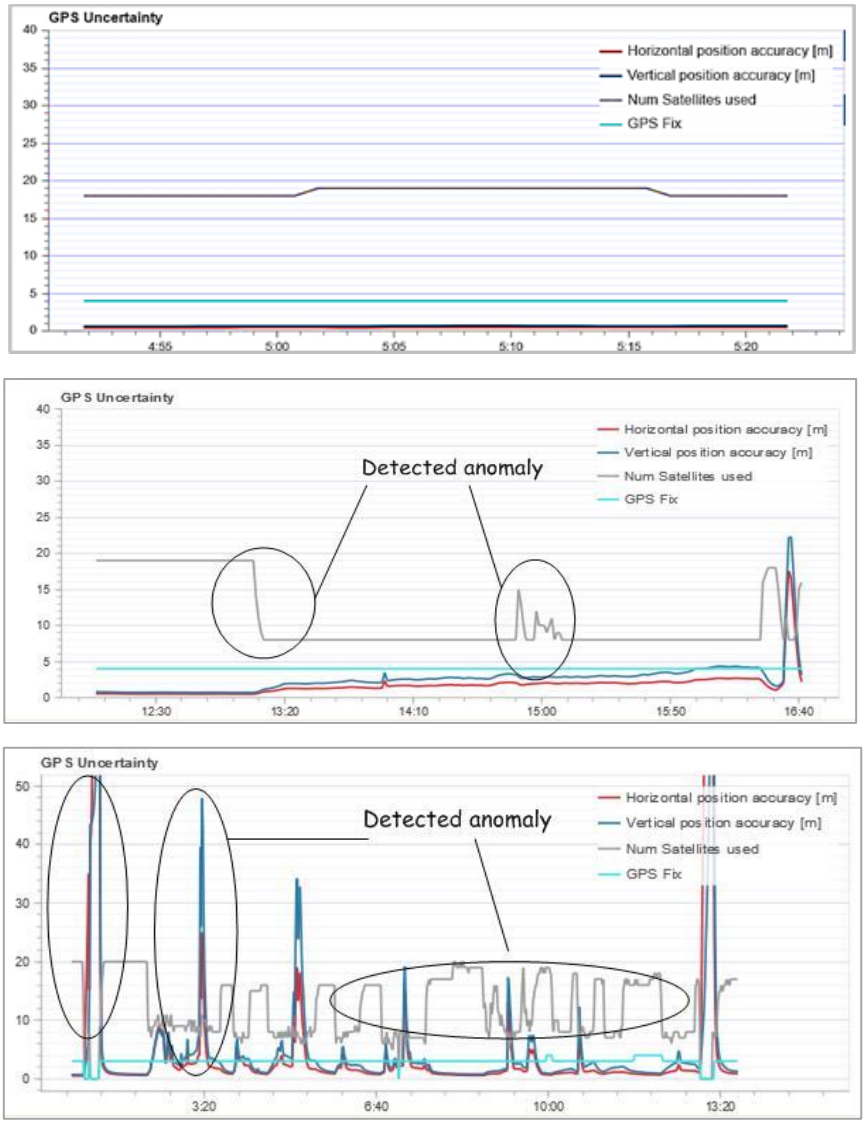


(c)

Figure 1: UAV altitude graph (a) during normal flight (b) with a short-term attack (c) with a long-term attack term attack (c) with a long-term attack

Let us analyze the changes in the UAV flight altitude indicator. Figure 1 shows that during a short-term attack, as shown in Figure 1 (b), the flight altitude changed slightly within the range from 15 to 20 meters, only at the end we see a small sharp takeoff of the UAV to an altitude of more than 20 meters. At the same time, it can be seen from Figure 1 (c) that there is a significant change in the flight altitude readings obtained from the GPS sensor (red line in the graphs), while the accelerometer readings (blue line in the graphs) remain stable. This suggests that, in fact, the quadcopter could not change the flight altitude, the attacker simply could not guess the exact flight altitude and therefore the graph has peak values. Thus, the altitude indicator may be susceptible to attack, or it may not, it depends on the preparedness of the attacker. Moreover, this indicator changes only in relation to the measurements made by the GPS sensor, the readings of the accelerometer are stable. As can be seen from graph 1 (a), during normal flight, when there is no attack, if the flight altitude changes, then both sensors and the accelerometer and the GPS receiver will show the same values.

Let us analyze the indicator - the number of GPS satellites detected by the UAV. The GPS readings during normal flight make it clear that the GPS system is working stably, there is no sharp loss of GPS fixation and the satellites used, there is also no abrupt change in the UAV positioning, which is typical during an attack, as can be seen from Figure 2.

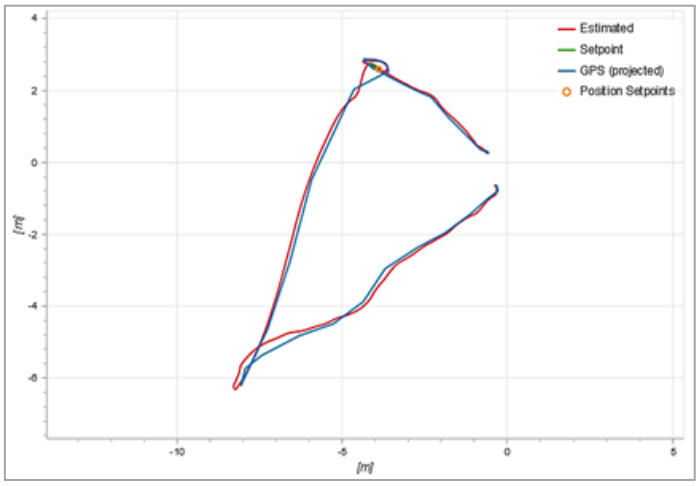


(a)

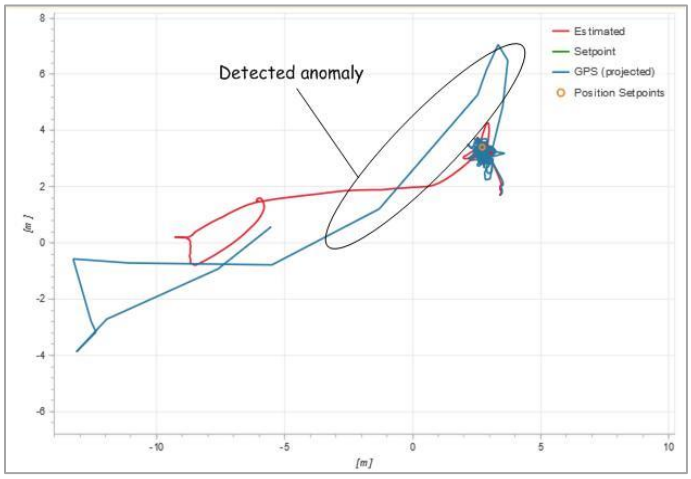
(b)

(c)

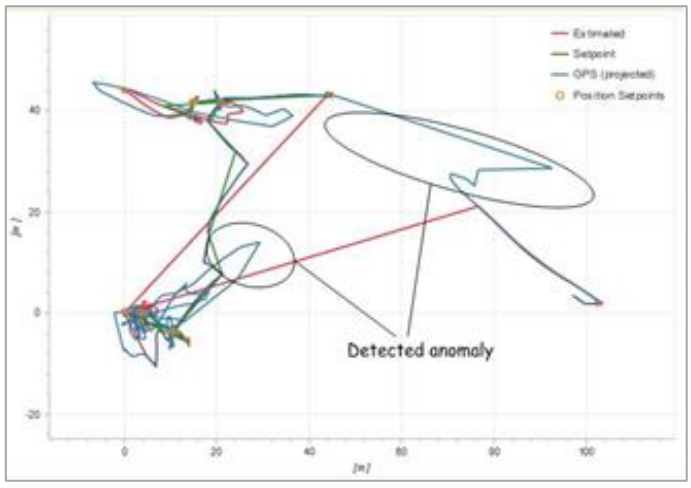
Figure 2: The number of GPS satellites used (a) during normal flight (b) during a short-term attack on the UAV's GPS system (c) during a prolonged attack



(a)



(b)



(c)

Figure 3: Actual and calculated UAV flight paths (a) during normal flight (b) during a short attack (b) during a prolonged attack

Figure 3 (a) shows a complete coincidence of the flight path obtained from the accelerometer and from the GPS receiver. In a short-term attack on the GPS, the goal was to move the UAV from the starting point to fix it at the point indicated by the attacker. Figure 3 (b) shows that the UAV was displaced, as evidenced by the shift of the red line to the lower left corner (initially, the UAV was in the upper right corner). But the trajectories of the red and blue lines do not coincide. On closer inspection, we can see that the red line repeats the blue pattern only with a smaller radius. Nevertheless, it is clearly seen that the UAV positioning system is in an unstable state and shows different coordinates

by GPS and from the inertial system. In Figure 3 (c), the UAV should be fixed in the lower left corner. The attacker tried to move it first to the upper left corner and then to the lower right corner. At the same time, the picture seems confusing at first glance. In fact, the attacker is trying to smoothly move the UAV by picking up the coordinates and gradually moving the UAV. At the same time, by the end of the attack, the UAV was displaced, which is confirmed by the coincidence of the red and blue lines in the lower right corner of the figure. Thus, an attack can be detected by a mismatch in the coordinates recorded by the GPS sensor and the accelerometer, and other sensors.

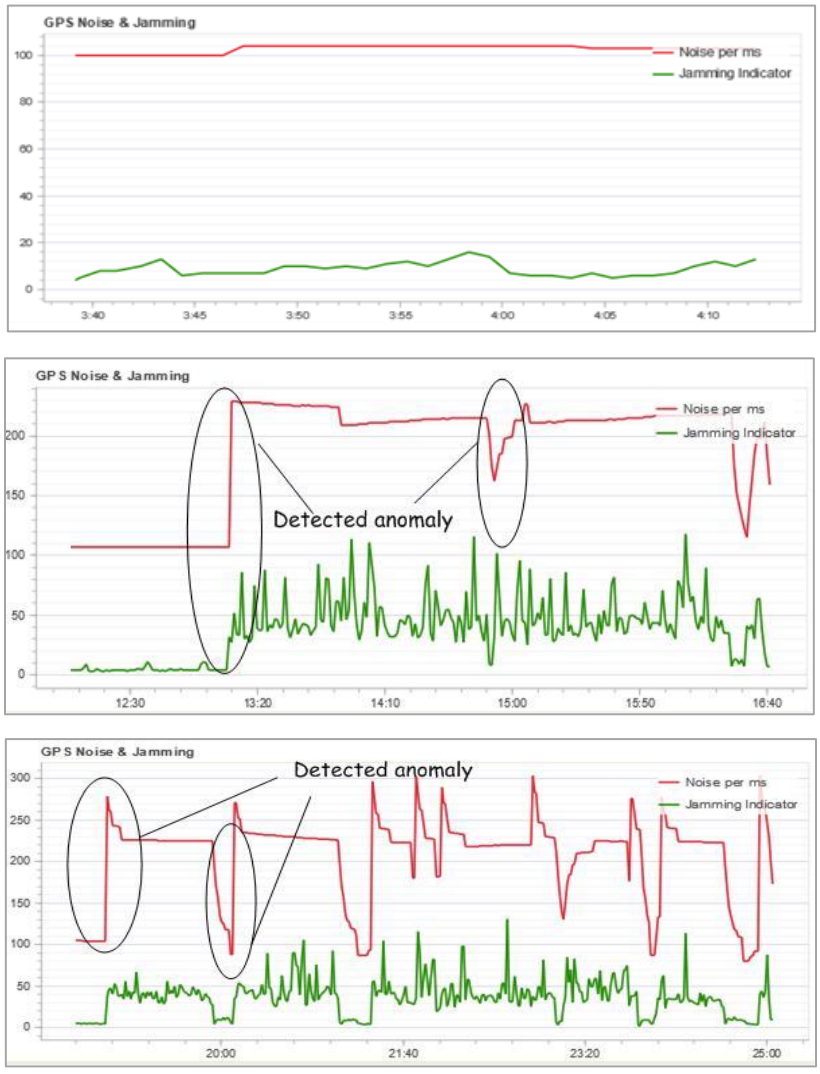


Figure 4: Graph of GPS noise readings (a) during normal flight (b) with a short-term attack (c) with a long-term attack

The norm for GPS noise is 80, in this case, as can be seen in Figure 4 (a), during normal flight the noise is slightly higher than the norm, this is not a critical reading, it may be due to the terrain on which the flight was carried out, as well as weather conditions. For example, during the period of this experiment, strong gusts of wind were observed. One of the indicators that will allow detecting an attack with high accuracy is the GPS noise level. This is because despite the possibility of falsifying the exact number of satellites, calculating the flight altitude, smoothly displacing the UAV from a given trajectory, thereby, having a minimal effect on the previous parameters, an attacker will not be able to fake the GPS noise level parameter. This is because the main feature of the attack is the generation of a stronger GPS signal so that the true GPS signal from the satellites is blocked by the attacker's signal. Figure 4 shows the results of changes in GPS noise. However, it should be noted that the graph of the noise level during normal flight at the same level throughout the flight is the same, there are minor

changes. For a situation where an attack is carried out, everything is obvious. From graph 4 b, c it becomes clear that up to a certain period a normal flight took place, after the attack, the graph clearly shows the consequences - a sharp and large deviation from the norm of the GPS noise level. Also, the green line makes it clear that there is a sharp jamming of the GPS signal. Figures 4 (b), (c) show that there is a sharp increase in the noise level to 200, then this value does not stay at the same level but changes the readings all the time.

Consider two parameters by changing which one can indirectly judge the presence of an attack. Before that it was considered parameters directly connected with the coordinates of the UAV or drone navigation system, but the attack may affect other parameters of the UAV. Let us analyze how the CPU utilization parameter changed. Figure 5 shows the results of changing the CPU, both during normal flight and during an attack.

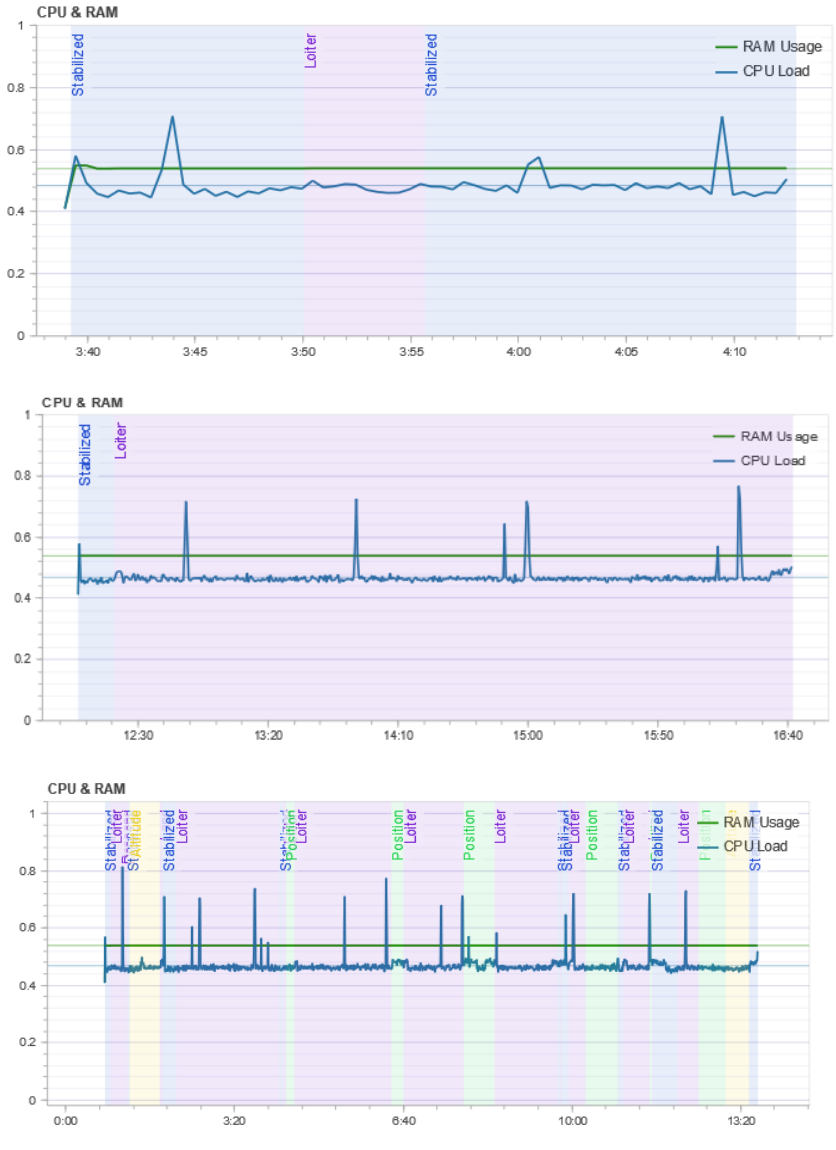


Figure 5: Graph of readings of changes in the CPU load level (a) during normal flight (b) during a short-term attack (c) during a long-term attack

As can be seen from the graphs, when there is an attack, CPU load peaks is starting to be more. The more intense the attack, the more the CPU utilization changes, as can be seen from Figure 5 (c) the peaks of the utilization level during an intense attack are much larger. This is because the UAV is constantly trying to move to the point indicated by the attacker, while resistance arises from inertial systems that try to keep the UAV at the point indicated by the operator. The UAV performs many additional movements.

Next, consider the power consumption level changes in different flight conditions, in Figure 6.

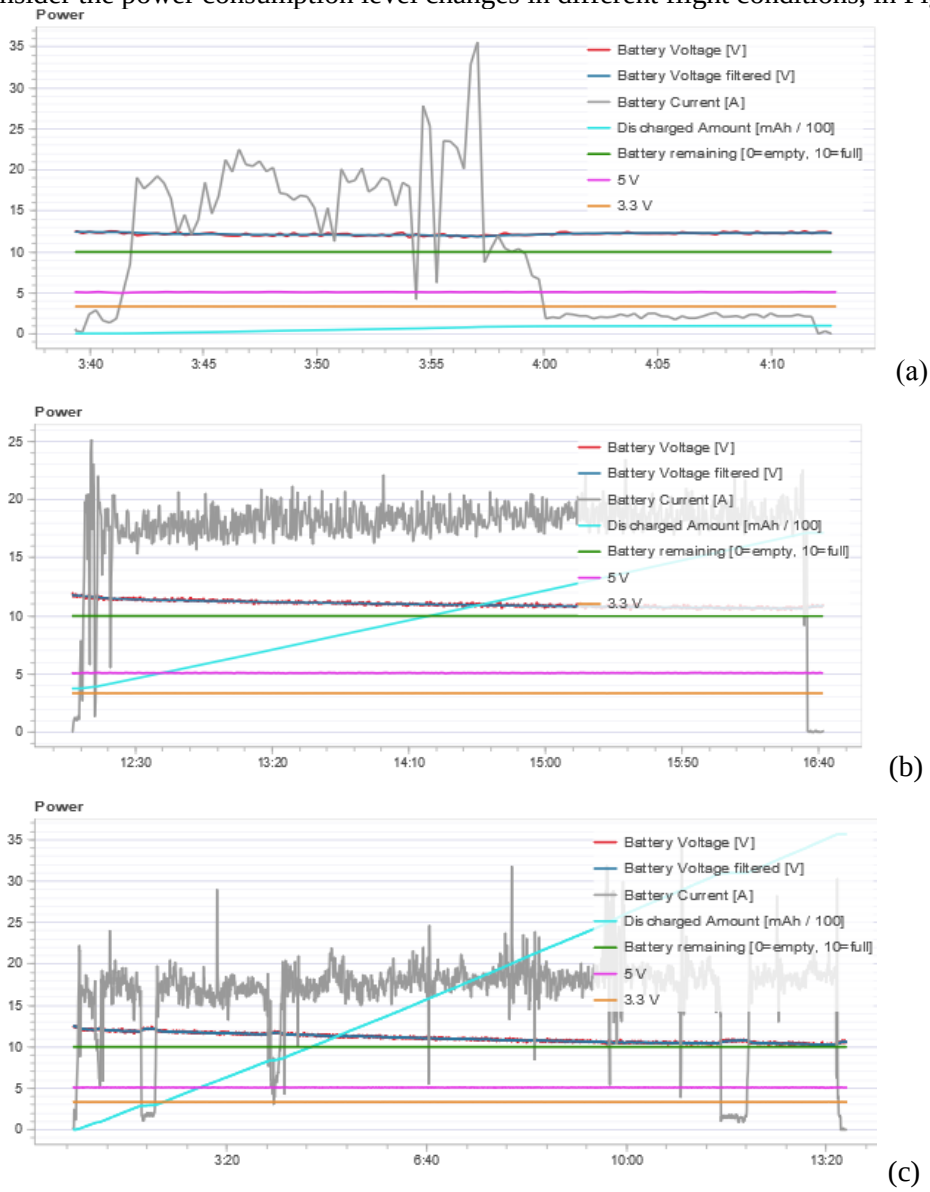


Figure 6: Graph of readings of changes in the level of consumed power (a) during normal flight (b) with a short-term attack (c) with a long-term attack

Figure 6 shows that the power consumption parameter underwent the greatest changes during an intense attack. As with the CPU changes, this involves multiple movements of the UAV. For example, an attacker may aim to disable a UAV by exhausting its resources; the more UAVs moves, the faster its battery will be discharged. Given the limited resources of the UAV, this can become a significant problem.

5. Conclusion

Typical signs of an attack on the GPS system are most often recognized by a sharp decrease in the number of satellites used by the system and the difference in readings between the actual flight path and the trajectory built by the GPS system, so an attack can be identified by a sharp increase in GPS noise and signal jamming, and by changing the altitude readings of the UAV [26]. Despite the large number of methods for countering attacks aimed at spoofing navigation signals, this topic is still relevant. Today, there are cases of successful implementation of attacks on the navigation system of

UAVs [27]. Based on the results of an experimental study and analysis of the on-board log of the UAV that was attacked and that was received during normal flight, the following was determined. When conducting an attack, such parameters as: flight altitude, GPS noise level, the number of GPS satellites recorded, the level of power consumption by the battery and the level of CPU utilization. From Figure 3, where the UAV's flight path is shown, it abruptly changed its flight path and moved unevenly. Initially, the UAV was supposed to stay at one point, and in Figure 3, where the flight path is presented, there is a point and around it there are small changes in the blue line, but then the trajectory changes sharply. All other changes in the parameters of the UAV are related to this, which just indicated the presence of an attack. In general, we can say that such changes in the flight trajectory could indicate a change in the behavior or scenario of the UAV's behavior. But because a high level of noise and jumps in the number of satellites were recorded, we can say that this is an attack. Correlation of the analyzed parameters can unambiguously reveal the attack and determine its type. Each attack affects a certain number of subsystems, you can set which parameters which attack affects to determine its type [28]. The collected data 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 will help decide about the presence of an attack. In addition, it should be noted that the addition of new parameters for analyzing the presence of an attack may allow detecting new threats to the security of the UAV. For example, when the power consumption of the battery increases, there is a threat of exhausting the resources of the UAV. When the CPU load increases, the UAV mission is threatened, because computing power is spent not on calculations according to the algorithm, but on a constant change in the flight route.

6. Acknowledgements

Research related to UAV attack experiments and analysis of experimental data, as well as an attack scenario supported by the Russian Science Foundation grant number 21-79-00194, https://rscf.ru/project/21-79-00194/ in Southern Federal University. UAV design and normal behavior is supported in the context of the collaboration between Sapienza, NCFU and SFU.

7. References

[1] C. Li and X. Wang, "Jamming research of the UAV GPS/INS integrated navigation system based on trajectory cheating," 2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), Datong, 2016, pp. 1113-1117, doi: 10.1109/CISP-BMEI.2016.7852880.

[2] D. Shepard, T. Humphreys and A. Fansler, "Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks", In: International Journal of Critical Infrastructure Protection, 2012.

[3] J. Warner and R. Johnston, "A simple demonstration that the global positioning system (gps) is vulnerable to spoofing", In: Journal of Security Administration, 2003.

[4] E. T. Lester, "Military position source challenges for worldwide ads-b out compliance", In: Integrated Communications Navigation and Surveillance Conference, 2013.

[5] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures", Homeland Security J., vol. 25, no. 2, pp. 19-27, Dec. 2003.

[6] Clifton A. Ericson, Software safety in a nutshell. http://www.dcs.gla.ac.uk/~johnson/teaching/safety/reports/Clif_Ericson1.htm

[7] S.-H. Seo, B.-H. Lee, S.-H. Im and G.-I. Jee, "Effect of spoofing on unmanned aerial vehicle using counterfeited gps signal", Journal of Positioning Navigation and Timing, pp. 57-65, 06 2015.

[8] "Global positioning system directorate", In: Systems engineering and integration Interface Specification IS-GPS-200G Technical Report, 2012.

[9] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni and N. Kaabouch, "Detection of GPS Spoofing Attacks on Unmanned Aerial Systems," 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2019, pp. 1-6, doi: 10.1109/CCNC.2019.8651804.

[10] M. Riahi Manesh, A. Quadri and N. Kaabouch, "An Optimized SNR Estimation Technique Using Particle Swarm Optimization Algorithm", IEEE Computing and Communication Workshop and Conference, pp. 1-7, 2017
[11] M. R. Manesh, Y. Arjoune and N. Kaabouch, "A bit error rate estimation method for wireless communication systems," 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2018, pp. 835-840, doi: 10.1109/CCWC.2018.8301620.
[12] D. Mendes, N. Ivaki and H. Madeira, "Effects of GPS Spoofing on Unmanned Aerial Vehicles," 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan, 2018, pp. 155-160, doi: 10.1109/PRDC.2018.00026.
[13] S. Leyuan, H. Wende, Z. Yifan, W. Yueke and Y. Jun, "GPS Spoofing Detection of Unmanned Aerial Vehicles by Dynamics Identification," 2018 IEEE CSAA Guidance, Navigation and Control Conference (CGNCC), Xiamen, China, 2018, pp. 1-6, doi: 10.1109/GNCC42960.2018.9019147.
[14] G. Panice et al., "A SVM-based detection approach for GPS spoofing attacks to UAV," 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, 2017, pp. 1-11, doi: 10.23919/IConAC.2017.8081999.
[15] H. Sedjelmaci, S. M. Senouci and N. Ansari, "A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1594-1606, Sept. 2018, doi: 10.1109/TSMC.2017.2681698.
[16] E. Basan, M. A. Lapina, M. Mecella, "Protected Group Control System for Mobile Robots",CEUR workshop proceedings: Proceedings of the International Workshop on Data Mining and Knowledge Engineering, Stavropol, Sun SITE, 2020, pp. 4-12.
[17] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal and J. Fagan, "Countermeasures for GPS signal spoofing", Proc. 18th Int. Tech. Meeting Satellite Div. Inst. Navig., pp. 1285-1290, 2005.
[18] D. P. Shepard, J. A. Bhatti, T. E. Humphreys and A. A. Fansler, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks", Proc. ION GNSS Meeting, pp. 1-15, 2012.
[19] A. Kim, B. Wampler, J. Goppert and I. Hwang, "Cyber attack vulnerabilities analysis for unmanned aerial vehicles", Proc. Infotech@Aerospace Conf., pp. 1-30, 2012.
[20] I. Hwang, S. Kim, Y. Kim and C. E. Seah, "A Survey of Fault Detection, Isolation, and Reconfiguration Methods," in IEEE Transactions on Control Systems Technology, vol. 18, no. 3, pp. 636-653, May 2010, doi: 10.1109/TCST.2009.2026285.
[21] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar and O. Tonguz, "Routing in sparse vehicular ad hoc wireless networks", IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1538-1556, Oct. 2007.
[22] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal and J. Fagan, "Countermeasures for GPS signal spoofing", Proc. 18th Int. Tech. Meeting Satellite Div. Inst. Navig., pp. 1285-1290, 2005.
[23] J. Leško, M. Schreiner, D. Megyesi and L. Kovács, "Pixhawk PX-4 Autopilot in Control of a Small Unmanned Airplane," 2019 Modern Safety Technologies in Transportation (MOSATT), Kosice, Slovakia, 2019, pp. 90-93, doi: 10.1109/MOSATT48908.2019.8944101.
[24] R. P. Hudhajanto et al., "Low Cost Nano Satellite Communication System Using GNURadio, HackRF, and Raspberry Pi," 2018 International Conference on Applied Engineering (ICAE), Batam, 2018, pp. 1-4, doi: 10.1109/INCAE.2018.8579395
[25] M. Ö. Demir, G. K. Kurt and A. E. Pusane, "On the Limitations of GPS Time-Spoofing Attacks," 2020 43rd International Conference on Telecommunications and Signal Processing (TSP), Milan, Italy, 2020, pp. 313-316, doi: 10.1109/TSP49548.2020.9163444.
[26] N. Proshkin, E. Basan and M. Lapina, "Radio Frequency Method for Emulating Multiple UAVs", 2021 17th International Conference on Intelligent Environments (IE), 2021, pp. 1-4, doi: 10.1109/IE51775.2021.9486599.
[27] E. Basan, M. Lapina, N. Mudruk, E. Abramov, "Intelligent Intrusion Detection System for a Group of UAVs". In: Tan Y., Shi Y. (eds) Advances in Swarm Intelligence. ICSI 2021. Lecture Notes in Computer Science, vol 12690. Springer, Cham. https://doi.org/10.1007/978-3-030-78811-7_22.
[28] E. Basan, O. Peskova, M. Lapina, "Analysis of communication channels for the organization of control and interaction of UAVs from the security viewpoint", CEUR Workshop Proceedings. – 2021, vol. 3047, pp. 17 - 23.