Stealthy GPS Spoofer Design by Incorporating Processing Time and Clock Offsets

Conference Paper · February 2022

DOI: 10.1109/INDICON52576.2021.9691592

2 authors:

Srihari Pathipati
National Institute of Technology Karnataka
56 PUBLICATIONS **67** CITATIONS
SEE PROFILE

Pardhasaradhi Bethi
National Institute of Technology Karnataka
25 PUBLICATIONS **15** CITATIONS
SEE PROFILE

Stealthy GPS Spoofer Design by Incorporating Processing Time and Clock Offsets

Bethi Pardhasaradhi
Department of ECE
National Institute of Technology Karnataka
Surathkal, India, 575025
bethipardhasaradhi.ec16f02@nitk.edu.in

Pathipati Srihari
Department of ECE
National Institute of Technology Karnataka
Surathkal, India, 575025
srihari@nitk.edu.in

2021 IEEE 18th India Council International Conference (INDICON) | 978-1-6654-4175-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/INDICON52576.2021.9691592

***Abstract*—GPS receivers are ubiquitously present to provide position, navigation, and time (PNT) information for civilian and military applications. These GPS receivers can be misguided by intentional interference like jamming, meaconing, and spoofing. This paper presents efficient spoofer design by incorporating spoofer's processing time (spoofers receiver end to transmitter end processing delay), tracker processing time (delay due to state estimation), the difference in clock offsets (spoofer and target have different clock offsets) into account for generating spoofed measurements. These delays are incorporated in the spoofer's external delay to create a spoof measurement set. A spoofer with a target tracking module was proposed earlier without considering the significance of time delay information. The delay due to the tracker processing time has also been considered in this proposed spoofer design. The simulations are carried out for two test cases: the processing time delay and the difference in clock offset delay. Interactive multiple models (IMM) based dynamic state estimation filter is used to track the target (GPS receiver) of interest owing to its best performance compared with other filters. The proposed spoofer design outperforms the existing spoofer designs in position root mean square error (PRMSE). In addition to that, we also accomplished high performance of spoofing by increasing the number of spoofed satellite signals.**

***Index Terms*—GPS Spoofer, track filters, GPS receivers, IMM filters, transmission delay**

I. Introduction

GPS-based navigation is trendy owing to relatively inexpensive sensors for civilian applications. GPS receiver is an essential component in all navigational systems. The GPS receivers can be misguided easily with electronic countermeasures (ECM) like jamming, meaconing, and Spoofing. The GPS spoofing is relatively easy, as the blueprints to simulate the GPS-based satellite signals are readily available [1].

. Jamming is an ECM technique wherein a radio frequency (RF) waveform is generated at the narrowband or wideband and illuminates these waveforms towards the targeted receiver. Therefore, the receiver is unable to generate the pseudo ranges to estimate its position, navigation, and time information [2]. Jamming denies PNT determination for GPS receivers as long as it is present. However, its presence can be determined by using various ECCM techniques. The second type of intentional interference (ECM) present in GPS receivers is spoofing; it is a clever technique to deceive the GPS receiver by altering and re-transmit the actual satellite-based signals towards the targeted GPS receiver [3]. After that, the victim receiver is in confusion to judge between actual satellite-based signals and spoofed signals. Hence, there is a high likelihood that the spoofer takes over the GPS receiver due to its higher power signals [4]. As a result of these ECM techniques, the farmer denies the position information, whereas the latter deceives the GPS receiver with incorrect positioning. Furthermore, the spoofer either simulates or delays the authentic satellite signals. Spoofing is a significant threat among these two techniques as incorrect positioning is more dangerous than no positional information.

Different spoofer models like simulator-based and other spoofers are presented in the literature. Among them, simulator-based Spoofing is a popular and well-established method. Authors in [5] presented proximity spoofing by locating the spoofer very nearer to the target. Besides this, Sim-gen software-based spoofing attack is suggested in [6], which used optical fiber cable to demonstrate the attack successfully. The above spoofers are very nearer to the target, and there is hardly any need to estimate the target position. Authors in [7] proposed a generalized pseudo-Bayesian 2 (GPB2) filter-based spoofer and illustrated the need for a target tracking module in the spoofing process.

The necessity of the target tracking module in spoofer design is recently demonstrated by the authors in [8] and [9]. In [8], the impact of the target tracking module was illustrated with various multiple model track filters, and the results revealed that IMM based track filter provided improved performance compared with other track filters. Moreover, in [9], the authors assumed that the range between the spoofer and the target is precisely known (this assumption is not valid in practical spoofing scenarios). In these contributions, the spoofer processing time and the tracker processing time are ignored. However, to accurately represent the spoofer design with the target tracking module, these delays must be accounted for while designing the efficient spoofer. Besides this, data transmission delays and data packet loss is added to precisely represent the spoofer design.

The paper is organized as follows: Section II provides the mathematical model for the proposed spoofer design. In Section III, the IMM filter-based tracker is presented.

The results and discussion, and conclusion are presented in Section IV and Section V, respectively.

II. Mathematical Modeling for GPS Spoofing Scenario

This section provides the mathematical formulation for repeater-based spoofer by considering the possible practical aspects. The design includes bias due to mismatched receiver clocks (the clock offset of spoofer and the clock offset of the targeted receiver) and processing delays within the spoofer (spoofer receiver-to-transmission delay, tracking delay)

In GPS positioning, un-intentional interference's (multi-path, ill-conditioned signals) produce up to tens of meters of inaccuracy. Whereas, intensional interference effect can impose tens of meters to thousands of meters of inaccuracy for the GPS receiver. This inaccuracy is due to the locking of spurious signals (spoofed signals or meacon signals) into the receiver. In a clean environment, the GPS receivers use the satellite has transmitted signals $\{S_i(t)\}_{i=1}^{N}$ in the range to estimate its PNT. Here, N represents the number of satellites invisibility. The transmitted satellite signals are clock synchronized. The satellite signal $\psi_i(t)$ consists of satellite location Φ_i, time-stamp, and satellite health. The signal strength of the received GPS signal is meager (in the range of -165dBW) owing to the tropospheric and ionosphere attenuation of the signals. A receiver is located at ϕ^t, estimates its own location with the help of pseudorange measurement set $\{z_i^t\}_{i=1}^{N}$.

In an intentional interference scenario, the GPS position estimator gets a pseudorange set $\left\{z_i^f\right\}_{i=1}^{N}$, the position estimate is ϕ^f. This ϕ^f very much deviates from the ϕ^t. During the attack, though the target is positioned at ϕ^t, the GPS shows ϕ^f. Since, the intentional interference source transmits spoofed signals with larger power, the fake signals are more likely to get locked onto the GPS receiver and unknown to the GPS receiver in the process of internal screening. The intentional interference sources for the GPS receiver are jammers, meaconers, and spoofer. Here, we are considering a repeater-based spoofer. The repeater is a device, which contains both receiver and transmitter modules. Spoofer is a device which transmits GPS like signals either by playing back or altering the received authentic signals with external delays being computed by the spoofer. Let us consider, a spoofer is present at ϕ^s in the surveillance, the geo-location of the spoofer is known. Here s indicates the spoofer, and Φ is the notation to represent for the position. The position of the spoofer in three dimensional Cartesian coordinates is $\phi^s = [x^s, y^s, z^s]$. A GPS receiver is located at ϕ^t; the receiver relies on the received GPS signals to estimate its position. Here, t represents the actual target; the target can be a GPS receiver or a receiver mounted on any moving object. The spoofer creates a fake position of ϕ^f, even though the target physically located at ϕ^t as shown in Fig. 1.

To generate precise fake signals, the spoofer must have knowledge about the state dynamics of the target. Hence, in this scenario, we considered that the target tracker is standalone in the surveillance and observing a target (mounted GPS receiver on a drone or any moving vehicle). The tracker estimates the state dynamics of the target and reports the estimates to the spoofer.

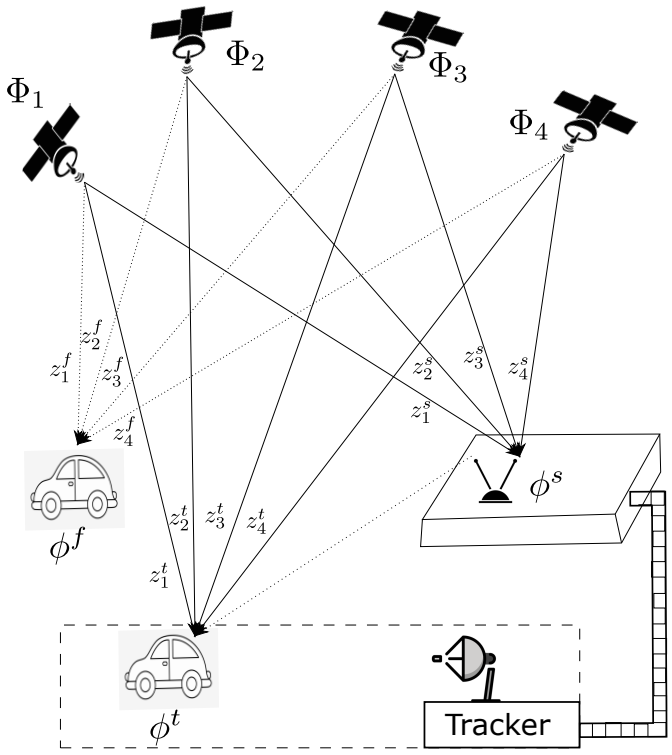

Fig. 1. Tracking the true target using radar, using the tracking information to mislead the target. (dotted lines represent the fake signals, and dark lines represent the authentic signals)

A. Spoofer Mathematical Model

The repeater-based spoofer is considered in this model. Where, the repeater posses a receiver to receives the satellite signals and transmitter to retransmit the signals after processing. The spoofer located at ϕ^s receives all the available authentic satellite signals in the range as

$$\psi\left(\phi^s, t\right) = \sum_{i=1}^{N} A_i \psi_i \left(t - \frac{\mid \Phi_i - \phi^s \mid}{c}\right) + w\left(\phi^s, t\right). \quad (1)$$

Where A_i is the signal attenuation due to transmission from Φ_i to ϕ^s and $w\left(\phi^s, t\right)$ is the background noise. Here, $\mid \Phi - \phi^s \mid$ is the geometrical range between Φ_i to ϕ^s. The global time of the satellites is t', the receiving time of the receiver is t. Hence there is an offset between there due to various clocks. However, the costly clocks like cesium are not feasible for the civilian applications. The relation between the global time, time of the receiver and the offset is

$$t = t' + \Delta_1 \quad (2)$$

by subsisting the global time in the above equation, the modified equation is

$$\psi\left(\phi^s, t'\right) = \sum_{i=1}^{N} A_i \psi_i \left(t - \frac{z_i^s}{c} - \Delta_1\right) + w\left(\phi^s, t'\right). \quad (3)$$

where $z_i^s = \mid \Phi - \phi^s \mid$ is the geometrical range.These received signals are processed in different channels within the spoofer, and additional delays are introduced for the authentic signal, and then re transmits onto the targeted GPS receiver. The re transmitted signals are given by

$$\psi\left(\phi^s, t'\right) = \sum_{i=1}^{N} A_i \psi_i (t - \frac{z_i^s}{c} - \tau_i - \Delta_{Tx-Rx} - \Delta_{Tr} - \Delta_1) + w\left(\phi^s, t'\right). \quad (4)$$

Here τ_i is the external delay added by the spoofer. whereas, Δ_{Tx-Rx} is the additional term appeared due to spoofer processing time from the time of reception of signal to re transmission of signal towards the target. Here Δ_{Tr} is the tracking delay by the range measuring sensor. The distance between the spoofer and target can be calculated with the help of any range measuring sensors like radar, sonar, optical etc. As given in [7], to address the spoofing of a drone, one can use the frequency modulated continuous wave (FMCW) radars which are lost cost and readily available. If the range measuring sensor (FMCW radar) is associated with the spoofer module, we can consider both the radar and spoofer location as same. Usually radars work in local coordinate frames, i.e., assumes that they are located at the origin. With respect to the radar location at origin, reports the detection (range and azimuth). In this case, a simple range measuring sensor is sufficient. However, the measurement obtained by the radar is being corrupted with the Gaussian noise. Hence a tracker is employed to filter the measurement and to obtain the state. However, the trackers usually offers a delay for processing the measurements to obtain the state. Let the tracker offers an additional delay of δ_{tr}, this needs to be incorporated in the spoofer design. Directly the range measurement can be considered by ignoring the tracking delay, which makes $\delta_{tr} = 0$.

B. Target Model

The spoofer's re-transmitted signals gives an extra time delay of $\frac{\rho}{c}$. Therefore, the target receives all the spoofed signals as

$$\psi\left(\phi^t, t\right) = \sum_{i=1}^{N} A_i \psi_i (t - \frac{z_i^s}{c} - \tau_i - \Delta_{Tx-Rx} - \Delta_{Tr} - \Delta_1 - \frac{\rho}{c}) + n\left(\phi^t, t\right). \quad (5)$$

Converting the above equation in global time yeilds

$$\psi\left(\phi^t, t'\right) = \sum_{i=1}^{N} A_i \psi_i \left(t - \frac{z_i^s}{c} - \tau_i - \Delta_{Tx-Rx} - \Delta_{Tr} - \Delta_1 - \frac{\rho}{c} - \Delta_2 + n\left(\phi^t, t'\right). \quad (6)$$

Here Δ_2 is the clock offset arrises due to the spoofer and the targeted GPS receiver clock mismatch. After processing the signal, the time delay measurement is given by

$$\frac{\mid \Phi_i - \phi^s \mid}{c} + \tau_i + \Delta_{Tx-Rx} + \Delta_{Tr} + \Delta_1 + \frac{\rho}{c} + \Delta_2 \quad (7)$$

Here, the above time delay measurement can produce any spoof location ϕ^s. The geometrical range measurement set for the spoof location ϕ^f concerning to satellite locations Φ is $z_i^s = \Phi_i - \phi^f$. Therefore, equating the above equation to the spoof pseudorange gives

$$\frac{z_i^s}{c} = \frac{\mid \Phi_i - \phi^s \mid}{c} + \tau_i + \Delta_{Tx-Rx} + \Delta_{Tr} + \Delta_1 + \frac{\rho}{c} + \Delta_2 \quad (8)$$

On rearranging, we get the additional delay to be offered by the spoofer to the i^{th} satellite signal is

$$\tau_i = \left(\frac{z_i^f}{c} - \frac{z_i^s}{c}\right) - (\Delta_{Tx-Rx} + \Delta_{Tr}) - (\Delta_1 + \Delta_2) + \frac{\rho}{c} \quad (9)$$

where $z_i^f = \mid \Phi_i - \phi^f \mid$ is the geometrical range between the spoof location and the satellites. However, the distance between spoofer and the target determining is imprecise. Here $\phi^s = [x^s, y^s, z^s]'$ is the location of both radar and the spoofer. The distance between spoofer and target $\rho = \mid \phi^s - \phi^t \mid$ is crucial in the design, the precision of the sensor plays a vital role in both detection and the state estimation. Therefore the measurements for the radar is represented as

$$\rho = h(\phi^s, \phi^t) + n \quad (10)$$

where n is the range measurement error, which follows gaussian pdf with zero mean and variance σ^2. The estimated range after the filtering is $\hat{\rho}$. Hence after replacing the range with the filtered range output, we get

$$\tau_i = \left(\frac{z_i^f}{c} - \frac{z_i^s}{c}\right) - (\Delta_{Tx-Rx} + \Delta_{Tr}) - (\Delta_1 + \Delta_2) + \frac{\hat{\rho}}{c} \quad (11)$$

This $\hat{\rho}$ is the estimated output by the spoofer. Substituting the external delay in (5) gives

$$z_i^* = z_i^f + \rho - \hat{\rho} \quad (12)$$

This estimation error $\rho - \hat{\rho}$ in the spoofer is corresponding to the tracker; it is invetible to make perfect system with $\rho - \hat{\rho} = 0$.

III. IMM FILTER

In realtime applications, most of the filters uses the convereted measurements. Therefore, the converted discrete measurements $\mathbf{y}_k$ is

$$\mathbf{y}_k = H(X_k) + w_k. \quad (13)$$

Here $X_k = [\phi_k^t, \dot{\Phi}_k^t]'$ represents the state of the target, H_k is measurement transition matrix, and w_k follows white Gaussian noise with zero mean and R_k covariance. The target dynamics is

$$X_{k+1} = F_k X_k + \Gamma_k u_k. \quad (14)$$

where, F is the state transition matrix (follows constant velocity (CV) or constant turn (CT)). CV refers to straight-line motion and CT refers to curved trajectory. Γ_k and u_k are noise gain and process noise, respectively [10]. In Generalized pseudo bayesian filters, kalman filter (KF) filters increase exponentially and make it more impractical for the multiple models. Interactive multiple model (IMM) is an optimal approach by keeping only m filters for m hypothesis. At $k-1$ time step, there are only m estimates and their associated covariance which approximately summarizes the past $\mathbf{y}^{k-1}$. This is the key feature for the IMM algorithm and results in low complexity and provides excellent state estimates. The main drawback of MM algorithms is its inability to handle mode jumps. But in IMM, mode jumps enable in two ways by re initializing the filter and by introducing the transition probability π_{ji}, which facilitates as a priori information.

1) Model Conditioned Re initialization: The predicted model probability is given by

$$\mu^{(j)}_{\frac{k}{k-1}} = \sum_{j=1}^{2} \pi_{ij} \mu^{(j)}_{k-1} \tag{15}$$

The mixing probabilities are given by

$$\mu^{j|i}_{k-1} = \pi_{ji} \mu^{(j)}_{k-1} / \mu^{(i)}_{\frac{k}{k-1}} \tag{16}$$

The mixing state and covariance is given by

$$\begin{aligned} \hat{X}^{(j)}_{\frac{k-1}{k-1}} &= \sum_{i=1}^{2} \hat{X}^{(i)}_{\frac{k-1}{k-1}} \mu^{(i|j)}_{k-1} \\ P^{(j)}_{\frac{k-1}{k-1}} &= \sum_{i=1}^{2} \left[P^{(i)}_{\frac{k-1}{k-1}} + \tilde{X}_{k-1} \tilde{X}'_{k-1} \right] \mu^{(i|j)}_{k-1}. \end{aligned} \tag{17}$$

where $\tilde{X}_{k-1} = \left(X^{(j)}_{\frac{k-1}{k-1}} - \hat{X}^{(i)}_{\frac{k-1}{k-1}} \right)$

2) Model Conditioned Filtering: In a generalize context m models are possible, m KF blocks are required. The Kalman filter gives $\hat{X}_{\frac{k}{k}}$ and $P_{\frac{k}{k}}$ as the state and covariance estimates by considering all the measurement information up to k. i.e., $\hat{X}_{\frac{k}{k}} = E[X_k \mid \mathbf{y}^k]$ and $P_{\frac{k}{k}} = E\left[(X_k - \hat{X}_{\frac{k}{k}})(X_k - \hat{X}_{\frac{k}{k}})' \mid \mathbf{y}^k \right]$. Where $\mathbf{y}^k = \{\mathbf{y}_0, \mathbf{y}_1, \ldots \mathbf{y}_k\}$. The statistical assumptions for the KF are initial state has known mean and covariance $E\left[X(0) \mid \mathbf{y}^0\right] = \hat{X}_{\frac{0}{0}}$, cov $\left[X(0) \mid \mathbf{y}^0\right] = P_{\frac{0}{0}}$. The process noise and measurement noise are uncorrelated and their respective covariance are known.

3) Model Conditioned Filtering: The state prediction $\hat{X}_{\frac{k}{k-1}}$ and its associated state covariance $P_{\frac{k}{k-1}}$ are given by

$$\begin{aligned} \hat{X}^{(j)}_{\frac{k}{k-1}} &= F^{(j)}_{k-1} \hat{X}^{(j)}_{\frac{k-1}{k-1}} \\ P^{(j)}_{\frac{k}{k-1}} &= F^{(j)}_{k-1} P^{(j)}_{\frac{k-1}{k-1}} \left(F^{(j)}_{k-1} \right)' + Q^{(j)}_{k-1}, \\ \text{where} \quad Q & \text{ is process noise covariance.} \end{aligned} \tag{18}$$

The measurement residual $\tilde{\mathbf{y}}$ and its associated measurement residual covariance S_{k+1} are given by

$$\begin{aligned} \tilde{\mathbf{y}^{(j)}_k} &= \mathbf{y}^{(j)}_k - H^{(j)}_k \hat{X}^{(j)}_{\frac{k}{k-1}} \\ S^{(j)}_k &= H^{(j)}_k P^{(j)}_{\frac{k}{k-1}} \left(H^{(j)}_{k+1} \right)' + R^{(j)}_k. \end{aligned} \tag{19}$$

Here H is a linear matrix since both the state and measurements are in same coordinates. The filter gain G_k is given by

$$G^{(j)}_k = P^{(j)}_{\frac{k}{k-1}} \left(H^{(j)}_k \right)' (S^{(j)}_k)^{-1}. \tag{20}$$

The updated state $\hat{X}_{\frac{k}{k}}$ and updated covariance $P_{\frac{k}{k}}$ are given by

$$\begin{aligned} \hat{X}^{(j)}_{\frac{k}{k}} &= \hat{X}^{(j)}_{\frac{k}{k-1}} + G^{(j)}_k \tilde{\mathbf{y}}^{(j)}_k \\ P^{(j)}_{\frac{k}{k}} &= P^{(j)}_{\frac{k}{k-1}} - G^{(j)}_k S^{(j)}_k (G^{(j)}_k)^{-1}. \end{aligned} \tag{21}$$

4) Model probability update and fused estimate: The likelihood corresponds to i^{th} and j^{th} filter in k instant is given by

$$L^{(ij)}_k = p\left[\mathbf{y}_k \mid m^j_k, \hat{X}^{(i)}_{\frac{k-1}{k-1}}, P^{(i)}_{\frac{k}{k}} \right];\ i, j = 1, \ldots m \tag{22}$$

The merging probability is the probability that mode i was in effect at $k-1$ if mode j is in effect at k is conditioned on $\mathbf{y}^k$ as

$$\mu^{(j)}_k = \frac{L^{ij}_k p^{ij} \mu^i_{k-1}}{\sum_{i=1}^{2} L^{ij}_k p^{ij} \mu^i_{k-1}}. \tag{23}$$

Combining the model probability with the conditioned model estimates yields the updated state $\hat{X}_{\frac{k}{k}}$ and updated covariance $P_{\frac{k}{k}}$ as

$$\begin{aligned} \hat{X}_{\frac{k}{k}} &= \sum_{j=1}^{2} \hat{X}^{(j)}_{\frac{k}{k}} \mu^{(j)}_k \\ P_{\frac{k}{k}} &= \sum_{j=1}^{2} \left[P^{(j)}_{\frac{k}{k}} + \left(\hat{X}_{\frac{k}{k}} - \hat{X}^{(j)}_{\frac{k}{k}} \right) \left(\hat{X}_{\frac{k}{k}} - \hat{X}^{(j)}_{\frac{k}{k}} \right)' \right] \mu^{(j)}_k. \end{aligned} \tag{24}$$

IV. RESULTS AND DISCUSSIONS

A. Simulation Scenario

The true target and imposed false target trajectory are simulated based on the position gate pull-off strategy as given in [11]. The initial position of the target and false target is at $[700, 700, 0]$ and follows the trajectories as given in Table-I. The trajectories are as shown in Fig. 2. The measurements are converted to local coordinate frame (range-azimuth-elevation to x-y-z). The measurement covariance matrix is R=diag$\{25, 25, 0\}$. Since the investigation is carried out to evaluate the IMM filter performance, the data association and scheduling are ignored in the target tracking module.

TABLE I
THE TRAJECTORY PARAMETERS

True target trajectory				Fake target trajectory				Measurement noise		
model	duration	turn rate	velocity	model	duration	turn rate	velocity	x	y	z
CV	1-30s	-	30m/s	CV	0-30s	-	30m/s	5m	5m	0m
CT	31-60s	2^o/s	30m/s	LCT	31-60s	4^o/s	30m/s	5m	5m	0m
CV	61-90s	-	30m/s	CV	61-90s	-	30m/s	5m	5m	0m
CT	91-120s	1^o/s	30m/s	CT	91-120s	2^o/s	30m/s	5m	5m	0m
CV	121-150s	-	30m/s	CV	121-150s	-	30m/s	5m	5m	0m

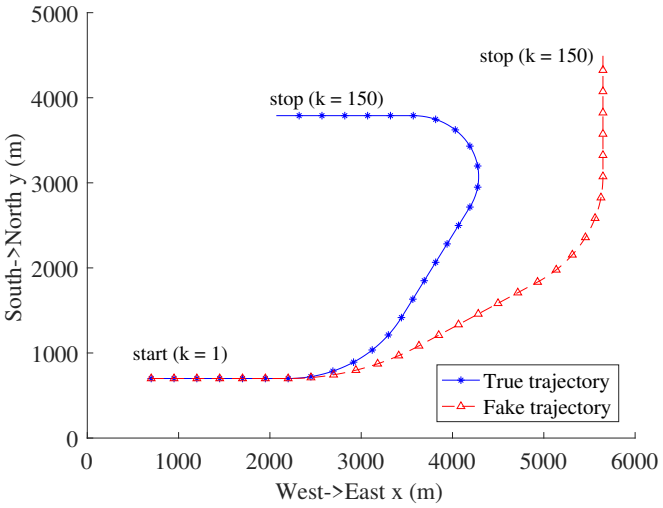

Fig. 2. True and fake target trajectory generation.

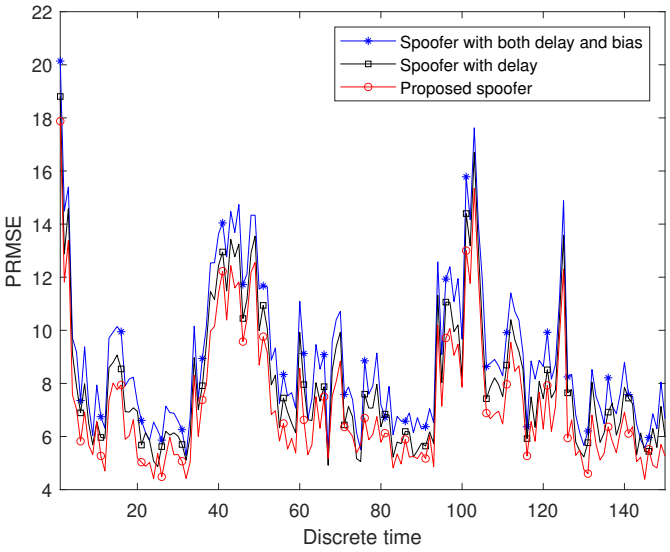

Fig. 3. PRMSE of proposed spoofer design (Number of satellites=4, offset bias=1m and speed delay product=1m).

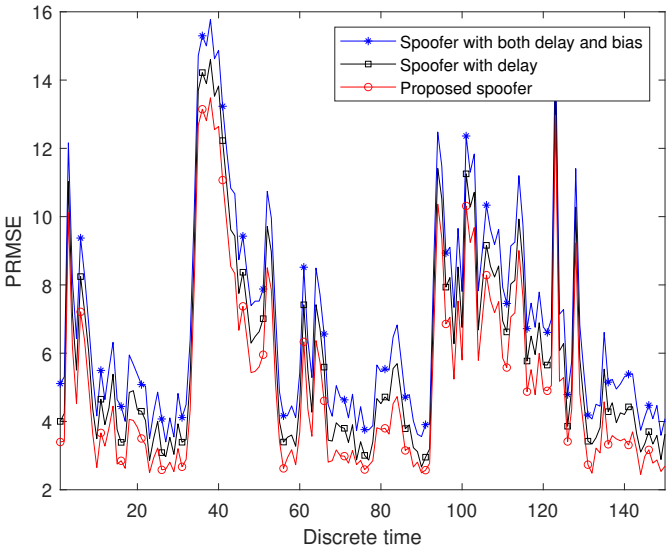

Fig. 4. PRMSE of proposed spoofer design (Number of satellites=6, offset bias=1m and speed delay product=1m).

B. Spoofing accuracy

The spoofing accuracy is computed by taking into account the number of satellites, delay due to the propagation and tracking, clock offset variation between the spoofer and target. Firstly, it is assumed that, the spoofer and the target has some clocks, and no difference in clock offset in this process. Hence, we make $\Delta_1 - \Delta_2 = 0$, and the simulations are performed. In another scenario, we consider both the difference in clock offsets, spoofer processing delay, and the tracker processing delay into consideration.

1) Case-1: High precision devices: In high precision devices, both the clocks are nearly equal and produce very little error. So, the difference in clock offset is taken as 3.33ns. This scenario is generally seen in the high-precision GPS sensors for defense applications. Moreover, the spoofer device can be processed by using the on-board processing unit. Therefore, the processing delays are considered as 3.33ns. The simulation results are depicted in Fig. 3, and 4 for four satellites and six satellites respectively. Here, satellite signal refers to spoofed satellite signals.

We can observe that, for the lower number of satellites, the error is 1m, and with the increased number of satellites, the error decreased.

2) Low precision devices: For low precision devices, we considered the processing time as $10ns$, and the difference of the offset is also $10ns$. In this case, since the other

spoofers devices offer lower precision, we can observe a massive difference in the PRMSE value, which is almost two-fold performance. With the increased number of satellites, we plotted Fig. 5 and Fig. 6 for four and six satellite signals, respectively. By this, one can understand that the more processing time effect and mismatch of offset clock results in huge error. One should consider these effects in the spoofer design.

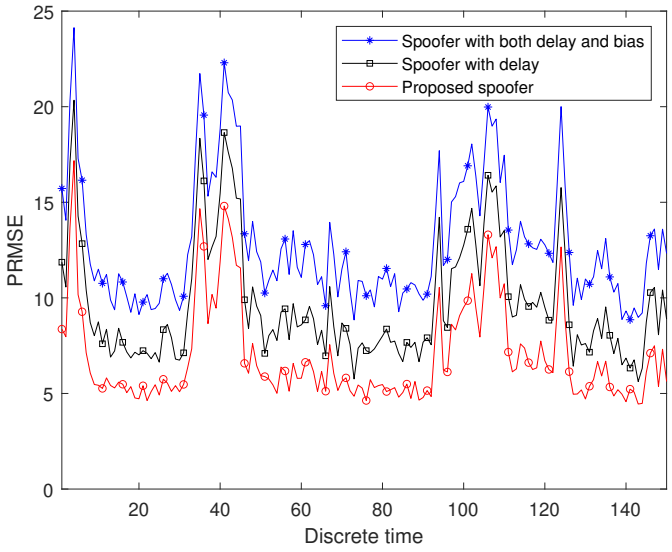

Fig. 5. PRMSE of proposed spoofer design (Number of satellites=4, offset bias=3m, and speed delay product=3m).

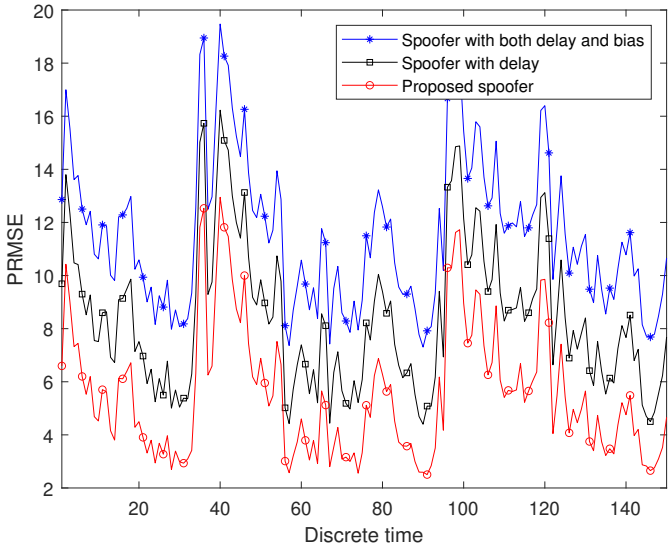

Fig. 6. PRMSE of proposed spoofer design (Number of satellites=6, offset bias=3m, and speed delay product=3m).

V. Conclusion

This paper proposed a novel spoofer design by incorporating spoofer's processing time (spoofers receiver end to transmitter end processing delay), tracker processing time (delay due to state estimation), the difference in clock offsets (spoofer and target have different clock offsets) into account for generating spoofed measurements. The simulations are carried out for three different cases 1. existing spoofer design without considering the processings delays and difference in clock offsets. 2. existing spoofer design without considering the processing delays. 3. The proposed spoofer design by incorporating both processings delays and difference in offset delays. The simulation results demonstrate that the proposed spoofer provides a two-fold improvement compared to the existing spoofer design. Further, the results also reveal that the processing of more spoofed signals results in improved spoofing accuracy. One can carry out the research to implement the proposed spoofer design on the hardware platforms with efficient digital signal processing architectures to achieve high throughput and less latency.

References

[1] H. Wen, P. Y. Huang, J. W. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," 2005.

[2] A. Grant, P. Williams, N. Ward, and S. Basker, "GPS jamming and the impact on maritime navigation," *The Journal of Navigation*, vol. 62, no. 2, pp. 173–187, 2009.

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

[4] T. Kim and C. Sin, "Analysis of the GPS meaconing signal generator for the live gps L1 signal," *Journal of Satellite, Information and Communications*, vol. 11, no. 4, pp. 15–20, 2016.

[5] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011, pp. 75–86.

[6] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *NAVIGATION, Journal of the Institute of Navigation*, vol. 64, no. 1, pp. 51–66, 2017.

[7] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[8] P. Bethi, S. Pathipati, and A. P, "Impact of target tracking module in GPS spoofer design for stealthy GPS spoofing," in *2020 IEEE 17th India Council International Conference (INDICON)*, 2020, pp. 1–6.

[9] B. Pardhasaradhi, P. Srihari, and P. Aparna, "Navigation in GPS spoofed environment using M-best positioning algorithm and data association," *IEEE Access*, pp. 1–1, 2021.

[10] Y. Bar-Shalom, X. R. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation: Theory Algorithms and Software*. John Wiley & Sons, 2004.

[11] P. Bethi, S. Pathipati, and P. Aparna, "Stealthy gps spoofing: Spoofer systems, spoofing techniques and strategies," in *2020 IEEE 17th India Council International Conference (INDICON)*. IEEE, 2020, pp. 1–7.