Survey on Effective GPS Spoofing Countermeasures

Zeeshan Haider[1], Shehzad Khalid[2]
Bahria University
Pakistan
zeshan_hyder@hotmail.com
shehzad@bahria.edu.pk

ABSTRACT: *There is an overwhelming dependence on Global Positioning System (GPS) in every sector, ranging from civil to military. The over dependence on GPS and its potential vulnerabilities has raised many concerns among government, scientists and all those who employ GPS for their business and other critical applications. It is due to the fact that GPS receivers can be easily be spoofed and the operations of any system can be disturbed and compromised which may result in a catastrophe. Many techniques have been proposed to meet the challenge of protecting GPS receivers from spoofing threat but none of these techniques are in use. Researchers are trying desperately to find a complete solution to meet this threat. This paper will present an analytical overview of the techniques that have been proposed to protect civilian GPS receiver. This survey analyzes different alternative solutions to prevent spoofing and explore a combination of two or more techniques that can provide most effective spoofing countermeasure technique.*

Keywords: Global, Positioning, Spoofing, System; Satellite, Transmitters, Recievers

Received: 25 July 2016, Revised 29 August 2016, Accepted 3 September 2016

1. Introduction

Global Positioning System (GPS) is a space based navigation system comprising of 24 satellites positioned into space by US Government Department of Defense[1]. The original application of GPS was in military but in 1980 this service was also made available for civilian to use all over the world. Today, GPS can be found in any industry sector wherever information about location, velocity, heading and timing is required. Common applications of GPS include navigation, surveying, agriculture, security, mining and aviation. The transmitters on GPS satellites produce different signal for military and civilian use respectively. The military signal is encrypted and therefore is more secure as compared to unencrypted civilian signal. Due to unencrypted transmission of signal for civilians and US Government unwillingness to provide higher protection level to civilian GPS signal, has left the civilian sector GPS users open to different types of GPS Spoofing threats.

GPS Spoofing is an attack to provide false information to GPS receivers by broadcasting counterfeit signals similar to original

GPS signal or by recording original GPS signal captured somewhere else in some other time and then retransmitting the signal [2]. The Spoofing attack causes GPS receivers to provide wrong information about position and time. There are variety of techniques to perform a successful spoofing attack depending on sophistication level of the techniques, software and hardware tools [2] [3].

To understand the significance of spoofing prevention and countermeasure let's Imagine that you are responsible to transport a very sensitive and top secret cargo from one location to another by air and someone intends to hijack the plane and steals the sensitive cargo. A typical approach is to take over the plane through armed attempt, but in this case it is not possible as the aircraft transporting the sensitive equipment is not a commercial airline therefore only authorized personals are allowed to enter in the aircraft. A more sophisticated approach is to, somehow misguide the aircraft, deviate it from its original flight path and make it land on desired location. For this purpose, the onboard GPS receivers can be spoofed to accomplish the task explained above. Similarly, there are many other critical tasks that heavily relay on GPS navigation and no one can afford a loss in terms of human causality or sensitive cargo etc. Due to commonly available tools and hardware to perform spoofing and proliferation of spoofing techniques it is vital to conduct research on the development of techniques to effectively detect and prevent GPS spoofing attacks. There are many techniques proposed by researchers and students all over the world to find a way for protection against GPS spoofing attacks. Every technique has its own advantages and lacking. In this paper we will present and study most commonly used techniques and then compare each technique with our defined criteria of effective GPS spoofing countermeasure, so that we can find out which technique is the best technique.

The paper is organized in five sections. Introduction is given in Section 1. Section 2 provides basic information about spoofing types and their advantages and disadvantages. Section 3 briefly describes each technique including hardware setup and the components used. Section 4 will present the analysis of each technique with respect to criteria defined. Section 5 provides the conclusion of our survey.

2. Spoofing Technqiues

There are a variety of techniques to perform a successful spoofing attack depending on sophistication level of the techniques, software and hardware tools. The three common GPS spoofing technique with different sophistication levels are simplistic, intermediate and sophisticated techniques [2]. The simplistic spoofing attack is the most commonly used technique to spoof GPS receivers as this kind of attack only uses a commercial GPS signal simulator, amplifier and antenna to broadcast signals towards target GPS receiver. A successful simplistic GPS spoofing attack was performed in 2002 by researchers at Los Almos National Laboratory [4]. Simplistic GPS Spoofing is easy to perform but the cost of commercial GPS signal simulator can be as high as $400K and very heavy which makes it less mobile. Further signal broadcasted by simulators are not synchronized by available original GPS signal therefore simplistic spoofing attempts can easily be detected and can only work as jammer instead of spoofing device to feed false information to target GPS receiver [2][3].

In Intermediate spoofing attack, the spoofing component consists of GPS receiver to receiver genuine GPS signal and spoofing device to transmit fake GPS Signal. The main idea in this type of spoofing attack is to estimate the target receiver antenna position and velocity and then broadcast fake signal relative to genuine GPS signal. This type of spoofing attack is difficult to detect and can be partially prevented by the use of Inertial Measurement Unit [2].

Sophisticated spoofing attacks are the most advanced type of GPS spoofing attack. In this type of spoofing multiple receiver-spoofer devices target the GPS receiver from different angle and directions. The angle-of-attack defense against GPS Spoofing in which the angle of reception is monitored to detect spoofing, fails in this spoofing scenario. The only defense successful against such type of attack is cryptographic authentication [2].

3. Brief Overview of Spoofing Countermeasures

Global Positioning System is offering tracking services to many applications. Some of applications uses GPS for variety of sensitive and critical tasks. Due to growing threat of GPS spoofing many techniques have been proposed to detect and prevent GPS spoofing attempts and attacks on GPS receivers. This section will discuss some of the techniques that are proposed to protect GPS receivers from spoofing attack.

3.1 Multi-test Detection and Protection Algorithm against Spoofing Attacks on GNSS Receivers (Aleksandar Jovanovic and Cyril Botteron)

This paper describes in detail, the basics of GPS Spoofing, types of GPS Spoofing and also presented different prevention schemes to defend against spoofing attacks on GPS. To evaluate the performance of proposed countermeasure scheme, an attack was performed on GNSS receiver through GSS8000 full constellation simulator attached with rooftop antenna [5]. The countermeasure method presented in this paper relies on statistical properties of GPS Signal, signal power level, Doppler frequency offset and carrier to noise ratio. The method monitors the above mentioned statistical properties and checks for inconsistency to detect the presence of GPS spoofer signal. The test results show that the proposed countermeasure method can successfully detect spoofing signal with low probability of false alarm. The method also offers a protection module in which once a spoofer signal is detected, the GNSS receiver will go to protection mode, where the tracking history is further evaluated to re-establish the lock on correct signal. This method works perfectly against typical or simplistic spoofing attacks and offers little protection to intermediate and more sophisticated spoofing attempts. The implementation of the system is easy and cost effective as it requires changes only on GNSS receiver, not on the whole GPS infrastructure.

3.2 GPS Spoofing Countermeasures (Jon S. Warner, and Roger G. Johnston)

The paper discussed the vulnerability of civilian GPS signal to spoofing attack. It also describes how GPS works and discuss in detail the structure of GPS Signal. It describes several approaches to detect GPS Spoofing attempt, including monitoring GPS signal strength, satellite identification codes, checking time intervals, timing comparison and counter check through use of accelerometer [6]. The paper is a good material for anyone who is interested to learn about GPS Spoofing countermeasure but the countermeasure techniques discussed in this paper were generally discussed rather being specific and narrow. The effectiveness of approaches and strategies to defend against spoofing mentioned in this paper, cannot be measured because no tests were performed to evaluate the performance of each method. Thus effectiveness could not be measured as methods were not implemented and tested. Majority of strategies discussed are based on the monitoring of signal properties.

3.3 An Asymmetric Security Mechanism for Navigation Signals (Markus G. Kuhn)

The paper describes a new and different approach for prevention against GPS spoofing attacks. The technique discussed in this paper is based on cross-correlation and short term information hiding [7]. It is proposed that each satellite transmitter will transmit a signal known as hidden mark signal at regular interval of time with power level lower than the receiver noise level. After transmission of each mark signal, a signed data signal is transmitted with power level above the receiver noise level. The hidden mark signal can only be accessed by GPS receivers after receiving signed data signal. This approach is best for replaying GPS spoofing attack, in which the attacker captures original GPS signal and then rebroadcast with equal power level. The crystal oscillators inside GPS receivers can easily measure the delay between data signal and hidden mark signal despite being less accurate as compared to onboard atomic clocks of satellite. The technique can be defeated by relaying attack and is also very less effective if at least four highly directional antennas are used in selective delay attack. An example in this paper states that if the power of hidden mark signal is set to -170dBW then the SNR will be 34dBW due to expected noise power level of -204dBW. The SNR equal to 34dBW will ensure that Noise peaks in resultant cross co-relation output will always be smaller than the hidden marker peak. Even with Omni- directional antenna and noise temperature of 100k leaves -137dBW noise power which is 34dB above the signal energy and therefore will make the broadcasted signal unrecognizable.

3.4 A Cross-Layer Defense Mechanism against GPS Spoofing Attacks on PMUs in Smart Grid (Yawen Fan, Zhenghao Zhang, Matthew Trinkle, Aleksandar D. Dimitrovski, Ju Bin Song, and Husheng Li)

The countermeasure technique described in this method is a proposed solution to protect the Electrical Grid PMU's (Phasor measurement Unit) from possible GPS Spoofing attack. The protection method consists of cross layer protection [8]. The first layer known as physical layer will receive signals from hybrid antenna's which consists of monopole and patch antenna, and then measure AOA (Angle of Arrival) of the signals of all GPS receivers. By considering the fact that the, AOA will be same for all GPS receivers if the signals are being received from GPS satellite as compared to different AOA. In case of reception from spoofer device, the AOA measurement is a good defense against spoofing attack. The second layer also known as upper layer receives input from first layer of protection, and then perform processing using state based estimation technique to detect bad data. The technique is feasible as it only requires additional GPS receiver and antenna for this technique to be implemented but modifications are required if the same techniques needs to be used for protection of GPS receivers outside smart grids. The method discussed in this paper is effective against simple and cooperative attack.

3.5 Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing (J. Magiera and R. Katulski)

In this paper the author has presented a method to protect GPS Receivers from spoofing attempts through uses of spatial processing [9]. The proposed method not only detects a spoofing of GPS receivers but it also reduces the impact of spoofing on the GPS receiver. The method requires reception of signal through multiple antennas and the perform the angle of arrival

detection procedure. Then phase delay measurement is used to distinguish between fake and original GPS signals. The accuracy of the process was also measured by measuring the chances of false alarm and detection of spoofing when multiple signals (4 to 8) were received. The result of accuracy and precision measurement was 99% when carrier to noise ratio is at least 46dbhz. The proposed method can work both as standalone solution and can also be combined with other systems to further improve detection.

3.6 GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals (Mark L. Psiaki, Brady W. O'Hanlon, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys)

In this paper, the author has proposed a cross-layer detection mechanism to detect multiple spoofing attacks against smart grid [10]. In physical layer, we propose the angle-of-arrival based mechanism. By obtaining the distribution of the normal and spoofed standard derivation of the difference of the C/No from different antennas, we calculate the prior probability of spoofing, which is fed to the upper layer for further detection. In the upper layer, we apply the Kalman filter to estimate the state of power system and use the measurement error to calculate the trustworthiness value of being spoof. Finally, we combine the information from both physical layer and upper layer to integrate the cross-layer mechanism. Numerical results have demonstrated that the cross-layer detection scheme can efficiently detect the spoofing attack.

4. Analysis

Criteria	Definition	Possible Values
Quick Implementation	Ability to apply the technique quickly and as soon as possible	Yes / No
Cost effective	Cost should be low and affordable to apply the technique either in small scale or large number of production	Yes/ No
Prevent Simplistic Attack	Ability to detect simplistic attack	Yes/ No
Prevent Intermediate Attack	Ability to detect intermediate type of attack	Yes/ No
Prevent Sophisticated Attack	Ability to detect sophisticated and advanced types of attacks	Yes/ No
Requires Changes to satellite transmitters	Requires changes to satellite transmitters for implementation of technique	Yes/ No
Requires changes to receiver side	Requires changes to receiver for implementation of technique	Yes/ No
Validation	How easy to test	Yes/ No
Interoperability	Machine Independence	Yes/ No
Requires External Hardware	Does the technique require	Yes/ No

Table 1. Effectiveness Criteria

Table 1 describes all the criteria that we have set to evaluate each technique and find the most effective GPS spoofing countermeasure technique. Table 2 briefly presents an analysis of each technique with respect to criteria set in Table 1. Ten papers were studied to understand the proposed techniques of GPS spoofing countermeasure. There are five techniques which are completely different in terms of detection and implementation. In Table 2 we can easily see that almost all techniques provide the ability to defend against simplistic spoofing attack [5] [7] [8] [9] [10]. Similarly, only two techniques can offer protection against sophisticated type of attack [7] [10]. But this doesn't mean that, these two techniques are the most effective techniques. Because for most effective spoofing countermeasure solution, other criteria listed in Table 1 also need

to be satisfied. From implementation point of view, Table 2 clearly shows that, techniques listed on serial no 2 and 5, require a lot of time. They are not considered cost effective and interoperable as one of them require changes to all satellite transmitters which is very expensive and time consuming process. As we can observe that there is no technique which can provide a complete solution that meet all the criteria for effective GPS spoofing. Also the effectiveness of techniques does not only depend on the technique itself but also depends on the requirement and constraints defined by user. This implies that a technique that meets all the criteria defined in table 1 is an ideal technique and they don't exist in reality. Further the analysis of techniques in Table 2 also show that it is possible to combine two or more techniques to provide most effective GPS spoofing countermeasure solution according to user defined specifications and requirements.

S.No	Technique	Quick Implementation	Cost effective	Prevent Simplistic Attack	Prevent Intermediate Attack	Prevent Sophisticated Attack	Changes to satellite transmitters	changes to receiver side	Validation	Interoperability	Requires External Hardware
1	Multi-test Detection and Protection Algorithm against Spoofing Attacks on GNSS Receivers	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	No
2	An Asymmetric Security Mechanism for Navigation Signals	No	No	Yes	Yes	Yes	Yes	Yes	No	No	No
3	A Cross-Layer Defense Mechanism against GPS Spoofing Attacks on PMUs in Smart Grid	Yes	Yes	Yes	Yes	No	No	No	Yes	No	Yes
4	Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing	No	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes
5	GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals	No	No	Yes	Yes	Yes	No	No	Yes	No	Yes

Table 2. Analysis of spoofing techniques w.r.t to effectiveness criteria

5. Conclusion

In this paper, different set of parameter and criteria were defined which are necessary for a GPS spoofing countermeasure technique to meet in order to perform optimal. After this, each technique is further studied and analyzed with respect to the criteria set. As a result of our analytical study and comparison between the techniques, we observed that, there is no technique which can meet all the criteria. Which means that a system that meets all the criteria is an ideal technique. Further we also observed that, effective technique also depends on the requirement of user that deploys GPS spoofing countermeasure. This is because we have learnt that any technique to protect against GPS spoofing will be the trade-off between certain parameters and criteria defined in this document. Moreover, two or more techniques can be combined to provide a desired technique. With this survey paper we have provided the students and researchers a glance on what has been already been done in this particular field and what are things that still need to be done.

References

[1] GPS.gov. what is GPS, www.gps.gov/systems/gps/

[2] Humphreys, Todd E., Ledvina, Brent M., Psiaki, Mark L., Hanlon, Brady W. O'., Kintner, Paul M (2008). Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer, *In:* 2008 ION Conference Savana, GA, September 16-19.

[3] Tippenhauer, Nils., Ole Pöpper, Christina., ÇCapkun, Srdjan (2011). On the Requirements for Successful GPS Spoofing Attacks, *In*: 18th ACM conference on Computer and communications security, Chicago, IL, USA — October 17 - 21, 2011

[4] Warner J., Johnston R. A simple demonstration that the System (GPS) is vulnerable to spoofing, *The Journal of Security Administration*

[5] Jovanovic, Aleksandar., Botteron, Cyril. (2014). Multi-test Detection and Protection Algorithm Against Spoofing Attacks on GNSS Receivers, *In*: 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014, Monterey, CA, 5-8 May

[6] Warner, Jon S., Johnston, Roger G. GPS Spoofing Countermeasures, *The Journal of Security Administration*

[7] Kuhn, Markus G.. (2015). An Asymmetric Security Mechanism for Navigation Signals, *In*: 6th Information Hiding Workshop, Toronto, Canada, 23-25 May

[8] Fan, Yawen., Zhang, Zhenghao.,Trinkle, Matthew., Dimitrovski, Aleksandar D., Song, Ju Bin., Li, Husheng (2015). A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids, *IEEE Transactions on Smart Grid* 6 (6).

[9] Magiera, J., Katulski, R. (2015). Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing, *Journal of Applied Research and Technology*, 13, p. 45-47, Feb

[10] Psiaki, Mark L., Hanlon, Brady W. O' ., Bhatti, Jahshan, A., Shepard, Daniel P., Humphreys, Todd E. GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals, *IEEE Transactions on Aerospace and Electronic Systems*, 49 (4) 2250-2267.