Software Defined Radio based Security Analysis For Unmanned Aircraft Systems

Harry Romesburg III
St. Bonaventure University
St. Bonaventure, NY 14778 USA
Email: romesbh18@bonaventure.edu

Jian Wang
Embry-Riddle Aeronautical University
Daytona Beach, FL 32114 USA
Email: wangj14@my.erau.edu

Yushan Jiang
Embry-Riddle Aeronautical University
Daytona Beach, FL 32114 USA
Email: jiangy2@my.erau.edu

Huihui Wang
St. Bonaventure University
St. Bonaventure, NY 14778 USA
Email: hwang@sbu.edu

Houbing Song
Embry-Riddle Aeronautical University
Daytona Beach, FL 32114 USA
Email: h.song@ieee.org

***Abstract*—With the development of unmanned aerial systems (UAS), the ubiquitous deployment of UAS is becoming a trend. With the digital transceiver, the remote pilot can control the UAS remotely and effectively. With the deployment of 5G technology on a large scale, the convenience of remote control is becoming obvious and stable. However, the convenience of remote control technologies also brings more vulnerabilities to UAS. Software defined radio (SDR) has been explored to play system exploitation and penetration test for the radio system widely. With block programming, an SDR can become a hands-on system exploitation tool for research. With the adjustment of antennas and programmings, we can exploit the vulnerabilities of the UAS system and fixed the problem in advance. In this paper, we introduce an approach to leverage SDR to realize signal spoofing for GPS location and injection for digital communication. Based on SDR, we analyze the security of UAS on the GPS and digital connections. With the adjustment of antennas, we can define the SDR into a GPS spoofing tool and inject the packets in the communication of the digital transceiver. The evaluation shows the approach can delay the GPS searching for tens of minutes and disorder the connections between ground control station to UAS.**

1. Introduction

With the development of lightweight electrical components [1], UAS is becoming a useful tool for many fields like education, agriculture, industry, and civilian applications [2], [3], [4], [5]. With easy assembling and cheap materials for replacement, a fleet of UAS can be formed in a short time. With regular cameras, the UAS can provide high-resolution images for aerial photography for civilian applications [6], [7]. With multispectral cameras, the UAS can provide infrared images and multiple information extraction for the researchers and engineers to make explore and analyze the target areas for development and searching. With hyperspectral cameras, UAS can provide multiple photos in hundreds of different spectrums. Due to the variable reflecting characteristics, the hidden features can be amplified in some specific spectrum which can be a good reference for the industrial detection and crop survey. With other accessories, UAS can provide the variable functions for civilian, industrial, agricultural and educational applications.

UAS can provide many convenient applications in different fields with quality assurance. However, the convenient connections and flexibility lead UAS is becoming a threat to public safety and private property including privacy [8]. With many external sensors assistance, UAS can achieve accurate control of the locations and operations for the specific missions. However, good performance assurance is vulnerable to the attacks of spoofing, injection, and hijacking. Once the UAS is under attack, the attackers can leverage the penetration technologies to take over the priorities of UAS. With control of UAS, the attackers can operate the UAS to fly into the public areas and make threats to public safety. At the same time, the UAS with cameras can be a malicious eavesdropping tool for attackers to disclose other people's privacy without permission. With the development of SDR, the SDR can be a hands-on tool for attackers to play attacks on public safety and disclose private properties. To defend the attacks from SDR, a comprehensive SDR based security analysis for UAS is crucial [9], [10], [11], [12].

As the crucial component of UAS, GPS provides localization and navigation for UAS. The accuracy of GPS can help UAS finish missions in the complex environment and the continuity of GPS localization can assure the GPS in the desired trajectory. The localization mechanism is dependent on the signal transmitted from multiple satellites correctly. The GPS of UAS is vulnerable to attacks on GPS spoofing. With GPS spoofing, a UAS can be manipulated in malicious attackers' trajectory [9]. To detect the GPS spoofing signal, [13] tried to leverage errors and thresholds checking to decide whether the UAS is under GPS spoofing. With machine learning technologies, the researchers in [14] adopted a support vector machine (SVM) to classify the signal received by GPS on UAS. Apart from GPS, the digital transceiver also plays a pivotal role in the operation

978-1-6654-4331-9/21/$31.00 ©2021 IEEE

of UAS remotely. The remote pilot can leverage the digital transceiver to connect the ground control station (GCS) to UAS in wireless [15]. The digital transceiver leverages micro aerial vehicle link (MAVLink) to exchange packets which involves monitoring and commands. If the attackers hijack the connection between UAS and GCS, the attackers can manipulate the UAS and disclose the privacy [16] of remote pilots. In [17], the researchers presented and introduced many attacks on MAVLink which contains spoofing, eavesdropping, and hijacking on the MAVLink. The surveys [18], [19] and simulations [20] presented vulnerabilities existing in MAVLink.

In this paper, we focus on SDR based security analysis for UAS. We will leverage SDR and multiple antennas configurations to transfer SDR into different types of penetration tools. With the evaluation of UAS, we presented the vulnerabilities of UAS on the GPS and MAVLink. Based on the evaluation, we presented a practical scheme for the researchers to evaluate the vulnerabilities of UAS.

2. Related Work

As of recently, the increase in demand for UAVs has caused the integrity of their security to be called into question. The majority of responses to this call have been to scrutinize the ability of the UAV to prevent security incidents as opposed to responding to them due to the ramifications following the time a UAV is exploited. In a recent study [14], [21], a prevention algorithm was presented which would counteract vulnerabilities in the UAVs' sensory data. It was discovered that the onboard sensory data of UAVs were able to be replicated to avoid detection of GPS spoofing. They deduced that gaining access to this data would be the equivalent of gaining full control of the drone itself. This approach however is limited since it becomes vastly difficult to ensure that the onboard data is accurate and has not to be tampered with. Additionally, the issue of large quantities of data comes into concern as it is difficult to ensure that each piece of data is safe and not causing a location for an incident. To avoid these problems, others have looked to use pre-installed hardware on the UAV to counteract GPS spoofing techniques. The most studied piece of hardware is the abilities of the UAV's camera to communicate with satellites to determine if the onboard data is properly accounted for a Vision-Based GPS-Spoofing Detection Method for Small UAVs [22], [23]. This method allows for there to be a level of protection offboard of the UAV in the situation that the UAV itself becomes compromised. It was determined that this implementation is efficient and feasible as they are using an already implemented hardware piece to create another level of security.

Meng et al. proposed the implementation of their spoofing detection algorithm that was aimed at combating GPS spoofing [21], [24] using optical flow fusion. They explored the vulnerabilities of the sensory data onboard UAVs and ways to prevent exploitation rooted in these insecurities. Through the method of data analysis before and after a set path a UAV took, they compared the data to see if an attack could be detected using their novel algorithm. This algorithm was able to detect that the onboard data of the sensors had been exploited which they determined would ultimately lead to the attacker gaining control of the UAV. Their implementation to prevent this kind of exploitation leads to the creation of a potential algorithm that could aid in preventing attacks through the vector of onboard UAV sensors.

Qiao et al. identified the possibility of creating a level of security through onboard hardware of UAVs through the often-attached camera [25]. This method was proposed to be efficient as communication with satellites to compare with the drone would add a level of security that would allow the drone to be far more secure than without the communication. This implementation is also beneficial as there are little to no adjustments that need to be made on the hardware end as they are using an already installed piece of hardware. They found that using the onboard camera in communication with satellite imaging was a sufficient way to prevent security incidence in civilian UAVs. This discovery allows for the security of civilian UAVs to be improved while not having to adjust many aspects of the drone itself, unlike implementations [26], [27], [28] of other research. This makes this method potentially more effective than other research as it would be far less resource-intensive to implement.

3. Methodology

To achieve a better performance of exploitation on GPS spoofing, we adopt SDR to generate the spoofing signal and leverage the spoofing signal to disorder localization of UAS. As shown in Figure 1, with receiving GPS signal, the UAS can locate itself. SDR acquire the signal from GPS and generate the fake signal to the UAS. The signal generated from SDR is stronger than the signal derived from a satellite. The GPS module will choose the SDR signal as the priority source of localization. Based on the mechanism, we can modify the packet content to lead the GPS to conduct another position.

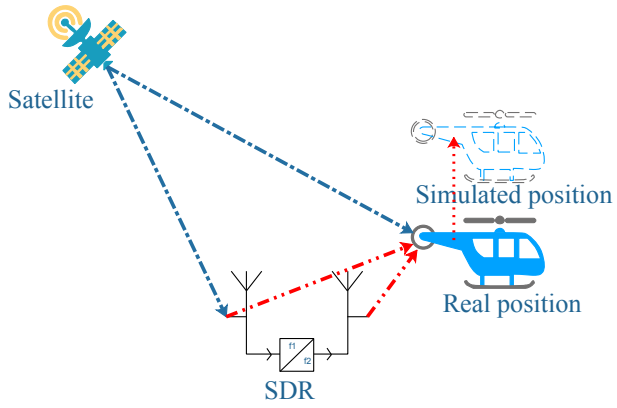

Figure 1. GPS spoofing

To generate a GPS signal, we need to use SDR to receive a GPS signal and derive the Earth-centered Earth-fixed (ECEF) position or NMEA GGA stream. To make sure accuracy, the sample rate for the GPS signal is set to 10 Hz.

With a GPS broadcast ephemeris file, the UAS's GPS satellite constellation can be derived. The GPS broadcast ephemeris file can be downloaded from the NASA GNSS website. Based on the ephemeris file, SDR can generate the simulated pseudo-range and Doppler for GPS satellites which is important to the digital signal generation. The digital generation is based on the interface for SDR signal generation of the IO interface.

Based on I/O generation and enough signal strength, the SDR can broadcast the sequential signal for GPS spoofing. Once the UAS receives the signal, the priority mechanism of GPS can abort the lock from the satellite signal and re-generate the lock to the SDR signal to achieve the localization data. And then the GPS of UAS is being spoofed.

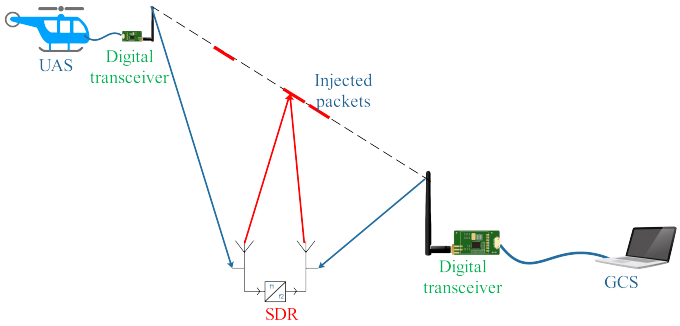

Figure 2. MAVLink injection

For MAVLink injection, the mechanism is similar to GPS spoofing. MAVLink is constructed based on the digital transceiver. The digital transceiver is a pair of devices. Both can transmit and receive the packets with on the channels of 433 MHz or 915 MHz. The SDR receives the signal derived from the digital transceiver on GCS and extracts the parameters of the connection. Thereafter, the SDR generates the injection signal to UAS to disorder the packets.

4. Evaluation

In this section, we will present our evaluation of security analysis on UAS. The evaluation is executed on MATLAB 2019b.

The configuration of the GPS module is shown as TABLE 1 and the SDR configuration is shown as TABLE 2.

We leverage the tools of GPS-spoofing-sim to generate spooring signals to disorder the movement of UAS. As Figure 3 shows, the drifting of the localization for GPS is around 0.05 before the spoofing is played at 800 s. We derive the localization data in the axis of x, y, and z from the UAS GPS module. At 800 s, we broadcast the spoofing signal to GPS module of UAS for 200 s. Figure 1 shows the error for the localization is increasing and fluctuates.

TABLE 1. GPS MODULE CONFIGURATION

Carrier	1575.42 MHz
Modulation	BPSK
Base clock	10.23e-6
Lchip	0.2

TABLE 2. SDR CONFIGURATION

Input	1
Output	1
Sample rate	10 Hz
Antenna	Vert 400

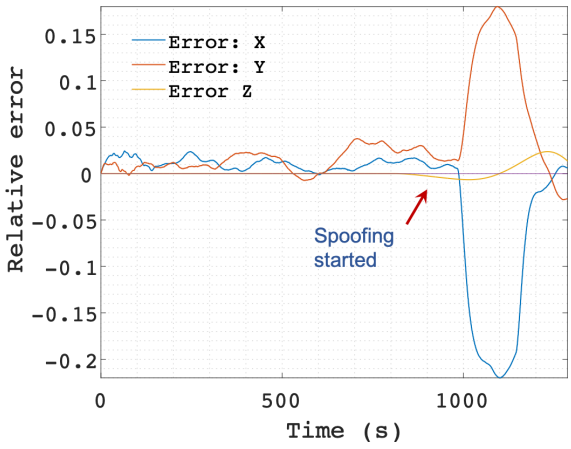

Figure 3. Relative error under GPS spoofing

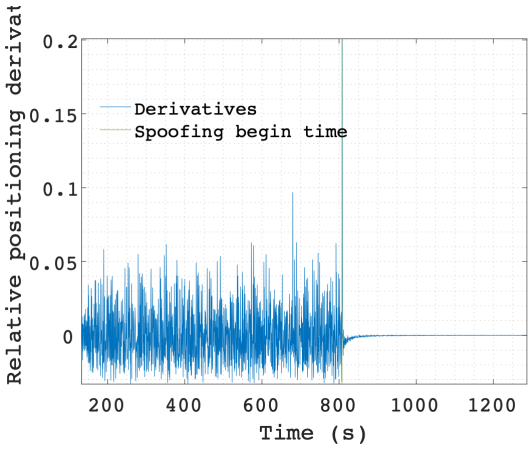

Figure 4. Relative positioning derivatives

Figure 4 shows the relative positioning derivatives for GPS spoofing attacks. We can find the derivatives keeps fluctuating from 0 s to 800 s. When we played the spoofing attacks, the derivative keeps steady. From the status of the GPS module, the GPS receiver is suffering from a low signal-to-noise ratio (SNR) from 0 s to 800 s and keeps high SNR when the spoofing is played. The source of the satellite signal is locked to the source of SDR which can have an SNR.

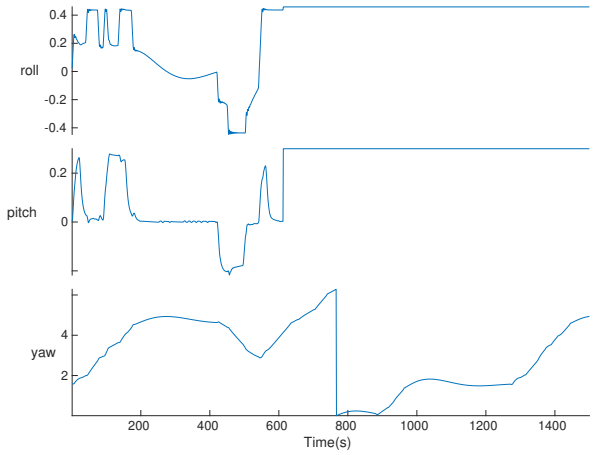

Figure 5. Mavlink injection

Figure 5 shows the injection processing of Mavlink. We use SDR to simulate HackRF to pretend a digital transceiver. HackRF receives a signal transmitted from UAS and derives the configuration of the digital transceiver. Figure 5 shows the monitoring data derived from the digital transceiver. At time 700 s, we played the injection attack to the ground control station. The roll and the pitch are injected to the maximum value. The ground control station transmitted commands to adjust the posture of UAS at 761 s. The results show the yaw turns a sharp swift in the flight. The yaw value shows the injection is successful.

5. Conclusion

In this paper, we introduce an approach to leverage SDR to realize signal spoofing for GPS location and injection for digital communication. Based on SDR, we analyze the security of UAS on the GPS and digital connections. With the adjustment of antennas, we can define the SDR into a GPS spoofing tool and inject the packets in the communication of the digital transceiver. The evaluation shows the approach can delay the GPS searching for tens of minutes and disorder the connections between ground control station to UAS. The results show that GPS spoofing can cause errors in the localization of UAS which can lead UAS to mistake operations. We injected false data into the packets of Mavlink in the ground control station. The injection causes the ground control station to adjust the posture of UAS.

Acknowledgment

This research was supported by the National Science Foundation under Grant No. 1956193.

References

[1] X. Yue, Y. Liu, J. Wang, H. Song, and H. Cao, "Software defined radio and wireless acoustic networking for amateur drone surveillance," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 90–97, 2018.

[2] H. Song, R. Srinivasan, T. Sookoor, and S. Jeschke, *Smart cities: foundations, principles, and applications*. John Wiley & Sons, 2017.

[3] H. Song, D. B. Rawat, S. Jeschke, and C. Brecher, *Cyber-physical systems: foundations, principles and applications*. Morgan Kaufmann, 2016.

[4] B. Jiang, J. Yang, H. Xu, H. Song, and G. Zheng, "Multimedia data throughput maximization in internet-of-things system based on optimization of cache-enabled uav," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3525–3532, 2019.

[5] X. Liu, H. Song, and A. Liu, "Intelligent uavs trajectory optimization from space-time for data collection in social networks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 853–864, 2021.

[6] J. Yang, C. Wang, B. Jiang, H. Song, and Q. Meng, "Visual perception enabled industry intelligence: State of the art, challenges and prospects," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 2204–2219, 2021.

[7] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, 2016.

[8] C. Constantinides and P. Parkinson, "Security challenges in uav development," in *2008 IEEE/AIAA 27th Digital Avionics Systems Conference*. IEEE, 2008, pp. 1–C.

[9] J. Su, J. He, P. Cheng, and J. Chen, "A stealthy gps spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 291–296, 2016.

[10] H. Song, G. A. Fink, and S. Jeschke, *Security and privacy in cyber-physical systems: Foundations, principles, and applications*. John Wiley & Sons, 2021.

[11] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 616–644, 2020.

[12] W. Li and H. Song, "Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

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

[14] G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, and A. Pescapè, "A svm-based detection approach for gps spoofing attacks to uav," in *2017 23rd International Conference on Automation and Computing (ICAC)*. IEEE, 2017, pp. 1–11.

[15] Y. Jiang, S. Niu, K. Zhang, B. Chen, C. Xu, D. Liu, and H. Song, "Spatial-temporal graph data mining for iot-enabled air mobility prediction," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[16] K. Zhang, Y. Liu, J. Wang, H. Song, and D. Liu, "Tree-based airspace capacity estimation," in *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*, 2020, pp. 5C1–1–5C1–8.

[17] Y.-M. Kwon, J. Yu, B.-M. Cho, Y. Eun, and K.-J. Park, "Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles," *IEEE Access*, vol. 6, pp. 43 203–43 212, 2018.

[18] G. Zogopoulos-Papaliakos, M. Logothetis, and K. J. Kyriakopoulos, "A fault diagnosis framework for mavlink-enabled uavs using structural analysis," in *2019 International Conference on Robotics and Automation (ICRA)*. IEEE, 2019, pp. 676–682.

[19] A. Koubâa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "Micro air vehicle link (mavlink) in a nutshell: A survey," *IEEE Access*, vol. 7, pp. 87 658–87 680, 2019.

[20] P. Śmigielski, M. Raczyński, and Ł. Gosek, "Visual simulator for mavlink-protocol-based uav, applied for search and analyze task," in *2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*. IEEE, 2017, pp. 1177–1185.

[21] L. Meng, S. Ren, G. Tang, C. Yang, and W. Yang, "Uav sensor spoofing detection algorithm based on gps and optical flow fusion," in *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, 2020, pp. 146–151.

[22] N. Xue, L. Niu, X. Hong, Z. Li, L. Hoffaeller, and C. Pöpper, "Deepsim: Gps spoofing detection on uavs using satellite imagery matching," in *Annual Computer Security Applications Conference*, 2020, pp. 304–319.

[23] J. Gaspar, R. Ferreira, P. Sebastião, and N. Souto, "Capture of uavs through gps spoofing," in *2018 Global Wireless Summit (GWS)*. IEEE, 2018, pp. 21–26.

[24] A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: A game-theoretic countermeasure for protecting uavs against gps spoofing," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2840–2854, 2019.

[25] Z. Li, W. Qiao, Y. Lu, and H. Lei, "Optimal controller placement in mec-aided software-defined uav networks against jamming attack," in *Proceedings of the 2020 2nd International Conference on Robotics, Intelligent Control and Artificial Intelligence*, 2020, pp. 74–79.

[26] J. A. Marty, "Vulnerability analysis of the mavlink protocol for command and control of unmanned aircraft," Theses and Dissertations, Tech. Rep., 2013. [Online]. Available: https://scholar.afit.edu/etd/613

[27] R. Sierzputowski, R. Polak, D. Wojtyra, and D. Laskowski, "Advanced protection methods of unmanned aircraft vehicle against attack by radio techniques," in *Radioelectronic Systems Conference 2019*, vol. 11442. International Society for Optics and Photonics, 2020, p. 114420Y.

[28] F. Le Roy, C. Roland, D. Le Jeune, and J.-P. Diguet, "Risk assessment of sdr-based attacks with uavs," in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*. IEEE, 2019, pp. 222–226.