Detection of GPS Spoofing

Joseph Le

AAE 575

Purdue University

Abstract

GPS (Global Positioning System) spoofing is the act of interfering with the workings of various parts of the system such that a false location is determined. Since the codes and signal structures for GPS are available to the public, attackers are able to reproduce, alter, and overpower these signals that are received by a receiver and interferes with the algorithm that calculates the positioning. This is typically done by transmitting false signals that assume the codes/signals of various satellites such that the receiver calculates the location that was determined by the transmitter, this desired false location may be a determined location that is spoofed or a random mix of signals that return random or nonsensical on the receiver end (Chapman).

The risks of GPS spoofing vary in many ranges. This may include interference with the power grid, takeover of the control of remotely controlled vehicles (O'Hanlon, Brady W et al.), and risks in cybersecurity either in civilian cases or government and military applications. These risk not only harms the workings of society but could also physically affect people within it.

Detection of these spoofed transmissions has been a deep field yielding several methods that make use of various properties of signals and the way that the GPS works. Such methods may include detection through correlation of the signals, doppler and electromagnetic properties, and

several new cutting-edge methods. The detection of these GPS spoofing signals is important to improve the security, safety, and overall workings of society and advert the risks that these spoofing attacks may contain.

Literature Review

Spoofing Methodology

The first method of spoofing is to bombard the target with a simulated GPS signal that can contain false data and has much higher power than that of the true GPS signal. This will cause the receiver to lock onto the false signal rather than the true GPS signal. This works due to the automatic gain control (AGC) [3] units that are present in many receivers which adjust the gain and power that that receiver locks onto as a spoofed signal's power is increased. The simulated signal does not need to be fully synchronized with the authentic GPS signal [9] but commercial receivers with less robust methods of detecting spoofing, will still be susceptible to this attack. This is the simplest method of spoofing, and many modern receivers are able to easily detect this type of spoofing with monitoring of signal parameters, consistency checks, and other measurements available in certain systems such as movement.

Another method of spoofing is to use a receiver to match the characteristics of a GPS signal more closely. The spoofer uses a receiver that may be nearby to the target receiver and collects the same data as target receiver in order to simulates the authentic GPS signal. The spoofer then injects a false signal into the true signal and transmits towards the target receiver at such a low power that it is in the noise floor of the true signal. After the infected signal is received by the target receiver from the spoofing transmitter, the spoofer then slowly increases the power of the false GPS signal to the point that receiver locks onto the false signal rather than the legitimate signal. The spoofer then is able to shift the false signal to a determined code which changes the calculations that are done by the target receiver which changes the location that is determined by the target. The closer this spoofing apparatus is to the target receiver the easier it is to work since the GPS data received by the spoofer (delay, carrier freq., phase, etc.) are much

closer to the receiver and requires less work to match. Since the signals that are transmitted match up closely and are synchronized to that of the intended GPS signal, it is hard to detect with the previous methods that were mentioned. This method of spoofing is also known as repeater spoofing.

A more sophisticated method of spoofing, which is also the most complex method, is receiver-based spoofers [9]. Though this method is hardest to detect it is also the hardest to implement, where the position of the target receiver must be known down to the centimeter level in order to perfectly mimic the code and carrier phases in the spoofing signal. Once this information is known, an array of transmitters are utilized which must also match the array manifold of the target receiver in order to circumvent any angle of arrival filters in the receiver. This method of spoofing is very robust and can defeat many spoof detection methods, but this is offset by the complexity and the limited range of this approach to spoofing.

Dangers and Vulnerabilities in GPS Dependent Systems

A major danger of the effects of GPS spoofing come in the form of vehicle control [2]. Being able to provide false positioning date, a spoofer is capable of hijacking the autopilot system of boats, planes, and other vehicles [5]. This is a concern especially for military vehicles that may have weapons and sensitive data onboard, posing a security issue. Though military GPS signals are encrypted using P codes [1] which hinder the efforts of spoofing, there are still cases of GPS spoofing hijack as occurred in 2011 when Iran captured US drones [4].

Other major attacks that may occur are those on societal infrastructure that depend on GPS data. This includes the telecommunication network [5] which depends on the

synchronization between the clocks in the towers which reduces the interference between the towers. A spoofer could disturb the synchronization between certain towers which renders the tower inoperative until the attack is halted. Similarly, city power grids depend on the GPS system to synchronize and time stamp measurements to detect variations and other data within that power grid. A spoofing attack could cause instabilities and distortions in the system or cause false readings that may lead to blackouts and damage to the system [5].

Description of Spoofing Detection Methods and Limitations

The first method of spoofing detection is monitoring the power of the received GPS signals. Within this method, various parameters can be used to monitor the signal, one such parameter is the signal to noise ratio (C/N0) [5]. This method relies on the fairly stable signal to noise ratio that is received from the GPS, while as an attacker tries to interfere with the signal by using a higher power, the signal to noise ratio may change. The simplicity of this method also indicates its robustness. If a spoofer can recreate the ratio that the receiver detects, then they are able to bypass the signal to noise ratio checks. Other power monitoring methods include absolute power monitoring [5] and power variation vs. movement monitoring. Absolute power monitoring has similar vulnerabilities as the signal to noise ratio monitoring, but cross referencing the movements of a receiver to the power variation may be a safer bet. This method is based on the power variations that occur when a receiver is moving (doppler shift), cross referencing this to the movements checks if the GPS signal that is received is legitimate, while a GPS spoofer that does not consider the motion of a receiver may not be able to bypass these checks. A limitation of this method is that not all receivers are free to move, thus leaving stationary receivers vulnerable.

Spatial processing makes use of multiple antennas to cross reference between each other to determine the legitimacy of a GPS signal. This is effective against GPS spoofers that make use of a single antenna to transmit counterfeit signals. Multiantenna spoofing discrimination [9] uses the separation of multiple fixed antennae to detect the phase differences between the antennae, this information can be used to calculate the distances between the antennae with GPS data and compare them to the actual distance between the antennae. A single antenna spoofer transmitting illegitimate signals that are received by an antenna array will result in incorrect orientation calculations which will result in the detection of the spoofer. The limitation of this method is the physical complexity of the array of antennae which cannot be used on mobile receivers or smaller receiver facilities.

The last method of GPS spoofing detection that will be discussed is signal quality monitoring. Signal Quality Monitoring (SQM), which was used originally for multipath detection, focuses on the PRN codes that are sent out by GPS satellites. As a spoofing signal slowly takes over the tracking of an authentic signal, the phases in the code will also slowly shift and separate from each other [10], this will then affect the correlated signal where the signal from a spoofer will match up with the signal from a GPS signal. SQM employs two tests (ratio and delta) [9] which detect any type of “flatness” peaks in the correlated signals of the received signals and abnormal asymmetry in said signal. These tests are done through vector tracking which monitors the PRN phase, doppler shift, and carrier phase. The method keeps track of these values and compares them to the signal that is transmitted by a spoofer to determine the authenticity of the signal, if the doppler shift and PRN code phase end being nonzero after the algorithm is implemented it is considered a counterfeit signal. A limitation of this method is that it assumes that the receiver has already locked onto an authentic signal peak before being

attacked by a spoofer, also, since SQM is used for multipath monitoring, this method is unable to detect the difference between a signal that is being reflected and a signal that is being spoofed.

References

[1] O'Hanlon, Brady W et al. "Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals." Navigation (Washington) 60.4 (2013): 267–278. Web.

[2] Kerns, Andrew J et al. "Unmanned Aircraft Capture and Control Via GPS Spoofing." Journal of field robotics 31.4 (2014): 617–636. Web.

[3] Akos, Dennis M. "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)." Navigation (Washington) 59.4 (2012): 281–290. Web.

[4] Zhang, Heng et al. "Review on GPS Spoofing-Based Time Synchronisation Attack on Power System." IET generation, transmission & distribution 14.20 (2020): 4301–4309. Web.

[5] Ahmad, Mukhtar et al. "Impact and Detection of GPS Spoofing and Countermeasures Against Spoofing." 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). IEEE, 2019. 1–8. Web

[6] Chapman, Adam. "GPS Spoofing." 2017. https://sites.tufts.edu/eeseniordesignhandbook/files/2017/05/Red_Chapman.pdf.

[7] Troglia Gamba, Micaela et al. "Hypothesis Testing Methods to Detect Spoofing Attacks: a Test Against the TEXBAT Datasets." GPS solutions 21.2 (2017): 577–589. Web.

[8] T.E. Humphreys, J.A. Bhatti, D.P. Shepard, and K.D. Wesson, "The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques," Proc. ION GNSS, Nashville, TN, 2012.

[9] Jafarnia-Jahromi, Ali et al. "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques." International journal of navigation and observation 2012 (2012): 1–16. Web.

[10] Zhang, Xinran & Li, Hong & Yang, Chun & Lu, Mingquan. (2020). Signal Quality Monitoring Based Spoofing Detection Method for GNSS Vector Tracking Structure. IET Radar, Sonar & Navigation. 14. 10.1049/iet-rsn.2020.0021.