Journal of the Indian Society of Remote Sensing (March 2021) 49(3):585–591
https://doi.org/10.1007/s12524-020-01225-1

REVIEW ARTICLE

Unmanned Aerial Vehicle's Vulnerability to GPS Spoofing a Review

Eshta Ranyal[1] · Kamal Jain[1]

Received: 19 October 2020 / Accepted: 22 October 2020 / Published online: 16 November 2020

Abstract
The Unmanned Aerial Vehicle often known as UAV plays a central role in providing multifarious services which can be encapsulated under following major categories namely military, research and civil. Various studies have revealed that unlike the military UAV the civil UAV uses unauthenticated, unencrypted and predictable signals and thus can be easily manipulated. With the burgeoning dependency on UAVs for time-critical response operations and many other, there is a need to secure the civil unmanned aerial system which lacks direct human interference. The goal of this paper is to focus on how Global Positioning System (GPS) signal spoofing allows the authentic ground control to change hands with threat actors. Spoofing forces erroneous location to be computed by target receiver by transmitting the counterfeit Global Navigation Satellite System like signals. The intention is to misinform the user about its location. In this paper, the UAVs vulnerability, resulting in complete command and control under the captor's influence, consequent to GPS spoofing, is analyzed and an analysis of the countermeasures to identify spoofing proposed by various researchers is done. While some countermeasures are computationally complex unsuitable for lightweight UAVs there are others that have been experimented on simulators. Very few have been established on real sensor data and have limitations of their own.

Keywords Unmanned aerial vehicle · Global positioning system · Spoofing · Cyber security · Threat analysis

Introduction

Infrastructural services, military operations and research applications are mounting to turn out to be indispensable without the use of UAVs. UAV development continues to evolve, as researchers incessantly find ways to maximize the potential of its usage in various fields. Real-time analysis is one of the critical areas where UAV services have become vital because of their exactness. The extensive use of UAVs has given rise to an excess of security concerns. Reliable navigation in UAVs bank totally on GPS (He et al. 2014). Localization and time synchronization in UAVs are also vastly reliant on GPS. Because of their ease of availability to the public, civilian GPS signals contrary to military UAVs are readily spoofable posing a potential hazard. They make the GPS receivers accept as true that they exist in locations other than their actual physical sites (Tippenhauer et al. 2011). In Spoofing attacks the signals that are moderately identical to the genuine satellite signals are generated. When a receiver collects in fake signals and real signals it can't distinguish between the two and hence the power of the counterfeit signals is adequately raised it takes charge of the GPS receiver. Now it is under the attackers command and can be induced with any kind of position or time. GPS spoofing is a furtive attack, where on one hand GPS signal jamming can be detected at the receivers end, it is difficult to identify spoofing attacks. Attacks of this kind counter a UAV result in communication loss with the ground control stations. UAVs used by military use GPS signals with encryption code superimposed on them thus making it a difficult attack vector. However unencrypted communication links are mostly used by civilian drones thereby making the transmission of false and malicious data quite a possibility. An attack is considered successful when an attacker is able to direct malicious directions to the UAV. This type of attack is the hardest to detect since the UAV has no way to

✉ Eshta Ranyal
eshtaranyal@gmail.com

Kamal Jain
kjainfce@iitr.ac.in

[1] Department. of Civil Engineering, Indian Institute of Technology Roorkee, Roorkee, India

authenticate if the Ground Control Station's been exploited. (Javaid et al. 2012)

In the paper spoofing attacks on UAVs with civilian GPS are investigated and analyzed. The civilian GPS signals are insecure (Wallischeck 2016). The GPS signals for military use are encrypted thus secure, but unavailable to the public. Upgradation of existing GPS systems is a necessity, but addition of encryption or validation to the civilian GPS signal is not a possibility.

At Earth's surface, the GPS signal strength when measured is about–160dBw. Once the antenna of the GPS receiver is shielded, it becomes easy to obstruct the signal. Blockage of GPS signal can efficiently take place by a signal of an analogous frequency, but superior strength. Blocking of signals and jamming them, nevertheless, are not the utmost security hazard, as in these cases, the GPS receiver discontinues receiving the GPS signals needed to resolve time and position. Serving the receiver of the GPS false signals such that it considers to be located elsewhere is a much more malicious attack. This kind of attack is further sophisticated than signal jamming as it is underhanded. To carry out the spoofing attack, a counterfeit GPS signal is broadcasted with a greater signal power than the original signal. The GPS receiver considers the fake signal to be the true GPS signal from the satellites, and disregards the original signal. The receiver thereby continues to compute the wrong position or time evidence grounded on this false signal.

The organization of the paper is as follows. "GPS Working" section discusses the working of GPS. The GPS spoofing problem is discussed in "Spoofing Problem" section. In "Overt Spoofing" section, probable countermeasures against GPS spoofing attacks are explored. "Covert Spoofing" section presents the conclusion followed by references in "Threat Assessment"section.

GPS Working

The Global Positioning System (GPS) consists of a network of about 27 satellites in 6 distinct orbits that repetitively broadcast timestamped packets characterizing their locations in space. This allows the users of GPS the capacity to acquire a 3-D position, velocity and time to fix in totally all sorts of weather. GPS operators can trace their location within ± 5m or ± 10–20m. in the poorest case (US Air Force 2003).

The timestamped messages are used by the GPS receivers to decide the duration it takes the signals from individual satellites, respectively, to reach the receiver. The distances between the respective satellites and receiver can be computed by taking a product of the time by the light's speed (Fig. 1). These pseudoranges may be collectively used to decide the receiver's position and what time it is. Two signals are transmitted by each GPS satellite, an unencrypted signal(civilian) and an encrypted signal(military)

The signals are received by the receiver from several satellites of the GPS network concurrently. Consequently, the distances to numerous satellites are recognized at any point in time. Given the distance of three GPS satellites, the below-given Fig. 2 gives an outline of the approximate distance calculated.

Spoofing Problem

There is no secret in the GPS signal's structure. The frequencies that it uses can be effortlessly generated with commercial-off-the-shelf equipment. This makes it relatively easy and inexpensive to construct a system to produce signals to fool a receiver into believing that the incoming signals are from GPS satellites. Transmission of these fabricated GPS signals causes receivers to catch onto the fabricated signals in lieu of the true signals. This is known as GPS spoofing (Humphreys et al. 2008). Adjustments to the delays in time can be made to inform the receiver about its distance from each satellite, so that it can adjust its position that the receiver resolves for. Therefore, spoofing offers a way to effectually take control UAVs which totally rely on GPS to determine their location.

Overt Spoofing

When an effort is made to camouflage an attack, it is called overt spoofing. It uses the jam-then-spoof strategy. The forged signals are broadcasted at a considerably higher strength than the true signals. By the time, the original signals reach the Earth's surface (Humphreys et.al. 2008) they are very weak. This results in the loss of true signals beneath the spoofer's more influential signals, affecting the receiver at the target to try to regain connection with the satellites. During this process of regaining the connection with the satellite, the receiver learns the spooler's signals, letting take over by the spoofer. The difficulty with this method is that the receiver drops its GPS connection for some time owing to jamming, thereafter the spoofer's signals may possibly result in a high in the positioning solution. Simple checks can be used to overcome overt, however, the bulk receivers in UAVs–do not implement anti-spoofing.

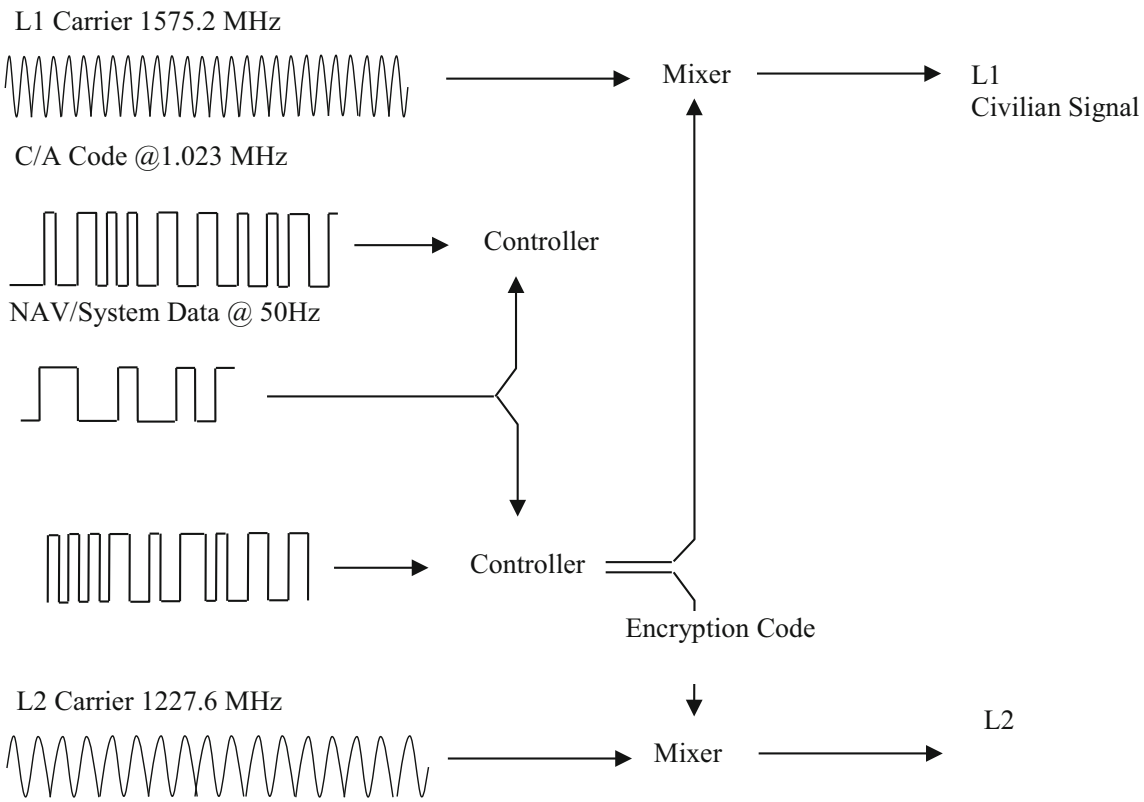

Fig. 1 GPS Signal Structure Source: Jon S. Warner et al., GPS Spoofing Countermeasures

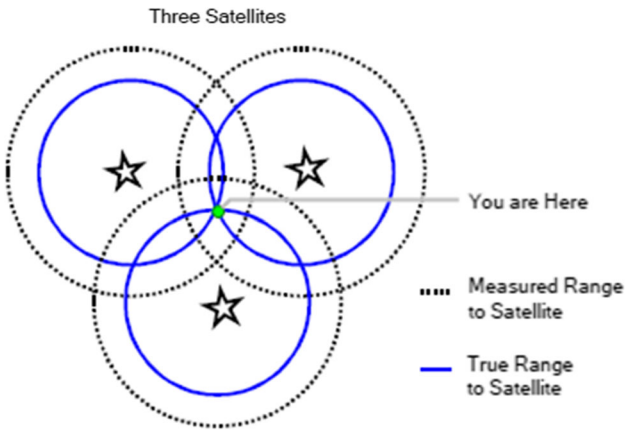

Fig. 2 Location approximation, Source: Jon S. Warner et al.,

Covert Spoofing

Covert spoofing involves the alignment of the forged signals with true GPS signals, then increasing the spoofer's strength to allow the receiver lock onto the fabricated signals (Psiaki et al. 2016). Thus, preventing the GPS lock to lose its grip on the signal, and the receiver catches on to the spoofer's uninterrupted signals from the true satellites.

A graphical explanation of the same is provided in Fig 3 as seen. The spoofer adjusts the delays, drawing the

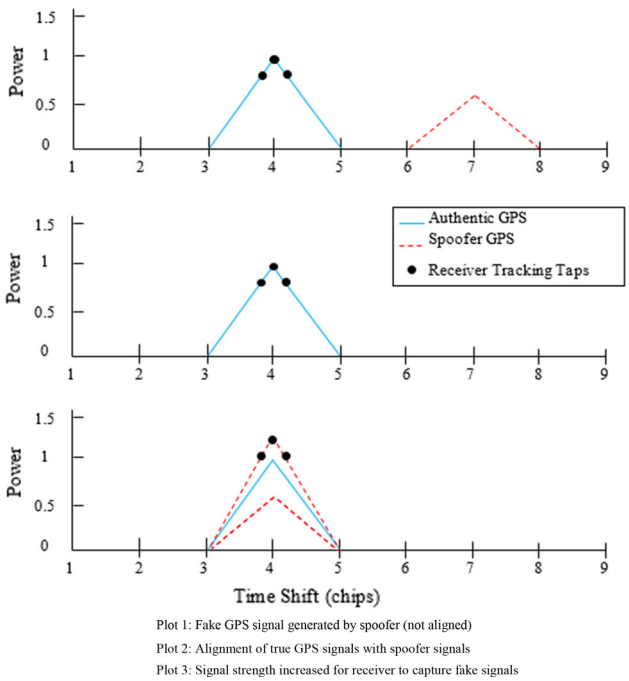

Fig. 3 Alignment of fake signals with GNSS signals, Source: Jon S. Warner et al., GPS Spoofing Countermeasures

receiver away from the real satellites, thus resulting in erroneous positioning Bhatti 2015 (Kerns 2014). This

approach necessitates tracking of the victim and proper timing of the signals to ensure aligned arrival with the authentic signals. (He et al. 2014)

Threat Assessment

The spoofing threat can be roughly divided into simplistic, intermediate and sophisticated attacks (Assessing the spoofing threat-GPS World 2009).

Simplistic Attack

This type of attack is generally achieved with the assistance of a simulator. A power amplifier and an antenna attached to the signal simulator is all that is required to transmit the RF signal toward the target receiver. Though easy to be carried out, this attack has its limitation due to cost of modern simulators. Size is another drawback because of its heaviness and bulkiness. Attacks carried out in the vicinity of the target make it challenging and visually apparent. Lack of synchronization of simulators output with GPS signals can cause easy detection of such attacks. It behaves like signal jamming because of asynchronization. Though simulator attack is easy to defend, still GPS receivers remain vulnerable to these attacks until equipped with spoofing countermeasures.

Intermediate Attack

This attack is generally carried out with the help of a portable spoofer receiver. A successful attack can be executed if the exact location and velocity of the victim receiver's antenna is known. This allows the counterfeit signals to be precisely positioned relative to the authentic signal at the receiver. It is easy to detect such a spoofing attack without accurate positioning. The spoofer's receiver needs to be placed in proximity of the target receiver thereby allowing the spoofer receiver to accurately draw in the position, time and velocity. The unavailability of commercial off the shelf portable receiver-spoofer decreases the likelihood of such an attack. Nevertheless, the growth of software-defined GPS receiver may narrow the gap to such attacks. Also, relatively cheap off the shelf components can be assembled to construct a receiver spoofer. It would be moderately difficult to discover a portable spoofer receiver attack because of its correctness of alignment with the GPS signals. The only known user-equipment-based countermeasure effective against such an attack is angle-of-arrival discrimination as continuous replication of the relative carrier phase is impossible between a couple (at least) of antennas of a suitably furnished victim receiver.

Sophisticated Attack

This is a synchronized attack which involves that many spoofer receivers as antennas over the victim receiver. It is achieved by mounting atop the target antenna, very small in size on the spoofer receiver. The receiver and transmitting antenna is placed on the upper and lower faces of the device safeguarded from each other to avoid self-spoofing. With several such spoofer receivers mounted on each target antenna sharing the same communication link, the angle of arrival defense fails. Needless to state such a type of attack accedes to all the challenges of placing the spoofer receivers atop the antennas. The only defense against this attack is cryptographic authentication.

Thus, a spoofing attack owing to simulators poses a great threat in the near future. Due to the augmented awareness in spoofing, numerous works on the spoofing methods have been carried out. Humphreys et al.(2008) examined the consequence of spoofing signals on single channel. A technique was recommended by (Tippenhauer et al. 2011) in which numerous receivers were spoofed at numerous locations dependent on the spoofer's position, and established the consequence of the spoofer signal generation parameter for the satellite-locking takeover of the receiver. Shepard et al. (2012) carried out spoofing by influencing the carrier phase, code phase and Doppler frequency by receiving genuine GPS signals at a spoofer. In a relevant study (Kerns et al. 2014), time-delayed spoofing signals were produced by deciphering legitimate GPS signals, and the effect of the time-delayed spoofing signals on UAV was examined. As mentioned above, work on the spoofing of UAV using real spoofing signals as well as work on the spoofing technique has unceasingly been carried out.

Countermeasures

Spoofing attacks on UAVs can be very detrimental. They can result in misleading position information which is tough to detect. Thus, it becomes imminently significant to develop practices to sense spoofing reliably. Several such practices have been suggested which are discussed in this section.

Encrypted signals are one way of detecting spoofing. Encryption techniques demand a communication link of high-bandwidth amid the spoofing attack of a prospective victim and a trustworthy supply of coding data and involvement of substantial latency between attack and detection (Lo 2009) (Levin et al. 2011) (Psiaki et al. 2011) (Turner 2013) (Li, Performance Analysis of a Civilian GPS Position Authentication System, Winter 2013) (U.S. 2014)

Another category of approaches applies advanced Receiver Autonomous Integrity Monitoring (RAIM)-type techniques. Rather than considering solely pseudo-range consistency, these RAIM techniques inspect additional signal features like distortion of the PRN code correlation function on the early/late axis, absolute power levels, the attainable existence of numerous dissimilar correlation peaks in signal-acquisition-type calculations, and alternative signal or receiver characteristics. Such ways are comparatively straightforward in the appliance as they do not need much additional hardware but can have hassles differentiating among multipath and spoofing or between jamming and spoofing (Pini et al. 2011) (Wesson 2011) (afarnia-Jahromi 2012) (Dehghanian 2012) (Humphreys 2012) (Li 2013) (Hwang 2014) (Jovanovic 2014).

A third category recommends the addition of Navigation Message Authentication bits. Here, the low-rate navigation data message is encrypted in parts. Such methods require alteration of the navigation data message and can result in long latencies between the onset of a spoofing attack and its detection (Wesson K. R, Sept. 20-23,) (Wesson 2012) (Konovaltsev 2013)

A fourth category takes advantage of the differing signal-in-space mathematics of spoofed signals as compared to true GNSS signals. All spoofed signals usually arrive from a similar direction, however, true signals arrive from a multi-array of directions. A number of these ways use receiver antenna motion to attain direction-of-arrival sensitivity. Others use an array of 2 or additional receiver antennas. (U.S 2011) (Bardout, 2011) (Nielsen 2011a) (Broumandan 2012) (Psiaki 2013)

The most powerful of those detection ways exploit models of the consequences on carrier-phase information of antenna motion or antenna-array geometry. This information could also be partial as a result of an unknown antenna-array perspective might have to be determined as a part of the detection calculation. Their power originates from the high degree of precision with which an archetypal GNSS receiver can determine beat carrier phase.

The countermeasure methods proposed by Jon S. Warner and Roger G. Johnston (Johnston) are on the basis of monitoring the signal power and on the fact that the strength of the signal for fake signals is at first higher than the original signals. This involves monitoring, recording and then comparing observed strength of signal with the expected strength. A threshold is fixed, which, if exceeded results in sounding an alert. This countermeasure method is based on the assumption that GPS satellite simulators are being used which deliver signal strengths of magnitude larger than any probable satellite signal. This is an unambiguous symptom of a spoofing attack. Another way involves recording and comparing the signal's average strength moment to moment. If the signal exceeds a set threshold, it raises an alarm to alert the user. Extending the above two techniques, the relative and absolute signal strengths can be tried independently for the incoming satellites signals, respectively. GPS satellite simulators create signals of equal strength, whereas true satellite signals differ from satellite to satellite temporally. Thus, if the characteristics of signals are perfect, there is a probability that something is wrong, and the user is warned. Another approach as given by Jon S. Warner and Roger G. Johnston (Johnston) is to monitor the satellite identification codes and the number of satellite signals**.** The authentic signals transmitted by space satellites are generally less in comparison with the GPS satellite simulators at a given time. GPS receivers of UAVs can be altered to record satellite identification information which can then be compared with previously recorded data. Methods to record information of the received satellite signals in terms of number, and the identification codes of satellites are also adopted to detect foul play. Another method would involve monitoring time intervals of picking up signals from space satellites and generated satellite signals. If the difference in time is a constant, the user can be alerted with a notification. Also accurate GPS clocks may be used to compare the time resulting from GPS signal, which can be used to check the validity of the signal. Deviation beyond a set threshold may be used to alert the likelihood of a spoofing attack. The above-mentioned strategies can be realized by adding components to existing GPS receivers, redesigning them is not necessary.

S. Khanafseh et al. developed an INS batch RAIM monitor that detects GPS spoofing attacks in (Khanafseh 2014). This monitor evaluates the integrity risk of the position solution and the probability of missed detection.

B. Ali et al. presented an architecture called the spoofing-aware receiver architecture that can detect spoofing attacks, categorize the spoofing and authentic signals, and alleviate the damaging effect of fake spoofing signals in (Ali Broumandan 2015). It showed effective detection of fake signals created from a single-point source with the help of different metrics, namely AGC level.

W. Myrick et al. implemented a method termed MAGIC with the help of anti-jam/anti-spoofing single antenna (Wilbur L Myrick 2015). It replaced a standard C/A code correlator with a reduced-rank MMSE-based C/A code correlator for improved anti-jam/anti-spoofing capability. This method is solely for single antenna GPS receivers.

J. Mead et al. developed a hardware termed sandboxing (Joshua Mead 2016), for runtime observation of boundary signals and isolation to detect and isolate undesirable behavior.

A. Ranganathan et al. proposed a detection method called SPREE which uses the auxiliary peak in a GPS receiver enabling detection of an attacker capable of

accomplishing the seamless GPS-spoofing attack (Aanjhan Ranganathan 2016)

Spoofing Detection with Two-Antenna Differential Carrier Phase by (Mark L. Psiaki 2014) is a novice method that detects spoofing attacks which are resistant to standard RAIM method and can detect an attack in seconds without outward aiding. The signal-in-space features applied to sense spoofing are the associations of the arrival directions of the signal to the vector pointing from one antenna to other.

The above-mentioned methods have common drawbacks which require special hardware devices that significantly escalate the weight and cost of the UAV. Therefore, these methods are not applicable to lightweight civil drones.

Conclusion

The broad reliance on GPS and the prospect for fiscal addition or prominent harm makes spoofing a gathering threat. In this paper, the competence to affect the behavior of an autonomous UAV by transmitting falsified GPS signals was investigated. The techniques for overt and covert capture of a UAV were pondered which disclose that an attack against a UAV is possible both in fact and operationally. With the software-defined receiver-spoofer, it is easy to mount an assault that would topple most hardware-based spoofing countermeasures. With every modernized GNSS signal's addition, the ramifications of escalating a spoofing assault rises evidently.

Significantly, extra research and assets be committed for improvement and testing of user equipment for spoofing countermeasures. Further investigation into cryptographic procedures for validation ought to be sought, as it seems that only cryptographic measures can result in safeguarding against a spoofing attack. The dangers of common GPS spoofing and practices of stringent countermeasures ought to be considered seriously. Manufacturers of GPS user equipment for commercial purpose should implement at least elementary spoofing countermeasures.

Though the countermeasures suggested in the paper will not result in termination of spoofing attacks, they will caution GPS receiver's user to doubtful activity. Thus, lessening the chances for a spoofing attack to become successful, and compelling the adversaries to implement advance refined techniques in-lieu of simplistic attacks.

References

Assessing the spoofing threat-GPS World. (2009, january 1). (GPS World Staff) Retrieved from https://www.gpsworld.com/defense security-surveillanceassessing-spoofing-threat-3171/

Bardout, Y. (2011). Authentication of GNSS position: An assessment of spoofing detection methods. In *Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011)* (pp. 436-446).

Broumandan, A., Jafarnia-Jahromi, A., & Lachapelle, G. (2015). Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. *GPS Solutions, 19*(3), 475–487.

Broumandan, A., Jafarnia-Jahromi, A., Dehghanian, V., Nielsen, J., & Lachapelle, G. (2012, April). GNSS spoofing detection in handheld receivers based on signal spatial correlation. In *Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium* (pp. 479-487). IEEE.

Dehghanian, V., Nielsen, J., & Lachapelle, G. (2012). GNSS spoofing detection based on receiver C/No estimates. In *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)* (pp. 2878-2884).

Dovis, F. C. (2011). *Detection of Spoofing Threats by Means of Signal Parameters Estimation*. Portland: ION GNSS.

He, L., Li, W., Guo, C., & Niu, R. (2014, December). Civilian unmanned aerial vehicle vulnerability to gps spoofing attacks. In *2014 Seventh International Symposium on Computational Intelligence and Design* (Vol. 2, pp. 212-215). IEEE.

He, L., Li, W., Guo, C., & Niu, R. (n.d.). Civilian Unmanned aerial vehicle Vulnerability to GPS Spoofing Attacks. IEEE.

Humphreys, T. E. (2008). *September)*. Assessing the spoofing threat: Development of a portable GPS civilian spoofer.

Humphreys, T. E., Bhatti, J. A., Shepard, D., & Wesson, K. (2012). The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques. In *Radionavigation Laboratory Conference Proceedings*..

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Radionavigation laboratory conference proceedings*.

Hwang, P. Y., & McGraw, G. A. (2014, May). Receiver Autonomous Signal Authentication (RASA) based on clock stability analysis. In *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014* (pp. 270-281). IEEE..

Jafarnia-Jahromi, A., Lin, T., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). *Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver*. Newport Beach, CA: ION ITM.

Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012, November). Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *2012 IEEE Conference on Technologies for Homeland Security (HST)* (pp. 585-590). IEEE.

Jovanovic, A., Botteron, C., & Fariné, P. A. (2014, May). Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers. In *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014* (pp. 1258-1271). IEEE.

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics, 31*(4), 617–636.

Khanafseh, S., et al. (2014). GPS spoofing detection using RAIM with INS coupling. *IEEE/ION Position, Location and Navigation Symposium*. https://doi.org/10.1109/PLANS.2014.6851498

Konovaltsev, A., Cuntz, M., Haettich, C., & Meurer, M. (2013). Performance analysis of joint multi-antenna spoofing detection and attitude estimation. In *Proceedings of ION International Technical Meeting 2013 (ION ITM 2013)*.

Levin, P., De Lorenzo, D., Enge, P., & Lo, S. (2011). *Authenticating a Signal Based on an Unknown Component Thereof*. US Patent 7,969,354B2.

Li, Z., & Gebre-Egziabher, D. (2013). Performance analysis of a civilian gps position authentication system. *Navigation, 60*(4), 249–265.

Li, Z. a.-E. (Winter 2013). Performance Analysis of a Civilian GPS Position Authentication System. Navigation, Vol. 60, No. 4.

Lo, S., De Lorenzo, D., Enge, P., Akos, D., & Bradley, P. (2009). Signal authentication: A secure civil GNSS for today. *inside GNSS*, *4*(5), 30-39.

Mead, J., Bobda, C., & Whitaker, T. J. (2016, December). Defeating drone jamming with hardware sandboxing. In *2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)* (pp. 1-6). IEEE.

Nielsen, J., Broumandan, A., & Lachapelle, G. (2011). GNSS spoofing detection for single antenna handheld receivers. *Navigation, 58*(4), 335–344.

Nielsen et al. (2011). *Method and System for Detecting GNSS Spoofing Signals*. US Patent 7,952,519 B1, filed Apr 16, 2010, and issued May 31, 2011.

O'Hanlon, B. W., Psiaki, M. L., Bhatti, J. A., Shepard, D. P., & Humphreys, T. E. (2013). Real-time GPS spoofing detection via correlation of encrypted signals. *Navigation, 60*(4), 267–278.

Pini, M., et al. (2011). Signal quality monitoring applied to spoofing detection. In *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)* (pp. 1888-1896)..

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS Spoofing and Detection. *Proceedings of the IEEE*, *104*(6), 1258–1270.

Psiaki, M. L., Powell, S. P., & O'Hanlon, B. W. (2013). GNSS spoofing detection: Correlating carrier phase with rapid antenna motion. *GPS World, 24*(6), 53–58.

Psiaki, M. et al. (2014).*GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase*. US Patent 8,712,051 B2, issued Apr 2014.

Psiaki, M.L., B.W. O'Hanlon, J.A. Bhatti, D.P. Shepard, & Humphreys, T.E. (2011). Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals. In *Proceedings of ION GNSS*. Portland, Oregon.

Ranganathan, A., Ólafsdóttir, H., & Capkun, S. (2016, October). Spree: A spoofing resistant gps receiver. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking* (pp. 348-360).

Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., & Capkun, S. (2011). On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security* (pp. 75-86)..

Turner et al., (2013, September). PROSPA: Open service authentication. In *Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2013)* (pp. 2992-2996)..

US Air Force, GPS Support Center. (2003). Retrieved from https://www.peterson.af.mil/GPS_Support/

Wallischeck, E. (2016). Volpe, John A. National Transportation Systems Center, Vulnerability ment Of The Transportation Infrastructure Relying On The Global Positioning System, Final Report., Department of Transportation. Retrieved from https://www.navcen.uscg.gov/archive/2001/Oct/FinalRep

Warner, J. S., & Johnston, R. G. (2003). *GPS spoofing countermeasures, vulnerability assessment team, los alamos national laboratory research paper LAUR-03-6163*. New Mexico, USA: Los Alamos.

Wesson, K. R. (2012). Practical cryptographic civil gps signal authentication navigation. *Journal of the Institute of Navigation, 59*(3), 177–193.

Wesson, K. R. (2011) A Proposed Navigation Message Authentication Implementation for Civil GPS Anti-Spoofing,. *Proc. ION GNSS,* Portland.

Wesson, K. S. (2011). An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing. *Proc. ION GNSS 2011*. Portland.

Wilbur L Myrick, M. P. (2015). Multistage anti-spoof GPS interference correlator (MAGIC). IEEE Military Communications Conference. IEEE, 1497–1502