Int. J. Nonlinear Anal. Appl. In Press, 1–13
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2026.34060.5081

Evaluation of GPS Signal Vulnerabilities against Time Synchronization Attacks

Z. Bagheri[1], N. Orouji[1], M. R. Mosavi[1,*]

Department of Electrical Engineering, Iran University of Science and Technology, Narmak, Tehran 16846-13114, Iran

(Communicated by Haydar Akca)

Abstract

A spoofing attack is an intervention aimed at forcing the GPS receiver to obtain and track invalid navigation data. Time Synchronization Attack (TSA) is a type of spoofing attack that changes the receiver clock information, such as clock offset and drift. The purpose of TSA is to create an error in the estimated time of the receiver. These attacks usually target static receivers that use GPS signals for their time-synchronization applications. One of the main countermeasures for any security vulnerabilities is comprehending the process of thread generation and weak points of the system. In this research, for the first time, theephemeride TSA generation process is discussed and explained in detail. The proposed method demonstrates the feasibility of a spoof attack on the GPS receiver. The attack is defined as an optimization problem that aims to maximize the receiver clock offset error while maintaining the receiver position. The decision variables in the optimization problem are the coordinates of the receiver and the satellite's ephemerides variables. The constraints are such that the decision variables and satellite positions calculated from solving the optimization problem are close to pre-attack values to avoid possible detection schemes that examine large mutations in the values of these variables. Due to the ability to solve complex problems, simple concepts, and easy implementation of Metaheuristic Optimization Algorithms (MOA), Chimp Optimization Algorithm (ChoA), Grey Wolf Optimization (GWO) and Particle Swarm Optimization (PSO) algorithms are exploited. According to the achieved solutions, the maximum modification in the receiver clock offset is 1.6 ms, which is a severe attack based on IEEE $C37.118$ standard. This result is achieved despite a change of 10 meters in the coordinates of the receiver position.

Keywords: Spoofing attack, Time synchronization attack, Optimization problem, Attack generation
2020 MSC: Primary xxxxx (mandatory); Secondary xxxxx, xxxxx (optionally)

1 Introduction

Global Navigation Satellite System (GNSS) signals are subject to various problems that cause significant positioning errors. GNSS-based networks are vulnerable to intentional or unintentional interferences. In some cases, they may not be able to determine the exact position and time, or they may not be accurate. Amongst various attacks threatening the GNSS system security, GPS spoofing is the most malicious and difficult to detect. Spoofing attack is one of the

*Corresponding author
Email addresses: zahra_bagheri@elec.iust.ac.ir (Z. Bagheri), niloofar_orouji@elec.iust.ac.ir (N. Orouji), M_Mosavi@iust.ac.ir (M. R. Mosavi)

Received: May 2024 *Accepted:* July 2026

most destructive threats to GNSS receivers, which causes problems in the system calculations. This issue leads to government and research organizations working on vulnerabilities in radio navigation systems to provide appropriate compensatory measures against system-level interference threats, such as providing security specifications on signals and at the receiver level and signal processing methods.

A Time Synchronization Attack (TSA) targets a static receiver that uses GPS to synchronize its time [1]. In practical terms, the TSA changes the clock offset estimation by misleading a GPS receiver into tracking counterfeit GPS signals. In general cases, there are two types of TSA attacks. In the first type, the spoofer changes a valid signal so that the clock offset changes abruptly. In the second type, the spoofer modifies the valid signal in such a way that the clock offset gradually changes over time. The main difference between the two types of attacks is the attack generation rate which depends on the spoofer's abilities. Type I and II attacks can be the result of a data-level spoofing attack, signal level attack, recording and replay attack, or a combination of these attacks. Defense schemes have been designed to detect, reduce and mitigate these attacks to protect the signal against these attacks.

Due to the increasing importance of security in telecommunication and electronic systems, various methods of signal protection are proposed and investigated. For example, the use of artificial intelligence methods has expanded greatly. One of the best artificial methods is to use neural network as a learning machine and modern computing method in complex systems. The first countermeasures applied to mitigate malicious attacks on GPS receivers are Receiver Autonomous Integrity Monitoring (RAIM). RAIM consistency checks are performed to identify measurement errors. For example, the residual variance of the GPS solution is checked and an error is detected if it exceeds a predetermined threshold. But they are vulnerable to smarter attacks that bypass these checks.

Researchers in [2, 3] propose criteria for anomaly detection, which include changes in amplitude, arrival time, polarity changes, arrival angle, and signal strength. Spoofing attack can be detected by checking the domain and arrival time changes through software implementation. Multiple antennas are needed to check the polarity changes and the arrival angle, and with the complexity of the attacks, these checks are ineffective. In [4], cryptographic authentication methods have been extensively reviewed. Encryption methods require significant changes to the current GPS signal encryption scheme, which will not happen anytime soon. But there have been many advances in encryption methods, such as Navigation Message Authentication (NMA) and Signal Authentication Sequences (SAS), which allow minimal changes to systems [5, 6, 7].

The promising non-cryptographic anti-fraud method is Vestigial Signal Defense (VSD). VSD is a software-independent defense, meaning it is low-cost and does not increase the size or weight of the receiver. Its effectiveness depends on the attenuation level of the valid GPS signal during a spoofing attack. If the spoofer generates a signal whose phase is in sync with the center of the receiver antenna phase, part of the valid signal remains, and distortion of the correlation function becomes apparent [8].

The proposed algorithm in [9] uses NNs to detect abnormal correlation distortion to detect spoofing. The signal index exceeds the threshold level by exploiting the NN, and the deception attack is detected when the attacker intends to occupy the receiver correlation peak. This method does not require additional hardware and does not increase receiver size or production costs. Also, after training, no valid signal is required. In [10], a CNN-based multi-path detection method is proposed to identify multi-path in the GPS correlation output stage.

The utilization of the Recursive Neural Network (RNN) has been investigated in [11] to detect the abnormal behavior of the Unmanned Aerial Vehicle (UAV). Since the UAV is easily affected by wind and air currents in air communications, it has little direction change. Initially, RNNs are used to train and construct the UAV's natural behavior model. The Direction of Arrival (DOA) estimation algorithm is used to obtain a large number of the current two-dimensional input angles of the UAV, as RNN training data, to ensure the position angle accuracy. An appropriate threshold level is selected during the experiments to measure the Normalized Root Mean Square Error (NRMSE) between the actual position and the position provided by normal behavior models; thus, it can detect the abnormal behavior of the UAV.

The paper is organized as follows. Section 2 explains TSA and discusses the parameters which can be exploited in TSA generation. Section 3 clarifies the TSA generation problem and its specifications in detail. Sections 4 and 5 are dedicated to TSA results evaluations on single samples and multiple ones, respectively. Discussions and conclusions are presented in Section 6.

2 Time Synchronization Attack

The TSA is a type of spoofing attack that targets the receiver clock information such as clock offset and clock drift. In the general case, a TSA causes a time estimation error by adding a spoofed signal to a valid pseudo-range

signal. The spoofing attack can be generally modeled as Eq.s (1) and (2):

$$\rho_s[k] = \rho[k] + s_p[k] \tag{2.1}$$
$$\dot{\rho}_s[k] = \dot{\rho}[k] + s_{\dot{p}}[k] \tag{2.2}$$

where $\rho[k]$ and $\dot{\rho}[k]$ demonstrate the actual pseudo-range and the pseudo-range rate, $s_p[k]$ and $s_p[k]$ show the spoofing attack signal and its derivative, and $\rho_s[k]$ and $\dot{\rho}_s[k]$ are the values of the spoofed pseudo-range and its rate. The spoofer changes the authentic signals gradually and the clock offset over time [12, 13], which can be modeled as Eq.s (3) and (4):

$$s_p[k] = s_p[k-1] + s_p[k]\Delta t \tag{2.3}$$
$$s_{\dot{p}}[k] = s_{\dot{p}}[k-1] + \dot{s}_{\dot{p}}[k]\Delta t \tag{2.4}$$

where $s_p[k]$ and $\dot{s}_p[k]$ are called velocity and acceleration that equivalent with attack distance, respectively.

In [14], the Phasor Measurement Unit (PMU) GPS receiver is subjected to a spoofing attack. By maximizing the receiver clock difference (according to GPS time measured by internal satellite clocks) before and after the attack, an optimization problem is posed and solved. The PMU, which uses this clock offset to calculate the synchronized timestamp for its measurements, is in error, and a corresponding phase error is introduced in the voltage or current phase measurements provided by the PMU. In [1], a robust estimator that counteracts TSA is presented. This powerful estimator is a state estimation algorithm that does not require noise information, initial parameters or other states and coefficients, requires less memory, and has good estimation capabilities against spoofing and TSA attacks. In this method, PVT is estimated through a dynamic model and the attack is described on the same model. The proposed algorithm in [1] considers only a fixed number of N satellites in which these N satellites can change in real-time without affecting the algorithm or robust estimator design. The algorithm can operate in any reasonable initial condition, meaning that the estimate must converge regardless of the choice of initial conditions. This algorithm can be implemented on devices with low memory without requiring intensive computing effort or an internet connection. The proposed algorithm in [1] has no stopping condition; therefore, it can be executed real-time.

A method for rejecting or reducing the effects of TSA on GPS receivers is presented in [15]. The proposed method mitigates the attack impact by estimating the clock offset (bias) and clock drift at the beginning of the attack, and it starts to correct it. The proposed method is summarized to solve a simple quadratic program with only a few variables. Therefore, it can be exploited in real-time. For example, efficient implementations of quadratic programming solutions are readily available in low-level programming languages. Therefore, this method can be simply implemented in GPS receivers and electronic devices and does not require the creation of new libraries.

Authors in [16] provide a way to execute a TSA based on changes in time data in higher-order derivatives. In all TSAs, the spoofer tries to change the clock offset without changing the location and speed of the receiver. Therefore, in type I attacks, the amount of spoofed applied to the pseudo-range of all visible satellites must be the same. In [16], smooth attacks are interpreted as a change in the dynamic behavior of the receiver clock. This change is estimated by examining the higher-order derivatives of the receiver clock. Therefore, TSAs are based on the derivatives domain of the clock offset.

3 Explaining the Problem

The proposed method focuses on designing a TSA by solving an optimization problem. The attack is designed by taking the idea from the proposed method in [14] and changing the ephemerides variables. In this method, the amount of receiver clock offset can be maximized by changing the ephemerides and the receiver location and solving the optimization problem with new optimization algorithms such as Chimp Optimization Algorithm (ChoA) [17], Grey Wolf Optimization (GWO) [18], and Particle Swarm Optimization (PSO) [19]. Changes in receiver position and satellite location are bounded to avoid detection by protection schemes. These boundaries are used in solving the optimization problem.

3.1 Ephemerides

The receiver calculates the satellite's ECEF coordinates at any time through the specifications in the GPS signal. These characteristics are called ephemerides. Ephemerides characteristics are usually uploaded to the satellites once a

day from the GPS control section and then sent to the receiver as part of the navigation data. The rotational motion of the satellite is characterized by Kepler elements. These elements are time-variable. Table 1 presents a complete explanation of the ephemerides relations for calculating the position of the satellite [20].

Table 1: Coordinate system elements

Parameter	**Equation/Value**
WGS 84 value of the earth's gravitational constant for GPS user	$\mu = 3.986005 \times 10^{14}\,\text{meters}^3/\text{sec}^2$
WGS 84 value of the earth's rotation rate	$\dot{\Omega}_e = 7.2921151467 \times 10^{-5}\,\text{rad/sec}$
Semi-major axis	$A = (\sqrt{A})^2$
Computed mean motion (rad/sec)	$n_0 = \sqrt{\frac{\mu}{A^3}}$
Time from ephemeris reference epoch	$t_k = t - t^*_{oe}$
Corrected mean motion	$n = n_0 + \Delta n$
Mean anomaly	$M_k = M_0 + nt_k$
Kepler's equation for eccentric anomaly (may be solved by iteration) (radians)	$M_k = E_k - e\sin E_k$
True anomaly	$v_k = \tan^{-1}\left(\frac{\sin v_k}{\cos v_k}\right)$ $= \tan^{-1}\left(\frac{\sqrt{1-e^2}\sin E_k/(1-e\cos E_k)}{(\cos E_k - e)/(1-e\cos E_k)}\right)$
Eccentric anomaly	$E_k = \cos^{-1}\left(\frac{e+\cos v_k}{1+e\cos v_k}\right)$
Argument of latitude	$\phi_k = v_k + \omega$
Second harmonic perturbations	$\delta u_k = C_{us}\sin 2\phi_k + C_{uc}\cos 2\phi_k$ $\delta r_k = C_{rs}\sin 2\phi_k + C_{rc}\cos 2\phi_k$ $\delta i_k = C_{is}\sin 2\phi_k + C_{ic}\cos 2\phi_k$
Corrected argument of latitude	$u_k = \phi_k + \delta u_k$
Corrected radius	$r_k = A(1 - e\cos E_k) + \delta r_k$
Corrected inclination	$i_k = i_0 + \delta i_k + (\text{IDOT})t_k$
Positions in orbital plane	$x'_k = r_k\cos u_k$ $y'_k = r_k\sin u_k$
Corrected longitude of ascending node	$\Omega_k = \Omega_0 + (\dot{\Omega} - \dot{\Omega}_e)t_k - \dot{\Omega}_e t_{oe}$
Earth-fixed coordinates	$x_k = x'_k\cos\Omega_k - y'_k\cos i_k\sin\Omega_k$ $y_k = x'_k\sin\Omega_k + y'_k\cos i_k\cos\Omega_k$ $z_k = y'_k\sin i_k$

3.2 Positioning

The primary purpose of GPS navigation is to estimate the position, velocity, and time of the receiver at any given time, known as the PVT solution. In this section, the radio navigation method used in GPS is briefly described. The GPS receiver uses satellite range signals which contain satellite parameters such as ephemerides data to estimate the satellite position for determining the user's position. The position of the user (GPS receiver) can be shown in the Earth-Center, Earth Fixed (ECEF) coordinate as $s_u = (x_u, y_u, z_u)$ [21].

Similarly, the position of the nth satellite for $N = 1, 2, \ldots, N$ during each satellite transmission time t_n is displayed as $s_n = (x_n(t_n), y_n(t_n), z_n(t_n))$. In addition, it should be noted that the signal reception time at the receiver is t_r. The actual distance between the user and the satellite can be defined as $d_n = \|s_n - s_u\|_2$, where $\|\cdot\|_2$ represents the 2-norm. The distance can be expressed as the difference between the time of signal transmitting and receiving as $d_n = c(t_r^{GPS} - t_n^{GPS})$ where t_r^{GPS} and t_n^{GPS} are the exact time of sending and receiving, respectively, and c is the speed of light propagation. By introducing the receiver time offset, the receiver clock inaccuracy is modeled as $t_r = t_r^{GPS} + b_u$ and similarly for the satellite transmission time as $t_n = t_n^{GPS} + b_n$ where b_u and b_n show the receiver and satellite clock offset [1]. The presence of this offset makes the measured distance different from the real value. This measured value $\rho_n = c(t_r - t_n)$ is called pseudo-range. The pseudo-range relation can be expressed using the real range d_n:

$$\rho_n = \|s_n - s_u\|_2 + c(b_u - b_n) + \varepsilon_{\rho_n} \tag{3.1}$$

where s_n is the satellite position at the time of transmission, s_u is the receiver position at the time of reception, b_u and b_n are the change in the clock of the receiver and the satellite (in seconds), and ε_{ρ_n} is combined errors due to atmospheric delays and thermal noise, respectively. Pseudo-range, satellite locations, and satellite clock offset are recognized or calculated by the receiver, while s_u and b_u are estimated using the pseudo-range relation.

Similarly, the receiver can measure the Doppler (residual) frequency change above the carrier frequency due to the relative difference between the v_n as satellite speed and the v_u as user speed, which is also expressed in three-dimensional coordinates. This estimated Doppler residue is related to the rate at which the pseudo-range measurement changes over time and is denoted by $\dot{\rho}_n$ (in meters per second). The pseudo-range rate is expressed as Eq. (3.2):

$$\dot{\rho}_n = (v_n - v_u)^{\mathrm{T}} \frac{s_n - s_u}{\|s_n - s_u\|_2} + \dot{b}_u + \varepsilon_{\dot{\rho}_n} \tag{3.2}$$

where v_n is the satellite's speed obtained from the navigation message, v_u is the user's speed, $\dot{b}_u$ is the clock drift, and $\varepsilon_{\dot{\rho}_n}$ is the modeled noise. Similarly to Eq. (3.1), the unknowns to be estimated from Eq. (3.2) are b_u and v_u. For a typical receiver, the goal of PVT is to obtain the user's position, speed, clock offset, and the clock drift. This includes a total of eight unknown variables, usually calculated by Weighted Least Squares (WLS) or dynamically using the Extended Kalman Filter (EKF). The dynamic state equation of an eight-state EKF is equivalent to a stochastic walking model [18]:

$$x_k = \begin{pmatrix} \phi & 0 & 0 & 0 \\ 0 & \phi & 0 & 0 \\ 0 & 0 & \phi & 0 \\ 0 & 0 & 0 & \phi \end{pmatrix} x_{k-1} + w_k \tag{3.3}$$

where $x \equiv [x_u, \dot{x}_u, y_u, \dot{y}_u, z_u, \dot{z}_u, cb_u, c\dot{b}_u]^T$ is the state vector, cb_u and $c\dot{b}_u$ are the clock offset and clock drift of the user, (x_u, y_u, z_u) is the user location in meters, $(\dot{x}_u, \dot{y}_u, \dot{z}_u)$ indicates the user speed in m/s, w_k is process noise, and ϕ is a transition state matrix for the discrete time instant k that belongs to each position-velocity and ϕ is defined as Eq. (3.4) [1, 21]:

$$\phi = \begin{bmatrix} 1 & \Delta t \\ 0 & 1 \end{bmatrix} \tag{3.4}$$

where Δt is discrete time instant for any measurement. The measurements given by the Eq.s (3.1) and (3.2) are used for pseudo-range, the pseudo-range rate, and eight-state EKF, Eq. (3.3) is used for dynamic PVT solving. For a static receiver, the position of the receiver (s_u) is determined, and v_u is assumed zero; therefore, only clock offset and drift should be estimated. The pseudo-range relationships and pseudo-range rate relationships are expressed as:

$$\begin{bmatrix} cb_u[k] \\ c\dot{b}_u[k] \end{bmatrix} = \phi \begin{bmatrix} cb_u[k-1] \\ c\dot{b}_u[k-1] \end{bmatrix} + w[k] \tag{3.5}$$

$$\begin{bmatrix} \rho[k] \\ \dot{\rho}[k] \end{bmatrix} = C \begin{bmatrix} cb_u(k) \\ c\dot{b}_u(k) \end{bmatrix} + c_l[k] + e[k] \tag{3.6}$$

$$C = \begin{bmatrix} 1_{N\times 1} & 0_{N\times 1} \\ 0_{N\times 1} & 1_{N\times 1} \end{bmatrix} \tag{3.7}$$

$$c_l[k] = \begin{bmatrix} \|s_1[k] - s_u[k]\| - cb_1[k] \\ \vdots \\ \|s_N[k] - s_u[k]\| - cb_N[k] \\ (v_1[k] - v_u[k])^{\mathrm{T}} \frac{s_1[k]-s_u[k]}{\|s_1[k]-s_u[k]\|_2} - c\dot{b}_1[k] \\ \vdots \\ (v_N[k] - v_u[k])^{\mathrm{T}} \frac{s_N[k]-s_u[k]}{\|s_N[k]-s_u[k]\|_2} - c\dot{b}_N[k] \end{bmatrix} \tag{3.8}$$

where w and $e[k]$ indicate the measurement noise. The c_l vector is based on the specified parameters of position, speed and clock of the receiver.

3.3 TSA as an Optimization Problem

Spoofing attack is done to maximize the difference of the receiver clock before and after the attack, which is done by solving an optimization problem. To prevent attack detection by spoofing detection schemes, limits are set on the absolute value of the differences between the receiver's true position and the receiver's position calculated with fake GPS signals, true real times and fake fluctuations, real satellite positions and fake satellite positions and real pseudo-ranges and fake pseudo-ranges. For example, the changes in the receiver position before and after the attack should be less than the level of position accuracy provided by the GPS receiver. Furthermore, for the absolute value of the difference between the true satellite positions and the fake satellite positions, the range of variation should be less than the margin of error of the GPS almanac. The components of ephemerides and the receiver position are considered as variables in the optimization problem, so that by changing them we can reach the maximum desired difference.

For four satellites in sight the clock offset t_u is expressed as Eq. (3.9) [14]:

$$t_u = -\frac{1}{4}\sum_{i=1}^{4}(\rho_i - \tau_i(\bar{s}_i, \bar{s}_u)) \tag{3.9}$$

where $\bar{s}_i$ is the position vector of the satellite and $\bar{s}_u$ is the position vector of the receiver. The dependence between the satellite position vector and the receiver position vector is demonstrated. The position of the satellite is also influenced by ephemerides through the relations mentioned in Table 1. In the optimization problem, the receiver clock offset should be maximized as follows:

$$\begin{aligned}
&\underset{\bar{s}_u, \bar{\delta}_i, \rho_i}{\text{maximize}} && (t_u - t_u^*)^2 \\
&\text{subject to} && \rho_i = \tau_i - ct_u \quad i = 1,2,3,4 \\
& && |s_u(l) - s_u^*(l)| \le \varepsilon_{s_u}(l) \quad l = 1,2,3 \\
& && |\delta_i(j) - \delta_i^*(j)| \le \varepsilon_{\delta_i}(j) \quad j = 1,2,3,\ldots,m \\
& && |s_i(k) - s_i^*(k)| \le \varepsilon_{s_i}(k) \quad k = 1,2,3
\end{aligned} \tag{3.10}$$

where $\bar{\delta}_i$ is a vector containing the i^{th} satellite's ephemerides. The difference between the values of the decision variables s_u, δ_i and their pre-attack values (denoted by *) are bounded by ε_{s_u} and ε_{δ_i}, respectively. Also, the change of position of the satellite is limited by ε_{s_i}. If the receiver does not consider sudden changes as a way to detect spoofing attack, then these limits can be reduced to infinitely positive.

In the proposed method for changing the ephemerides, a parameter is selected to change according to the range of changes of the variables. The variable that is changed in this method is displayed with M_0. According to the Table 1, M_0 directly affects the mean anomaly M_k and changes the states of the receiver, including the location and time. By plotting the values of M_0 for a number of received time samples in Fig. 1, we see that the variation range of the variable M_0 is in the range of $[-3, 1.5]$.

The ephemerides variations are bounded to 2% to change the receiver clock offset. Small changes in ephemeris values result in large changes in the receiver location. Therefore, constraints must be imposed to prevent the attack from being detected by receiver location changes. The ephemerides and position of the receiver are considered optimization variables. In the design, the maximum location changes of the receiver are limited to 10 meters in each dimension. MATLAB programming software on a Core i7 computer is used to implement and view the results. Raw satellite data and information are extracted from [1].

4 Evaluation of the Generated TSAs on a Single Sample

As optimization problems become more difficult to solve, Metaheuristic Optimization Algorithms (MOAs) have gained more importance in engineering applications [17]. The simple concepts and structures of these algorithms and non-derivative mechanisms are the main reasons for the popularity of these algorithms so that researchers can learn

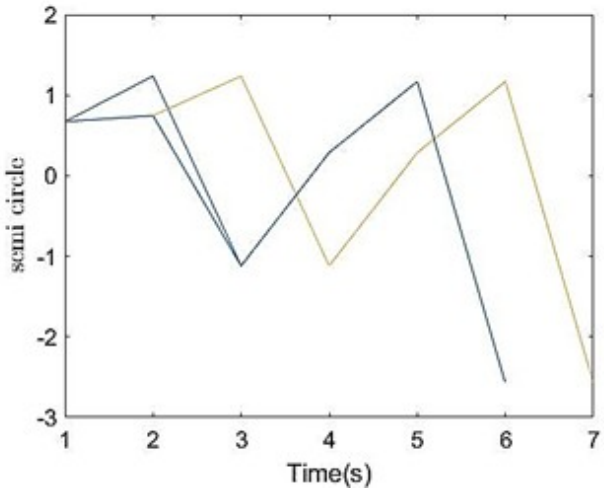

Figure 1: Variation range of M0 ephemerides parameter

them more easily and use them in solving their problems. These algorithms are less trapped in local minima than normal optimization algorithms. Another feature of MOAs is the parallel structure of these algorithms, which makes hardware implementation easier, and parallel computing improves the speed and performance of these algorithms. Using different MOAs, the best solution among the different algorithms is identified in terms of aspects such as execution time and change in receiver location. As mentioned, evolutionary algorithms were selected due to their superior efficiency and accuracy. In addition, the chimpanzee algorithm was proposed in previous research by the authors of the paper and sufficient information is available about its exact performance.

The attack is simulated for available and real signal samples to evaluate the attack proposed in the previous section. The attack is solved as an optimization problem. As explained, in this case, the goal is to maximize the receiver clock offset error by changing the receiver position and the ephemerides values. It means that the objective function in this problem is the receiver clock offset and the decision variables are the receiver position and ephemerides, which leads to a variation in the values of the receiver ephemerides (parameter M_0) and the receiver location.

First, the attack optimization algorithms are compared at a specific time, and then the problem is solved for more samples. The attack is performed at $t = 11$s. At this time, five satellites ($n = 5$) are in sight. For the five in sight satellites, the five components of ephemerides and the three components of the receiver position as decision variables are defined in the optimization problem. In this case, eight unknowns are assumed to solve the problem. Equation (4.1) shows the problem assumption where x represents the unknown vector in solving the optimization problem:

$$x(1:8) = [x(1:5)\ x(6:8)] \rightarrow \begin{cases} x(1:5) = M_0 \\ x(6:8) = [x\ y\ z]_u \end{cases} \tag{4.1}$$

Vector $x(1:5)$ represents the ephemerides variables, and $x(6:8)$ indicates the receiver position. For five satellites in view, we define five ephemerides components and three receiver location component as decision variables in the optimization problem. The objective function of the optimization problem is the same as Eq. (3.10).

4.1 Results of ChOA

The ChOA is proposed by M. Khishe and M.R. Mosavi in [17]. It simulates the group behavior of chimps while hunting as an optimization algorithm. In a chimp colony, there are four types of chimpanzees: barrier, chaser, driver, and attacker. Each group of chimps independently explores the search space with its strategy. This variety will be necessary for a successful hunt. Each chimp can change its tasks during the hunt or maintain the same task throughout the hunt. The hunting process consists of two stages: exploration and exploitation. The use of semi-random chaotic maps avoids local optimization and achieves a faster convergence rate. It also has extensive discovery space because it divides chimpanzees into independent groups and allows them to behave differently.

The ChOA is executed with 30 chimp agents and 100 iterations to search for the best solution. The best achieved time by the chimpanzee optimization algorithm is about 1.6 ms for the receiver clock offset changes at $t = 11$s.

According to IEEE C37.118 standard [22, 23], any clock offset error higher than 26 μs is considered a spoofing attack. Therefore, the generated attack is a severe TSA. Fig. 2 demonstrates the response of the ChOA. The variations of receiver location are acceptable values, which demonstrate the suitable performance of the exploited constraints. Receiver position changes are shown in Fig. 3. The variations are in the range of the GPS receiver accuracy; therefore, the spoofing detection schemes based on the location variations cannot detect them.

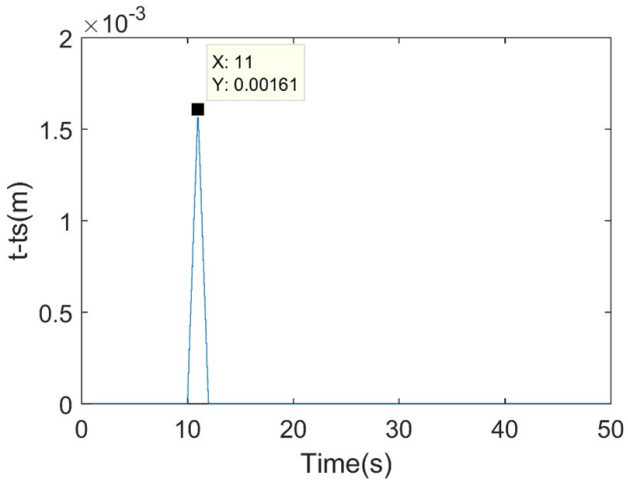

Figure 2: The maximum achieve offset error by ChOA, GWO and PSO (TSA attack at $t = 11$s)

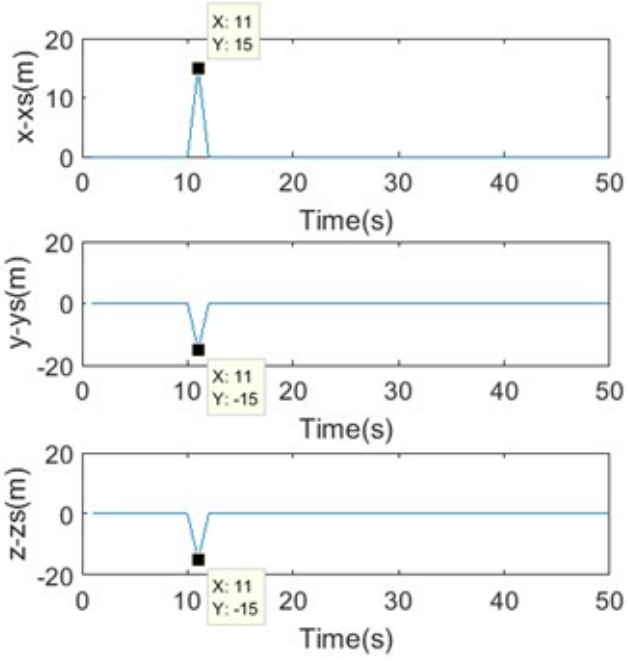

Figure 3: The variations of position under the ChOA-generated TSA

4.2 Results of GWO Algorithm

The Grey Wolf Optimizer (GWO) exploits the characteristics of the hunting process and leadership of wolves. Similar to ChOA, there are four types of agents in this optimizer: alpha, beta, delta, and omega. Furthermore, there are three phases of the hunt: target seeking, surrounding it, and attacking the prey [18]. GWO achieved significant results in challenging and unknown space problems; thus, it is selected to solve the TSA optimization problem. According to Fig. 2 and Fig. 4, the GWO with 100 runs and 30 search agents delivers an answer similar to ChOA. The attack is applied on $t = 11$s, and the receiver position maintains the original one.

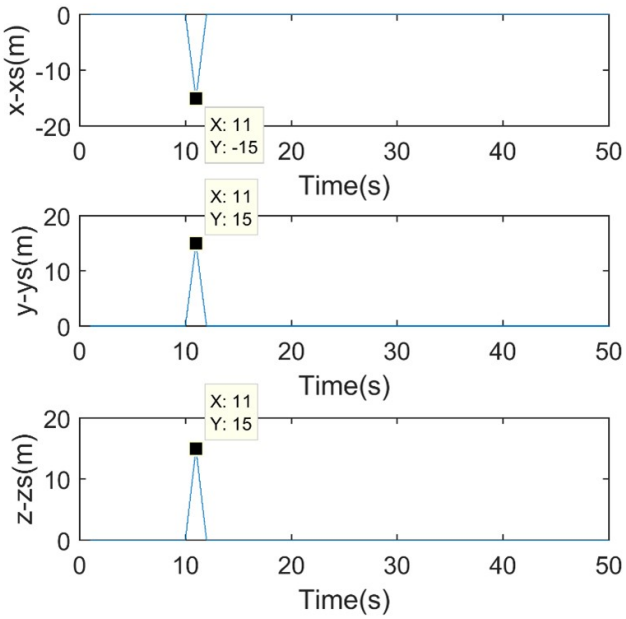

Figure 4: Receiver location changes after attack at time $t = 11$s using GWO

4.3 Results of PSO Algorithm

The PSO is a population-based stochastic search method developed by Eberhart and Kennedy [19]. It has a high convergence rate and is used in various applications easily. Each swarm contains a set of particles that are moving in the search space. Each particle has a position and velocity vector. The algorithm starts with the initial value and motion of the particles in the search space. A random velocity is assigned to each particle, which determines the particle's path in the search space. Each particle follows the path associated with its best solution, which is calculated based on the objective function. The algorithm consists of a population that each particle represents a solution to the optimization problem. At each stage, by setting the path of each particle to its best location and the best particle location in the population, the best global optimum is found. At each point in time, the position of the particles is updated.

The PSO algorithm with 100 iterations performs better than ChOA and GWO. In this algorithm, the execution time of the algorithm is also shorter. Its response is shown in Fig. 2 similar to ChOA and GWO. The receiver position is demonstrated in Fig. 5. It should be noted that the position variations of PSO are less than other algorithms.

4.4 Results Comparison for TSA on a Single Sample

As demonstrated in Table 2, the GWO and PSO algorithms have achieved a relatively better answer. The PSO algorithm has a faster execution time compared to the other two algorithms and also causes less spatial variation in the receiver y dimension. As the number of iterations increases, the execution time of the algorithm increases a lot, but due to the high convergence rate of the algorithms, the results do not change significantly. It is worth noting that the execution speed of the algorithms depends on the software specifications of the systems; these results were implemented from a laptop with specifications of Intel(R) Core(TM) i7-6500U CPU @ 2.50GHz 2.60 GHz and 8GB RAM.

Table 2: Comparison of the results of different optimization algorithms in problem solving

Optimization algorithm	Execution time (second)	Resultant clock offset error in ms
ChOA	840.527388	1.60763
GWO	565.329693	**1.6099**
PSO	**130.837347**	**1.6099**

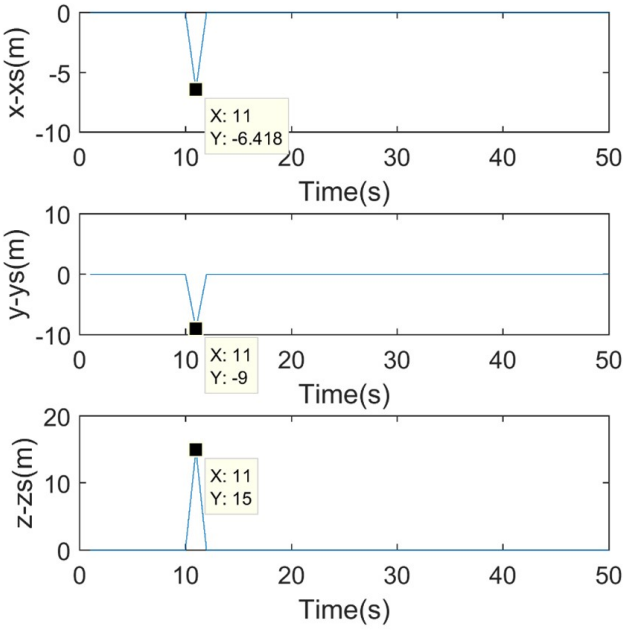

Figure 5: Receiver position variation after TSA generated by PSO

5 Attacking Several Samples

In the previous section, the optimization problem of TSA generation has been solved for one sample. In this section, the optimization problem is solved for more time samples, and the resultant clock offset errors are examined. Attack is performed at times $t = 9$ to $t = 29$ for 20 samples. For these 20 time samples, the PSO optimization problem is solved with 20 iterations to reduce implementation time. Restrictions are set on the variations in the receiver's location and ephemerides values to prevent the attack from detection schemes. Fig. 6 shows variations of the receiver clock offset. Fig. 7 demonstrates the location of the receiver after the TSA using the PSO optimization in different directions to ensure that variations are in the desired range.

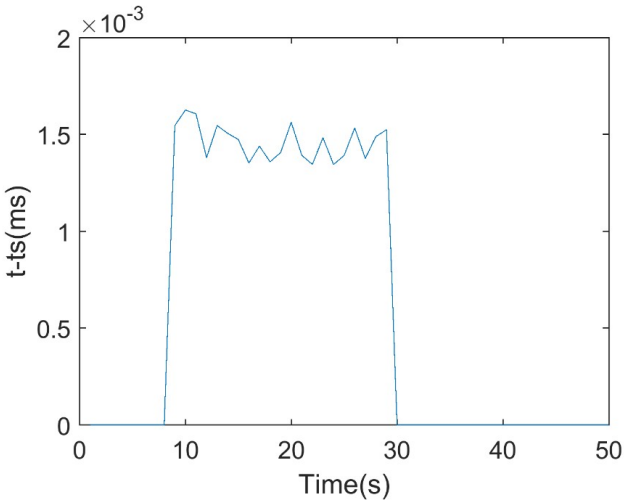

Figure 6: Clock offset variation after applying PSO from $t = 9$ to $t = 29$

According to the considered constraints, the variations in the receiver position is due to the change of the ephemerides, which is bounded to 15 meters. Therefore, if the detection threshold is more than 15 meters, the generated TSA will not be detected.

By reducing the range of receiver position variations, the clock offset can be varied up to 1.6 ms. Fig. 8 demonstrates

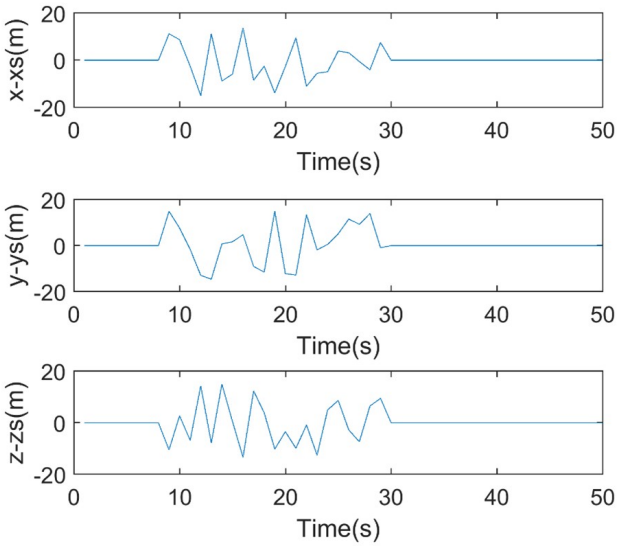

Figure 7: Receiver position variations in multi-sample attack generation

the results of adjusting the receiver location variations to a range of 10 meters. The achieved clock offset error is slightly higher in the previous cases (as shown in Fig. 9).

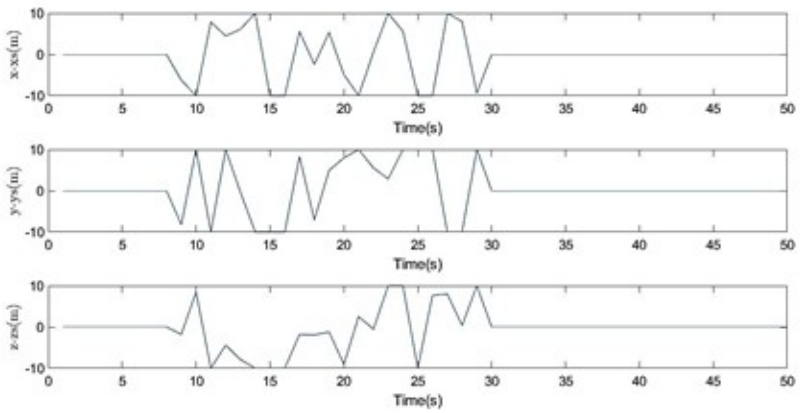

Figure 8: Receiver position variations after TSA with 10m position constraint

5.1 Results Comparison with Other Methods

In the method reported in (Jiang, 2013), it is assumed that the change in each satellite's ephemerides is limited to ±2% of the pre-attack value, and the GPS receiver position variations to 15 meters. Also, no constraints are applied to variations in satellite position. Furthermore, the range of pseudo-range variation is zero. The attack occurs 24 seconds after the simulation. The maximum achieved clock offset error is 2.6 ms. However, the authors did not mention the solving process of the optimization problem. Therefore, the computational cost and execution time is not available.

The proposed attack in (Jiang, 2013) is based on the number of in view satellites and the achieved error for receiver clock offset is 2.1 ms. Also, the changes in the receiver's position according to the set conditions are 15 meters. The decision variables are the ephemerides and pseudo-range and receiver position. However, there is no explanation about how the ephemerides variables are changed or the optimization problem is solved.

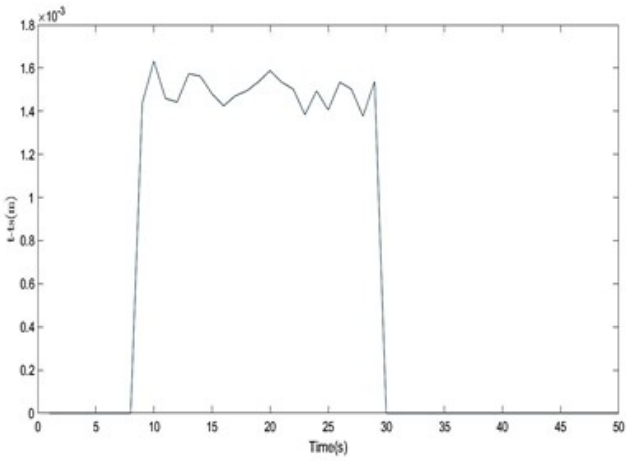

Figure 9: Receiver clock offset errors after TSA with 10m constraint for receiver position

6 Conclusion

In this paper, a time spoofing attack is proposed by changing the ephemerides in the GPS signal. By imposing constraints on the receiver position before and after the attack, the changes in the receiver clock offset are maximized by solving an optimization problem. Big and sudden changes in the decision variables will cause deception detection by the spoofing detection scheme in the receiver, so it is proposed to solve the problem of constrained optimization. MOAs such as PSO, ChOA and GWO are used to solve the optimization problem.

In this study, the process of attack generation is explained in detail for the first time. The clock offset error of about 1.6 ms is achieved by solving an optimization problem. One of the disadvantages of the proposed method is its long implementation time of PSO, ChOA, and GWO. Furthermore, for the number of in sight satellites, several proportional variables must be considered, which complicates the programming and problem-solving. As mentioned in previous sections, these attacks can be easily detected by spoofing detection schemes. In real-time implementation of MOAs, there are challenges such as computation speed, data complexity, and algorithm tuning. To improve real-time performance, parallel processing, distributed computing, and hybrid approaches that combine multiple strategies are often used.

There is numerous researches and studies to mitigate the effects of such TSAs. A Multi-Layer Perceptron Neural Network (MLP NN) that detects TSAs and compensates the clock offset errors is proposed by the authors of this research [24, 25]. Furthermore, a tuning-free, low-memory, and robust-estimator can effectively reduce the effects of the proposed TSA [1]. The most important goal of this research is to clarify the vulnerabilities of the GPS signals to more researchers and encourage them to suggest effective detection and mitigation schemes.

References

[1] J. Lee, A. F. Taha, N. Gatsis, and D. Akopian, "Tuning-free, low memory robust estimator to mitigate gps spoofing attacks," *IEEE Control Systems Letters*, vol. 4, no. 1, pp. 145–150, 2019.

[2] E. L. Key, "Techniques to counter gps spoofing," tech. rep., MITRE Corporation, Bedford, 1995.

[3] J. S. Warner and R. G. Johnston, "Gps spoofing countermeasures," *Homeland Security Journal*, vol. 25, no. 2, pp. 19–27, 2003.

[4] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, pp. 1543–1552, 2003.

[5] O. Pozzobon, L. Canzian, M. Danieletto, and A. D. Chiara, "Anti-spoofing and open gnss signal authentication with signal authentication sequences," in *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pp. 1–6, IEEE, 2010.

[6] O. Pozzobon, C. Wullems, and M. Detratti, "Security considerations in the design of tamper resistant gnss

receivers," in *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pp. 1–5, IEEE, 2010.

[7] O. Pozzobon, "Keeping the spoofs out: Signal authentication services for future gnss," *Inside GNSS*, vol. 6, no. 3, pp. 48–55, 2011.

[8] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil gps anti-spoofing," in *24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, pp. 2646–2656, 2011.

[9] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency gps receivers," *The Journal of Navigation*, vol. 71, no. 1, pp. 169–188, 2018.

[10] C. Bonebrake and L. R. O'Neil, "Attacks on gps time reliability," *IEEE Security & Privacy*, vol. 12, no. 3, pp. 82–84, 2014.

[11] K. Xiao, J. Zhao, Y. He, C. Li, and W. Cheng, "Abnormal behavior detection scheme of uav using recurrent neural networks," *IEEE Access*, vol. 7, pp. 110293–110305, 2019.

[12] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks," in *International Journal of Critical Infrastructure Protection*, vol. 5, pp. 146–153, 2012.

[13] F. Zhu, A. Youssef, and W. Hamouda, "Detection techniques for data-level spoofing in gps-based phasor measurement units," in *2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)*, pp. 1–8, IEEE, 2016.

[14] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domi, "Spoofing gps receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3253–3262, 2013.

[15] A. Khalajmehrabadi, N. Gatsis, D. Akopian, and A. F. Taha, "Real-time rejection and mitigation of time synchronization attacks on the global positioning system," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 8, pp. 6425–6435, 2018.

[16] E. Schmidt, J. Lee, N. Gatsis, and D. Akopian, "Rejection of smooth gps time synchronization attacks via sparse techniques," *IEEE Sensors Journal*, vol. 21, no. 1, pp. 776–789, 2020.

[17] M. Khishe and M. R. Mosavi, "Chimp optimization algorithm," *Expert Systems with Applications*, vol. 149, p. 113338, 2020.

[18] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey wolf optimizer," *Advances in Engineering Software*, vol. 69, pp. 46–61, 2014.

[19] D. Wang, D. Tan, and L. Liu, "Particle swarm optimization algorithm: An overview," *Soft Computing*, vol. 22, pp. 387–408, 2018.

[20] O. N. G. J. Program, "Interface specification is-gps-200, revision d, navstar gps space segment/navigation user interfaces," tech. rep., 2004.

[21] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver: a Single-Frequency Approach*. Springer Science & Business Media, 2007.

[22] K. E. Martin, "Synchrophasor standards development-ieee c37.118 & iec 61850," in *44th Hawaii International Conference on System Sciences*, pp. 1–8, IEEE, 2011.

[23] IEEE Standard C37.118.1-2011, "Ieee standard for synchrophasor measurements for power systems," tech. rep., 2011.

[24] N. Orouji and M. R. Mosavi, "A multi-layer perceptron neural network to mitigate the interference of time synchronization attacks in stationary gps receivers," *GPS Solutions*, vol. 25, pp. 1–5, 2021.

[25] N. Orouji, M. R. Mosavi, and D. Martín, "A lightweight and real-time hardware architecture for interference detection and mitigation of time synchronization attacks based on mlp neural networks," *IEEE Access*, vol. 9, pp. 142938–142949, 2021.