This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099968, IEEE Access

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Digital Object Identifier

Spoofer-to-Target Association in Multi-Spoofer Multi-Target Scenario for Stealthy GPS Spoofing

BETHI PARDHASARADHI, (Member, IEEE), PATHIPATI SRIHARI, (Senior Member, IEEE), and APARNA. P, (Senior Member, IEEE).
ECE Dept., National Institute of Technology Karnataka, Surathkal, India, 575025
Corresponding author: Pathipati Srihari (e-mail: srihari@nitk.edu.in).

ABSTRACT Global navigation satellite system (GNSS) based navigation is omnipresent in today's world, providing position, velocity, and time (PVT) information with inexpensive GPS receivers. These receivers are highly vulnerable to intentional interference like GPS spoofing and meaconing. The spoofing of a single GPS receiver using a spoofer setup is widespread, and the concept of spoofing multiple targets with multiple distributed spoofers is also equally adaptable. Traditionally, in distributed spoofers, the multiple spoofers in the surveillance region work independently without knowing other spoofers being installed. Multiple spoofers deployment and its management are optimal for misguiding the multiple GPS receivers in the given surveillance. This paper presents a generalized mathematical model for the multi-spoofer multi-target (MSMT) scenario, spoofer management, and spoofer-to-target association. The received power of spoofed signals is considered as an evaluating parameter for locking the spoofed signals onto the GPS receivers. Three novel centralized networking-based spoofing techniques are proposed to overcome spoofer-to-target association in distributed networking. Firstly, the global nearest neighbor (GNN) based centralized spoofing is proposed. The overall cost of the function is minimized by assigning a unique spoofer-ID to a unique target-ID. In GNN-based centralized spoofing, the overall global cost minimizes, but it does not ensure that every target-to-spoofer assignment is minimum. Secondly, the spoofers of opportunity-based centralized spoofing with the GNN association is proposed to resolve the spoofer-to-target association and to increase the hit ratio. However, it is hard to install more spoofers; therefore, a tunable transmitting power-based centralized spoofing with the GNN association is presented to accomplish efficient spoofer-to-target association and higher hit-ratio. The spoofing efficiency is evaluated using spoofer-to-target association, hit ratio, and position root mean square error (PRMSE). All the proposed algorithms outperform the distributed spoofing. We also observe that the tunable power-based spoofing is an optimal solution in MSMT scenario.

INDEX TERMS GPS spoofing, GPS positioning, multi-spoofer multi-target, stealthy spoofing, spoofer-to-target association.

I. INTRODUCTION

Global positioning systems (GPS) receivers are pretty famous for positioning, navigation, and timing (PNT) services due to global acceptance of operation, low-cost sensors, and reasonable accuracy. The GPS services are open to a wide range of applications like transportation, aviation, maritime, surveying [1]. Because of the availability of GPS standards and the blueprints, the signal generation is more accessible and enables the vulnerabilities of jamming, spoofing, and meaconing [2].

Jamming is a process in which a jammer device generates radio frequency (RF) signals to completely deny the positioning information of the GPS receiver [3]. On the other hand, in the spoofing process, the spoofer transmits the fake signals (fake refers to spoofed signals) onto the target (target refers to GPS receiver) with a higher power. These spurious signals remain unnoticed in the screening techniques used within the receiver. Once the target receiver is locked to these fake signals generated by the spoofer, it results in false PVT estimates [4]. Spoofing is the primary concern in GPS receivers compared to jamming since false positioning is highly vulnerable to position estimate's unavailability. For example, a target like a yacht or an airplane relies on GPS-based position information; the spoofer can intentionally control the receiver of the target and mislead to the wrong destination. This unauthorized access and control over the target receiver is a threat to humankind and comes under electronic warfare (EW) [5]. In another critical example, automated stock trades rely on the GPS's estimated time information for precise transaction timing. Here a spoofer is capable of falsifying the timestamps of the stock trades and results in loss of millions of dollars to a firm; unauthorized access of information comes under information warfare (IW) [5].

Different types of spoofers and spoofing strategies are proposed in the literature [6]–[8]. The literature regarding spoofer development and spoofing strategies is minimal due to the following reasons. 1. The professional obligation to development of EW devices that impose a threat to society, 2. Most of the information related to spoofers is classified. Firstly, a simulator-based spoofer is popular and practically demonstrated on unmanned air vehicles (UAV), yacht, trucks, and power grid [4], [9], [10]. The mathematical framework was derived for single-spoofer single-target scenario and practically misled the trajectory of UAV [9]. In simulator-based spoofing, the spurious signals are generated with the historical knowledge of the legitimate GPS signals [2]. Secondly, repeater-based spoofing was proposed in the literature. The spoofer captures authentic signals and re-transmitted them onto the target receiver by altering the delays [7]. Besides, meaconing is one class of the repeater-based technique of misguiding, where repeater intercepts and rebroadcasts the intercepted signals after some time or in another place [11]. The mathematical derivation of repeater-based spoofer system and influence of tracking parameters has also been studied in [12]. Furthermore, the hardware trojan is the third category, in which there is no need for signal reception or transmission required since the signals combine within the receiver hardware. In [10], the spoofing demonstrated with SimGen software by simulating both authentic satellite signals and spoof satellite signals; after that, successfully carried out the spoofing by using an optical fiber connection.

Comprehensive survey of anti-spoofing techniques has been presented in [13]–[16]. Spoofing attack detection is achieved by signal monitoring techniques like software-defined positioning, monitoring the power, checking the clock, code, and phase consistency rate [17]. Regarding the power, the monitoring of autocorrelation distortion is proposed in the literature by assuming that the spoofed signals have higher power than legitimate signals [18], [19]. However, if spoofed signals' average received power equals authentic satellite signals' power level, the autocorrelation distortion-based technique fails to perform. Moreover, cryptographic authentication is one of the efficient anti-spoofing techniques. Nevertheless, the main problem with cryptographic modulation-based authentication is expensive and can be deployed where the cost of the GPS receiver is not the criteria [20], [21]. The above cryptographic and signal monitoring techniques require the receiver's redesign, as these detection algorithms are based upon the internal signal measurements outside the receiver. Besides these methods, there are spatial processing and reference positioning-based anti-spoofing techniques without redesigning the receiver module [22]–[24]. The spatial processing techniques include the direction of arrival discrimination multiple antennas or a single antenna with multiple feeds or oscillatory motions [25]. The drawback of this approach is the dependence on multiple numbers of antennas and antenna motion-induced effects. Here, trusting a reference position includes the availability of inertial navigation system (INS), ranging sensors in platoon construction, visual positioning, and trajectory planning [26]–[28]

In most research works, single-spoofer and single-target scenarios have been considered, and the spoofing process is carried out in open space or via optical cables [6], [10], [29]. However, it is hard to expect a single target with a clean environment to carry out the spoofing process in real-time. In [29], the impact of Omni-directional spoofer on multiple targets and impact of multiple spoofers on a single target is theoretically presented. During multi-spoofer multi-target spoofing, it is not necessarily true that generated spoofed signals are locked onto the targeted receiver due to the following reasons: 1. All the targets get affected by the spoofing by using the Omni-directional antenna. 2. Due to spoofers' nearby deployment, there is highly likely that multiple spoofers target the same receiver. 3. Because of closely spaced targets, multiple targets lock onto the same spoofer. Therefore, there is a strong need to understand the impact of spoofing multiple targets and multiple spoofers in the given surveillance region. Moreover, the above anti-spoofing algorithms [17]–[28] may or may not work in the presence of multiple spoofers. The motivation to work for the stealthy spoofing and considering a multi-spoofer multi-target (MSMT) scenario is to understand the worst-case threat. Therefore, efficient anti-spoofing algorithms can be developed shortly. Hence this paper considered an MSMT scenario and developed a generalized mathematical model for transmitting spoofed signals by the multiple spoofers and reception of spoof signals by the GPS receivers. Spoofers are deployed, and they are working without any communication between them. In this scenario, spoofing may likely results in the wrong spoofer-to-target association. As a result, there is a requirement to develop efficient spoofer-to-target association algorithms for efficient spoofer design. Hence, we formulated the spoofer-to-target association problem as a two-dimensional cost matrix and subjected as every spoofer should handle only one target. The key contributions of this paper are:

- A generalized mathematical model for the MSMT scenario is derived by considering the signal transmission from multiple spoofers and its reception for multiple targets.
- Initially, the impact of distributed spoofing with random assignment is explored. After that, the centralized spoofing-based GNN algorithm is proposed to resolve the spoofer-to-target association.

- However, it is hard to achieve a higher hit ratio in the case of closely spaced spoofers and targets. Therefore, to address this issue of nearby targets, the spoofers of opportunity-based centralized spoofing with the GNN association are proposed to achieve a higher hit ratio by increasing the number of spoofers in the surveillance.
- It is hard to have a large number of spoofers deployed in the environment. Hence an optimal solution is proposed by using tunable transmit power-based spoofers and centralized spoofing with GNN association to accomplish a higher hit ratio with fewer spoofers in given surveillance.
- Moreover, this paper studies the performance of the proposed algorithms by varying the number of spoofed signals and pseudorange measurement noise.

The rest of the paper is organized as follows. In Section II, the generalized mathematical model for MSMT scenario is presented. Further, Section III presents three novel approaches to address the spoofer-to-target association. Finally, the discussion of results for various algorithms and conclusion of the work is incorporated in Section IV and V respectively.

II. MATHEMATICAL MODEL FOR MULTI-SPOOFER MULTI-TARGET SCENARIO

The GPS spoofing problem is formulating for the MSMT scenario. In GPS spoofing, the spoofer (s) transmits mimic GPS signals either by playback of previously captured signals or simulate the GPS signals. Let L number of spoofers are deploying in the surveillance region, all spoofers are static in position, and their locations are precisely known. The spoofers locations set S is

$$S = \{\mathbf{x}_k^s\}_{k=1}^{L} \; ; \; \mathbf{x}_k^s \in \mathbb{R}^3 \tag{1}$$

In the same surveillance region, M targets (GPS receiver) are present. The targets location set T is given by

$$T = \left\{\mathbf{x}_j^r\right\}_{j=1}^{M} \; ; \; \mathbf{x}_j^r \in \mathbb{R}^3 \tag{2}$$

Here, The superscript r represents the real position or the physical position of the GPS receiver. The spoofer k intends to create a fake-position $\mathbf{x}_{k,j}^f$ for the target j which is being located at $\mathbf{x}_j^r \in \mathbb{R}^3$ as shown in Fig. 1. The superscript f represents the fake or spoofed, or false position. The subscript $\{k, j\}$ indicates the spoofer-to-target pre-association, which is defined as spoofer-to-target mapping before the spoofing process begins.

The GPS uses twenty-four satellites in the constellation to transmit the navigation signals $\psi_i(t)$ to provide the PVT information anywhere on the globe. The signal $\psi_i(t)$ consists of timestamps of signal transmission (t'), satellite location $\mathbf{X}_i$, satellite health, and deviations from the satellite's predicted trajectories. The satellite signals propagate with the speed of light (c). Here in the given surveillance, the visibility of satellites is limited to N satellite. The positions of the satellite are given by

$$X = \{\mathbf{X}_i\}_{i=1}^{N} \; ; \; \mathbf{X}_i \in \mathbb{R}^3 \tag{3}$$

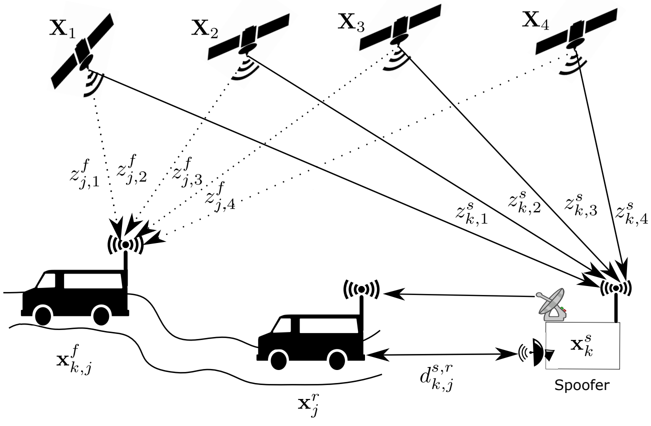

FIGURE 1. Illustration of location spoofing of a truck on a road scenario. The physical location of the truck is $\mathbf{x}_j^r$ and its spoofed location is $\mathbf{x}_{k,j}^f$, the spoofing achieved by using a spoofer which is being located at $\mathbf{x}_k^s$. (The dark lines from satellite-to-target represent the authentic signals. The dotted lines from satellite-to-target are due to transmission of spoofed signals from spoofer)

Usually, clean environment (without any spoofing), the GPS receivers rely on the authentic satellite signals coming from the constellation. Nevertheless, the spoofer generates the mimic satellite signals with the higher power, and thus spoofed signals locking probability is high compared to that of the authentic signals. The authentic satellite signal reception for the true target being located at $\mathbf{x}_j^r$ and number of spoofers are not shown in Fig. 1 for proper visualization. In the working principle of Fig. 1, the spoofer located at $\mathbf{x}_k^s$ is having a receiver module to receive N authentic satellite signals; the received signals gets modify by the spoofer according to the intended spoof location $\mathbf{x}_{k,j}^f$ and transmit onto the target located at $\mathbf{x}_j^r$.

A. TRANSMITTED SPOOF SIGNALS MODELING

A repeater-based spoofer is considered in this formulation to combat the anti-spoofing algorithms like constellation check, offset check, online satellite positioning [14]. The spoofer located at $\mathbf{x}_k^s$ receives all authentic satellite signals in the range as

$$\psi\left(\mathbf{x}_k^s, t\right) = \sum_{i=1}^{N} A_{i,k}\psi_{i,k}\left(t - \frac{\mid \mathbf{x}_k^s - \mathbf{X}_i \mid}{c}\right) + n\left(\mathbf{x}_k^s, t\right), \tag{4}$$

where $A_{i,k}$ is signal attenuation due to transmission from $\mathbf{X}_i$ to $\mathbf{x}_k^s$. Whereas, $\mid \mathbf{x}_k^s - \mathbf{X}_i \mid$ and $n\left(\mathbf{x}_k^s, t\right)$ represents euclidean distance and background noise respectively. The GPS receivers cannot have two-way clock synchronization due to un affordability of highly stable clocks like cesium oscillators; this yields in clock offset δ. The exact time at receiver is equal to summation of satellite system time and offset. Therefore, the exact time is $t = t' + \delta$. The modified received combined signals is

$$\psi\left(\mathbf{x}_k^s, t'\right) = \sum_{i=1}^{N} A_{i,k}\psi_{i,k}\left(t - \delta_{i,k}^s\right) + n\left(\mathbf{x}_k^s, t'\right). \quad (5)$$

Here, $\delta_{i,k}^s$ is the time-delay corresponding to the pseudorange $z_{i,k}^s$ and is given by

$$z_{i,k}^s = \sqrt{(x_k^s - X_i)^2 + (y_k^s - Y_i)^2 + (z_k^s - Z_i)^2} + b. \quad (6)$$

Where $\mathbf{X}_i = [X_i, Y_i, Z_i]'$, $\mathbf{x}_k^s = [x_k^s, y_k^s, z_k^s]'$, and b is the bias due to offset. The extraction of navigation signals from the received composite signal can be achieved by using spreading code-phase technique [30]. The spoofer k modifies the time delays of individual satellite signals in different channels, and then re-transmits them onto target j. The re-transmitted signal with modified delay is given by

$$\psi\left(\mathbf{x}_k^s, t'\right) = \sum_{i=1}^{N} A_{i,k}\psi_{i,k}\left(t - \delta_{i,k}^s - \delta_{i,k,j}\right) + n\left(\mathbf{x}_k^s, t'\right). \quad (7)$$

The external time delay offered to the i^{th} satellite signal by the k^{th} spoofer to the j^{th} target is given by $\delta_{k,j,i}$. This external delay being offered in MSMT is analogous to derivation of single-target single-spoofer external delay calculation as given in [9], [12]. By following the geometrical derivation as given in [9], [12], the calculated external delay by the spoofer k for target j pertaining to signal i is $\delta_{i,k,j}$, given by

$$\delta_{i,k,j} = \frac{z_{i,j}^f - z_{i,k}^s - d_{k,j}^{s,r}}{c}. \quad (8)$$

Here $z_{i,j}^f$ is the spoofed pseudorange between $\mathbf{X}_i$ and $\mathbf{x}_{k,j}^f$ and is given by

$$z_{i,j}^f = \sqrt{(x_j^f - X_i)^2 + (y_j^f - Y_i)^2 + (z_f^r - Z_i)^2} + b \quad (9)$$

Whereas $\mathbf{x}_j^r = [x_j^r, y_j^r, z_j^r]'$, and $z_{i,k}$ is the pseudorange between $\mathbf{X}_i$ and $\mathbf{x}_j^s$, as shown in Fig. 1. The distance between spoofer k to the target j is $d_{k,j}^{s,r}$. In practice, this distance calculation is carried out by using any range measuring devices like radar, visual sensor, and lidar, etc. In one of our previous works, the effect of target tracking on generating GPS spoofed measurements is presented in [12]. But, to simplify this problem, we assumed that the distance between spoofer and target is known precisely. The $d_{k,j}^{s,r}$ is the euclidean distance or the range between spoofer and target, is represented as

$$d_{k,j}^{s,r} = \sqrt{(x_k^s - x_j^r)^2 + (y_k^s - y_j^r)^2 + (z_k^s - z_j^r)^2}. \quad (10)$$

B. RECEIVED SPOOFED SIGNALS MODELING

The re-transmitted signals by the spoofer propagate with velocity of light in open space and then received by the GPS receiver. During this process, it is not necessarily true that the generated spoofed signals are associated with the targeted receiver. This is because the multiple-spoofers are Omni-directional, and hence other spoofer signals might be associated owing to the higher power of signals within the vicinity. Besides, the nearby deployment of spoofers can also lead to the wrong association. The scenario of Omni-directional spoofer and multi-target is as shown in Fig. 2, where the target of interest is $\mathbf{x}_j^r$, but the near by target is $\mathbf{x}_l^r$. The simulated repeater signals for target $\mathbf{x}_j^r$ locked onto the target $\mathbf{x}_l^r$. So the generalized receiving signal is modeled for any target in the surveillance. Therefore, in general the target located at $\mathbf{x}_l^r$ receives the composite signal as

$$\psi\left(\mathbf{x}_l^r, t'\right) = \sum_{i=1}^{N} A_{i,l}\psi_{i,l}\left(t - \delta_{i,l}^s - \delta_{i,k,j} - \frac{d_{k,l}^{s,r}}{c}\right) + n\left(\mathbf{x}_l^r, t'\right). \quad (11)$$

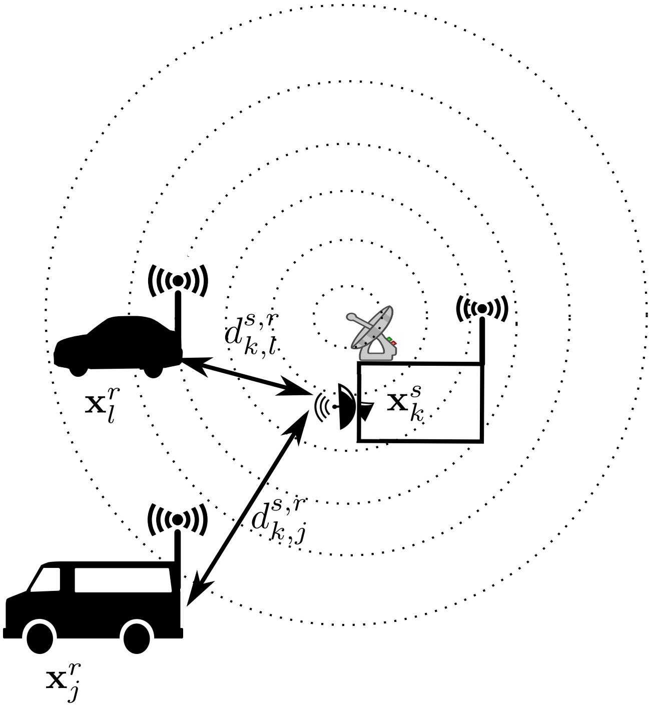

FIGURE 2. Illustration of multiple targets and single omni-directional spoofer scenario (The dotted circle represents the direction of the spoofed signals generated by the spoofer).

Here $l \in \{1, \ldots, M\}$. For $l = j$, the above equation states that all the signals transmitted by spoofer k are locked onto the targeted j^{th} target of interest. This implies that pre-association is equal to post-association. Post-association refers to the spoofer-to-target association after locking the spoofed signals onto the GPS receiver. Whereas for $l \neq j$, the above equation states that all the signals transmitted by spoofer k are locked onto l^{th} target, which is not a target of interest. That is, the pre-association and post-associations are different; this is considered as unsuccessful spoofing. After processing the $\psi\left(\mathbf{x}_l^r, t'\right)$ signals, the pseudorange measurements obtained are given by

$$z_{i,k,l}^{s,r} = c\left(\delta_{i,k}^s + \delta_{i,k,j} + \frac{d_{k,l}^{s,r}}{c}\right). \quad (12)$$

Substituting $\delta^s_{i,k} = \frac{z^s_{i,k}}{c}$ and (8) in (12) yields

$$z^{s,r}_{i,k,l} = c\left(\frac{z^s_{i,k}}{c} + \frac{z^f_{i,j} - z^s_{i,k} - d^{s,r}_{k,j}}{c} + \frac{d^{s,r}_{k,l}}{c}\right). \tag{13}$$

Solving the above (13) gives

$$z^{s,r}_{i,k,l} = z^f_{i,j} - d^{s,r}_{k,j} + d^{s,r}_{k,l}. \tag{14}$$

Here $\{k,j\}$ is the pre-association and $\{k,l\}$ is the post-association. If this pre-association and post-association are equal, then the spoofing is successful, else unsuccessful. The (14) is the compact form to generate GPS measurements in the MSMT scenario. In spoofing process, the pseudorange measurement set obtained at the target l due to spoofer k is $\left\{z^{s,r}_{k,l,i}\right\}_{i=1}^{N} = \{z_i\}_{i=1}^{N}$. Now, we are removing the superscripts and subscripts to avoid further confusion in the mathematical equations in the following Subsection-II-C. However, we use the actual terms whenever required without loosing the generality.

C. GPS POSITIONING AND VALIDATION

The generalized form of pseudorange measurement z_i is given by

$$z_i = \sqrt{(X_i - x)^2 + (Y_i - y)^2 + (Z_i - z)^2} + c(dt_i - dt) + w_i \tag{15}$$

where $c(dt_i$-$dt)$ is the bias term equivilanet to b. The geometrical range is $\sqrt{(X_i - x)^2 + (Y_i - y)^2 + (Z_i - z)^2}$. Here $\mathbf{x}$ is an unknown position $[x, y, z]'$, and w_i represents zero-mean white Gaussian noise with covariance R. The measurement noise includes the troposphere noise, ionosphere noise, and external noises. Geometrically, every measurement equation translates into a sphere with $\mathbf{x}_i$ as a center. The unknown vector to be estimated is $[x, y, z, dt]'$. Hence, at least four pseudoranges are required to achieve three-dimensional positioning. Here a unique solution is obtained by solving any four equations from N. The unknown vector can be solved by using algorithms like least squares (LS), iterative least squares (ILS), weighted least square (WLS), and Newton's method [31].

The initial position estimate assumed as the center of the earth as we are assuming no prior information is available. If any prior state is available, then nominal state is assumed as the prior. Let n be the iteration number and n_{max} be the total number of iterations i.e., $n = 1, 2, ..., n_{\text{max}}$. The position estimate improves iteratively. Generalizing, the nominal state for n^{th} iteration is $\hat{\mathbf{x}}_n = [x_n, y_n, z_n, dt_n]'$. The approximate pseudorange that is computed from the satellite position $\mathbf{x}_i$ to nominal position $\mathbf{x}_n$ is given by $\rho_{i,n}$. Where $\rho_{i,n} = \sqrt{(X_i - x_n)^2 + (Y_i - y_n)^2 + (Z_i - z_n)^2}$ is the range computed from the i^{th} satellites position to the approximate receiver position $[x_n, y_n, z_n]$. The incremental change vector $[\Delta x_n, \Delta y_n, \Delta z_n]'$ is added to the approximate receiver position $[x_n, y_n, z_n]$ to update the receiver position as

$$\begin{aligned} x_{n+1} &= x_n + \Delta x_n, \\ y_{n+1} &= y_n + \Delta y_n, \\ z_{n+1} &= z_n + \Delta z_n. \end{aligned} \tag{16}$$

Based on the relation, the right hand sided of (16) is linearized using the first order Taylor series expansion. whereas the Taylor series expansion for $\rho_{i,n+1}$ is

$$\rho_{i,n+1} = \rho_{i,n} + \frac{\partial \rho_{i,n}}{\partial x_n}\Delta x_n + \frac{\partial \rho_{i,n}}{\partial y_n}\Delta y_n + \frac{\partial \rho_{i,n}}{\partial z_n}\Delta z_n. \tag{17}$$

The partial derivatives are given by

$$\begin{aligned} \frac{\partial \rho_{i,n}}{\partial x_n}\Delta x_n &= \frac{X_i - x_n}{\rho_{i,n}}, \\ \frac{\partial \rho_{i,n}}{\partial y_n}\Delta y_n &= \frac{Y_i - y_n}{\rho_{i,n}}, \text{ and} \\ \frac{\partial \rho_{i,n}}{\partial z_n}\Delta z_n &= \frac{Z_i - z_n}{\rho_{i,n}}. \end{aligned} \tag{18}$$

The first ordered linearized form of observation equation is

$$\begin{aligned} z_{i,n} = {} & \rho_{i,n} - \frac{X_i - x_n}{\rho_{i,j}}\Delta x_n - \frac{Y_i - y_n}{\rho_{i,n}}\Delta y_n \\ & - \frac{Z_i - z_n}{\rho_{i,n}}\Delta z_n + c(dt_n - dt) + w_i, \end{aligned} \tag{19}$$

where b_n is the estimated clock error at the receiver. Rearranging the above equation yields

$$\begin{bmatrix} -\frac{X_i - x_n}{\rho_{i,n}} & -\frac{Y_i - y_n}{\rho_{i,n}} & -\frac{Z_i - z_n}{\rho_{i,n}} & 1 \end{bmatrix} \begin{bmatrix} \Delta x_n \\ \Delta y_n \\ \Delta z_n \\ cdt_i \end{bmatrix} = b_{i,n}, \tag{20}$$

where $b_{i,n} = z_{i,n} - \rho_{i,n} + cdt_i - w_i$. The number of unknowns in the equation are four, hence at-least four satellite ranges are required to form a system of linear equations. $b_n = \begin{bmatrix} b_{1,n}, & \cdots & b_{N,n} \end{bmatrix}$. The least square problem is

$$\min || \, A_n \hat{\mathbf{x}}_n - b_n \, ||, \tag{21}$$

where

$$A_n = \begin{bmatrix} -\frac{X_1 - x_n}{\rho_{1,n}} & -\frac{Y_1 - x_n}{\rho_{1,n}} & -\frac{Z_1 - x_n}{\rho_{1,n}} & 1 \\ -\frac{X_2 - x_n}{\rho_{2,n}} & -\frac{Y_2 - x_n}{\rho_{2,n}} & -\frac{Z_2 - x_n}{\rho_{2,n}} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ -\frac{X_N - x_n}{\rho_{N,n}} & -\frac{Y_N - x_n}{\rho_{N,n}} & -\frac{Z_N - x_n}{\rho_{N,n}} & 1 \end{bmatrix}, \tag{22}$$

and $\mathbf{x}_n = [\Delta x_n, \Delta y_n, \Delta z_n, cdt_n]$. The approximate receiver position is updated for every iteration. This iteration process continues until the solution reaches to desired accuracy or till n_{max}. Here from (21), we can observe that $\hat{\mathbf{x}}$ minimizes the length of the error vector $\hat{e}_n$. The sum of squares of N separate errors is given by

$$|| \, e_n \, ||^2 = (b_n - A_n \mathbf{x}_n)'(b_n - A_n \mathbf{x}_n). \tag{23}$$

By minimizing the quadratic form (23) gives

$$\hat{\mathbf{x}}_n \quad = \quad (A_n' A_n)^{-1} A_n' b_n. \tag{24}$$

However, the accuracy of the estimation depends on the dilution of precision (DOP) value, which is defined as the square root of the trace of the matrix $(A'A)^{-1}$.

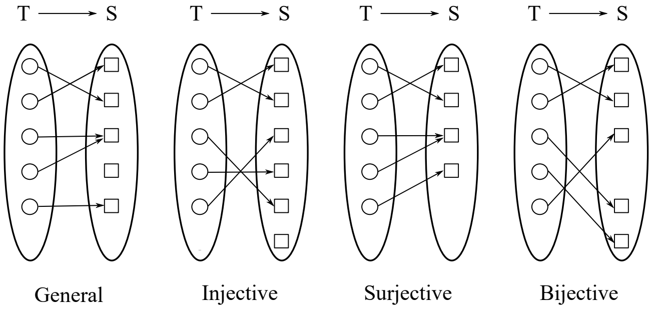

FIGURE 3. Different types of assignments involved in multi-spoofer multi-target scenario.

III. SPOOFER-TO-TARGET ASSOCIATION

Generally, in a single-spoofer single-target (SSST) scenario, the spoofer generates spurious signals with higher power than authentic signals. It transmits them onto a target to successfully spoof the target. The received power of the signals plays an important role in locking the spurious signals onto the target. In MSMT, a set of spoofers S and set of targets T are present. Where, T is the set of targets given by $\{T_j\}_{j=1}^{M}$ and S be the set of spoofers represented as $\{S_k\}_{k=1}^{L}$. Here T_j and S_k are target-ID and spoofer-ID respectively. Traditionally, the transmitting power of the spoofers is a constant value and equal to p_k^s. The distance between spoofers and targets follows inverse square law. The received power by the target j due to the transmitting power of spoofer k is given by

$$p_{k,j}^{s,r} = \frac{p_k^s}{4\pi \left(d_{k,j}^{s,r}\right)^2}. \tag{25}$$

The $d_{k,j}^{s,r}$ is the euclidean distance as given in (10). In distributed spoofing, some spoofers are very near to unintended targets. The unintended targets are likely to be associated with the wrong spoofer due to the vicinity (higher power) and lead to wrong spoofing. All the targets should be spoofed to their respective fake positions to achieve stealthy GPS spoofing. Hence, each target should be handled by a unique spoofer, and no spoofer should engage more than one target.

A. DISTRIBUTED SPOOFING WITH RANDOM ASSOCIATION

All the sensors work in a distributed configuration, in which each spoofer is not aware of other spoofers and targets are being deployed in the surveillance. To engage each target with a unique spoofer ID, the number of spoofers should be equal to the number of targets ($L = M$). Therefore, M spoofers are governing M targets in the given surveillance region. The pre-association between T and S is given by $\mho_{BS}$ and selected randomly. Here subscript BS indicates association given before-spoofing or pre-association. Since there is no communication between the spoofers, the assignment is random, and the pre-association variable $\mho_{BS} \ : \ T \rightarrow S$ is a bijective as shown in Fig. 3. The bijective assignment states that every element in T has S, and every element has a unique mapping, and no element is left out in these sets.

$$\begin{aligned}\mho_{BS} =&\{(T_j, S_k) \mid j,k \in \mathbb{R};\ j,k = 1, \cdots M \\ &\text{Association is bijective}\}\end{aligned} \tag{26}$$

After spoofing, there is a likelihood that multiple targets are associated with the same spoofer, and the relation between T and S becomes general, as shown in Fig. 3. A general assignment where S can have many elements from T and few elements in S may/may not be assigned. The association after spoofing is represented as $\mho_{AS}$. Where $\mho_{AS} \ : \ T \rightarrow S$ is a general assignment. The modified mapping after spoofing is

$$\begin{aligned}\mho_{AS} =&\{(T_j, S_k) \mid j,k \in \mathbb{R};\ j,k = 1, \ldots, M \\ &\text{Association is a general}\}\end{aligned} \tag{27}$$

Since the received power and the euclidean distance are inversely related, therefore euclidean distance based MM grid formation is considered. The constructed cost matrix is given by

$$D = \begin{bmatrix} d_{1,1}^{s,r} & \cdots & d_{1,j}^{s,r} & \cdots & d_{1,M}^{s,r} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ d_{k,1}^{s,r} & \cdots & d_{k,j}^{s,r} & \cdots & d_{k,M}^{s,r} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ d_{M,1}^{s,r} & \cdots & d_{M,j}^{s,r} & \cdots & d_{M,M}^{s,r} \end{bmatrix} \tag{28}$$

Here the association after the spoofing is nearest neighbor (NN). The association after spoofing is represented by an optimization function

$$D_{NN} = \min_{k,j} \sum_{k}^{M} \sum_{j}^{M} d_{k,j}^{s,r} \psi_{k,j} \tag{29}$$

subjected to

$$\sum_{j}^{M} \psi_{k,j} = 1 \ \forall k$$

where $\psi_{k,j}$ is binary association variable such that $\psi_{k,j} = 1$, if the spoofer is associated with a candidate target. Otherwise, it is zero.

Since the spoofer-to-target pre-association is random, this conflicts with the post-association and leads to unsuccessful spoofing. So, there should be a communication between the spoofers to form a pre-association to generate the spoofing signals.

B. CENTRALIZED SPOOFING WITH GNN ASSOCIATION

Centralized spoofing is a technique in which all the spoofers are connected to decide spoofer-to-target association. Unlike the distributed spoofing, here M spoofers and M targets in the surveillance are involved in forming the pre-association $\mho_{BS}$. The primary objective of the global nearest neighbor (GNN) association is to find the most likely set of assignments such that each spoofer is associated with only one target. The second objective of the GNN association is to minimize the cost by assigning the nearby spoofers and targets to accomplish each spoofer is assigned with only one target. The above cost matrix (28) is solved as following

$$D_{GNN} = \min_{k,j} \sum_{k}^{M} \sum_{j}^{M} d_{k,j}^{s,r} \psi_{k,j} \tag{30}$$

subjected to

$$\sum_{j}^{M} \psi_{k,j} = 1 \; \forall k$$

$$\sum_{k}^{M} \psi_{k,j} = 1 \; \forall j$$

Where $\psi_{k,j}$ is a binary association variable such that $\psi_{k,j} = 1$ if the spoofer is associated with a particular target. Otherwise, it is set to zero. By optimizing the above problem, the pre-association is $\mho_{BS} \; : \; T \rightarrow S$ is bijective as shown in Fig. 3. In GNN, the overall cost is minimum. Every time, the minimum cost will not ensure that all spoofers are mapped to the nearby targets. There might be some cases, even though the spoofer-to-target distance is minimum but not considered in the overall cost minimization. The post-association $\mho_{AS} \; : \; T \rightarrow S$ becomes general for multiple targets are assigned to the same spoofer, else it is bijective. When the function is general, the overall spoofing efficiency decreases. Hence, there is a strong need to develop a novel algorithm to efficiently utilize the existing spoofers and deploy additional spoofers whenever needed to carry out efficient spoofing.

C. CENTRALIZED SPOOFING WITH SENSORS OF OPPORTUNITY BASED GNN ASSOCIATION

When the spoofer-to-target pre-association and post-association are not equal in the above methods, the spoofers of opportunity in the surveillance is considered and form a centralized node to make pre-association. Let K additional spoofers be included in the set S and existing M spoofers to complete the set S. Now, the total number of spoofers in the set S be $L = M + K$. The extra spoofers are included in the existing spoofers set S to form a new post-association as

$$D_{NN}^{*} = \min_{k,j} \sum_{k}^{L} \sum_{j}^{M} d_{k,j}^{s,r} \psi_{k,j} \tag{31}$$

subjected to

$$\sum_{j}^{M} \psi_{k,j} = 1 \; \forall k$$

Algorithm 1 Pre-association using centralized spoofing with sensors of opportunity

```
procedure ASSOCIATION($\{\mathbf{x}_k^s\}_{k=1}^{M}, \{\mathbf{x}_j^r\}_{j=1}^{M}, \{\mathbf{x}_k^s\}_{k=1}^{K}$)
    for $i = 0 : 1 : K$ do
        Compute $d_{k,j}^{s,r}; k = 1, \ldots, M, j = 1, \ldots, M + i$
        Compute $D_{NN}^{*}$ and $D_{GNN}^{*}$
        if $D_{NN}^{*} == D_{GNN}^{*}$ then
            Report the associated spoofers and exit
        else if $i == K$ then
            report partial association tuple {k,j}, 100% hit ratio not possible and exit
        end if
    end for
end procedure
=0
```

Similarly, the GNN association for the new S is

$$D_{GNN}^{*} = \min_{k,j} \sum_{k}^{M} \sum_{j}^{L} d_{k,j}^{s,r} \psi_{k,j} \tag{32}$$

subjected to

$$\sum_{j}^{M} \psi_{k,j} \leq 1 \; \forall k$$

$$\sum_{k}^{M} \psi_{k,j} = 1 \; \forall j$$

Where $\psi_{k,j}$ is a binary association variable such that $\psi_{k,j} = 1$ if the spoofer is associated with a given target. Otherwise, it is set to zero. The removal of existing spoofers and deployment of additional spoofers and their spatial location is calculated by using Algorithm-I. By optimizing the above problem, if the deployed spoofers are sufficient to run the algorithm, then the pre-association is $\mho_{BS} \; : \; T \rightarrow S$ is injective as shown in Fig. 3. Injective is a class of sets, where all the elements in T are uniquely mapped onto S and few elements of S are empty, i.e., not mapped to any element in T.

$$\mho_{BS} = \{(T_j, S_k) \mid j, k \in \mathbb{R}; \; j = 1, \ldots, M \text{and } k = 1, \cdots L \;\; \text{Association is injective}\} \tag{33}$$

In this approach, it is not a specific event that to achieve 100% hit-ratio because of lesser spoofers of opportunity. Even though when few spoofers available, the algorithm reports partial associations. Partial associations believe that only $M - P$ targets can get correct association out of M targets. Therefore, after removing the undesired associations, pre-association is given by $\mho_{BS} \; : \; T \rightarrow S$ is bijective and is represented as

$$\mho_{BS} = \{(T_j, S_k) \mid j, k \in \mathbb{R}; \; j, k = 1, \cdots M - P \;\; \text{Association is bijective}\} \tag{34}$$

The post-association $\mho_{AS} : T \rightarrow S$ becomes surjective, i.e., every S has at least one mapping from T, no element in S is left out and the relation $\mho_{AS}$ is given by

$$\begin{aligned}\mho_{AS} =& \{(T_j, S_k) \mid j,k \in \mathbb{R};\ k = 1, \cdots M-P, j = 1, \dots M \\ & \text{Association is surjective}\}\end{aligned} \tag{35}$$

In this case, although higher hit ratio is not achieved, it diminishes the unwanted deployment of spoofers in the surveillance region.

D. CENTRALIZED SPOOFING WITH TUNABLE POWER BASED GNN ASSOCIATION

Algorithm 2 Pre-association using centralized spoofing with sensors of opportunity and tunable power

```
0: procedure ASSOCIATION($\{\mathbf{x}_k^s\}_{k=1}^{M}$, $\{\mathbf{x}_j^r\}_{j=1}^{M}$, $\{\mathbf{x}_k^s\}_{k=1}^{K}$, $\{p_k\}_{k=1}^{L}$)
0:   for $i = 0:1:K$ do
0:     Compute $p_{k,j}; k = 1, \dots, M, j = 1, \dots, M+i$
0:     Compute $\Omega_{BS}$,and $\Omega_{AS}$
0:     if $\Omega_{BS} == \Omega_{AS}$ then
0:       Report the associated spoofers and exit
0:     else
0:       Calculate the partial associations and find n
0:       for l=1:n do
0:         Tunable power $p_l^* = p_l + \delta p$ and examine the effect of partial associations on total associations
0:         Check step 5, if it is true, report {k,j} associations
0:       end for
0:     end if
0:   end for
0: end procedure=0
```

The cost matrix for the given spoofers and targets is constructed by assuming all the spoofers possess the same transmitting power. So the assignment of spoofer-to-target is carried out by maximizing the cost function consisting of the received powers at the multiple receivers. The cost matrix corresponding to LM received power grid is

$$P = \begin{bmatrix} p_{1,1}^{s,r} & \cdots & p_{1,j}^{s,r} & \cdots & p_{1,M}^{s,r} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ p_{k,1}^{s,r} & \cdots & p_{k,j}^{s,r} & \cdots & p_{k,M}^{s,r} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ p_{L,1}^{s,r} & \cdots & p_{L,j}^{s,r} & \cdots & p_{L,M}^{s,r} \end{bmatrix} \tag{36}$$

The above cost matrix is formulated as

$$P_{GNN}^* = \max_{k,j} \sum_{k}^{L} \sum_{j}^{M} p_{k,j}^{s,r} \psi_{k,j} \tag{37}$$

subjected to

$$\sum_{j}^{M} \psi_{k,j} \leq 1 \; \forall k$$

$$\sum_{k}^{L} \psi_{k,j} = 1 \; \forall j$$

where $\psi_{k,j}$ is a binary association variable such that $\psi_{k,j} = 1$ if the spoofer is associated with a specific target. Otherwise, it is set to zero. Since the transmitting power of every spoofer is different, the distance-based optimization is no longer valid. Hence, the post-association based is given by

$$P_{NN}^* = \max_{k,j} \sum_{k}^{L} \sum_{j}^{M} p_{k,j}^{s,r} \psi_{k,j} \tag{38}$$

subjected to

$$\sum_{j}^{M} \psi_{k,j} = 1 \; \forall k$$

The results obtained by the power maximization are equal to the distance minimization. However, in both cases, the hit ratio is poor for fewer spoofers in the surveillance. To obtain the higher hit ratio, here the altering the spoofer transmitting power is considered. Let the modified transmitting power by the k^{th} spoofer is p_k^*. Hence, the received power by r^{th} target is p_{kj}^*. The selection of modified transmitting powers is calculated by using the Algorithm-II

IV. RESULTS AND DISCUSSIONS

A. SCENARIO GENERATION

The satellite location set $\{\mathbf{x}_i\}_{i=1}^{N}$ is modeled using WGS-84 model and follows the assumption of circular orbits. The mathematical model for satellite locations is given by

$$\begin{aligned} X(t) &= D\left[\cos\theta(t)\cos\phi(t) - \sin\theta(t)\sin\phi(t)\cos 55^o\right] \\ Y(t) &= D\left[\cos\theta(t)\sin\phi(t) + \sin\theta(t)\cos\phi(t)\cos 55^o\right] \\ Z(t) &= D\sin\theta(t)\sin 55^o \end{aligned} \tag{39}$$

where D is the radius ($D = 26,560$Km) of the circular orbit, ϕ and θ are right ascension and angular phase in the circular orbit respectively. The right ascension and angular phase are given by

$$\begin{aligned} \theta(t) &= \theta_0 + (t - t_0)\frac{360}{43082}\text{deg and} \\ \phi(t) &= \phi_0 - (t - t_0)\frac{360}{86164}\text{deg} \end{aligned} \tag{40}$$

respectively. The initial positions of the satellites are given in Table-1. In MSMT scenario, eight spoofers and five targets are deployed in the given surveillance. The coordinates of the spoofer, target and fake target locations in the coordinate

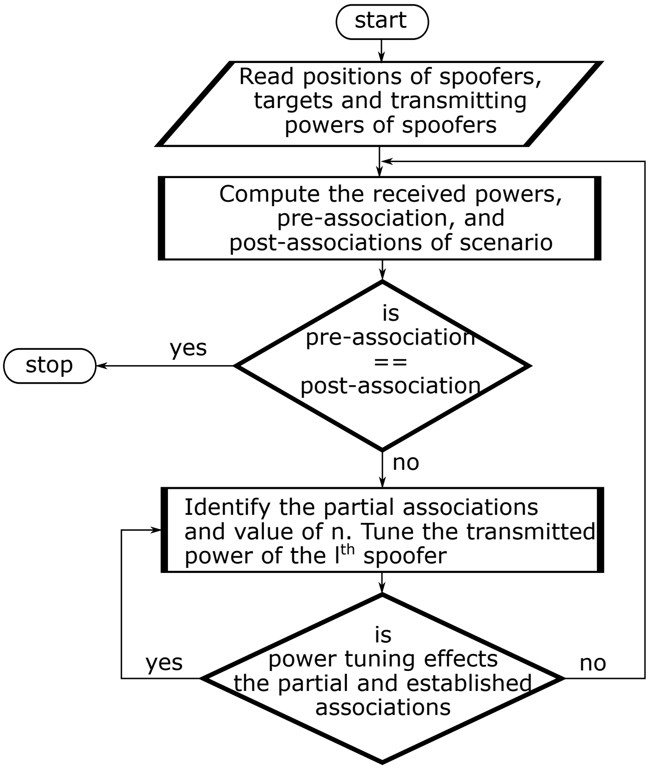
start
Read positions of spoofers, targets and transmitting powers of spoofers
Compute the received powers, pre-association, and post-associations of scenario
is pre-association == post-association
yes
stop
no
Identify the partial associations and value of n. Tune the transmitted power of the l^th spoofer
is power tuning effects the partial and established associations
yes
no

FIGURE 4. Flow chart for Algorithm-2.

TABLE 1. The satellite initial positions (angles $\theta(0)$ and $\phi(0)$)

N	1	2	3	4	5	6
$\theta(0)$	325.7	25.7	85.7	145.7	205.7	265.7
$\phi(0)$	72.1	343.9	214.9	211.9	93.9	27.9

frame are shown in Table. 2. In Table. 2, the indexes k and j indicates the spoofer-ID and target-ID respectively. The $\mathbf{x}_k^s$ and $\mathbf{x}_j^r$ are physical locations of spoofer-ID k and target-ID j respectively. The spoofer k intended to spoof the target j which is located at $\mathbf{x}_j^r$ position to a fake position $\mathbf{x}_{k,j}^f$.

TABLE 2. The spoofer-to-target mapping and its respective positions in local coordinates

k	$\mathbf{x}_k^s$	j	$\mathbf{x}_j^r$	$\mathbf{x}_{k,j}^f$
1	[20,30,0]	1	[20,0,0]	[30,40,0]
2	[40,70,0]	2	[0,30,0]	[60,60,0]
3	[100,70,0]	3	[30,60,0]	[80,100,0]
4	[130,50,0]	4	[100,120,0]	[120,100,0]
5	[80,10,0]	5	[50,44,0]	[20,100,0]
6	[140,10,0]	-	-	-
7	[50,100,0]	-	-	-
8	[50,30,0]	-	-	-

B. PERFORMANCE OF SPOOFER-TO-TARGET ASSOCIATION

In this subsection, the performance of the proposed methods is evaluated using the hit ratio as a metric. The hit ratio is defined as the correct associations to the total number of associations.

1) Random Association

In this case, the spoofers are distributed independently, and the spoofing is carried out without any prior knowledge about other spoofers and targets in the surveillance. Therefore, each spoofer from the set S is assigned to spoof a unique target from the target set T. Five spoofers are assigned to five targets randomly to perform the spoofing. The spoofer-to-target pre-association is random and is given by $\mho_{BS}$: $\{1 \rightarrow 1, 2 \rightarrow 2, 3 \rightarrow 3, 4 \rightarrow 4, 5 \rightarrow 5\}$. Here, the $T_j \rightarrow S_k$ denotes that the target-ID T_j is to be locked with the sensor-ID S_k. The visualization of the spoofers individual locations and target physical locations and projected fake locations are represented in Fig. 5. Moreover, the pre-association is also depicted in the Fig. 5 as (T_j, S_k).

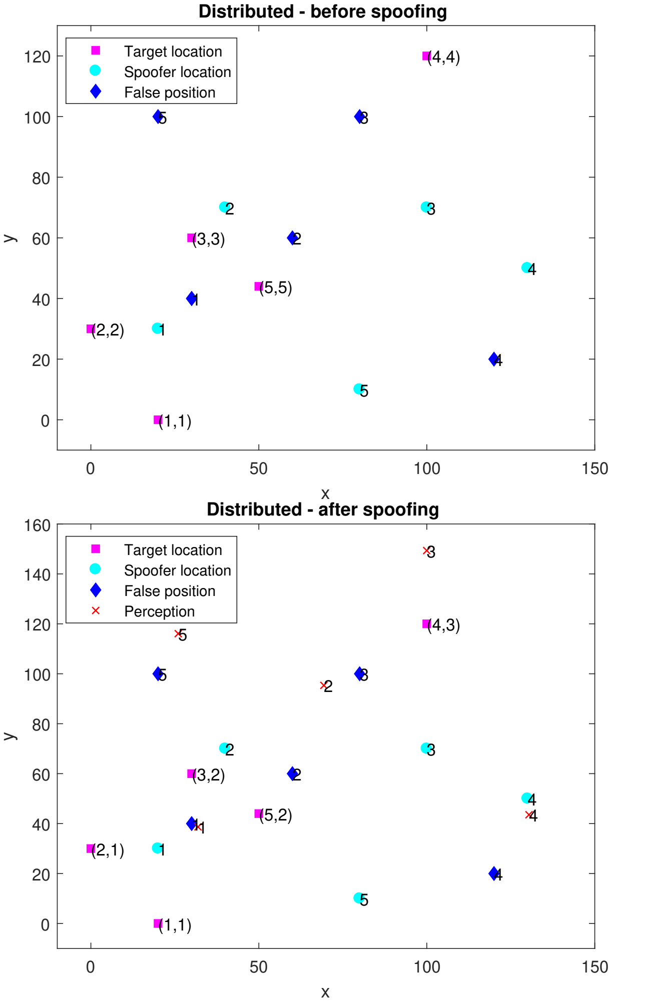

FIGURE 5. The pre-association and post association in distributed spoofing

Since the spoofers are carrying out the spoofing in Omni-directional fashion, this influences the other targets in the vicinity. We can see that the spoofer-3 location and target-3 location are far from each other. Because of the transmitted power of spoofer-3, other nearby targets may locked onto the spoofer-3. Moreover, some spoofers are very close to the intended target, and some spoofers are far from the desired target. This results in abnormal behavior of locking the signals to the undesired targets. For a better understanding, how the other spoofers influence the targets, we are constructing a cost matrix of the NN as given in (29)

	$\mathbf{x}_1^r$	$\mathbf{x}_2^r$	$\mathbf{x}_3^r$	$\mathbf{x}_4^r$	$\mathbf{x}_5^r$
$\mathbf{x}_1^s$	**30**	**20**	31.6	120.4	33.1
$\mathbf{x}_2^s$	72.8	56.5	**14.1**	78.1	**27.8**
$\mathbf{x}_3^s$	106.3	107.7	70.7	**50**	56.3
$\mathbf{x}_4^s$	120.8	131.5	100.4	76.1	80.2
$\mathbf{x}_5^s$	60.8	82.4	70.7	111.8	45.3

From the cost matrix, the bold index are the resultant of post-association. The acquired post-association is $\mho_{AS}\ :\ \{1 \to 1, 2 \to 1, 3 \to 2, 4 \to 3, 5 \to 2\}$. The post-association for the random assignment is given in Fig. 5. Where we can observe that the spoofer-1 is generating the spoof signals to mislead the target-1. However, these signals are locking onto the target-1 and target-2 receivers due to higher power compared to all available signals at the receiver. Similarly, target-3 and target-4 are locking onto the spoofer-2. Further, target-4 is locking onto the spoofer-3 rather than spoofer-4. Here, we can notice that multiple targets are locking onto the same spoofer results in decreased spoofing efficiency. Therefore the hit ratio is defined as

$$\text{Hit ratio (HR)} = \frac{\text{Number of correct associations}}{\text{Total number of associations}} \tag{41}$$

From $\mho_{BS}$ and $\mho_{AS}$, we can observe that only one assignment are incorrect and rest of the assignments are failed. So the HR is evaluated to be one hit in a five assignments, that is HR=0.2.

2) GNN association

Unlike the previous case, all the selected five spoofers are centralized to decide about spoofer-to-target pre-association. All the actual positions regarding the targets and spoofers are sent to a central node. This association is based on the minimization of cost function as given (30), the pre-associations are presented in Fig. 6. Therefore, the spoofer-to-target pre-association after solving the minimization problem (30) is $\mho_{BS}\ :\ \{1 \to 5, 2 \to 1, 3 \to 2, 4 \to 3, 5 \to 4\}$. Thereafter, the spoofing is evaluated and the obtained post-association from the Fig. 6 is $\mho_{AS}\ :\ \{1 \to 1, 2 \to 1, 3 \to 2, 4 \to 3, 5 \to 2\}$. From $\mho_{BS}$ and $\mho_{AS}$ sets, we can observe that only three correct associations out of five, that is HR=0.6. Even though this algorithm provides improved HR compared to random assignment, still it is not achieving 100% HR.

3) Opportunistic Spoofers

All the spoofers are considered, including the spoofers of opportunity to make a centralized decision about spoofer-to-target pre-association. The association is based on Algorithm-I. The algorithm considers five sensors out of eight sensors, i.e., ${}^8C_5$ combinations evolved, and finally, the algorithm provides a HR of 0.8 with four correct associations out of five. The pre-association provided by Algorithm-1 is presented in Fig. 7 and the pre-associations set is $\mho_{BS}\ :\ \{1 \to 5, 2 \to 1, 3 \to 2, 4 \to 3, 5 \to 8\}$. We can observe that the algorithm utilizes the spoofer-8 into account to form an association for the target-5. Thereby, we can understand that increased number of opportunistic spoofers can raise HR. However, by increasing the number of spoofers, it is not guaranteed to get a 100% HR.

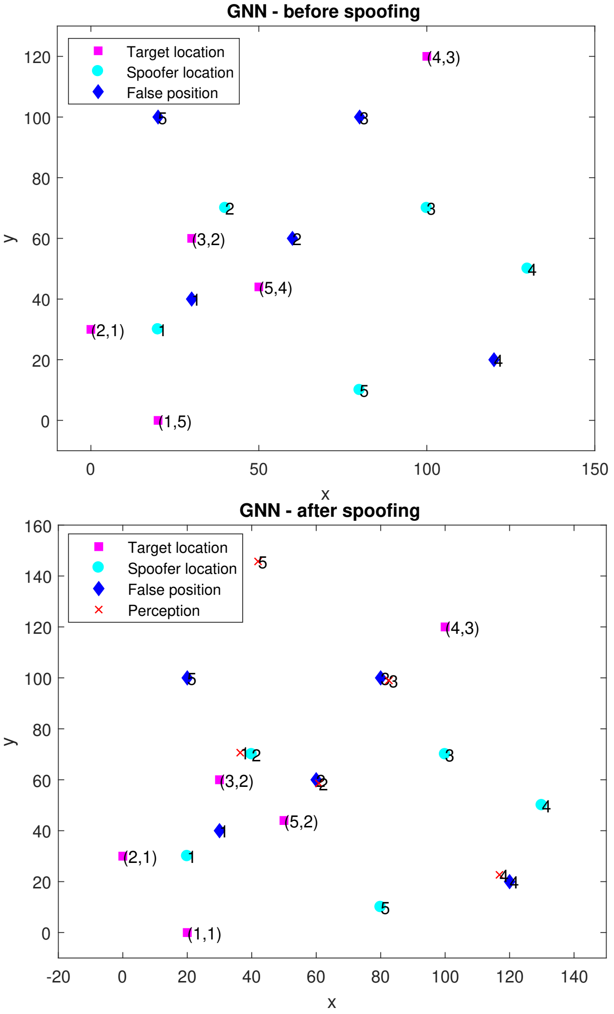

FIGURE 6. The pre-association and post association in centralized GNN spoofing

Unlike the previous two methods, here we observed that the HR is increased. This algorithm provides 100% HR if any nearby spoofer is installed near target-1 and is not in conflict with other targets. However, we seldom find such scenarios. The post-association set is $\mho_{AS}\ :\ \{1 \to 1, 2 \to 1, 3 \to 2, 4 \to 3, 5 \to 2\}$. In addition, due to the new association of $(5, 8)$, the target-5 is in successful spoofing and is observed in Fig. 7. From Fig. 7, we notice that the projected false position and the perception of the receiver are the same and is observed as blue $\diamond$ and $\times$ are

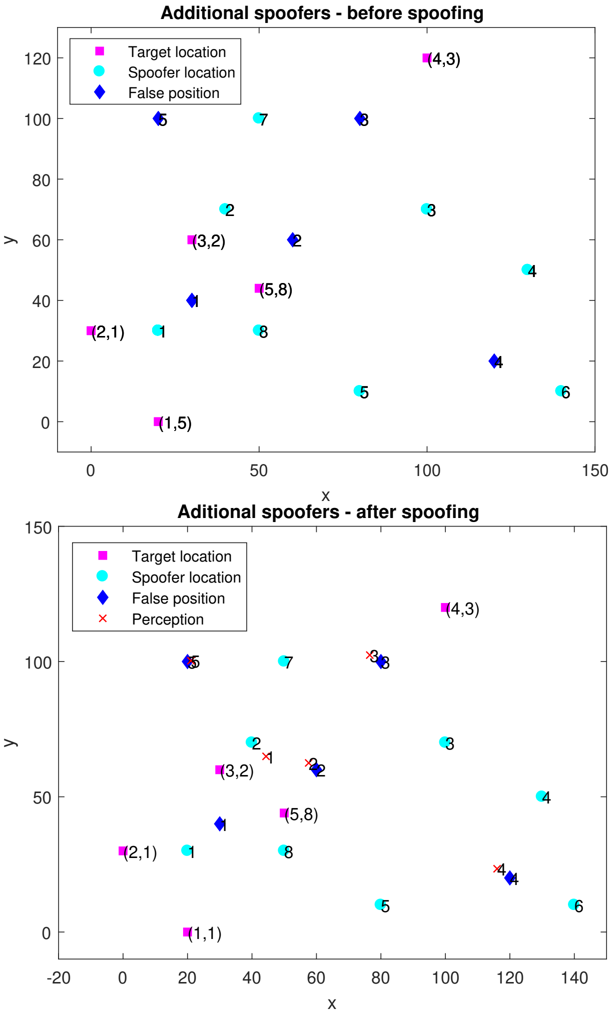

FIGURE 7. The pre-association and post association in opportunistic GNN spoofing

at the same point around x=20 and y=100 coordinates. The rise in the number of spoofers increases HR. However, this is a sub-optimal solution due to the unavailability of dense spoofers.

4) Power Tunability

Algorithm-2 works with the given number of sensors, unlike the opportunistic spoofers. The method utilizes the tunability of spoofer transmitting power so that at the receiver end, the received power varies, and accordingly, the generated spoofed signals lock onto the intended receiver. The power levels after optimization is $p_4 > p_5 > p_3 > p_2 = p_1$ and the pre-association after solving the maximization problem of (37) is shown in Fig. 8. Here, we can observe that the target-5 is associating with spoofer-4. Target-1 is associating with the spoofer-5, which is the same solution as obtained with GNN method. It is worth noting that, even though both the pre-associations are equal, the major difference in GNN method is minimization problem with constant power and Algorithm-2 is maximization problem with tunable power. Hence, the pre-association mapping is $\mho_{BS} : \{1 \to 5, 2 \to 1, 3 \to 2, 4 \to 3, 5 \to 4\}$.

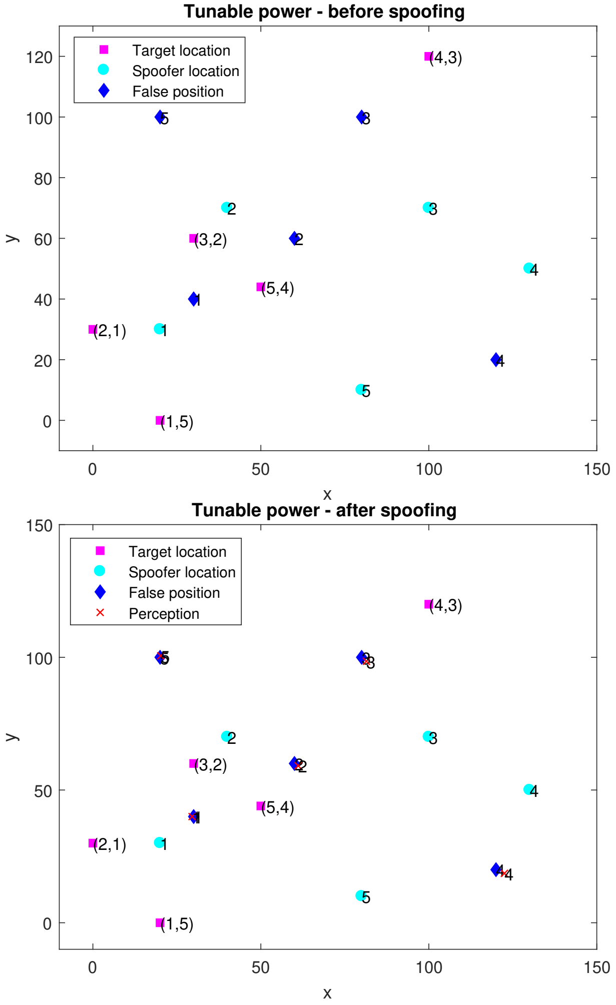

FIGURE 8. The pre-association and post association in tunable power of spoofers

For the given tunable power and the set of spoofers, the post-association set is $\mho_{AS} : \{1 \to 5, 2 \to 1, 3 \to 2, 4 \to 3, 5 \to 4\}$ and is visualized in Fig. 8. We can notice that all the pre-associations and post-associations are equal and achieve a 100% HR in this case. Both the projected false positions and the perception of the targets are the same for all five targets. This method is an optimal way to spoof all the targets to the desired false positions by employing a tunable power-based spoofer-to-target association.

C. PRMSE ANALYSIS

In this subsection, we explored the impact of other variables on the position root mean square error (PRMSE) for the false position to the perception of the estimate. This section considers three different impacts, namely spoofer-to-target association, number of signals, and the measurement noise. For correct spoofer-to-target association, the projected false position and the perception are equal. Whereas in the wrong spoofer-to-target association, the projected false position and the perception are not equal. It is a general statement that as the number of signals increases, the estimate precision increases. Hence we varied the number of signals from four to eight. The minimum number of measurements is four since there are four unknowns to be calculated. Moreover, the spoofing efficiency depends on the association and the type of GPS receivers being used by the targets. The high precession GPS receivers always provide a better position estimate compared to regular GPS receivers. To evaluate this impact, we considered the measurement noise of the receiver as 1 m for the high precision GPS receivers. Similarly, the low-cost GPS receivers are considered with the measurement noise as 5 m.

Fig. 9 shows the target-1 PRMSE for all the four scenarios with a different number of signals (four-eight) and different measurement noise (low and high). Once the GPS signals are locked onto the receiver, the GPS position estimation is carried out by using the ILS algorithm. From Fig. 9, we can infer that random assignment and power tunability algorithms achieves lesser PRMSE for the case of low measurement noise and is in the range of [2-5]m which is in agreement with civilian GPS. Moreover, for the higher value of measurement noise, the PRMSE is in the range of [15–25]m; this is usually seen in low precision GPS devices. The GNN assignment and opportunistic algorithms fail to make a correct target-to-spoofer assignment. Hence, we can observe very high PRMSE around [50–70]m, usually seen in urban scenarios with multi-path effects. Therefore, correct target-to-spoofer assignment is essential to enhance the spoofing performance. The PRMSE is depicted in logarithmic scale by varying the number of signals on the x-axis. The PRMSE of target-2 and target-3 are shown in Fig. 10 and Fig. 11 respectively. The target-2 and target-3 have a correct spoofer-to-target assignment for GNN, opportunistic, and power tunability cases. The PRMSE due to correct association and wrong association is differentiable for the target-1, target-2, and target-3.

The PRMSE corresponding to target-4 and target-5 are presented in Fig. 12 and Fig. 13 respectively. Interestingly, we observe that the PRMSE with wrong association in low measurement noise case is comparably equal to PRMSE due to correct association in high measurement noise case. This observation conveys that spoofing low precision GPS receivers is quite easy, and the anti-spoofing algorithms cannot distinguish between the spoofing and non-spoofing. From Fig. 12 we can observe that opportunistic spoofers-based spoofing with correct association (four signals and high measurement noise) is equal to that of random assignment with wrong spoofer-to-target association (four signals and low measurement noise). This peculiar behavior infers us that spoofing is much easy in the low precession devices. So the civilian GPS receivers are vulnerable to the spoofing process. The proposed algorithm is capable of spoofing both high precision as well as low precision GPS receivers.

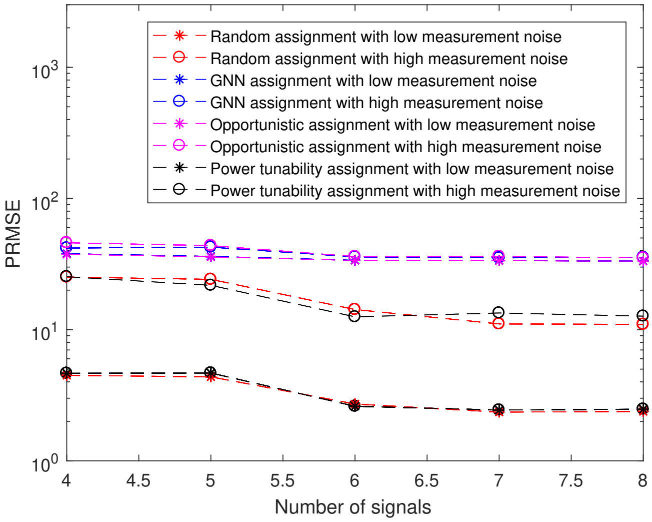

FIGURE 9. The target-1 PRMSE for various scenarios

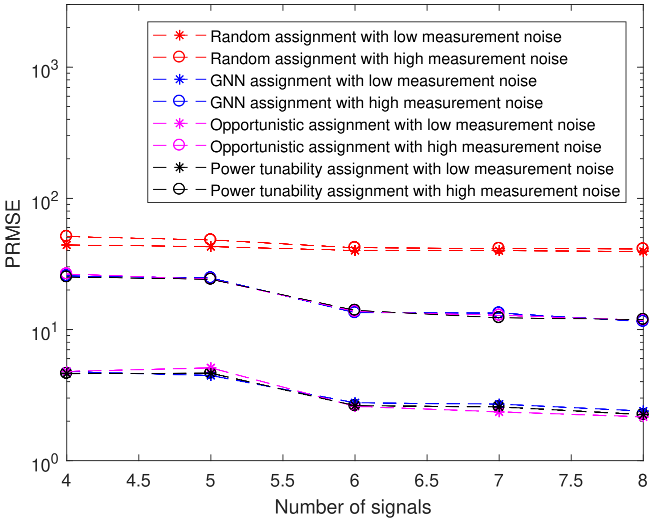

FIGURE 10. The target-2 PRMSE for various scenarios

V. CONCLUSION

In this paper, we derived a generalized mathematical model for transmission and reception of GPS spoofed signals in multi-spoofer multi-target scenario. Further, formulated the spoofer-to-target association as an optimization problem subjected to constrains of unique mapping between spoofer and target. Three novel centralized networking-based spoofing techniques are proposed to overcome spoofer-to-target association in distributed networking. Firstly, the global nearest neighbor (GNN) based centralized spoofing is proposed, in which the overall cost of the function is minimized by assigning unique spoofer-ID to an unique target-ID. It is evident from the simulation results that only lower hit ratios are possible with this approach. Secondly, the spoofers of opportunity-based centralized spoofing with GNN associa-

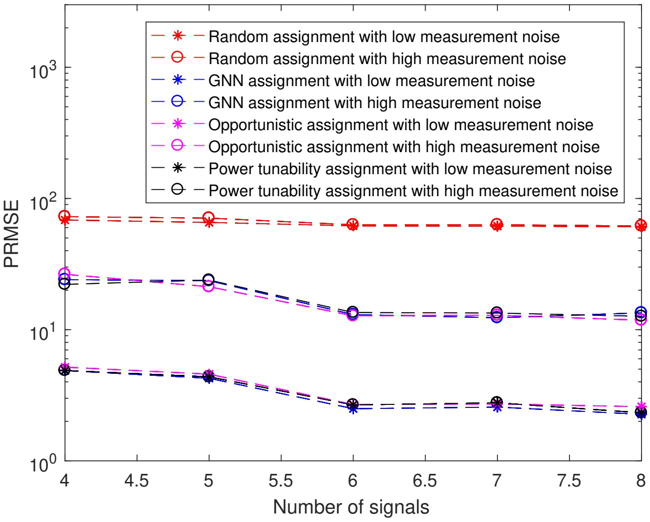

FIGURE 11. The target-3 PRMSE for various scenarios

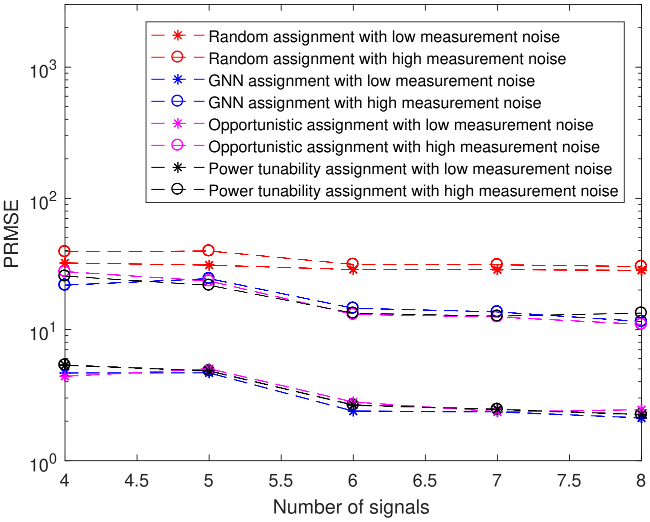

FIGURE 12. The target-4 PRMSE for various scenarios

tion is proposed to resolve the spoofer-to-target association and observed the improvement in hit-ratio as the number of spoofers of opportunity increases. Finally, since huge number of spoofers deployment is impractical, a tunable transmitting power-based centralized spoofing with the GNN association is presented. The power tunability method accomplish 100% hit-ratio and outperform the distributed configuration, centralized configuration, and spoofers of opportunity methods. Furthermore, the simulation results of this method shows that spoofer-to-target association followed by spoofing is outperforming the distributed spoofing without prior knowledge of the environment. Moreover, it is evident from the PRMSE analysis, that the proposed algorithms are very stealthy to spoof both high precision and low precession GPS receivers.

The future possible directions of this work are as follows.

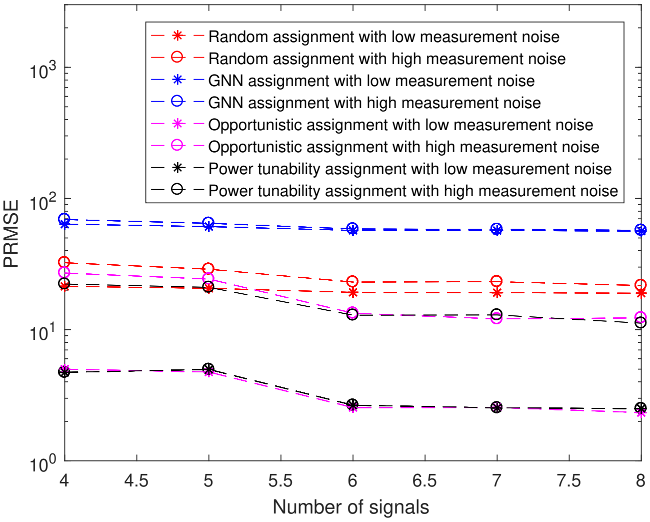

FIGURE 13. The target-5 PRMSE for various scenarios

1. This paper assumed that the spoofer-to-target line of sight exists and accordingly derived the cost functions. One can relax this constrain and develop novel algorithms, which can be adaptable to urban scenario. 2. This paper dealt with static target and static spoofer configuration. One can potentially solve the time varying dynamics of target and spoofer scenario with the help of sensor management and power allocation techniques. 3. Existing wireless sensor network algorithms can be adapted to effectively carryout the spoofing process during the sensor failures.

ACKNOWLEDGMENT

The authors would like to thank Prof. T. Kirubarajan and Dr. R. Tharmarasa for providing valuable inputs during the stay at ETF laboratory, McMaster University, Canada.

REFERENCES

[1] B. W. Parkinson, P. Enge, P. Axelrad, and J. J. Spilker Jr, Global positioning system: Theory and applications, Volume II. American Institute of Aeronautics and Astronautics, 1996.

[2] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, “A blueprint for civil GPS navigation message authentication,” in IEEE/ION Position, Location and Navigation Symposium - PLANS 2014, May 2014, pp. 262–269.

[3] 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.

[4] J. S. Warner, R. G. Johnston, and C. L. Alamos, “A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing,” The Journal of Security Administration, vol. 25, no. 10, pp. 19–28, 2002.

[5] R. Schroer, “Electronic warfare.[a century of powered flight: 1903-2003],” IEEE Aerospace and Electronic Systems Magazine, vol. 18, no. 7, pp. 49–54, 2003.

[6] 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 Radionavigation laboratory conference proceedings, 2008.

[7] S. F. Bian, Y. F. Hu, C. Chen, Z. M. Li, and B. Ji, “Research on GNSS repeater spoofing technique for fake position, fake time and fake velocity,” in 2017 IEEE International Conference on Advanced Intelligent Mechatronics (AIM), Jul. 2017, pp. 1430–1434.

[8] P. Bethi, S. Pathipati, and A. P, "Stealthy GPS spoofing: Spoofer systems, spoofing techniques and strategies," in 2020 IEEE 17th India Council International Conference (INDICON), 2020, pp. 1–7.
[9] 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, Apr. 2014.
[10] 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, May 2017.
[11] C. Bonebrake and L. Ross O'Neil, "Attacks on GPS time reliability," IEEE Security Privacy, vol. 12, no. 3, pp. 82–84, May 2014.
[12] 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.
[13] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," International Journal of Navigation and Observation, vol. 2012, no. 127072, pp. 1–16, Jul. 2012.
[14] C. Günther, "A survey of spoofing and counter-measures," NAVIGATION: Journal of The Institute of Navigation, vol. 61, no. 3, pp. 159–177, Jun. 2014.
[15] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," ACM Computing Surveys (CSUR), vol. 48, no. 4, p. 64, May 2016.
[16] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," Proceedings of the IEEE, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.
[17] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," IEEE Transactions on Aerospace and Electronic Systems, vol. 54, no. 2, pp. 739–754, 2017.
[18] X. Fan, L. Du, and D. Duan, "Synchrophasor data correction under GPS spoofing attack: A state estimation-based approach," IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4538–4546, 2017.
[19] E. G. Manfredini, "Signal processing techniques for GNSS anti-spoofing algorithms," Ph.D. dissertation, Doctoral Dissertation, Politecnico di Torino, 2017.
[20] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," NAVIGATION: Journal of the Institute of Navigation, vol. 59, no. 3, pp. 177–193, 2012.
[21] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing module for legacy civil GPS receivers," Proceedings of the ION ITM, San Diego, CA, pp. 698–712, Jan. 2010.
[22] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM," in Proc. of the 25th Int. Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, Sep. 2012, pp. 3007–3016.
[23] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A low-complexity GPS anti-spoofing method using a multi-antenna array," Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012), Nashville, TN, vol. 2, pp. 1233–1243, Sep. 2012.
[24] Y. Hu, S. Bian, B. Li, and L. Zhou, "A novel array-based spoofing and jamming suppression method for GNSS receiver," IEEE Sensors Journal, vol. 18, no. 7, pp. 2952–2958, Apr. 2018.
[25] C. H. Kang, S. Y. Kim, and C. G. Park, "Adaptive complex EKF based DOA estimation for GPS spoofing detection," IET Signal Processing, vol. 12, no. 2, pp. 174–181, Sep. 2017.
[26] P. F. Swaszek, S. A. Pratz, B. N. Arocho, K. C. Seals, and R. J. Hartnett, "GNSS spoof detection using shipboard IMU measurements," Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014), Tampa, Florida, pp. 745–758, Sep. 2014.
[27] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," IEEE Transactions on Aerospace and Electronic Systems, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.
[28] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "An INS monitor to detect GNSS spoofers capable of tracking vehicle position," IEEE Transactions on Aerospace and Electronic Systems, vol. 54, no. 1, pp. 131–143, Feb. 2018.
[29] 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.
[30] A. Malyshev, I. Malay, and M. Ozerov, "Algorithm for separating GNSS signals into components," in 2018 IEEE East-West Design & Test Symposium (EWDTS). IEEE, 2018, pp. 1–4.
[31] J. S. Abel and J. W. Chaffee, "Existence and uniqueness of GPS solutions," IEEE Transactions on Aerospace and Electronic Systems, vol. 27, no. 6, pp. 952–956, Nov. 1991.

BETHI PARDHASARADHI received his B.Tech degree in Electronics and Communication Engineering from Jawaharlal Nehru Technological University, Kakinada (JNTU-K), Andhra pradesh, India, in 2014. M.Tech degree in VLSI Design from Indian Institute of Information Technology and Management, Gwalior (IIITM), Madya pradesh, India, in 2016. Since 2016 he has been pursuing his full-time Ph.D degree at National Institute of Technology Karnataka (NIT-K), Surathkal, India. Mr. Pardhasaradhi is a receipt of Sir C.V.Raman award from Institution of Engineering and Technology (IET) for outstanding academics and research. He was a visiting Ph.D scholar at McMaster University, ETF lab, Canada, under the supervision of Prof. T. Kirubarajan in 2018-19. His research interests includes intentional interference in navigation, target tracking, and information fusion.

PATHIPATI SRIHARI received B.Tech, Electronics and Communication Engineering from Sri Venkateswara University and completed masters degree in Communications Engineering and Signal Processing from University of Plymouth, England, UK. He obtained Ph.D from Andhra University in the field of Radar Signal Processing in 2012. He is currently working as an Assistant Professor at National Institute of Technology Karnataka, Surathkal,India. He worked as a visiting Assistant Professor at McMaster University, Canada in 2014. Dr. Srihari received 2010 IEEE Asia Pacific Outstanding Branch Counselor Award. He is a Senior Member of IEEE and a Senior Member of ACM. He is a Fellow of IETE and a member of IEICE, Japan. He received young scientist award from the department of science and technology (DST), New Delhi to carryout sponsored research project entitled Development of efficient target tracking algorithms in the presence of ECM. His research interests are radar target tracking, radar waveform design and efficient DSP algorithms for radar applications.

APARNA P is associated with NITK, Surathkal since 2002 under various capacities. She is working as Assistant Professor at NITK, Surathkal since 2008. Her areas of interest are Bio-medical Signal processing, Signal Compression, Computer Architecture and Embedded Systems. She has presented a number of research papers in various International conferences. She has conducted a number of workshops in the area of Embedded systems and ARM processor. She has published more than 25 research papers in various journals and conference proceedings. She has guided two Ph.D student and currently guiding five other research students. Currently, she is working for two RD projects, one of which is under SMDP-VLSI C2SD by Govt Of India and other is by LRDE, DRDO, India. She is actively involved in the research activities in the area of signal processing since 10 years.