Modeling and Characterization of GPS Spoofing

Jonathan A. Larcom and Hong Liu*
Department of Electrical and Computer Engineering
University of Massachusetts Dartmouth
Dartmouth, MA, USA
{JLarcom, *HLiu*@UMassD.edu}
**Corresponding Author*

Abstract—**The Global Positioning System (GPS) grows into a ubiquitous utility that provides positioning, navigation, and timing (PNT) services. As an essential element of the global information infrastructure, cyber security of GPS faces serious challenges. Some mission-critical systems even rely on GPS as a security measure. However, civilian GPS itself has no protection against malicious acts such as spoofing. GPS spoofing breaches authentication by forging satellite signals to mislead users with wrong location/timing data that threatens homeland security. In order to make civilian GPS secure and resilient for diverse applications, we must understand the nature of attacks. This paper proposes a novel attack modeling of GPS spoofing with event-driven simulation package. Simulation supplements usual experiments to limit incidental harms and to comprehend a surreptitious scenario. We also provide taxonomy of GPS spoofing through characterization. The work accelerates the development of defense technology against GPS-based attacks.**

Keywords-Cyber security; attack modeling and characterization; Global Positioning System (GPS); GPS spoofing; authentication; secure and resilient GPS-based systems; federal networks; wireless security.

I. Introduction

The Global Positioning System (GPS) is a federally operated service that provides global positioning, navigation, and timing (PNT) to its users free of charge. GPS contains three main parts that all work in conjunction to produce the PNT results. The first segment is in space and consists of a constellation of satellites that operate in six separate orbits around the earth. These satellites transmit signals to GPS receivers with each satellite's position and time. The second is the control segment composed of the monitoring/control stations on the ground that maintain the satellites in space. Finally, the third segment is the user, i.e., a GPS receiver that picks up the satellites' signals and computes its 3D position and time. Each GPS satellite broadcasts two classes of signals, one encrypted for military and the other for civilian. GPS becomes an essential element of global information infrastructure and finds endless applications in every sector worldwide from precision agriculture to disaster relief [1].

Although GPS has been regarded as a security measure for some mission-critical applications such as collision avoidance in surface transportation, GPS was not intended for safety [2]. Like the Internet, society's ever-growing reliance on GPS has attracted the attention of malicious parties to tamper with the unprotected civilian signals that everyday users depend on. *GPS spoofing* breaches security by fooling GPS receivers with false information about location and timing; these cyber attacks are simple and inexpensive [3]. The nation is recognizing detrimental GPS threats to our homeland security [4]. Current defense technology for civilian GPS is in its infancy since traditional wireless security schemes are impractical in most GPS applications [5]. A systematic analysis of GPS spoofing attacks has become the pressing need to make GPS-based systems resilient for national security.

This paper models and characterizes GPS spoofing attacks from a system's perspective. The attack model explores various scenarios to analyze every vulnerable aspect of civilian GPS. We are the first to introduce event-driven simulation of GPS attacks. Current approaches of modeling GPS attacks use GPS satellite signal simulators to experiment under controlled circumstances. Besides the legal/regulation issues and the incidental harm of society, these hardware-based approaches are incomprehensible to devise effective attacks due to their constraints of practical implementation and lack of systematic view. Through extensive literature search, the work classifies both existing and upcoming GPS spoofing attacks by the characterizations unique to GPS-based systems. The outcome of the research would accelerate the development of defense technology against GPS spoofing attacks.

The remaining paper is organized as follows. Section II defines the GPS spoofing attacks by briefing GPS and applications/systems. The GPS spoofing attacks documented are covered in Section III. The characterization and our modeling of GPS spoofing attacks are presented in Section IV and V, respectively. Section VI concludes our work and points to our future research direction.

Our major contributions have two folds. First, GPS security is examined systematically, resulting in taxonomy of GPS spoofing attacks by their characteristics. Second, a new branch of attack modeling is introduced to rehearse GPS attack scenarios with event-driven simulation and devise an effective attack before launching.

This research is sponsored in part by Massachusetts Transportation Information Consortium and by Scholarly Research Efforts 2012/2013 Fund jointly by UMass Dartmouth Provost Office and Graduate Studies Office.

978-1-4799-1535-4/13/$31.00 ©2013 IEEE

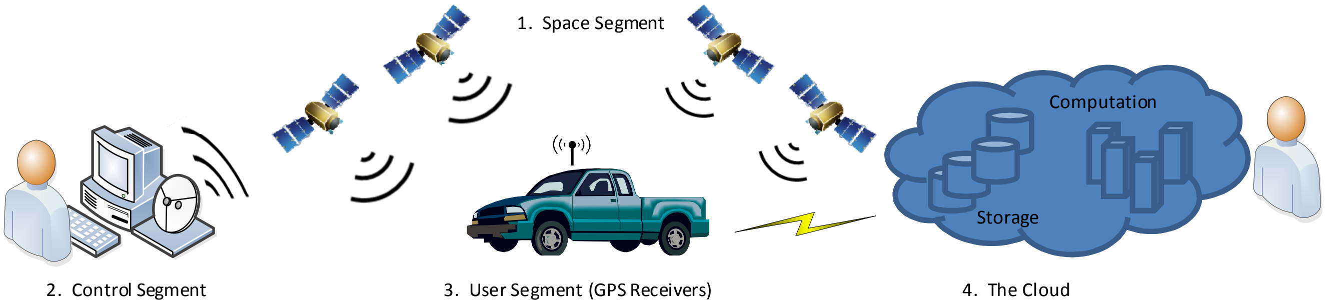


Figure 1. General Architecture of GPS-based System

II. GPS Spoofing Attacks

A. How GPS Works

Out of the three GPS segments mentioned in the previous section, this research focuses on the user segment, i.e. GPS receivers, where GPS spoofing is targeted. We consider the GPS Standard Positioning Service (SPS) broadcasting at the GPS L1 frequency (1575.2 MHz), one of the four GPS civilian signals [1]. GPS constellation satellites transmit L1 civilian signal that carries the satellite's unique identification, namely coarse/acquisition (C/A Code at 1.023 MHz repeating every 1ms), and the information about the satellite's position as well as timing from the atomic clock aboard (Nav/System Data at 50 Hz) [6]. Upon the reception of a satellite's ID code, a GPS receiver generates an internal copy of the code and compares its copy with that of the satellite to determine the clock offset δ and then infer the pseudo-range R without requiring a precise local clock:

$$R = d + \Delta \quad \text{and} \quad \Delta = c\delta$$

where d is the range and c is the speed of light.

With four unknowns, 3D-position and timing, but because of data noise, at least four satellites must be in the line of sight:

$$(x - x^S)^2 + (y - y^S)^2 + (z - z^S)^2 = (R - \Delta)^2 \qquad (1)$$

where (x, y, z) is the GPS receiver's position, (x^S, y^S, z^S) is each satellite's position. Solving the set of four equations (1), the GPS receiver can determine its own 3D-position (x, y, z) and its own clock error $\delta = \Delta/c$, together called a 3D-fix [7].

B. General Architecture of GPS-based Systems

The free, open, and dependable nature of GPS encourages the development of numerous applications/systems, affecting every aspect of modern life. Nearly every electronic device, from phones to automobiles, deploys GPS technology. For example, global positioning to track cargo convoys in real time, navigation in daily travel, and time synchronization for power grids and financial markets [1].

Generally, a GPS-based system contains four modules, as shown in Figure 1 above. In addition to the three GPS segments mentioned in Section I, the cloud serves as a good candidate of the fourth module as the backend servers of computation and/or storage. Take GPS tracking system for instance. A GPS receiver equipped on a truck locks with a set of at least four satellites in its current view and calculates geometrically its 3D-position on the globe and the time from the signals received. The microprocessor in the receiver relays, via wireless communication such as cellular towers and then the Internet, the information about the truck to a server backed by the cloud. The information is stored and processed by a monitor center to track the truck in real time.

C. Definition of GPS Spoofing

GPS spoofing is a cyber attack that fools GPS receivers with false locations and times differing from their actual physical locations and exact times. Spoofing is a much more surreptitious attack than other offenses such as blocking or jamming. Blocking prevents the satellite signal from reaching GPS receivers; a simple way is to rip off the antenna. Jamming interferes GPS receivers' functioning by disturbing the satellite signal. The 2001 Volpe report alarms [8], “A 1-Watt GPS-Like signal can prevent C/A code acquisition to more than 620 miles,” and “These jammers can be built by people with basic technical competence from readily available commercial components and publicly available information.” The ease of launching GPS jamming is due to the strength of GPS satellite signal being weakened to about 1×10^{-16} Watts when reaching the Earth, equivalent to seeing a 25-Watt light bulb in Japan from Los Angles [6]. Though destructive, users can notice both blocking and jamming attacks instantly by service interruption and then take remedial actions. Spoofing, however, when deployed strategically, leads damages without victims' awareness.

Literature has currently reached a consensus that GPS spoofing does not attack the receiver itself but aims at supplying bogus input to cause the receiver to report wrong information [3]. GPS spoofing involves two steps: taking over the legitimate GPS satellite signal and then transmitting the spoofing signal [7]. This research examines various facets of GPS spoofing beyond usual signal analysis methods at the physical layer of communication network protocol stack.

III. Related Work

Warner and Johnston [6] first reportedly demonstrate a spoofing attack on standard GPS receivers. Having a truck mounted with a WelNavigate GS720 satellite simulator following another truck with two handheld civilian GPS receivers onboard one DeLoreme Earthmate and one Magellan Meridian, they successfully attack the receivers. After breaking the existing receiver signal synchronizations with the legitimate satellites, they lock the receivers onto the simulator's counterfeit signals, and broadcast the fake GPS signals continuously from the attack truck. The locks are maintained when the trucks are either stationary or moving as long as they do not exceed 30 feet apart. Warner and Johnston [5] then propose seven anti-spoofing strategies that can be retrofitted onto existing GPS receivers. The strategies include monitoring GPS signal strength, tracking satellite identification codes, and checking time/location precision. These strategies can be applied to design effective attack models.

Early spoofers were built on satellite simulators that were designed for testing GPS receivers. They were costly and not suitable for long-range spoofing, as demonstrated by Warner and Johnston above. Humphreys et al [9] pioneered a C/A code spoofer that receives live GPS signals and then replays to victim GPS receivers with a delay adjusting pseudo-range measurements causing the receiver to output an incorrect navigation solution. To make attacks stealthy, the spoofer signal starts with a perfect replicate of the real broadcast signal and gradually introduces errors. Though it is hard to detect, this style of attacks takes time to achieve the target location.

Tippenhauer et al [7] generalize the process of successful GPS spoofing attacks in two steps: first to take over the legitimate GPS signal already locked onto by the receiver and second to send the receiver to lock onto the forged GPS signal. The first step deals with the practical issue of getting the receiver to switch from the legitimate GPS signal to the attacker's spoofed signal without being detected. In their controlled experiments, a Spirent GSS7700 GPS simulator generates two independent GPS constellations, one for the legitimate GPS satellites and the other for the attacker's signals, and sends them via a wire to a GPS receiver (an Antaris evaluation kit with ATR0600 GPS chip). They have discovered the requirements for seamless satellite-lock takeover of signal power; at least 2dB for consistent locks not detectable by power-based spoofing countermeasures, and time/location precision, the maximum offsets of 75ns and 500m within chip phase misalignment range is unnoticeable by location-error anti-spoofing methods. The second step deploys a sophisticated attacker model, effectively frustrating signal analysis for countermeasures. Attacker strategically positions a set of wireless transmitters to either send signals with modified locations or capture/replay existing signals. They have proven the ease of spoofing one location/victim and the difficulty of spoofing multiple locations (group of victims preserving their relative distances/times). Specifically, the attacker is restrained to a single set of spoofing locations when the group grows to five victims or more. Their insight leads to a new branch of GPS spoofing countermeasures, deploying multiple standard GPS receivers for plausibility/consistency checks.

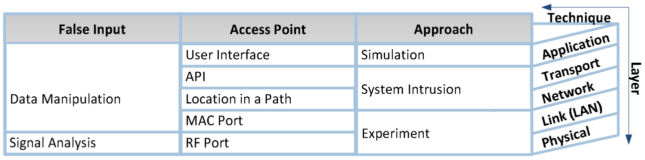
Catching the public attention, a research team from Carnegie Mello University and a private navigation company presented, at an international conference last year (2013) [3], a $2,500 GPS attack platform that could take 45 seconds to bring down a third of a global reference network such as CORS (Continually Operating Reference Station [10]). The platform, named GPS phase-coherent signal synthesizer (PCSS), receives live GPS signals and transmits altered signals in code phase sync with the real GPS satellites to launch GPS spoofing attacks stealthily. PCSS is similar to Humphreys' method [9], however instead of targeting GPS C/A code, PCSS exploits the GPS navigation message and is more effective at manipulating a variety of GPS data level attacks [3]. PCSS offers an API (Application Programming Interface) to generate good, bad, and malicious GPS data as well as to record and playback data with filtering for repeated experiments. They are among the first, besides the authors of this paper, to systematically investigate the attack surface for GPS and alarm the public to more dangerous GPS software attacks [11].

Independently, another team at the University of Texas Radionavigation Laboratory also created a code-phase coherent spoofer [12]. Recently, the researchers at the University of Illinois demonstrated the feasibility of spoofing GPS receiver clock offset to damage the nation's power grid. By controlling variables such as pseudo-ranges, they illustrated the effects on health-monitoring algorithms with forged timing to cause false alarms and misdetections [13].

As U.S. critical infrastructure sectors grow more dependent on GPS for positioning, navigation, and timing (PNT) services, the government renews scrutiny on GPS spoofing threat. The first comprehensive assessment of the vulnerability in the transportation infrastructure to civilian GPS disruptions was by the U.S. Department of Transportation, known as the 2001 Volpe report [8]. In recent years, the U.S. Department of Homeland Security (DHS) charged the Infrastructure Threat and Risk Analysis Center (HITRAC) to conduct a comprehensive risk assessment on using civilian GPS with experts from academia, finance, power, telecommunications, etc. DHS/HITRAC released the National Risk Estimate (NRE), on November 29, 2012, with two reports: one on *Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions* and the other on *Mitigating GPS Disruptions* [4].

IV. Taxonomy of GPS Spoofing

Our literature search, summarized in the previous section, discovers various ways to launch GPS spoofing attacks with numerous outcomes. Our rich research experience in cyber security, such as wireless body area networks and vehicular ad-hoc networks, enables us to foresee sophisticated GPS spoofing attacks. We devise a taxonomy of GPS spoofing attacks with two axes shown in Figure 2 below, one by the network protocol stack and the other by technical approaches.



False Input	Access Point	Approach	Layer
Data Manipulation	User Interface	Simulation	Application
	API	System Intrusion	Transport
	Location in a Path		Network
	MAC Port	Experiment	Link (LAN)
Signal Analysis	RF Port		Physical

Technique
Layer

Figure 2. Attack Surface of GPS Spoofing

A. *Protocol Stack*

Engineers organize communication network protocols in layers. We adopt the Internet protocol stack of five layers: Physical, Link including local area network (LAN), Network, Transport, and Application Layer. The other well-recognized protocol stack, proposed by the International Organization for Standardization (ISO) in late 1970s, is the Open System Interconnection (OSI) model of seven layers. Physical Layer encompasses protocols for various transmission medium, Link Layer protocols move data between two adjacent nodes that is why LAN is considered as a link, Network Layer performs two functions of routing and forwarding data from the source to the destination device, Transport Layer delivers application messages to the application endpoints on the devices, and Application Layer runs application-specific protocols.

Most reported GPS spoofing attacks are targeted at the Physical Layer. Humphreys's portable GPS spoofer adjusts C/A code for spoofing attacks at signal level [9] while Jiang's experiments modify Nav/System message to attack at data level [13].

Nighswander et al demonstrate attacks to the receiver's operating system (OS) or the entire GPS-based system by manipulating data at various layers. They have proven that more sophisticated GPS receivers are more susceptible to attacks because involving the full network protocol stack opens up a wide attack surface [3].

B. *Technical Aspect*

To launch a GPS spoofing attack successfully without being detected, one needs to consider many technical aspects. We characterize spoofers into three technical classes: False Input, Access Point, and Approach. Two ways to generate false input to GPS receivers are signal analysis and data manipulation. False input can be injected to GPS receivers or GPS-based systems at the access points aligning with the five layers: RF Port at Physical Layer via a receiver's antenna, MAC Port at Link Layer since most GPS receivers are equipped with USB port to update maps, Locations of both the victim(s) and the attacker along the path at Network Layer, Application Programming Interface (API) at Transport Layer, and user interface at Application Layer. White Hat hackers test GPS system security via three approaches of experiment with actual GPS devices, system intrusion to exploit software vulnerability in GPS receivers and GPS-based systems, and simulation of attack scenarios using computer package.

The related work briefed in Section III fit in this taxonomy. Warner-Johnson's demonstration on spoofing truck tracking would be placed at Physical Layer using Signal Analysis to RF Port with Experiment [6], as would Humphreys's portable spoofer [9] and Tippenhauer's study [7]. Tippenhauer et al explored the impact of the attacker's location to single or multiple victims [7]. PCSS by Nighswander et al [3] and the similar work by Wesson et al [12] also target at Physical Layer but uses Data Manipulation instead. In addition, Nighswander et al conducted System Intrusion to MAC Port using Data Manipulation at various layers [3]. Jiang et al demonstrated a spoofing attack at the Physical Layer using Data Manipulation to RF Port through Simulation, studying its impact on Application Layer to a GPS-based system for power grid [13].

This taxonomy allows us to predict future GPS spoofing attacks as GPS receivers evolve into more complicated cyber-physical systems. Our recommendation is to comply with the security principle of "KISS" (Keeping It Simple Stupid): Make GPS receivers tamper-proof with a single access point and simplify its functionality by offloading non-core PNT services to the fourth module of a GPS-based system.

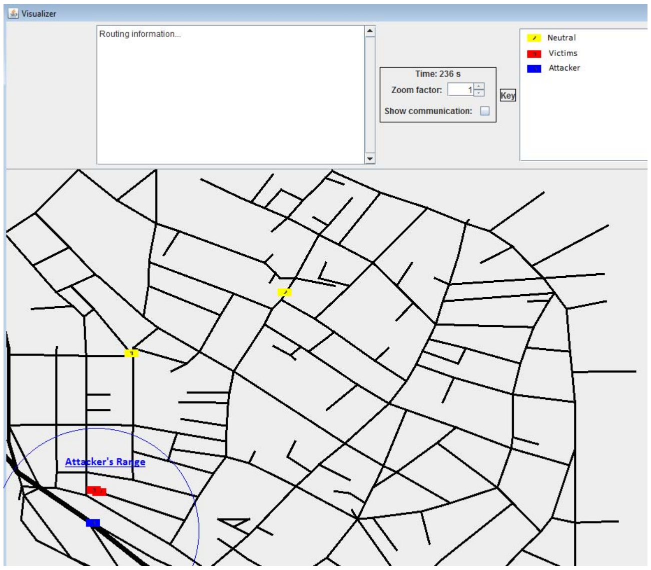
V. MODELING OF GPS SPOOFING

This section presents our simulation package that models GPS spoofing and interprets our simulation results. By trading off strength and performance [14], one can devise an effective attack scenario with the model. In addition, emerging technology in security, such as quantum cryptography [15], can be tested in an economic way.

A. *JiST/SWANS/GPS*

Our simulation is implemented in Java on top of an open source package called JiST/SWANS (Java in Simulation Time/Scalable Wireless Ad-Hoc Network Simulator) [16]. It can be downloaded from jist.ece.cornell.edu. We add modules to JiST/SWANS for realistic vehicular mobility and customized GPS-based system behaviors, renaming the new package JiST/SWANS/GPS.

A visual interpretation of our simulation is shown in Figure 3 below. We simulate a scenario involving one attacker and multiple cars. The attacker drives around a designated area, searching for a target to spoof. The attacker is represented in blue. Cars, in yellow, drive on the streets randomly, unaware of the attacker. Once the attacker acquires a target, it alters its own path to follow the selected victim now turned in red from yellow.



Routing information...

Time: 236 s
Zoom factor: 1
Show communication: □

Figure 3. JiST/SWANS/GPS simulation

Figure 4, on the next page, illustrates the attacker model. The attacker closes distance to be within the minimum required range of his radio broadcast. Checking periodically until the range requirement is met, the attacker approaches. If the target is already locked onto a GPS signal, the attacker must break that lock before broadcasting its false signal. This is typically done by producing a jamming signal to break the lock to the legitimate satellite. Once the lock is broken, provided the attacker maintains range requirements and they have not been detected by jamming, the attacker starts to broadcast their spoofed signal. The slightly higher frequency of the spoofed signal draws the victim to connect to it as opposed to the legitimate satellite constellation. Once the signal is locked, the attacker continues to broadcast the spoofed signal until either being detected, moving out of range, or manually ending the transmission.

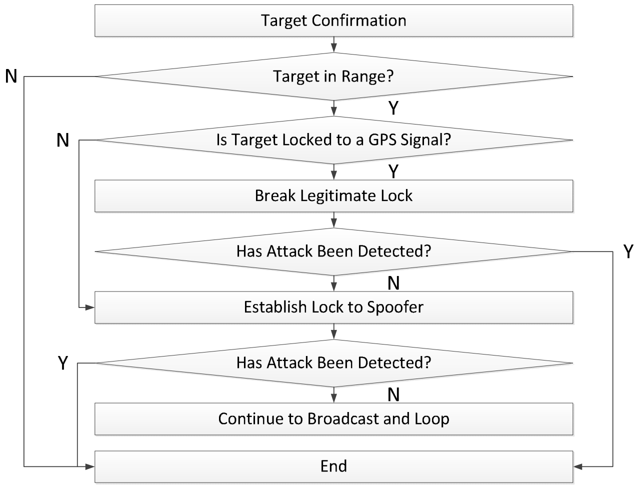

Target Confirmation
Target in Range?
N
Y
Is Target Locked to a GPS Signal?
N
Y
Break Legitimate Lock
Has Attack Been Detected?
Y
N
Establish Lock to Spoofer
Has Attack Been Detected?
Y
N
Continue to Broadcast and Loop
End

Figure 4. Attacker Model

Figure 5 below depicts the GPS receiver model, equipped on all cars except the attacker. The GPS receiver is on standby until activated by the vehicular operator. Once activated, the receiver begins searching for a GPS signal to connect to. Search will continue until a lock is obtained. Once locked, the receiver displays the obtained GPS timing and positioning data. Some receivers will be incorporated with an anti-intrusion system marked gray in Figure 5. In this case, once a signal is locked and data is being received, it will enter the intrusion detection sequence. If there is no intrusion detected, then the legitimate data is displayed. If an intrusion is detected, the anti-attack countermeasures will be applied before any data can be displayed to the user.

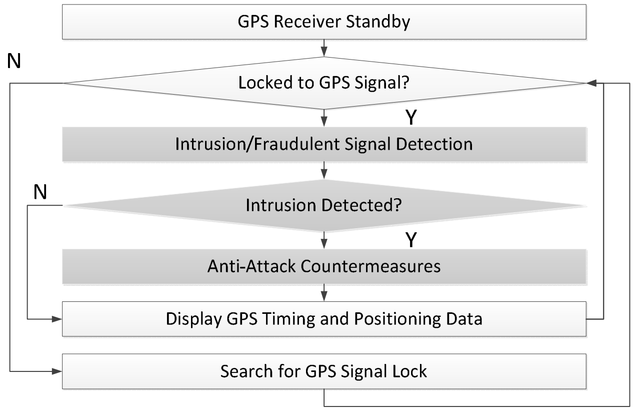

GPS Receiver Standby
N
Locked to GPS Signal?
Y
Intrusion/Fraudulent Signal Detection
N
Intrusion Detected?
Y
Anti-Attack Countermeasures
Display GPS Timing and Positioning Data
Search for GPS Signal Lock

Figure 5. Receiver Model

B. *Simulation and Resuts Interpretation*

Running our simulation, we obtain several key results. Information on distance to the victim is calculated on the fly and used as an input for our main function. The values for the time to break a lock, time to get the receiver to lock to your signal, and the required minimum range are all additionally input parameters whose initial values are entered into the program prior to execution. During run time, the program calculates several preliminary outputs to use as inputs for our primary function to determine if the attacker is successful or not. If the victim is already locked, the time left to break lock is calculated by taking the difference between time to break lock and the time elapsed since the attacker is in range. A similar operation is done to determine the spoofer lock. The probability of detection is also determined as an output but additionally used as the final input parameter to our overall success function. This probability depends on several factors including the distance between attacker and target as well as the duration of time they have been in range and the duration of time they have been broadcasting spoofed signals to the victim. Finally with all these values calculated, we can determine an overall success rate. The data from one simulation run is displayed below in several graphs. Here, the time to break lock, time to lock to spoofer, and minimum distance are all initialized to 10 sec, 30 sec, and 100 feet respectively.

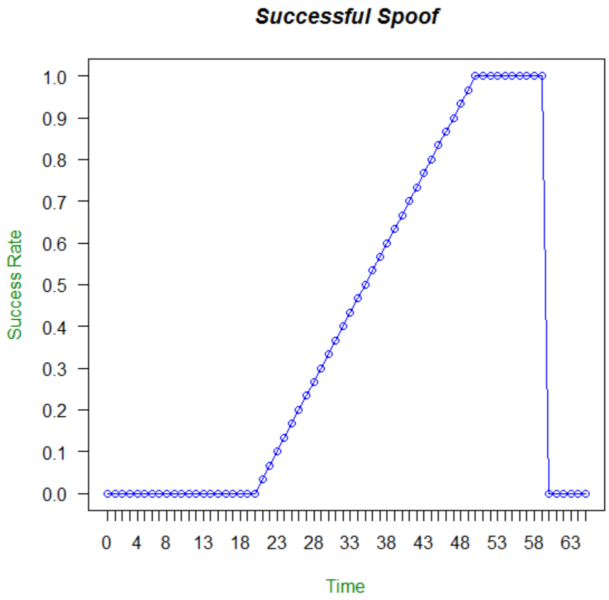


Figure 6. Successful Spoofing Scenario

Figure 6 above graphs the successful rate in a spoof cycle. At time 0, the target is not in range of the attacker. They are in range at the time tick 13, but the victim is locked to a legitimate signal, so there can't be a successful lock. Once the lock is broken, then the attack begins. You can see the success rate increase for 30 ticks until it reaches 1, signifying the attack is successful. The success is maintained until the attacker is detected, fallen out of range, or quitted the mission, resulting in the success rate dropped to 0.

Figure 7 summarizes the simulation results. The x-axis is Time, showing the entire duration of the simulation. Success represents the success rate of the spoofing attack in Figure 6 previously. Distance represents the distance between the attacker and its victim over the duration of the simulation. Initially, the distance is long, 155 ft, because the attacker is searching for a victim. Once a target is selected, the attacker closes distance until in range for broadcast. While in range, the attacker maintains the following distance, about 90 ft just within the range requirement of 100 ft, while broadcasting. Once significant data is obtained, the attacker moves off until out of range or ending the mission. This is shown with the increase in range back up to 115 ft near the end of the simulation duration. The last element shown is probability. This is the probability of being detected. In this scenario, the attack is never detected because the attacker moved out of range prior to detection, therefore, its value is never greater than or equal to 1.

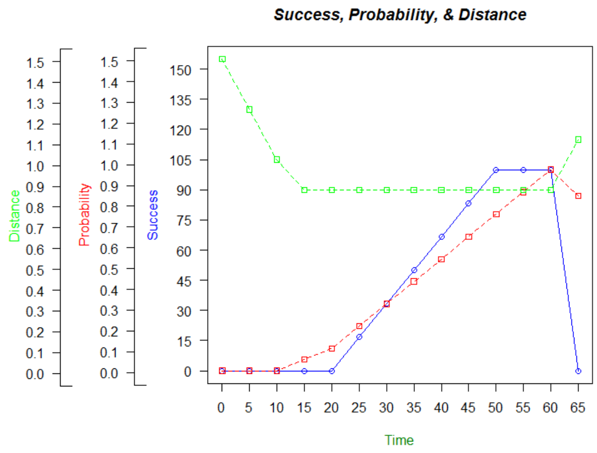


Figure 7. Simulation Results

VI. Conclusion

This paper is the first to model GPS spoofing attacks with event-driven simulation, called JiST/SWANS/GPS. Most “White Hat” hackers test GPS spoofing attacks with experiments using approved equipment under controlled circumstances. Our simulation approach supplements experiments to limit incidental harms and to comprehend surreptitious attacking scenarios. Our taxonomy of GPS spoofing attacks, considering the characteristics unique to GPS, not only exploits features of existing attacks but also foresees future attacks to design effective defense technology. These two results contribute a great deal to the cyber security field.

Our future work includes validating the simulation results with controlled experiments. We will also refine our taxonomy and examine various attack models with our JiST/SWANS/GPS.

References

[1] GPS.gov, "What is GPS?," National Coordination Office for Space-Based Positioning, Navigation, and Timing, 17 January 2013. [Online]. Available: www.gps.gov/systems/gps/.

[2] GPS.gov, "Interface Specification IS-GPS-200G," Global Positioning Systems Directorate Systems Engineering and Integration, 31 January 2013. [Online]. Available: www.gps.gov/technical/icwg.

[3] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley and D. Brumley, "GPS Software Attacks," in *Proceedings of the 2012 ACM conference on Computer and communications security (CCS'12)*, Raleigh, North Carolina, October 16-18, 2012.

[4] B. D. Wales, "National Risk Estimate: Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions," US DHS / Homeland Infrastructure Threat and Risk Analysis Center, November 29, 2012.

[5] J. S. Warner and R. G. Johnston, "GPS Spoofing Countermeasures," *Homeland Security Journal,* 2003.

[6] J. S. Warner and R. G. Johnston, "A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing," *The Journal of Security Administration,* 2002.

[7] N. O. Tippenhauer, C. Popper, K. B. Rasmussen and S. Capkun, "On the Requirements for Successful GPS Spoofing Attacks," in *Computer and Communications Security*, New York, 2011.

[8] J. Carroll, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," US DOT / Volpe National Transportation Systems Center, October 5, 2001.

[9] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O. Hanlon and P. M. Kintner, "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," in *Institute of Navigation GNSS (ION GNSS 2008)*, Savanna, GA, September 16-19, 2008.

[10] CORS, "Continuously Operating Reference Station (CORS)," NOAA, 03 January 2013. [Online]. Available: http://geodesy.noaa.gov/CORS/.

[11] J. A. Larcom and H. Liu, "GPS Vulnerability Analysis in Surface Transportation," UMass Dartmouth 19th Annual Sigma Xi Research Exhibit, Dartmouth, MA, 2013.

[12] K. Wesson, D. Shepard and T. Humphreys, "Straight talk on anti-spoofing," *GPS World,* pp. 32-63, January 2012.

[13] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela and A. D. Domınguez-Garcıa, "Spoofing GPS receiver clock offset of phasor measurement unit," *IEEE Transactions on Power,* vol. PP, no. 99, pp. 1-10, 06 February 2013.

[14] J. M. Adcock, D. M. Balenson, D. W. Carman, M. Heyman and A. T. Sherman, "Trading off strength and performance in network authentication: experience with the ACSA project," in *DARPA Information Survivability Conference and Exposition - DISCEX*, Hilton Head, South Carolina, 2000.

[15] M. Sharbaf, "Quantum Cryptography: An emerging technology in network security," in *IEEE Conference on Technologies for Homeland Security -HST*, Waltham, Ma, 2011.

[16] M. J. North, T. R. Howe, N. T. Collier and J. R. VOS, "A Declarative Model Assembly Infrastructure for Verification and Validation," in *Advancing Social Simulation: The First World Congress*, S. Takahashi, D. L. Sallach and J. Rouchier, Eds., Heidelberg, FRG, Springer, 2007, pp. 129-140.