DEVELOPMENT OF GPS SPOOFING AND ANTI-SPOOFING ALGORITHMS WITH DATA ASSOCIATION AND TARGET TRACKING FRAMEWORKS

Thesis

Submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

by

BETHI PARDHASARADHI

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA,

SURATHKAL, MANGALORE - 575025

SEPTEMBER 2022

Life changing quotes

The true benefit of thundering arises only when it rains.
– Sri. Bethi Koteswararao

No Association is Better than Wrong Track-to-Measurement Association
– Prof. T. Kirubarajan

DECLARATION

by the Ph.D. Research Scholar

I hereby declare that the Research Thesis entitled **DEVELOPMENT OF GPS SPOOFING AND ANTI-SPOOFING ALGORITHMS WITH DATA ASSOCIATION AND TARGET TRACKING FRAMEWORKS** which is being submitted to the **National Institute of Technology Karnataka, Surathkal** in partial fulfilment of the requirements for the award of the Degree of **Doctor of Philosophy** in **Electronics and Communication Engineering** is a *bonafide report of the research work carried out by me.* The material contained in this Research Thesis has not been submitted to any University or Institution for the award of any degree.

B. Pardha Saradhi

(EC16F02, Bethi Pardhasaradhi)

Department of Electronics and Communication Engineering

Place: NITK, Surathkal.

Date:

CERTIFICATE

This is to *certify* that the Research Thesis entitled **DEVELOPMENT OF GPS SPOOFING AND ANTI-SPOOFING ALGORITHMS WITH DATA ASSOCIATION AND TARGET TRACKING FRAMEWORKS** submitted by **BETHI PARDHASARADHI**, (Register Number: EC16F02) as the record of the research work carried out by him, is *accepted as the Research Thesis submission* in partial fulfilment of the requirements for the award of degree of **Doctor of Philosophy**.

Dr. Pathipati Srihari
Research Guide

Dr. Aparna P
Research Guide

Prof. Ashvini Chaturvedi
Chairman - DRPC

Acknowledgment

My Ph.D study had involved many people in its journey. Foremost I would like to express my sincere gratitude to my research guides **Dr. Pathipati Srihari**, Assistant Professor, Department of Electronics and Communication Engineering (ECE) and **Dr. Aparna P**, Assistant Professor, Department of Electronics and Communication Engineering (ECE), NITK, Surathkal, gave me an opportunity to pursue Ph.D. I greatly acknowledge their invaluable guidance, support and encouragement received throughout my research work. I deeply realize that for me, they are not only research guides who always reminds me to keep on right track, but also people with kind heart and humanity.

I express heartfelt thanks to my Research Progress Assessment Committee (RPAC) members **Prof. Ashvini Chaturvedi**, Professor and Head of the Department, ECE, and **Prof. B Venkatesa Perumal**, Professor in Department of Electrical and Electronics Engineering, for their invaluable suggestions and constant encouragement to improve my research work. I convey my special thanks to Doctoral Thesis Assessment Committee (DTAC) Members **Dr. Prasantha Kumar H**, ECE Dept, and **Prof. Lakshman Nandagiri**, WROE Dept, NITK. My special thanks to **Dr. Abhijit Bhattacharya**, DRDL, Hyderabad, Indian Referee for making his time and conducting the via-voce offline.

I would like to express my sincere gratitude to **Dr. T. Kirubarajan**, Distinguished Engineering Professor, Electrical and Computer Engineering (ECE) Department, McMaster University, Canada, who gave me an opportunity to work as a visiting Ph.D research scholar under his guidance and to be part of his research team at the Estimation, Tracking and Fusion Research Laboratory (ETFLab), McMaster University, Canada, during 2018-19. I greatly acknowledge all his invaluable suggestions, comments and guidance I received, without which I would not have been what I am

today. I also want to thank **Dr. R. Tharmarasa**, Professor, ECE Department, McMaster University, Canada, who wholeheartedly, enthusiastically and immediately accepted for research discussion every time I demand and gave valuable suggestions that put me on the right track. My hearful thanks to **Prof. Linga Reddy Cenkeramaddi**, Department of Information and Communication Technology, University of Agder, Norway, for his motivational words and providing an opportunity to work as a visiting research scholar in his Autonomous and Cyber-Physical Systems (ACPS) research group.

My appreciation goes to all my current and former research group members **Dr. Gnane Swarnadh Satapathi**, **Dr. Raghu J Mandya**, **Mr. Gunnary Srinath**, **Mr. Purushottama T. L.**, **Mrs. Ashok Mahipathi**, **Mr. Bobbili Nagabalarama Reddy**, **Mr. Bodduboina Gopala swamy**, **Mrs. Kumuda D K**, and **Miss. D S L Praharshitha** for their stimulated discussion throughout my stay at NITK. I extend my sincere thanks to all teaching staffs and non-teaching staff of the Department of ECE for their encouragement during my research work.

My special thanks to people **Dr. YVS Murthy, Mr. Gunnery Srinath, Mr. Odisetty Sai Kiran, Smt. Bhamidipati Nagalakshmi, Mr. A. Harish Kumar, Smt. Sowjanya Paila, Smt. Shruti Sharma, and Smt. Kavitha Neelangol**, who taught me the essence of life with their friendship and love.

Finally I express heartfelt thanks to my family and my relatives. Special thanks to my proud parents and brother **Smt. Bethi Venkata Lakshmi**, **Sri. Bethi Koteswararao**, and **Mr. Bethi Sai Phani Surendra** who poured showers of love and affection in addition to proudly sacrificing their entire life to allow me chase my dreams. Your perseverance, desire and blessings have driven me to reach this level with ease. I thank my soulmate **Sarada** for encouraging, providing solid support and standing behind me like a pillar to do everything possible that allows me pursue what I love. I deeply feel that without family members, surely, this research work would not have been possible. I also thank my well wishers, who directly or indirectly are

the reason behind my decision for taking different path rather than job.

Place: Surathkal Bethi Pardhasaradhi

Date:

Abstract

This thesis deals with the spoofing and anti-spoofing techniques in global positioning system (GPS) receivers by using data association and target tracking algorithms. Novel and efficient algorithms have been proposed in this research investigation by using estimation theory and optimization techniques.

Global navigation satellite system (GNSS) is generally used for providing the position, velocity, and time (PVT) for many civilian and military applications. GNSS, such as GPS, Galileo, GLONASS, BeiDou, NavIC, uses a receiver to receive the signals transmitted by the satellites. These received signals are processed to provide the receiver's position with an accuracy of a few meters. However, the recent advancements in radio frequency (RF) generation result in the simulation of various RF signals with inexpensive devices and leads to threats like jamming and spoofing.

The primary objective of this research work is to develop a stealthy GPS spoofer, spoofing techniques, and strategies. The available spoofers in the literature are detected with the simple anti-spoofing algorithms like constellation check (e.g., number of satellites available and software-defined satellite positions), monitoring the power (e.g., absolute, relative, and across satellites), checking the accuracy of clock components, reference monitor (e.g., inertial navigation system (INS), optical sensor, range sensor, bearings sensor), vestigial peak correlation, and verifying code and phase rate consistency. In this research work, we proposed a novel spoofer design, in which the spoofer relies on a target tracker and fusion module to track the motion of the target and spoof effectively. A strategy for the spatial deployment of multiple spoofers is formulated as an optimization problem to combat direction of arrival (DOA) anti-spoofing algorithms. In addition to that, the target kinematic information is used to adaptively change the transmitting powers of the spoofers and effectively combated the anti-spoofing algorithms like monitoring reception of an individual satellite's signal, and power thresholding. Further, distributed fusion of local estimates to improve the effectiveness of GPS spoofing for low-observable targets is proposed. Furthermore, multi-spoofer multi-target (MSMT) based efficient spoofing technique is developed. In distributed spoofing scenario, the spoofers work independently to each other with

out any prior information about number of spoofers and targets within the given surveillance, which results in lower hit ratio. To address this spoofer-to-target association problem, three novel centralized networking-based spoofing techniques are proposed, namely global nearest neighbor (GNN) based centralized spoofing, spoofers of opportunity-based centralized spoofing, and tunable transmitting power-based centralized spoofing. The proposed algorithms provide better hit ratio in comparison to the distributed spoofing.

The second objective of the research is to develop anti-spoofing algorithms for single and multiple GPS receivers. Most of the research works assume that the spoofing signals and the authentic signal attributes are different, and accordingly developed the anti-spoofing algorithms. This research proposed to consider both the authentic GPS and spoofed GPS pseudo measurements into the positioning algorithm and performing the robust positioning with all possible combinations. Further, to efficiently represent the robust positioning algorithm, the M-best positioning algorithm is proposed, which provides only M-best positions at a given epoch. Besides, this work is extended to time-varying targets with the help of Kalman filter and nearest neighbor (NN) data association approaches. The track swapping (TS) is occurring in NN framework due to the hard decision on the track-to-measurement association. This track-to-measurement association problem is resolved with the probabilistic data association (PDA) and attained lesser TS. Furthermore, this problem is extended to multiple GPS receiver problem and proposed an anti-spoofing algorithm by localizing the spoofer. In a clean environment, all the DOA are distinguishable since they are from different satellites. Whereas in spoofing scenario, all the DOAs are from the same direction and hence declared a spoofing attack. This research work proposes to install multiple GNSS receivers (on a target or in the given surveillance) to detect and mitigate the spoofing attack. While installing multiple GNSS receivers, we assume that each GNSS receiver's relative position vector (RPV) is assumed to be known precisely. The installed GNSS receivers use the extended Kalman filter (EKF) framework to estimate its PVT. We proposed to calculate the equivalent-measurement and equivalent-measurement covariance of each GNSS sensor in the Cartesian coordinates in tracklet framework. These tracklets are translated to the target platform center using RPV to obtain translated-tracklets. The generalized likelihood ratio test (GLRT)

based spoofing attack detection is derived at a given epoch using these translated-tracklets. In addition to that, these translated-tracklets are processed in a batch least square (LS) framework to obtain the platform's position. Once the attack is detecting at a specific epoch, it quantifies that the position information is false. Moreover, another detection test is also formulated by using DOA of signals. Once both the tests confirms the spoofing attack, the spoofer localization is performed using pseudo-updated states of GNSS receivers and acquired bearings in the iterative least-squares (ILS) framework. Mitigation of spoofing attack is achieved either by projecting the null beam in the direction of the spoofer or by launching the counter counter-measure on spoofer. The results demonstrate that the proposed algorithm performs detection of spoofing attack and ensures the continuity in navigation track.

The results obtained in this research investigation demonstrates superior performance in the spoofer design. Further, the anti-spoofing approaches proposed in this thesis work are novel and provides improved performance over existing techniques. Furthermore, the contributions made in this thesis incorporated significant domain knowledge in the area of spoofing and anti-spoofing algorithms based on target target and data association.

Contents

List of Figures

List of Tables

Abbreviations and Nomenclature

Abbreviations

2-D	Two-Dimensional
3-D	Three-Dimensional
S-D	S-Dimensional
ADSB	Automatic Dependent Surveillance-Broadcast
AMM	autonomous multiple model
CRLB	Cramar-Rao Lower Bound
CT	Coordinated Turn
CV	Constant Velocity
DOP	Dilution Of Precision
ED	Euclidean Distance
EKF	Extended Kalman Filter
EW	Electronic Warfare
FIM	fisher information matrix
GLRT	generalized likelihood ratio test
GNN	Global Nearest Neighbor
GNSS	Global navigation satellite system
GPB	Generalized Pseudo Bayesian

GPS	Global Positioning System
ID	Identity
ILS	Iterative Least Squares
IMM	Interactive Multiple Model
INS	inertial navigation system
IW	Information Warfare
KF	Kalman Filter
LOS	line of sight
LS	least-squares
MATLAB	MAtrix LABoratory
MC	Monte Carlo
MM	Multiple Model
MSMT	Multiple Spoofer Multiple Target
NIS	normalized innovation square
NN	Nearest Neighbor
PDA	probabilistic data association
PDOA	power difference of arrival
PRMSE	Position Root Mean Square Error
PVT	Position Velocity and Time
RF	Radio Frequency
RPV	relative position vector
RSF	Reduced State Filter

RSS	received signal strength
SCF	Separate Covariance Filter
SLAM	simultaneous localization and mapping
SSST	Single Spoofer Single Target
T2T	Track-to-track
TDOA	time difference of arrival
TS	track swap
UAV	unmanned air vehicle
WGN	White Gaussian Noise
WLS	weighted least square

Nomenclature

$< \cdot >$	Directional cosine
α	Variable parameter for spoofer deployment
β	Association probability
Δf	Doppler
δf_i^s	External doppler offered by the spoofer
δt_i^s	External delay offered by the spoofer
$\mathbf{\Delta x}$	Cartesian shift in fake location from the GPS physical location
$\delta \mathbf{x}$	Cartesian shift of GPS physical location from the assumed center of body
ϵ	Acceptable error
η	Binary variable

$\Gamma(\cdot)$	Noise gain matrix
$\hat{\mathbf{e}}(\cdot)$	Error vector
$\hat{\mathbf{p}}(\cdot)$	Measurement prediction vector
λ	Number of false alarms
$\Lambda(\cdot)$	Likelihood function
$\mathbb{R}^3$	Three dimensional Cartesian space
$\mathcal{H}$	Hypothesis
$\mathcal{N}$	Gaussian pdf
$\mathcal{P}$	probability mass function of Poisson distribution
$\mathcal{S}$	Spoofer set
$\mathcal{T}$	Target set
$\mathcal{X}$	Satellite set
$\lvert \cdot \rvert$	Euclidean operator
μ	Mixing probability
ω	Turn rate
Ω	right ascension of circular orbit
ϕ_a	Azimuth measurement
ϕ_e	Elevation measurement
π	Transition probability matrix
$\psi(\cdot)$	Navigation signal
ρ	Range measurement
ρ_i	Geometrical range between satellite i and GPS receiver

σ	Standard deviation
τ_i^{Rx-Tx}	Transmission delay within spoofer
$\mathbf{b}(\cdot)$	Bias vector
$\mathbf{F}(\cdot)$	State transition matrix
$\mathbf{F}_{CT}$	Constant turn state transition matrix
$\mathbf{F}_{CV}$	Constant velocity state transition matrix
$\mathbf{G}(\cdot)$	Gain matrix
$\mathbf{H}(\cdot)$	Linearized measurement transition matrix
$\mathbf{I}$	Identity matrix
$\mathbf{M}$	Equivalent measurement covariance matrix
$\mathbf{m}$	Equivalent measurement state vector
$\mathbf{O}$	zero matrix
$\mathbf{P}(\cdot)$	State covariance matrix
$\mathbf{p}(\cdot)$	Pseudorange measurement vector
$\mathbf{Q}(\cdot)$	Process noise covariance matrix
$\mathbf{R}(\cdot)$	Measurement noise covariance matrix
$\mathbf{r}(\cdot)$	Residual vector
$\mathbf{R_x}$	Equivalent measurement covariance corresponding to position
$\mathbf{S}(\cdot)$	Measurement residual covariance
$\mathbf{v}(\cdot)$	Process noise vector
$\mathbf{w}(\cdot)$	Measurement noise vector
$\mathbf{x} = [x, y, z]'$	Location vector in Cartesian space

$\mathbf{x}_j^f = [x_j^f, y_j^f, z_j^f]'$ Fake location vector of GPS receiver j

$\mathbf{x}_i^g = [x_i^g, y_i^g, z_i^g]'$ i^{th} GPS satellite location vector

$\mathbf{x}_j^r = [x_j^r, y_j^r, z_j^r]'$ Real location vector of GPS receiver j

$\mathbf{x}_m^s = [x_m^s, y_m^s, z_m^s]'$ m^{th} spoofer location vector

$\mathbf{x}^{r*}$ Perception of the GPS location vector (either true or false)

$\mathbf{x}_i^{\text{ref}}$ Reference satellite location

$\mathbf{Y}$ Set of measurements obtained from S scans of radar

$\mathbf{y}_q(k)$ q^{th} measurement vector of radar at scan k

$\mathbf{z}_{\mathbf{x}}$ Equivalent measurement corresponding to position

Θ Angular phase in the circular orbit

θ Arctan angel

ς Gating threshold

ξ Binary variable

ζ Sensor

a Acceleration

$A_{i,j}$ Received signal amplitude at GPS receiver j due to source i

b Bias due to clock

c Speed of light

D Radius of WGS-84 circular orbit

$d_{m,j}^{s,r}$ Distance between spoofer m and target j

f Fake target

$f(\cdot)$ State non-linear function

g	GPS satellite
$h(\cdot)$	Measurement non-linear function
I	Number of satellites
i	Satellite index
J	Number of targets
j	Target index
K	Total number of pseudorange measurements
k	Discrete time index
L	Total number of pseudorange measurements selected
l	Arbitrary index
M	Number of spoofers
m	Spoofer index
M_{conf}	Number of measurement frames associated for track conformation
M_{init}	Number of measurement frames associated for track initialization
M_{tent}	Number of measurement frames associated for tentative track
N	Number of filters in IMM filter
$n(\cdot)$	Signal background noise
n_x	Dimensions of the parameter vector
n_y	Dimensions of the measurement vector
N_{conf}	Number of measurement frames for track conformation
N_{init}	Number of measurement frames for track initialization
N_{tent}	Number of measurement frames for tentative track

$p(\cdot)$	Probability
P_D	Detection probability of a target
$p_F[\cdot]$	probability density function of measurement due to false alarm
$p_T[\cdot]$	probability density function of measurement due to target
P^r_{Rx}	Received power of the spoofing signal at the GPS receiver
P^s_{Rx}	Transmitted power of the spoofing signal at the spoofer
$p^f_{j,i}$	Fake Pseudorange measurement at GPS receiver j due to satellite i
$p^r_{j,i}$	True pseudorange measurement at GPS receiver j due to satellite i
$p^s_{m,i}$	Pseudorange measurement at spoofer m due to satellite i
q	Radar measurement index at a given scan
r	Real target
S	Total number of scans
s	Spoofer
T	Time duration
t	Time
U	Number of iterations
u	Iteration index
V	Volume of the radar surveillance
v	Velocity
$w(\cdot)$	Measurement noise

Chapter 1

Introduction

1.1 GPS Background

1.1.1 GPS

Global positioning System (GPS) is a satellite-based navigation system with coverage over the globe and allows any user to access position, velocity, and timing (PVT) information. GPS-based navigation is safest, low-cost, and efficient for all applications. It attains widespread impact in many applications, including navigation of ships in the ocean, automated vehicles, aircraft location, phasor measurement units (PMU), and handsets. GPS consists of three subsystems, namely

- **Space (Satellite system)**: In this segment, satellites are placed in constellation orbits to broadcast position, time, and message signals to the ground control units and users.

- **User (GPS receivers)**: The location, time, and message are determined by the received signal from the satellite constellation.

- **Ground Control unit**: This subsection helps to monitor satellite health, control of satellites, and update each satellite's information.

The GPS provides mainly two services namely standard position service (SPS) and precision position service (PPS). The GPS receiver estimation its PVT using acquired pseudorange measurements.

1.1.2 GPS Interference

A Unintentional Interference

This interference is widely spread due to the Radio Frequency (RF) interference in an electronic circuits to disrupt the receiver. The harmonics of digital video broadcasting terrestrial (DVBT), multi-path reflections, terrestrial reflectors are few unintentional interferences to affect the pseudo measurements.

B Intentional Interference

Jamming and spoofing are the intentional interference caused by the specialized equipment to deceive the actual GPS receiver. Jamming is a process in which a jammer device generates radio frequency (RF) signals to completely deny the positioning information of the GPS receiver. 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 to deceive the PVT. Once the target computes the PVT using the fake pseudoranges, it results in fake location even though the target is physically located at true location.

Some terminology

- **Target**: A moving or stationary object (ex. a GPS assisted vehicle).
- **Satellite**: An authentic source of GPS signals.
- **True pseudoranges**: The pseudorange measurements due to authentic satellite signals.
- **True location**: Estimated location of a target due to authentic GPS signals (typically estimated position gives less accuracy than three meters).
- **Spoofer**: A spurious source to generate mimic GPS like signals (ex. simulator, meaconer, repeater, and transponder).
- **Fake pseudoranges**: The pseudorange measurements due to spurious source.

- **Fake location**: Estimated location of a target due to false GPS signals (typically estimated position accuracy is tens or hundreds of meters).

1.1.3 Motivation

The deceiving of GPS receiver by false GPS measurements is called as GPS spoofing. The primary intention behind this spoofing is to misguide a vehicle concerning position, velocity and timing information. The spoofed measurements are capable of deceiving the receiver to estimate the false state and leads to hazard attacks. The concept of GPS spoofing was first reported in December 2011 by capturing Lockheed RQ-170 drone aircraft in northeastern Iran (Peterson and Faramarzi 2011). But it takes few years to prove practical possibility by misguiding a luxury yacht "White Rose" in June 2013 by aerospace group Cockrell School of Engineering at the University of Texas in Austin (Saarinen 2013). Recently, On June 2017, twenty ships in Black sea complained of GPS spoofing stating that the cargo ships are showing miles away from the actual location and caused maritime traffic (Foote 2017). A detailed report by Prof. Todd Humphreys confirmed that GPS navigation system was affected by spoofing. However, malicious spoofing attacks are not yet recorded anywhere regarding the threat to civilian and military services to destroy the relationship between the countries. However, it is not far due to the aggressive development of spoofers and spoofing attacks in the rapidly increasing science. Hence, there is a considerable research gap to develop efficient alternative techniques to detect the spoofing, secure own vehicle navigation, and countermeasures to spoofer.

1.1.4 Types of Spoofers

A Simulator based spoofer

In an open-loop simulator, the EM signals are generating based on the historical knowledge of signal, parameters associated with the signal, type of target, and working GPS constellation in the given field of view. This system is non-reactive (i.e., no receiver is associated with the spoofer to provide input information). The available standalone commercial spoofers are GPS signal simulators that radiate the RF signal with boosted power towards the target. The spoofed signals generated by the simulator are asynchronous with legitimated GPS signals in its vicinity due to lack of time

and Doppler off-set. This configuration was coined in literature as a non-coherent superposition, asynchronous spoofing attack, hard takeover, power takeover, etc. This asynchronous attack leads to failure in locking the authentic signals and causes reacquisition. Hence, this configuration is more likely suitable when the receiver has not yet acquired the legitimated satellite signals or lost track. Sometimes, the disruption of the existing track loop occurs due to the higher power of the spoofed signals. This suspicious reacquisition rise to spoofing attack but lacks to give desired spoofed position, velocity, and time. However, sometimes results in suspicious position and velocity.

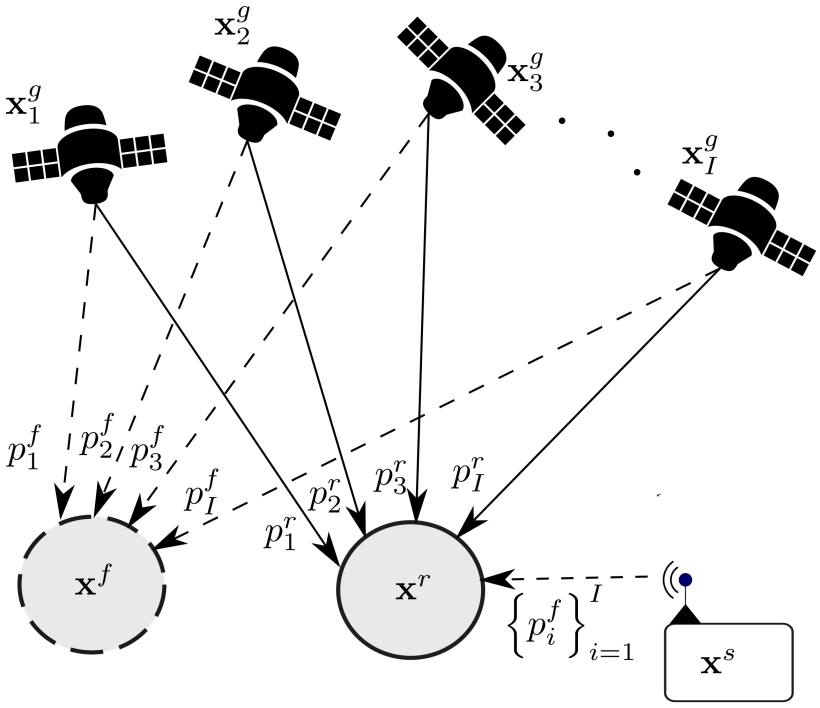

Figure 1.1: GPS simulator based spoofing.

Consider a single spoofer intended to mislead a single targeted GPS receiver. In spoofing attacks, spurious GPS signals are either generated by a simulator or playback the received signals at a different time for manipulating the targeted receiver's PVT. The spoofer located at $\mathbf{x}^s$ and its position is known precisely. Whereas, the target (vehicle) located at $\mathbf{x}^r$ and relies on the GPS receiver for estimating its own location. In a given satellite constellation, I active satellites are being located at $\{\mathbf{x}_i^g\}_{i=1}^{I}$. In a clean environment without spoofer, the target receives $\{p_i^r\}_{i=1}^{I}$ measurements from authentic satellites and estimates its location as $\hat{\mathbf{x}}^r$. Spoofer intends to create a spoof

position $\mathbf{x}^f$, which is estimated due to spoof measurement set $\left\{p_i^f\right\}_{i=1}^{I}$ for the target being located at $\mathbf{x}^r$ as shown in Figure 1.1. Dark lines represent authentic satellite signals and dotted lines represent spoofed satellite signals. During the spoofing attack, the targeted GPS receives two sets of measurements $\left\{p_i^r, p_i^f\right\}_{i=1}^{I}$, and the receiver generally locked onto measurements with the higher power. Since spoofed signals maintain high power, the receiver is more likely to lock $\left\{p_i^f\right\}_{i=1}^{I}$ measurements and inturn state estimation results to $\mathbf{x}^f$ even though the actual location is $\mathbf{x}^r$ as shown in Figure 1.1.

B Repeater based spoofer

These systems contain a receiver module to receive signals directly from satellites. The spoofer captures authentic satellite signals, amplifies, analyzes, modifies the delays, and retransmits it. The transmitting signals are called spoofed signals, directs towards the target to avoid spatial interferences. As shown in the Figure 1.2, initially, the repeater receives the authentic satellite $\{p_i^s\}_{i=1}^{I}$ and process them to form a spoofed signals. Dark lines represent authentic satellite signals and dotted lines represent spoofed satellite signals. The repeaters contain digital RF memory (DRFM) module to digitalizes the received signal, RAM, to store it. The type of technique, the distance between the target to spoofer d determines the memory: analog memories can achieve few microseconds of delay while longer delays require the digital memory. The playback of the signal creates a variety of deceptive position and velocity estimates to the target. This configuration can synchronize its signals to GPS time and proximity to the target antenna. An attack via receiver-analyze-delay-transmit could be hard to detect by techniques like synchronization, constellation, signal properties. The only known countermeasure that would be completely effective against an attack launched from a repeater with a single transmitting antenna is angle-of-arrival discrimination.

C Hardware Injection

There is no signal receive and transmission process in hardware injection since the signal combines with the receiver hardware. This configuration comes under a cooperative spoofing scenario where the target user wants to manipulate the position to

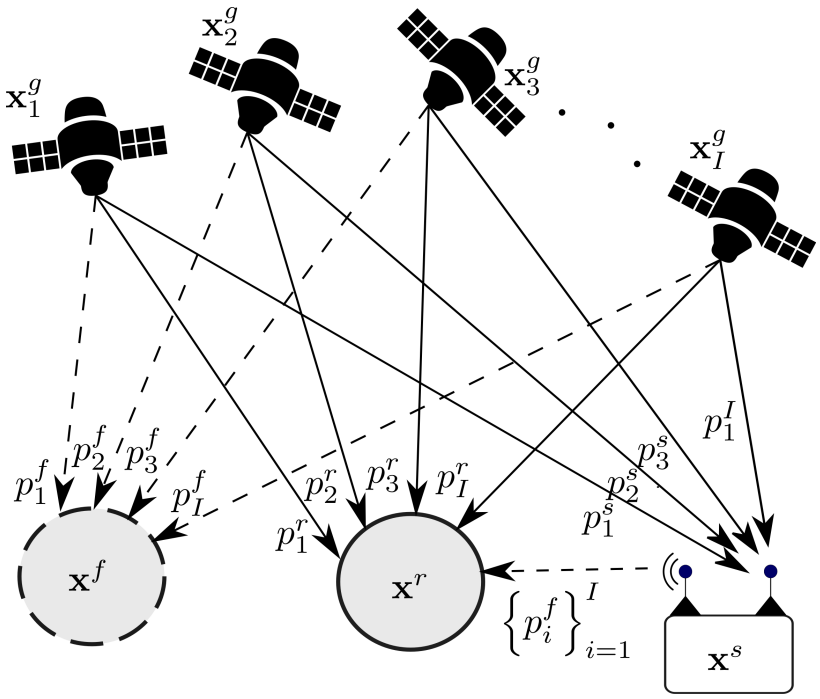

Figure 1.2: Repeater based GPS spoofing

misreport the PVT. This kind of attack is commonly useful in misreporting a vehicle or a vessel to a tracking base station.

1.1.5 Spoofer Operating Location

The spoofer systems are categorized based on the operating location of the spoofer concerning the target.

A On-board

In this case, the spoofer is placed on board the platform of the target to be spoofed. Here, the distance between spoofer and target is very less or negligible. All the three systems suits for this operating location. Whereas, on-board operating location and hardware system is not possible for security-critical applications.

B Stand-off

The spoofers operating location is far away from the target due to localization-based security and visibility-based countermeasures. Here, the distance between spoofer and target is unknown and calculated with radar or other devices. This operating location suits for military applications like spoofing the canons, cruise missile ships, airborne

crafts.

C Escort or Stand-in

The spoofers operating location is near the target and the distance between target and spoofer is very much aware. There are no countermeasures from the target. This operating location is very successful in literature by keeping spoofer at a fixed distance (d = 1-2m) from the target. The experimental evaluations are given for this configuration in the literature.

D Distributed

Several spoofers work together to spoof the target location. This configuration needs an established communication channel between the spoofers for maintaining the synchronization and strategy. This operating location is successful for military applications. The advantage is that it cannot be detected by DOA estimation by adequately planning the spoofer's spatial deployment. This configuration is more attentive in the scenario where any one of the system failures can happen. The spatial deployment in the field of a target is more efficient to countermeasure spatial mitigation capability of the target, and spatial interferences among targets.

1.1.6 Target to Spoofer Understanding

This section reveals the relation of Target (target user) and spoofer.

A Non-cooperative

In this scenario, the target is unaware of the spoofer and always try not to get into a spoofing attack. Here, the spoofer wishes to impose the false trajectory on the target to mislead and navigate towards threat (unwanted destination). The target is not cooperative to the spoofer, and countermeasure techniques are incorporated in the target to avoid spoofing.

B Cooperative

In this scenario, the target user intended to get into the spoofing effect. The user carries both target and the spoofer to carry out successful spoofing. The scenarios like misreporting positions of the target (trucks or cars) to the base stations (track

monitoring stations) to witness target reach the destination or within a given region are the critical examples.

1.1.7 Spoofing Techniques

This section presents two spoofing techniques, namely detection denial, and track break. Detection and acquisition denial techniques lead to denying the target receiver from detecting the authentic signals or acquiring the pseudo measurements for initializing the track. Whereas, the track break techniques are which gives the consistent false detections or false trajectory to mislead the track. Noise and false targets are the detection denial and acquisition techniques, whereas the position gate pull-off and velocity gate pull-off are suitable candidates for track break. Detection denial techniques are typically suitable for targets ready to start or static targets without track initialization. Track break techniques are suitable for dynamic targets. The perception of the target receiver is given by $\mathbf{x}^{r*}$.

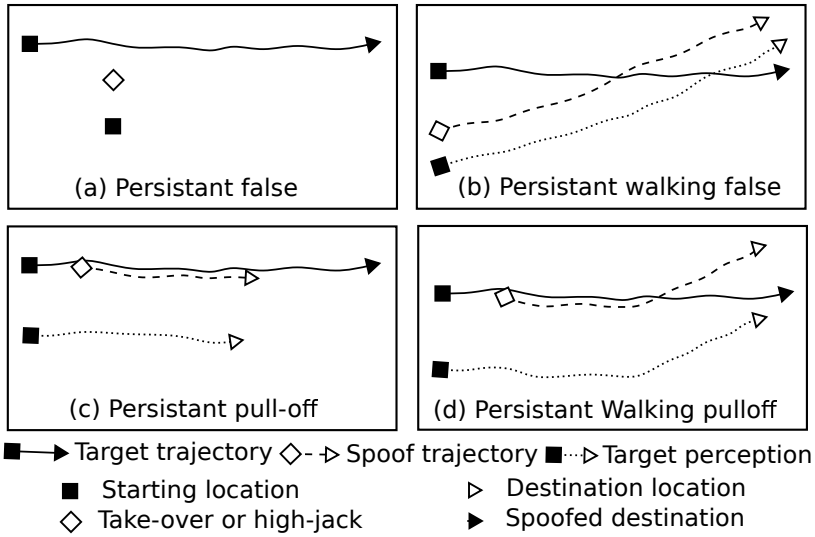

Figure 1.3: Various spoofing techniques to perform the position false target and position gate pull-off

A Position Denial Using Noise

Noise is a fundamental spoofing technique in which the spoofer puts energy into the receiver for all times, making it difficult to detect the authentic satellite signals. In another way, the noise is useful to cover the nearby frequencies of the RF receiver,

making the receiver challenging to acquire the signals. Here noise is position and Doppler denial technique because the spoofer prevents the receiver from acquiring the desired measurements. Open-loop simulator or hardware injection configurations can quickly implement this technique. The choice of operating location is on-board or stand-off or escort. By using distributed simulators, the spatial processing based anti-spoofing algorithms fail to detect the spoofing. However, this kind of spoofing or jamming can be successfully pretended by the target receiver by using signal processing techniques.

B Position and Velocity False Target

The false positioning and velocities are useful to confuse the target, especially during the acquisition of the tracking loop or initialization of track. The position and velocity false target techniques useful depending on the type of target to be attacked. Further, the placement of a false target from one sample to sample implemented in different ways. The false pseudorange generation by a spoofer is of the form

$$p_i^{r*} = p_i^s + c\delta_i^s \tag{1.1}$$

Where δ_i^s is the external delay incorporated by the spoofer. Here, p_i^s represents the pseudoranges received by the spoofer. Here, the target position for the next sample is related to the current sample. One form is a persistent false target (i.e., the receiver perception remains at the same position over one sample of time, as shown in Figure 1.3(a) $\mathbf{x}_{k+1}^{r*} = \mathbf{x}^{r*}$. If $\mathbf{x}_k^{r*}$ is the estimated position at k^{th} discrete time due to pseudorange set p^{r*}, then the position on the $k+1$ sample is given by

$$\mathbf{x}_{k+1}^{r*} = \mathbf{x}_k^{r*} \pm v(t_{k+1} - t_k) \tag{1.2}$$

Where v is the velocity of the false target. The target is in perception that it is walking in a given direction with linear walking, as shown in Figure 1.3(b) for any value of v rather than zero. Similarly, the false Doppler frequencies are given by

$$\Delta f_i^{r*} = \Delta f_i^r + \delta f_i^s \tag{1.3}$$

The selection of Doppler frequency from the sample to the next sample can be programmed depending on the persistent stationery or persistent walking. For persistent

stationary target $v_{k+1}^{r*} = v_k^{r*}$. For a linear walking false target

$$v_{k+1}^{r*} = v_k^{r*} \pm a(t_{k+1} - t_k) \tag{1.4}$$

where a is the acceleration, the nonlinear walking models can also be possible by changing the v and a in the above equations.

C Position Gate Pull-off

The goal of position pull-off is to generate spoofed measurements such that it replicates the target position or coincides with the position for a long time. As time progresses, the spoofer generates measurements in such a fashion to separate the target from the planned path with any realistic trajectory models. As time progresses, the physical location of the target is different from the perception of the target. The spoof target moves away from the actual target position, and at some time, the target can be terminated or hacked. Initially, the target's physical location is $\mathbf{x}_k^r$, the desired false target position to be generated as an actual target for some duration of time T. After that, the false target moves away from the target as walking.

$$\mathbf{x}_k^{r*} = \begin{cases} \mathbf{x}_k^r & ;\ t_k \leq t_o + T \\ \mathbf{x}_{k-1}^{r*} + v(t_k - t_{k-1}) & ;\ t_k > t_o + T \end{cases} \tag{1.5}$$

For value of $v = 0$, the target is in perception that it stopped at $t_o + T$ as shown in Figure 1.3(c). Whereas for a suitable choice of velocity, the target is in the perception of walking, as shown in Figure 1.3(d).

D Velocity Gate Pull-off

The concept of velocity gate pull-off is similar to the position gate pull-off. A false Doppler measurements replicate the target velocity for a specific duration of time, and then the velocity follows the stationary or walking models depend on the application. The velocity gate pull-off can be modeled as

$$v_k^{r*} = \begin{cases} v_k^r & ;\ t_k \leq t_o + T \\ v_{k-1}^{r*} + a(t_k - t_{k-1}) & ;\ t_k > t_o + T \end{cases} \tag{1.6}$$

1.1.8 Satellite Trajectories Modeling-WGS84

The satellite location set $\{\mathbf{x}_i^g\}_{i=1}^N$ WGS-84 model follows the assumption of circular orbits as

$$\begin{aligned} x^g(t) &= D\left[\cos\Theta(t)\cos\Omega(t) - \sin\Theta(t)\sin\Omega(t)\cos 55^o\right] \\ y^g(t) &= D\left[\cos\Theta(t)\sin\Omega(t) + \sin\Theta(t)\cos\Omega(t)\cos 55^o\right] \\ z^g(t) &= D\sin\theta(t)\sin 55^o. \end{aligned} \tag{1.7}$$

Here D is the radius (D = 26,560 Km) of circular orbit, Ω and Θ are right ascension and angular phase in the circular orbit respectively.

$$\begin{aligned} \Omega(t) &= \Omega(0) - (t - t(0))\left(\frac{360}{86164}\right)^o \\ \Theta(t) &= \Theta(0) + (t - t(0))\left(\frac{360}{43082}\right)^o \end{aligned} \tag{1.8}$$

The true satellite positions are collected at $t(0)$ instant, processed and re-transmitted at the same instant. The initial positions of the satellite are given in Table 1.1

Table 1.1: The satellite initial positions (angles $\Theta(0)$ and $\Omega(0)$)

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

1.2 Target Tracking Background

1.2.1 Estimation and Tracking

Estimation is the process of inferring the value of a quantity of interest from noisy data or observations. That is, estimation can be viewed as the process of selection of a point out of continuous space. The quantity of interest could be state of dynamic systems which is usually a vector consisting of kinematic and feature related information. Tracking is the estimation of the state of an object in motion. To be precise, tracking is the processing of measurements or observations obtained from targets of interest so as to maintain their present state. This state typically consists of the followings:

- Kinematic components such as position, velocity, acceleration, turn rate, etc.
- Feature components such as radiated signal strength, radar cross-section, target classification, etc.
- Constant or slowly varying parameters such as aerodynamic parameters etc.

Data or measurements are noise-corrupted observations related to the state of a target. These observation could be: range, azimuth and elevation; bearing only from the sensor; range rate (Doppler); time difference of arrival, direction of arrival etc.

Some terminology

- **Target**: A moving or stationary object (ex. car or airplane).
- **Sensor**: Device that observes the environment by reception of some signals (ex. radar or sonar or lidar).
- **Time stamp**: The time to which a detection pertains.
- **Observation**: refers to acquired measurements at sensor (ex. range, azimuth are measurements of 2D radar sensor).
- **State**: refers to stacked parameters of interest pertaining to target (ex. position, velocity, and acceleration)

1.3 Literature Review

1.3.1 GPS Spoofing - Spoofer Design

Different types of spoofers and spoofing strategies are proposed in the literature (Humphreys et al. 2008, Bian et al. 2017). The literature regarding spoofer development and spoofing strategies is minimal due to the following reasons.

- The professional obligation to development of electronic warfare (EW) devices that impose a threat to society
- 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 (Kerns et al. 2014, Warner et al. 2002, Bhatti and Humphreys 2017). The mathematical framework was derived for single-spoofer single-target (SSST) scenario and practically misled the trajectory of UAV (Kerns et al. 2014). In simulator-based spoofing, the spurious signals are generated with the historical knowledge of the legitimate GPS signals (Kerns et al. 2014). 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 (Bian et al. 2017). 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 (Bonebrake and Ross O'Neil 2014). 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. 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 (Bhatti and Humphreys 2017).

In traditional spoofing, spoofer is very near to the spoofed to carryout the spoofing Warner et al. [2002]. However in the real time applications like spoofing an aircraft or drone Tanil et al. [2018], Kerns et al. [2014], it is not possible to the spoofer to maintain the constant distance. The stealthy GPS spoofing of an aircraft is possible only in the scenario of precise estimation of target state and it is hard to mitigate using GPS/INU combinations Tanil et al. [2018]. The stealthy spoofers should estimate the kinematics of the targets and accordingly generate the spoof signals. However in Kerns et al. [2014], uses a GPB2 tracker to track the kinematics of the UAV to successfully manipulate the trajectory. There is a strong need of precise sensors for detecting the target and trackers to estimate the state of the target. The sensors (radar) receive measurements from potential targets in the surveillance region, each with a number of detections, not necessary equal to the number of targets. The source can be a real target, in which case the measurements are assumed to be a function of target state and the additive measurement noise, or a false alarm. In multiple spoofer case, the problem is modified as the multi sensor multi target state estimation problem with association and estimation. Association is the process of linking

the observations and the linked observations are filtered with estimation. In real time, the sensors produce wide range of measurements with different detection probability and false alarm rate. Hence, sophisticated trackers should be employed in the spoofer design to work for wide conditions of measurements origin uncertainty.

In most research works, SSST scenarios have been considered, and the spoofing process is carried out in open space or via optical cables (Bhatti and Humphreys 2017, Humphreys et al. 2008, Tippenhauer et al. 2011). However, it is hard to expect a single target with a clean environment to carry out the spoofing process in real-time. The impact of Omni-directional spoofer on multiple targets and impact of multiple spoofers on a single target is theoretically presented in (Tippenhauer et al. 2011). 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:

- All the targets get affected by the spoofing by using the Omni-directional antenna.
- Due to spoofers' nearby deployment, there is highly likely that multiple spoofers target the same receiver.
- 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 (Wesson et al. 2017, Fan et al. 2017, Manfredini 2017, Wesson et al. 2012, Ledvina et al. 2010, Meurer et al. 2012, Daneshmand et al. 2012, Hu et al. 2018, Kang et al. 2017, Swaszek et al. 2014, Humphreys 2013, Tanil et al. 2018) 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.

1.3.2 GPS Anti-spoofing

Comprehensive survey of anti-spoofing techniques has been presented in (Jafarnia-Jahromi et al. 2012, Günther 2014, Schmidt et al. 2016, Psiaki and Humphreys 2016).

Spoofing attack detection is achieved by signal monitoring techniques like software-defined positioning, monitoring the power, checking the clock, code, and phase consistency rate (Wesson et al. 2017). 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 (Fan et al. 2017, Manfredini 2017). 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 (Wesson et al. 2012, Ledvina et al. 2010). 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 (Meurer et al. 2012, Daneshmand et al. 2012, Hu et al. 2018). The spatial processing techniques include the direction of arrival discrimination multiple antennas or a single antenna with multiple feeds or oscillatory motions (Kang et al. 2017). 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 (Swaszek et al. 2014, Humphreys 2013, Tanil et al. 2018). Besides these techniques, there are spatial processing and navigation track-based anti-spoofing techniques (Psiaki et al. 2013). The spatial processing techniques include the direction of arrival (DOA) discrimination, using multiple antennas, by applying spatial diversity (Kang et al. 2017). Further, in (Milaat and Liu 2018), the exchange of measured GPS code based pseudoranges with neighboring vehicles (by using dedicated short-range communications) has been suggested to safeguard the vehicle from spoofing. In addition, the inertial sensor-based anti-spoofing techniques are proposed in (Liu et al. 2019). The range sensors, bearing sensors, and vision sensors are integrated to generate efficient anti-spoofing algorithms and are introduced in (Swaszek et al. 2014). Furthermore, the unknown sudden changes in system state variables are addressed in (Majidi et al.

2020). Managing the simultaneous localization and mapping (SLAM) and sensor fusion capabilities are presented in (Galar et al. 2020). The information of each vehicle's position and their relative distances are incorporated to effectively counter the spoofing and achieving the desired group performance has been suggested in (Ju et al. 2020).

In all the above contributions of autonomous vehicle positioning in GPS spoofing environment (Tayeb et al. 2017, Milaat and Liu 2018, Majidi et al. 2020, Galar et al. 2020, Ju et al. 2020), either authentication of signals or communication among the vehicles is applied to either detect the spoofing or secure the navigation track. Further, multiple vehicles and communications among them are seldom present in practical situations. Moreover, huge buildings and other man-made structures in the urban environment may create low observability of satellites. The majority of contributions reviewed so far reveal that most of the spoofing literature focus on detecting a spoofing attack. Since alleviating measures of this spoofing effect has been scarcely addressed in recent contributions, there is a need to develop mitigating methods with equal importance to GPS receiver design. Accordingly, the proposed work is motivated to investigate novel techniques and algorithms, to alleviate spoofing consequences, without altering / re-designing GPS receiver architecture. Hence, there is a strong requirement to develop an algorithm that should address the problem of a single GPS receiver in the low observable case, which can effectively counter the GPS spoofing.

The spurious attack mitigation can be carryout by localizing the source or null beam projection in the direction of spurious signals. The time difference of arrival (TDOA) method is explored in (Zhang and Zhan 2016) to detect the spoofing effect and localizing the source based on the fact that signals that are coming from the same source possess exact time. Similarly, the localization of jammer is also addressed with the TDOA in (Bhatti et al. 2012). The jamming localization problem is solved by rotating the UAV at multiple fixed positions to get the antenna gain pattern and estimate the strength and bearings (Perkins et al. 2015). In addition, based on the received signal strength (RSS) based measurements with networked receivers to localize the jammers is contributed in (Diana et al. 2013). Simultaneous localization of jammer and target with power difference of arrival (PDOA), and graph theory is jointly applied to accomplish desired performance (Bhamidipati and Gao

2019). Moreover, meaconer localization problem is addressed with the help of space-time double-difference models in (Shang et al. 2020). Furthermore, the localization of spoofer using a large-scale air traffic surveillance system is presented in (Jansen et al. 2017). The localization of spoofer is also explored by using a vehicle-to-vehicle communication in (Sanders and Wang 2020). In these contributions, the TDOA and PDOA measurements are not being influenced by the spurious sources (estimated position of the GNSS receiver) to solve the localization problem. Whereas in the case of localization with the help of direction of arrival measurements, the target position estimation is also a function of fake position in the presence of intensional interference. Hence, the localization performance degrades.

1.4 Objectives

Based on the research gaps identified from the literature review, the research problem has been identified. The objectives are achieving the stealthy spoofing by modifying the existing spoofer design, spoofing strategies. Another important research gap is to develop a novel anti-spoofing algorithms without any attribute information. The proposed algorithms should be equally adapted to multi-spoofer multi-target target scenario. The four objectives are

1. To develop stealthy GPS spoofer and strategies to counter-countermeasure the existing anti-spoofing state of arts.

2. To develop stealthy GPS spoofing algorithms in multi-spoofer multi-target environment.

3. To propose efficient anti-spoofing algorithms to detect and mitigate the GPS spoofing in single receiver configuration.

4. To propose efficient anti-spoofing algorithms to detect and mitigate the GPS spoofing in multiple receiver configuration.

1.5 Proposed Approaches for Each Identified Research Objective

1.5.1 Stealthy GPS Spoofing - Single-spoofer Single-target

A block-level design for a repeater based GPS spoofer is proposed in which the spoof trajectory is generated using the current satellite constellation and nullifying offset bias mechanism to counter-countermeasure the signal processing based anti-spoofing techniques like constellation check, power thresholding, offset and time synchronization. Unlike the traditional GPS spoofers, the proposed spoofer is taking the advantage of embedding target tracker in the spoofer design to track the target on which the GPS receiver is mounted, spoofer capable of operating from any operating location. The spatial deployment of multiple spoofers explored, the distributed spoofer configuration is capable of counter-countermeasure the DOA based anti-spoofing. In distributed spoofing, centralized fusion performed by fusing the estimates from the inbuilt trackers of individual spoofer to address the GPS spoofing accuracy for low detection probability (PD) targets. The spoofing performance is achieved by employing interactive multiple mode filter (IMM) and position pull-off strategy.

1.5.2 Stealthy GPS Spoofing - Multi-spoofer Multi-target

Traditionally, in distributed spoofers, the multiple spoofers in the surveillance region work independently without knowing other spoofers being installed. Because of the independent spoofer-to-target association, the spoofed signals lock onto other targets rather than intended targets and eventually results in a lower hit ratio. Multiple spoofers deployment and its management are optimal for misguiding the multiple GPS receivers in the given surveillance. This thesis presents a generalized mathematical model for the multi-spoofer multi-target 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 observe that the tunable power-based spoofing is an optimal way to realize the MSMT with the given number of spoofers.

1.5.3 Anti-spoofing - Single Receiver

This thesis presents a robust positioning algorithm, followed by a track filter, to mitigate the effects of spoofing. It is proposed to accept the authentic GPS signals and spoofed GPS signals into the positioning algorithm and perform the robust positioning with all possible combinations of authentic and spoofed pseudorange measurements. The pseudorange positioning algorithm is accomplished using an iterative least squares (ILS). Further, to efficiently represent the robust algorithm, the M-best position algorithm is proposed, in which a likelihood-based cost function optimizes the positions and only provides M-best positions at a given epoch. However, during robust positioning, the positions evolved due to spoofed pseudorange measurements are removed to overcome GPS spoofing. In order to remove the fake positions being evolved owing to wrong measurement associations in the ILS, a gating technique is applied within the Kalman filter (KF) framework. The navigation filter is a three-dimensional KF with a constant velocity (CV) model, all the position estimates evolved at a specific epoch are observations. Besides, to enhance this technique's performance, the track to position association is performed by using two data association algorithms: nearest neighbor (NN) and probabilistic data association (PDA). Simulations are carried out for GPS receiver positioning by injecting different combinations of spoofed signals into the receiver. The proposed algorithm's efficiency is given by a success rate metric (defined as the navigation track to follow the true trajectory rather than spoofing

trajectory) and position root mean square error (PRMSE).

1.5.4 Anti-spoofing - Multiple Receiver

This thesis proposes installing multiple GNSS receivers (on a target or in the given surveillance) to detect, localize, and track the intensional interference source. While installing multiple GNSS receivers, we assume that each GNSS receiver's relative position vector (RPV) is assumed to be known precisely. The installed GNSS sensors use the extended Kalman filter (EKF) framework to estimate their state. We proposed to calculate the pseudo-measurement and pseudo-measurement covariance of each GNSS sensor in the Cartesian coordinate frame using the tracklets. Once the tracklets are computed, these tracklets are translated to the target platform center using RPV to obtain translated-pseudo-measurement. The generalized likelihood ratio test (GLRT) based attack detection is derived at a given epoch using these translated-pseudo-measurements. Once the attack is detected at a specific epoch, it quantifies that the position information is falsified. Thereafter, the updated state of the EKF at a given epoch is discarded and replaced with the pseudo update state by using the last updated epoch information of the EKF. The localization of the source is performed jointly with the pseudo-update information and acquired bearings using the ILS framework. A spoofer is considered to demonstrate the effectiveness of the proposed algorithm of detection and localization of the intensional interference source. The results demonstrate that the proposed algorithm perform both detection and mitigation of the spoofing effect. It is evident from the results that the proposed pseudo-track updation technique gives better track compared to traditional track updation.

1.6 Contribution of the Thesis

In this thesis, some of the important problems that are associated with spoofer design, multi-spoofer multi-target environment, anti-spoofing are identified and addressed these issues using multiple proposed solutions. The key contributions of the thesis are as follows:

1. Proposed a target tracker assisted GPS spoofer design to counter-countermeasure

the existing anti-spoofing state-of-arts.

2. Presented novel assignment algorithms to address the problem of multi-spoofer multi-target association.

3. Suggested an M-best association and target tracking to detect and mitigate the spoofing attack in a single receiver configuration.

4. Proposed Tracklets and spoofer localization to detect and mitigate the spoofing attack in a multiple receiver configuration.

1.7 Overview

The rest of the thesis is organized as follows. The Chapter 2 presents the stealthy GPS spoofing in a single spoofer single target scenario. This chapter proposes the types of spoofers, spoofing strategies and techniques, tracker assisted GPS spoofer, power tunability, spatial deployment, and fusion for enhanced spoofing. The Chapter 3 dealt with multi-spoofer multi-target association, provides three novel spoofer-to-target association algorithms namely global nearest neighbor based centralized spoofing, spoofers of opportunity-based centralized spoofing, and tunable transmitting power-based centralized spoofing. The Chapter 4 attempts the anti-spoofing problem in a single receiver configuration and proposes M-best positioning and data association algorithms. Whereas, the Chapter 5 is an anti-spoofing algorithm in multiple receiver configuration, proposed generalized likelihood ratio test based attack detection in tracklet framework and the spoofing mitigation by spoofer localization. Finally, the conclusion and future work are presented in Chapter 6.

Chapter 2

Stealthy GPS Spoofing in Single-spoofer Single-target Scenario: Distributed Spoofers, Target Tracking and Sensor Fusion

2.1 Problem Formulation

The spoofing problem is formulated for single spoofer single targeted GPS receiver. In spoofing attacks, spurious GPS signals are either generated by a simulator or playback the received signals at a different time for manipulating the targeted receiver's PVT. Let the spoofer located at $\mathbf{x}^s$ and its position is known precisely. Whereas, the target (vehicle) located at $\mathbf{x}^r$ and relies on the GPS receiver for estimating its own location. In a given satellite constellation, I active satellites are being located at $\{\mathbf{x}_i^g\}_{i=1}^I$. In a clean environment without spoofer, the target receives $\{p_i^r\}_{i=1}^I$ measurements from authentic satellites and estimates its location as $\hat{\mathbf{x}}^r$. Spoofer intends to create a spoof position $\mathbf{x}^f$, which is estimated due to spoof measurement set $\left\{p_i^f\right\}_{i=1}^I$ for the target being located at $\mathbf{x}^r$ as shown in Figure 2.1. During the spoofing attack, the targeted GPS receives two sets of measurements $\left\{p_i^r, p_i^f\right\}_{i=1}^I$, and the receiver generally locked onto measurements with the higher power. Since spoofed signals maintain high power, the receiver is more likely to lock $\left\{p_i^f\right\}_{i=1}^I$ measurements and inturn state estimation results to $\mathbf{x}^f$ even though the actual location is $\mathbf{x}^r$ as shown in Figure 2.1.

In simulator-based spoofing, the spoofed measurements are generated based on the historical knowledge of the GPS measurements (Kerns et al. 2014) without considering the current satellite positions, and broadcasting using a directional antenna. In such

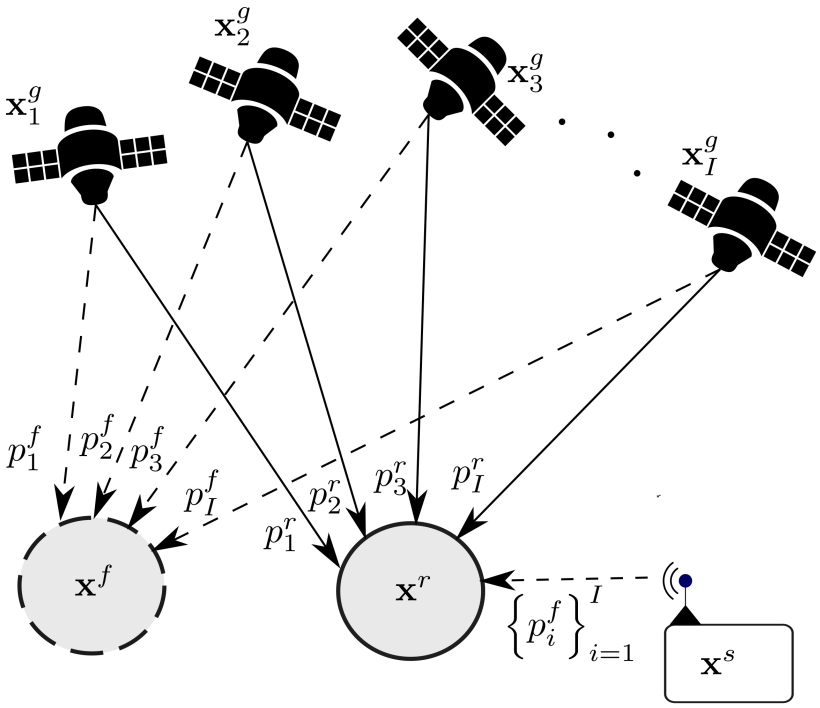

Figure 2.1: Illustration of GPS simulator, geometry, and pseudoranges involved in GPS spoofing attack. (dark lines represent authentic satellite signals and dotted lines represent spoofed satellite signals)

a scenario, the capturing of GPS receiver is effortless if no defense mechanisms (online constellation check, software-defined constellations, time synchronization) employed by the targeted receiver. In the software-defined constellation, a reference satellite position $\left\{\mathbf{x}_i^{\text{ref}}\right\}_{i=1}^{I}$ and time information is available for distinguishing the received satellite information (Günther 2014). Hence, in near future stealthy spoofers should be developed which can process both the spoof location and current working satellite.

A repeater based spoofing is necessary to access and reflect the current working satellites in the constellation. The repeater-based spoofer receives the authentic signals and modifies the signal with an external delay. This external delay calculation is given in (Kerns et al. 2014) as

$$\delta\tau_i = \frac{p_i^f - p_i^r - \mid \mathbf{x}^r - \mathbf{x}^s \mid}{c}. \tag{2.1}$$

The $\mid \cdot \mid$ is an equilidian operator and c is speed of light. In GPS receivers, the received power of the signal is one of the critical factors to lock the received signal. The received power is low due to the propagation losses from satellite transmitter to the GPS receiver. The multi-path signals and highly attenuated signals will not lock

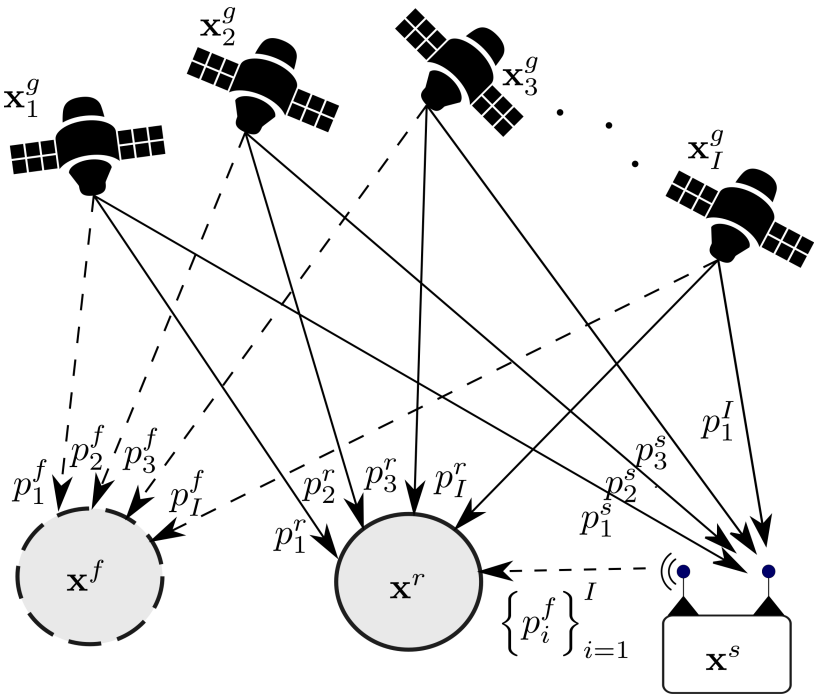

Figure 2.2: Illustration of repeater based GPS spoofing for true target and its perception spoof target with respect to geometry and pseudoranges involved (dark lines represent authentic satellite signals and dotted lines represent spoofed satellite signals)

onto the tracking loop owing to the inadequate received power. Whereas, the signals with over-rated received power leads to re-acquisition or loss of track or alert as a jam signal. However, in the spoofing process, it is advisable to maintain higher power levels than the actual satellite signals to lock the spoofed signals onto the receiver. Therefore, the maintenance of transmitted power of the spoofed signal is critical for achieving a successful spoofing attack. The received power and transmitting power follows the inverse square law relation as given in (Schmidt et al. 2016)

$$P_{\mathrm{Rx}}^{r} = \frac{P_{\mathrm{Tx}}^{s}}{4\pi \mid \mathbf{x}^{r} - \mathbf{x}^{s} \mid^{2}}. \tag{2.2}$$

Where P_{Rx}^{r} is received power of the spoofed signal at the GPS receiver. P_{Tx}^{s} is transmitted power of the spoofed signal at the spoofer's transmitter. From (2.1) and (2.2), it is evident that the distance between spoofer and target $\mid \mathbf{x}^{r} - \mathbf{x}^{s} \mid$ plays a major role in spoofing. In most of the field tests of GPS spoofing, the spoofer is operated at a constant distance (1–2m) and very near to the targeted GPS receiver (Bhatti and Humphreys 2017). In the real-time application of spoofing an aircraft taking off, aircraft landing, military canon, and huge ships, the spoofer is in stand-off location (1–

5Km) and hence the spoofer should estimate the target state (Kerns et al. 2014). To estimate the target state, range measuring sensors and trackers are generally applied. The additional sensors, like radar, visual, optical, and sonar, make the design complex and costly. The future spoofers should possess the tunable transmitting power capabilities, sensors to detect the target, and target tracker for accurately estimating the position of the target to be spoofed.

The direction of arrival (DOA) estimation based anti-spoofing technique is powerful for detecting the spoofing threat. The simulator or repeater based spoofing can be easily detected as a spoofing attack by observing all the sources of the signal arriving in the same direction (Kang et al. 2017). In addition, the spoofing attack can easily be mitigated by steering the null antenna beam in the direction of a spoofer. Therefore, the deployment of multiple spoofers and the trajectory planning of the spoofers is very much essential to counter-countermeasure the DOA based anti-spoofing.

The GPS receivers are mounted on different sized vehicles, and few of them are hard to detect and track. Depending on the RCS of the target and environment, the P_D varies. Here, the P_D is a detection probability of a target (vehicle) on which the GPS receiver is mounted. Track breakages or track segmentation is a frequently occurring problem in target tracking. Track breakages normally occur due to the following reasons: incorrect measurement associations, highly maneuvering targets, low detection probability, and large measurement errors. In the above scenarios, the performance of GPS spoofing is a cost function of the tracker. Hence the target trackers should be able to track effectively for both linear and maneuvering targets, and the fusion of the local state estimates of all spoofers are essentials for high-quality GPS spoofing.

The requirements for the next generation spoofers are as follows:

- A stealthy spoofer which can counter-countermeasure the signal processing based anti-spoofing techniques like time synchronization, constellation check, and offset.

- A spoofer which can operate in any location, estimate the position of GPS target to be spoofed accurately, and accordingly transmit the spoofed signals with tunable transmitting power to counter-countermeasure the anti-spoofing

techniques like received power thresholding, received power across the satellites.

- The spoofer should be spatially stealthy in deployment (distributed networking and communication between spoofers) to mitigate spatial mitigation technique like DOA.

- Spoofers capable of spoofing the low detection probability targets, spoofers are intelligent to analyze the target and imposing spoof trajectory to mislead the target.

2.2 Target Tracking

We proposed to incorporate the radar and target tracking module within the spoofer design. Hence, we are presenting the target tracking and fusion algorithms in this section, which will be used in the subsequent Sections.

2.2.1 Radar Measurement Model

Spoofer is equipped with radar, and hence we consider the location of radar is same as that of spoofer platform. The radar located at $\mathbf{x}^s$, receives S scans of measurements, the measurement set is given by

$$\mathbf{Y} = \{\mathbf{Y}(1), \mathbf{Y}(2), \ldots, \mathbf{Y}(S)\}, \tag{2.3}$$

in which the measurement set from the k^{th} scan is

$$\mathbf{Y}(k) = \left\{\mathbf{y}_j(k)\right\}_{j=1}^{m_k}. \tag{2.4}$$

Here $\mathbf{y}_j(k)$ is the j^{th} measurement vector at scan k with dimension n_y, whereas m_k is individual number of observations, which may or may not be target originated. Here $\mathbf{x}$ is the unknown parameter vector of dimension n_x to be estimated from the observation data $\mathbf{Y}$. If the measurement $\mathbf{y}_j(k)$ is target originated, the nonlinear discrete measurement equation is given by

$$\mathbf{y}_j(k) = h_k(\mathbf{x}(k)) + \mathbf{n}(k), \tag{2.5}$$

where $h_k(\cdot)$ is known nonlinear function of the target motion parameter $\mathbf{x}$, and $\mathbf{n}(k)$ is a white Gaussian noise with zero mean and covariance $\mathbf{R}(k)$. The probability density

function (pdf) of target originated measurement is $p_T[\cdot]$ is

$$p_T[\mathbf{y}_j(k) \mid \mathbf{x}] = \mathcal{N}\left(\mathbf{y}_j(k) - h_k(\mathbf{x}(k)), \mathbf{R}(k)\right), \tag{2.6}$$

where $\mathcal{N}(\cdot)$ is Gaussian pdf. Similarly the pdf of measurement due to false alarm is represented by $p_F[\mathbf{y}_j(k)]$. It is assumed that false alarm is a uniform distribution within the surveillance region with volume V is

$$p_F[\mathbf{y}_j(k)] = \frac{1}{V}. \tag{2.7}$$

Assume the target detection probability is P_D and is expected to have number of false alarms λ per unit volume. The number of false alarms in V follows Poisson probability mass function as

$$\mathbb{P}(m) = \frac{\exp\left(-\lambda V\right)\left(\lambda V\right)^m}{m!}. \tag{2.8}$$

Even with the change in time, the probability of detection and false alarms constant. In any scan k, the probability of having m_k measurements in volume V is

$$p_T(m_k) = \begin{cases} (1 - P_D)\mathbb{P}(0); \ m_k = 0 \\ (1 - P_D)\mathbb{P}(m_k) + P_D\mathbb{P}(m_k - 1); \ m_k > 0 \end{cases} \tag{2.9}$$

The (2.9) is composite form of observations together with target presence and false alarms.

2.2.2 Tracker

A IMM Filter

The target state vector $\mathbf{x}(k)$ is stacked vectors of position and its respective velocities of the target. The target motion is modelled as

$$\mathbf{x}(k+1) = \mathbf{F}(k)\mathbf{x}(k) + \Gamma(k)\mathbf{u}(k), \tag{2.10}$$

where, $\mathbf{F}(k)$ is a state transition matrix follows constant velocity (CV) or constant turn (CT) models. Whereas $\Gamma(k)$ is noise gain as given in (Bar-Shalom et al. 2004), the process noise is given by $\mathbf{u}(k)$, assumed to follow Gaussian with zero mean and covariance $\mathbf{Q}(k)$.

$$\mathbb{E}[\mathbf{u}(k)\mathbf{u}(k)'] = \mathbf{Q}(k) \tag{2.11}$$

To address both linear and maneuvering target, interactive multiple model (IMM) filter is considered. The tracker derivation with IMM filter and 2D assignment is presented in (Bar-Shalom et al. [2004], Kirubarajan et al. [2000]). IMM is an optimal approach by keeping only N filters for N hypothesis. At $k-1$ time step, there are only N estimates and their associated covariance which approximately summarizes the past. In IMM, mode jumps enable in two ways by re initializing the filter and by introducing the transition probability π_{vu}, which facilitates as a priori information. The predicted model probability is given by

$$\mu^{(v)}(k \mid k-1) = \sum_{v=1}^{N} \pi_{uv} \mu^{(v)}(k-1). \tag{2.12}$$

The mixing probabilities are given by

$$\mu^{v|u}(k-1) = \pi_{uv} \mu^{(v)}(k-1) / \mu^{(u)}(k \mid k-1). \tag{2.13}$$

The mixing state and covariance is given by

$$\hat{\mathbf{x}}^{(v)}(k-1 \mid k-1) = \sum_{u=1}^{N} \hat{\mathbf{x}}^{(u)}(k-1 \mid k-1) \mu^{(u|v)}(k-1) \tag{2.14}$$

$$\mathbf{P}^{(v)}(k-1 \mid k-1) = \sum_{u=1}^{N} \left[\mathbf{P}^{(u)}(k-1 \mid k-1) + \tilde{\mathbf{x}}(k-1) \tilde{\mathbf{x}}(k-1)' \right] \mu^{(u|v)}(k-1).$$

where

$$\tilde{\mathbf{x}}(k-1) = \left(\mathbf{x}^{(v)}(k-1 \mid k-1) - \hat{\mathbf{x}}^{(u)}(k-1 \mid k-1) \right) \tag{2.15}$$

In a generalize context N models are possible, N KF blocks are required. The KF contains three steps namely, predict, gain calculation, and update. The predicted state, predicted covariance and predicted measurement are calculated as

$$\hat{\mathbf{x}}(k|k-1) = \mathbf{F}(k-1) \hat{\mathbf{x}}(k-1|k-1), \tag{2.16}$$

$$\hat{\mathbf{P}}(k|k-1) = \mathbf{F}(k-1) \hat{\mathbf{P}}_j(k-1|k-1) \mathbf{F}(k-1)' + \mathbf{Q}(k-1), \tag{2.17}$$

and

$$\hat{\mathbf{y}}(k|k-1) = \mathbf{H}(k) \hat{\mathbf{x}}(k|k-1). \tag{2.18}$$

respectively. The residual and residual covariance are given as

$$\mathbf{r}(k|k-1) = \mathbf{y}(k) - \hat{\mathbf{y}}(k|k-1), \tag{2.19}$$

and

$$\mathbf{S}(k) = \mathbf{H}(k)\hat{\mathbf{P}}(k|k-1)\mathbf{H}(k)' + \mathbf{R}(k) \tag{2.20}$$

respectively. The filter gain is

$$\mathbf{G}(k) = \mathbf{P}(k|k-1)\mathbf{H}(k)'\mathbf{S}(k)^{-1}. \tag{2.21}$$

The updated state and its associated covariance are designated as

$$\hat{\mathbf{x}}(k|k) = \hat{\mathbf{x}}(k|k-1) + \mathbf{G}(k)\mathbf{r}(k) \tag{2.22}$$

and

$$\hat{\mathbf{P}}(k|k) = \hat{\mathbf{P}}(k|k-1) - \mathbf{G}(k)\mathbf{S}(k)\mathbf{G}(k)'. \tag{2.23}$$

respectively. The output of KF is state $\hat{\mathbf{x}}^{(v)}(k \mid k)$ and covariance $\hat{\mathbf{P}}^{(v)}(k \mid k)$. The likelihood corresponds to v^{th} and u^{th} filter at k instant is given by

$$\Lambda^{(uv)}(k) = p\left[\mathbf{y}(k) \mid m^v(k), \hat{\mathbf{x}}^{(u)}(k-1 \mid k-1), \mathbf{P}^{(u)}(k \mid k)\right];\ u, v = 1, \ldots N. \tag{2.24}$$

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

$$\mu^{(v)}(k) = \frac{\Lambda^{uv}(k)\mathbf{P}^{uv}\mu^u(k-1)}{\sum_{i=1}^{N} \Lambda^{uv}(k)\mathbf{P}^{uv}\mu^u(k-1)}. \tag{2.25}$$

Combining the model probability with the conditioned model estimates yields the updated state $\hat{\mathbf{x}}(k \mid k)$ and updated covariance $\mathbf{P}(k \mid k)$ as

$$\hat{\mathbf{x}}(k \mid k) = \sum_{v=1}^{N} \hat{\mathbf{x}}^{(v)}(k \mid k)\mu^{(v)}(k) \tag{2.26}$$

$$\mathbf{P}(k \mid k) = \sum_{v=1}^{N} \left[\mathbf{P}^{(v)}(k \mid k) + \left(\hat{\mathbf{x}}(k \mid k) - \hat{\mathbf{x}}^{(v)}(k \mid k)\right)\left(\hat{\mathbf{x}}(k \mid k) - \hat{\mathbf{x}}^{(v)}(k \mid k)\right)'\right] \mu^{(v)}(k).$$

B Data Association

The data association makes the decisions of associating the obtained measurements at k to the established tracks at $k-1$, and to update the track at k. In a clean environment, GNN is a 2D assignment that matches the m_k measurement list to the predicted tracks list by formulating the global optimization problem.

C Track Management

Total available tracks are classified into tentative tracks and confirmed tracks. Tentative tracks are the one which have fewer measurements associated than the required number over a specified time limit. Whereas confirmed tracks are the tentative tracks which receives more number of measurements and promoted as a confirmed ones. Also, the tentative tracks will be deleted if an inadequate number of measurements are associated with in specified time. For track maintenance, the logic based rule is used.

- For track initialization: out of the last N_{init} measurement frames if at least M_{init} measurements are associated together, then form a track and mark it tentative otherwise, do nothing.

- For a tentative track: out of the last N_{tent} measurement frames if at least M_{tent} measurements are associated to the track, then promote it as confirmed otherwise, delete the track.

- For a confirmed track: out of the last N_{conf} measurement frames if at least M_{conf} measurements are associated to the track, then do nothing otherwise, delete it.

D Information Fusion

Here, tracker provides updated state $\hat{\mathbf{x}}(k \mid k)$ consists of both estimated position and velocity of the target. The low probability of detection of the targets results in the track breakages, track termination, and considerable errors in the state estimation of the target. Let M radars are deployed in the space, where each radar is embedded with a local tracker. All the local trackers broadcast the predicted and updated state and covariance to the fusion center to attain global estimate. The predicted state and covariance of the target being estimated by the m^{th} tracker is $\hat{\mathbf{x}}^m_{k|k-1}$ and $\mathbf{P}^m_{k|k-1}$ respectively. Whereas, the updated state and covariance of the target being estimated by local m^{th} tracker is $\hat{\mathbf{x}}^m_{k|k}$ and $\mathbf{P}^m_{k|k}$ respectively. Predicted and updated estimates are fed to the information fuser to estimate the fused state and covariance as $\hat{\mathbf{x}}_{k|k}$ and $\mathbf{P}_{k|k}$ respectively. The state and covariance fusion equations are derived as given in

(Bar-Shalom et al. 2011)

$$\mathbf{P}^{-1}(k \mid k)\hat{\mathbf{x}}(k \mid k) = \mathbf{P}^{-1}(k \mid k-1)\hat{\mathbf{x}}(k \mid k-1) + \sum_{m=1}^{M} \left[\left(\mathbf{P}^{m}(k \mid k)\right)^{-1} \hat{\mathbf{x}}^{m}(k \mid k) - \left(\mathbf{P}^{m}(k \mid k-1)\right)^{-1} \hat{\mathbf{x}}^{m}(k \mid k-1) \right] \tag{2.27}$$

$$\mathbf{P}(k \mid k)^{-1} = \mathbf{P}^{-1}(k \mid k-1) + \sum_{m=1}^{M} \left[\left(\mathbf{P}^{m}(k \mid k)\right)^{-1} - \left(\mathbf{P}^{m}(k \mid k-1)\right)^{-1} \right] \tag{2.28}$$

E CRLB

Let us assume that observation set $\mathbf{Y}$ which has pdf $p[\mathbf{Y} \mid \mathbf{x}]$, measuring that the pdf depends on the parameter vector $\mathbf{x}$ which is to be estimated. The CRLB states that

$$E\{[\hat{\mathbf{x}}(\mathbf{Y}) - \mathbf{x}][\hat{\mathbf{x}}(\mathbf{Y}) - \mathbf{x}]'\} = \mathbf{J}^{-1} \tag{2.29}$$

where

$$\mathbf{J} = \mathbb{E}\{[\nabla_{\mathbf{x}} \ln \Lambda(\mathbf{x})] [\nabla_{\mathbf{x}} \ln \Lambda(\mathbf{x})]'\}_{\mathbf{x}=\text{truth}} \tag{2.30}$$

when we have measurement origin uncertainty, the number of measurements m_k at a particular scan k is also a random variable. Denote $p_j(m_k)$ is the probability that the j^{th} measurement at scan k is target originated and $p_o(m_k)$ is the probability that all the measurements are false. We require

$$\sum_{j=0}^{m_k} p_j(m_k) = 1 \tag{2.31}$$

if the m_k measurements are obtained at scan k. The likelihood function for scan k, averaged over all possible m_k, can be written using the total probability theorem as

$$\begin{aligned} p[\mathbf{Y}(k) \mid \mathbf{x}] &= \sum_{m_k=1}^{\infty} p_T[\mathbf{Y}(k) \mid x.m_k] P_T(m_k) \\ &= \sum_{m_k=1}^{\infty} \left[p_0(m_k) \frac{1}{V^{m_k}} + \sum_{j=1}^{m_k} p_j(m_k) \frac{1}{V^{m_k-1}} \mathcal{N}[\mathbf{y}_j(k) - f_k(\mathbf{x}), R(k)] \right] P_T(m_k) \end{aligned} \tag{2.32}$$

Assuming m_k independent across scans $k = 1, \ldots, K$, overall likelihood is

$$p[\mathbf{Y} \mid \mathbf{x}] = \prod_{k=1}^{K} p[\mathbf{Y}(k) \mid \mathbf{x}]. \tag{2.33}$$

by using the properties of logarithm, we can write

$$\mathbf{J} = \sum_{k=1}^{K} \mathbf{J}_k \tag{2.34}$$

where

$$\mathbf{J}_k(m_k) = \sum_{m_k=1}^{\infty} P_T(m_k)\mathbf{J}_k(m_k) \tag{2.35}$$

which can be written as

$$\mathbf{J}_k(m_k) = \mathbb{E}\left\{ \left(\nabla_{\mathbf{x}} \ln p[\{\mathbf{y}_j(k)\}_{j=1}^{m_k} \mid \mathbf{x}, m_k] \right) \left(\nabla_{\mathbf{x}} \ln p[\{\mathbf{y}_j(k)\}_{j=1}^{m_k} \mid \mathbf{x}, m_k] \right)' \right\}. \tag{2.36}$$

The FIM for scan k in the presence of measurement origin uncertainty is given by

$$\mathbf{J}_k(m_k) = q_m(P_D, \lambda V, m_k)\mathbf{J}_k^0, \tag{2.37}$$

where q_m is a scalar value and

$$\mathbf{J}_k^0 = \left(\nabla_{\mathbf{x}}[f_k(\mathbf{x})]'\right) R^{-1}(k) \left(\nabla_{\mathbf{x}}[f_k(\mathbf{x})]'\right)' \tag{2.38}$$

Here $\nabla_{\mathbf{x}}[f_k(\mathbf{x})]$ is Jacobian matrix and detailed derivation for q_m is presented in (Kirubarajan et al. 2001).

2.3 Repeater based Spoofing

2.3.1 Received Signal Model at Repeater

The navigation signal $\psi(t)$ transmitted by satellites includes current satellite position $\mathbf{x}_i^g$, signal transmission time, information related to the health of the satellite, and deviation in predicted trajectories. In open space, the EM signal travels with the speed of light. A spoofer located at $\mathbf{x}^s$ receives the combined signal of all satellites as illustrated in Fig. 2.2. The composite signal model is

$$\psi(\mathbf{x}^s, t') = \sum_{i=1}^{I} A_i \psi_i(t - \delta_i^s) + n(\mathbf{x}^s, t'). \tag{2.39}$$

Where A_i and t' are attenuation of signal and global satellite time. n is the background noise of the composite signal. δ_i^s is the time delay corresponding to pseudorange measurement p_i^s. Due to the properties of $\psi_i(t)$, the signal components extracted by the receiver using spread spectrum techniques. In a single spoofer based spoofing, all the signals are extracted and processed in different channels. Whereas, in case of distributed spoofing, each spoofer handles unique signal based on the satellite ID. The spoofer modifies the time delays and re-transmit towards the target GPS receiver.

2.3.2 Re-transmitted Signal Model at Repeater

The re-transmitted signal by the spoofer is given by

$$\psi(\mathbf{x}^s, t') = \sum_{i=1}^{I} A_i \psi_i(t - \delta_i^s - \delta_i) + n(\mathbf{x}^s, t'). \tag{2.40}$$

The spoofer calculates the external delays $\delta\tau_i$ to be added by the spoofer to the received signals for re-transmission. The spoofer adds an external delay only if $\delta\tau_i \geq 0$. Here $\delta\tau_i$ is the external delay incorporated by the spoofer. Unlike the traditional spoofing, here, the target state $\hat{\mathbf{x}}^r$ is being estimated by the tracker.

$$p_i^f = p_i^s + \mid \hat{\mathbf{x}}^r - \mathbf{x}^s \mid + c(\delta_i) \tag{2.41}$$

By rearranging the above equation, the external delay offered by the processor is given by

$$\delta_i = \frac{p_i^f - p_i^s - \mid \hat{\mathbf{x}}^r - \mathbf{x}^s \mid}{c} - \delta_i^{\text{Rx-Tx}}. \tag{2.42}$$

Here the additional term $\delta_i^{\text{Rx-Tx}}$ is the transmission delay within spoofer. For good precision, spoofer receiver to transmission propagation delay should be considered. The external delay being added to the actual signal and then retransmit towards the targeted GPS.

2.3.3 Re-transmitted Signal Model at GPS Receiver

The re-transmitted signals by the spoofer available at the GPS receiver as illustrated in Figure 2.2. Owing to huge power of the spoofed signals, all the spoofer generated signals are more likely to lock onto the GPS receiver. The target located at $\mathbf{x}^r$ receives the combined spoof signals as

$$\psi(\mathbf{x}^r, t') = \sum_{i=1}^{I} A_i \psi_i \left(t - \delta_i^s - \delta_i - \frac{\mid \mathbf{x}_i^s - \mathbf{x}^r \mid}{c} \right) + n(\mathbf{x}^r, t'). \tag{2.43}$$

Here $\frac{|\mathbf{x}_i^s - \mathbf{x}^r|}{c}$ term is due to transmission of signal from i^{th} spoofer (where number of satellite signals and spoofer signals are equal) to the target receiver. The received pseudomeasurement by the target receiver is

$$p_i^* = c(\delta_i^s + \delta_i) + \mid \mathbf{x}_i^s - \mathbf{x}^r \mid . \tag{2.44}$$

Substituting the values of δ_i^s and δ_i yields to

$$p_i^* = c\left(\frac{p_i^s}{c} + \frac{p_i^f - p_i^s - \mid \hat{\mathbf{x}}^r - \mathbf{x}_i^s \mid}{c} - \delta_i^{Rx-Tx}\right) + \mid \mathbf{x}_i^s - \mathbf{x}^r \mid . \tag{2.45}$$

Solving the above equation simplifies to

$$p_i^* = p_i^f + \mid \mathbf{x}^r - \hat{\mathbf{x}}^r \mid . \tag{2.46}$$

From (2.46), we can conclude that, after successful GPS spoofing, the pseudorange measurement received by the GPS receiver is the summation of projected spoof pseudorange measurement by the spoofer and the estimation error of the tracker. Here $\hat{\mathbf{x}}^r$ is the global estimate obtained by the distributed tracking and fusion.

The GPS receivers adopt pseudorange positioning algorithm, in which at least four satellites should be available to achieve the three-dimensional positioning. The pseudorange measurement equation is given by

$$p_i^* = g_i(\mathbf{x}^r) + w_i^r + \mid \mathbf{x}^r - \hat{\mathbf{x}}^r \mid; \quad i = 1, 2, ..., I. \tag{2.47}$$

Where $g_i(\mathbf{x}^r)$ represents the pseudorange, from the satellite located at $\mathbf{x}_i^g$ to target location $\mathbf{x}^r$, and w_i^r represents zero mean white Gaussian noise with variance $(\sigma_i^r)^2$. Geometrically, every measurement equation translates into a sphere with $\mathbf{x}_i^g$ as a center and is given by

$$g_i(\mathbf{x}) = \sqrt{(x_i^g - x^f)^2 + (Y_i - y^f)^2 + (Z_i - z^f)^2} + b. \tag{2.48}$$

Where b is the bias due to offset. The state consists of four unknowns. Hence, the unique solution is obtained by solving any four from I equations. In the case of more than four satellites, this solution becomes overdetermined and an unique solution is infeasible. The unknown vector can be solved by using algorithms like LS, WLS, iterative based solutions, and Newton's method (Abel and Chaffee 1991).

2.3.4 CRLB

From (2.47), the pseudomeasurement consists of white noise component w_i^r and $\mid \mathbf{x}^r - \hat{\mathbf{x}}^r \mid$. Since $\mathbf{x}^r$ and $\hat{\mathbf{x}}^r$ follows Gaussian distribution, the resultant $\mathbf{x}^r - \hat{\mathbf{x}}^r$ also folows the Gaussian with the minimum variance of $\frac{1}{\mathbf{J}}$. Where, $\mathbf{J}$ is the fisher information matrix obtained in the tracker. The MSE of the tracker depends on measurement

origin uncertainty (P_D, λ and V). Hence, to evaluate the CRLB of GPS position estimate given in (2.47), the minimum variance of the tracker should be evaluated first. The (2.47) can be rewritten as

$$p_i^* = g_i(\mathbf{x}^r) + w_i^r + w; \quad i = 1, 2, ..., I. \tag{2.49}$$

Here, the total variance of the pseudomeasurement noise is $\sigma^2 = \sigma_r^2 + \frac{1}{J}$. The Cramer-Rao lower bound ($CRLB$) is the mean square error corresponding to the estimator of a parameter that cannot be smaller than a certain value related to the likelihood function. The covariance matrix of an unbiased estimator is bounded as below

$$\mathbb{E}\{[\hat{\mathbf{x}}(p^*) - \mathbf{x}^s][\hat{\mathbf{x}}(p^*) - \mathbf{x}^s]'\} \leq \text{FIM}^{-1}. \tag{2.50}$$

The FIM is given by

$$\begin{aligned} \text{FIM} &= -\mathbb{E}\left[\nabla_{\mathbf{x}} \nabla_{\mathbf{x}}' \ln \Lambda(\mathbf{x})\right]_{\mathbf{x}=\mathbf{x}^s} \\ &= \mathbb{E}\{\left[\nabla_{\mathbf{x}} \ln \Lambda(\mathbf{x})\right] \left[\nabla_{\mathbf{x}} \ln \Lambda(\mathbf{x})\right]'\}_{\mathbf{x}=\mathbf{x}^s}. \end{aligned} \tag{2.51}$$

Where $\mathbf{x}^s$ is the true value of the vector $\mathbf{x}$

$$\nabla_{\mathbf{x}} \ln \Lambda(\mathbf{x}) = \frac{1}{(\sigma)^2} \nabla_{\mathbf{x}} g(\mathbf{x})[p^s - g] \tag{2.52}$$

Here $(\sigma)^2$ is the variance of the pseudo measurement noise, $p^* = [p_1^* \quad p_2^* \quad \dots \quad p_I^*]'$ and $g = [g_1 \quad g_2 \quad \dots \quad g_I]'$. The Jacobian matrix $\nabla_{\mathbf{x}} g(\mathbf{x})$ is given by

$$\nabla_{\mathbf{x}} g(\mathbf{x}) = \begin{bmatrix} \frac{\partial g_1}{\partial x^f} & \frac{\partial g_2}{\partial x^f} & \dots & \frac{\partial g_I}{\partial x^f} & 1 \\ \frac{\partial g_1}{\partial y^f} & \frac{\partial g_2}{\partial y^f} & \dots & \frac{\partial g_I}{\partial y^f} & 1 \\ \frac{\partial g_1}{\partial z^f} & \frac{\partial g_2}{\partial z^f} & \dots & \frac{\partial g_I}{\partial z^f} & 1 \end{bmatrix} \tag{2.53}$$

The fisher information matrix is

$$\begin{aligned} \text{FIM} &= \frac{1}{(\sigma)^4} \nabla_{\mathbf{x}} g \mathbb{E}\{[p^* - g][p^* - g]'\} \nabla_{\mathbf{x}} g \\ &= \frac{1}{(\sigma)^2} \nabla_{\mathbf{x}} g \nabla_{\mathbf{x}} g'. \end{aligned} \tag{2.54}$$

and the partial derivatives are

$$\begin{aligned}
\frac{\partial g_i}{\partial x^f} &= \frac{-(x_i^g - x^f)}{\sqrt{(x_i^g - x^f)^2 + (y_i^g - y^f)^2 + (z_i^g - z^f)^2}} \\
\frac{\partial g_i}{\partial y^f} &= \frac{-(y_i^g - y^f)}{\sqrt{(x_i^g - x^f)^2 + (y_i^g - y^f)^2 + (z_i^g - z^f)^2}} \\
\frac{\partial g_i}{\partial z^f} &= \frac{-(z_i^g - z^f)}{\sqrt{(x_i^g - x^f)^2 + (y_i^g - y^f)^2 + (z_i^g - z^f)^2}} \\
\frac{\partial g_i}{\partial b} &= 1
\end{aligned} \tag{2.55}$$

2.4 Spoofer Design and Deployment

In this section, the novel spoofer design is presented by embedding the spoof measurements generator and target tracker into existing spoofer design. Further, multiple spoofers scenario is considered; fusion of local tracks and spatial deployment of spoofers is proposed to achieve improved spoofing accuracy and counter countermeasure the DOA-based anti-spoofing technique respectively. Moreover, adaptive transmitting power of a spoofer is suggested to counter the power-based anti-spoofing.

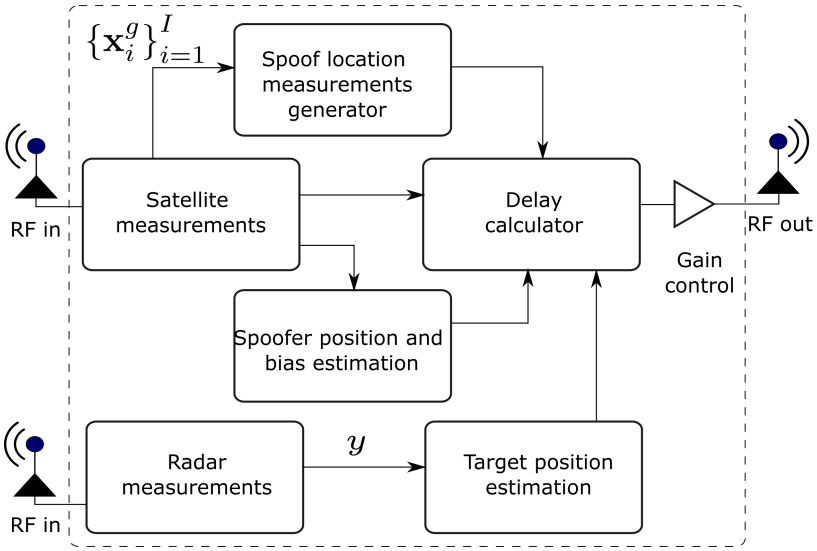

Figure 2.3: Modified Spoofer block diagram by incorporating target tracker, spoof measurements generator.

2.4.1 Spoof Location Measurement Generator

The spoof position and spoof trajectory are user-dependent; these spoof pseudorange measurement generation can be on-line or off-line depending on the interest of user intended to spoof. Here user refers to a person, who is carrying out spoofing for the victim target. The spoof trajectory generation follows the target motion as given by (in Cartesian coordinates)

$$\mathbf{x}^f(k) = \mathbf{F}(k-1)\mathbf{x}^f(k-1) + \Gamma(k)\mathbf{u}(k). \tag{2.56}$$

the spoof target state is given by $\mathbf{x}^f(k)$ consists of positions and its respective velocities of the target. $\mathbf{F}$ is a state transition matrix follows CV or CT models and $\Gamma(k)$ is noise gain (Bar-Shalom et al. 2004). However, converting this state into the corresponding pseudorange is trivial, and it depends on the constellation and trajectory of the satellites. If the conversion is not matching to the type of constellation and state of the satellites, the target can detect it by using anti-spoofing techniques like constellation check or software-defined constellations (Günther 2014). Further, the choice of improper satellite state results in wrong time delay measurements. The spoof position is a function of the satellite locations and pseudoranges obtained by assuming that target is located at $\mathbf{x}^f$ instead of $\mathbf{x}^r$.

$$\mathbf{x}^f = f(p_1^f, p_2^f, \dots p_I^f, \mathbf{x}_1^g, \mathbf{x}_2^g, \dots \mathbf{x}_I^g). \tag{2.57}$$

and

$$p_i^f = g_i(\mathbf{x}^f) + w_i^f; \quad i = 1, 2, ..., I \tag{2.58}$$

where $g_i(\mathbf{x}^f)$ represents the geometrical range from satellite located at $\mathbf{x}_i^g$ to false (spoof) location $\mathbf{x}^f$, w_i^f represents zero mean white Gaussian noise with variance $(\sigma_i^s)^2$. Here $\{z_i^s\}_{i=1}^N$ are the unknowns to be calculated. However, in the block diagram, the current location of the satellite is being fed to the spoof position generator. Hence the $\{\mathbf{x}_i^g\}_{i=1}^I$ positions are readily available. The Pseudorange set is euclidean distance between the satellite positions to the spoof location formulated as an optimization problem given by

$$\hat{z}_i^s = \arg\min_{z_i>0} \left(\mathbf{x}^s - f(p_1^f, p_2^f, \dots p_I^f, \mathbf{x}_1^g, \mathbf{x}_2^g, \dots \mathbf{x}_I^g) \right) \tag{2.59}$$

subjected to

$$\mathbf{x}^f - \hat{\mathbf{x}}^f \leq \epsilon. \tag{2.60}$$

Here $\hat{\mathbf{x}}^f$ is the estimated position using the obtained $\hat{p}_i^f$ pseudorange measurements for all I equations, and ϵ is the precision. The pseudoranges to position estimation is a well known problem and can be solved using algorithms like least mean square (LMS), least squares (LS), weighted least square (WLS), iterative based solutions, and Newton's method (Abel and Chaffee 1991). The alternative way to obtain the pseudorange measurements for the given satellite positions and spoof location is to calculate the euclidean distance between them rather than solving this optimization problem. Besides this, the satellite trajectories are modeled using WGS-84 (follows an assumption of circular orbits) and we can use any software tool to retrieve the current state of the satellite.

$$\begin{aligned} x_i^g(t) &= R\left[\cos\Theta(t)\cos\Omega(t) - \sin\Theta(t)\sin\Omega(t)\cos 55^o\right] \\ y_i^g(t) &= R\left[\cos\Theta(t)\sin\Omega(t) + \sin\Theta(t)\cos\Omega(t)\cos 55^o\right] \\ z_i^g(t) &= R\sin\Theta(t)\sin 55^o \end{aligned} \tag{2.61}$$

where R is the radius ($R = 26,560$Km) of circular orbit, Ω and Θ are right ascension and angular phase of the circular orbit respectively, given by

$$\begin{aligned} \Omega(t) &= \Omega_0 - (t - t_0)\frac{360}{86164}\text{deg} \quad \text{and} \\ \Theta(t) &= \Theta_0 + (t - t_0)\frac{360}{43082}\text{deg}. \end{aligned} \tag{2.62}$$

The periodical variation of Ω is due to the rotation of the earth and the time period is equal to $86,164$s which is nearly equals to 24 hours. Optimizing (2.59), provides the equivalent pseudorange set for the given spoof position $\mathbf{x}^f$ is $\left\{p_i^f\right\}_{i=1}^{I}$.

2.4.2 Spoofers Spatial Deployment

The spatial detection technique currently available for detecting the spoofing effect is by observing the DOA of received signals. If all the signals are arriving from the same direction, a null antenna beam is projected in that particular direction as an anti-spoofing mitigation technique. To counter-countermeasure this DOA technique,

the spoofers are spatially deployed in a distributed pattern as shown in Figure 2.4. However, if the distributed pattern aligns as an occlusion to the line of sight (LOS) of satellites to target, such spoofing is hard to mitigate by posing a null beam in a single direction. For a given I satellites, I spoofers are employed and i$^{\text{th}}$ spoofer placed on the LOS joining the target $\mathbf{x}^r$ and satellite $\mathbf{x}_i^g$. The unique parametric line equation passing through the target and satellite coordinates is given by

$$\mathbf{x}_i^s(k) - \hat{\mathbf{x}}^r(k) = \alpha_i < \mathbf{x}_i^g(k) - \hat{\mathbf{x}}^r(k) > . \tag{2.63}$$

To maintain this LOS distributed pattern, the spoofers have to move dynamically according to (2.63), where α is the tunable parameter. For $0 < \alpha < 1$, the spoofer location falls in between the target and satellite. Every radar posses the maximum range $R_i^{\max}$, after which the radar does not acquire the measurements. The spoofers cannot be installed very near to the target as a covert operation, therefore, the minimum range of the radar to be installed is $R_i^{\max}$. Therefore, the installed radar should fall with the maximum and minimum constants

$$\mid \mathbf{x}_i^s(k) - \hat{\mathbf{x}}^r(k) \mid \leq R_i^{\max} \tag{2.64}$$

and

$$\mid \mathbf{x}_i^s(k) - \hat{\mathbf{x}}^r(k) \mid \geq R_i^{\min} \tag{2.65}$$

respectively. For $\eta_i = 0$, the spoofer location $\mathbf{x}_i^s$ is located at a distance of $R_i^{\min}$ on the line joining the target and satellite. Therefore, at $\eta_i = 0$, the location of the spoofer is $\mathbf{x}_i^{s,\min}$. By substituting the minimum distance coordinates in (2.63) gives

$$\alpha_i^{\min} = \frac{\mathbf{x}_i^{s,\min}(k) - \hat{\mathbf{x}}^r(k)}{< \mathbf{x}_i^g(k) - \hat{\mathbf{x}}^r(k) >}. \tag{2.66}$$

Similarly for $\eta_i = 1$, the spoofer location $\mathbf{x}_i^r$ falls at a distance of $[R_i^{\min}, R_i^{\max}]$ on the line joining the target and satellite; and the location is designated as $\mathbf{x}_i^{s,\max}$. Therefore, the value for parameter α_i is

$$\alpha_i^{\max} = \frac{\mathbf{x}_i^{s,\max}(k) - \hat{\mathbf{x}}^r(k)}{< \mathbf{x}_i^g(k) - \hat{\mathbf{x}}^r(k) >}. \tag{2.67}$$

.

2.4.3 Tunable Power

In clean environment (no-spoofing), the received power of the signal is low at the GPS receiver owing to propagation losses. Losses occurs during the transmission of a signal from the satellite to the GPS receiver. The effective isotropic radiated power ($EIPR$) of a satellite is 478W (26.8dBW). The free space loss (FSL) occurred due to spherical spreading and the critical value of signal propagation towards the earth is -182.4dBW. The atmospheric losses (AL) is -2dBW and the mismatch losses (MM) is -2.4dBW. The received power of the target antenna with receiver power gain (G_r)of 0dBW is given by

$$\begin{aligned} P^r_{\mathrm{Rx}}(\mathrm{dBW}) =& EIPR + G_r + FSL - AL - MM \\ =& 26.8 + 0 - 182.4 - 2.0 - 2.4 \\ =& -156\mathrm{dBW} \end{aligned}$$

The above calculations are for the satellite at a height of $20,000$Km from medium earth orbit. Whereas in spoofing attack, the relation between received power and transmitted power follows inverse square law as given by (2.2). Since the distance between satellite and GPS target is significantly high, the variation in $\mid \mathbf{x}^g_i - \hat{\mathbf{x}}^r \mid$ has no influence on received power of the GPS signal. But in spoofing case, the minimal change in $\mid \hat{\mathbf{x}}^r - \mathbf{x}^s \mid$ predominantly affect the received power. The variation in the received power can be detected by the target, and mitigate the spoofing signal by rejecting or loss of track and fall back onto the authentic signals. In the proposed design, the spoof signals at k^{th} instant is transmitted adaptively based on the estimated position and range between target and spoofer.

$$P^s_{\mathrm{Tx}}(k) = 4\pi P^r_{\mathrm{Rx}} \mid \hat{\mathbf{x}}^r(k) - \mathbf{x}^s(k) \mid^2 \tag{2.68}$$

In the (2.68), the required $P^s_{\mathrm{Tx}}(k)$ is adaptively changed by assuming the P^r_{Rx} is constant (-159dBW) and high compared to added received authentic satellite signal power.

2.4.4 Anti-spoofing Techniques

We assumed that the target receiver under consideration posses anti-spoofing techniques to detect and mitigate the spoofing attack, namely: constellation check, time

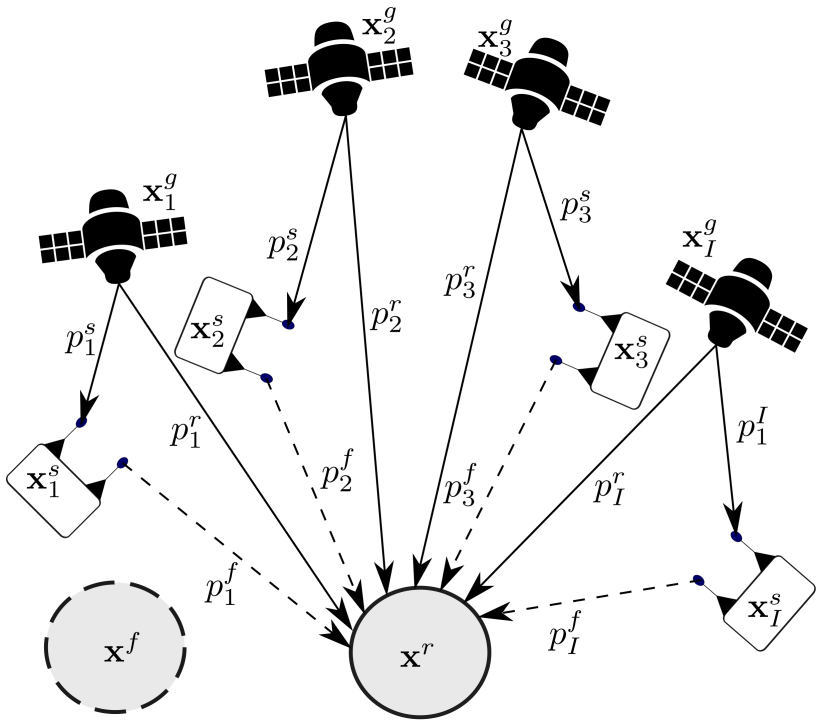

Figure 2.4: Illustration of distributed spoofing with I spoofers handling I satellite ID's for single point spoofing with repeaters based GPS spoofing

and offset synchronization, power threshold, observing power across the satellites, DOA, and normalized innovation square test (NIS) (Günther 2014, Liu et al. 2019, Tanil et al. 2018). With these capabilities, the target receiver sets spoof attack indicator ζ is zero for the case of clean environment or fail to detect the presence of spoofer. Whereas ζ sets to one for detecting the spoofing attack using above mentioned anti-spoofing algorithms during the spoofing attack.

Regarding the constellation of satellites, four different anti-spoofing techniques are possible: 1) Time synchronization, 2) offset bias estimation, 3) checking the number of satellites at a current time step, and 4) comparing the received satellite position with reference to satellite positions.

Received power of a signal is critical in analyzing the spoofing effect. The critical value of a received power of the GPS receiver is -155dBW for satellites in medium earth orbit of $20,000$Km. Some of the variations like satellite elevation, the orientation of antenna and change in altitude of the target causes the received power variation within $\pm$6dBW (Ippolito 2017). In all the spoofing experiments conducted in laboratory (Bhatti and Humphreys 2017) sofar, provides the significance of controlling

the signal strength in spoofing attack. The anti-spoofing techniques pertaining to the received power are checking the received power of each signal and the average power of the combined signals. In a clean environment, even though each satellite transmits with the same transmitting power, the received powers of the individual signals $\left\{P^t_{Rx_i}\right\}^I_{i=1}$ are distinguishable, as the satellite ranges are different. Whereas in a spoofing scenario, the received power of a signal remains same, since all the signals are coming from the same source location. The anti-spoofing technique based on the power monitoring is given by

$$\zeta = \begin{cases} 0 & ; \quad P_{Rx_i} \neq P_{Rx_j} \quad \forall \quad i,j = 1,2,\ldots N \quad \text{where} \quad i \neq j \\ 1 & ; \quad \text{else} \end{cases} \tag{2.69}$$

The anti-spoofing testing for individual received power of each signal or average power is given by

$$\zeta = \begin{cases} 0 & ; \quad (P^t_{Rx} < -149 \text{ dBW}) \,\&\&\, (P^t_{Rx} > -161 \text{ dBW}) \\ 1 & ; \quad \text{else} \end{cases} \tag{2.70}$$

Spatial processing based anti-spoofing methods gain more significance and is a powerful tool compared to other state of the arts (Günther 2014). The DOA estimation technique followed by placing a null beam in the direction of interference source is the most successful algorithm. The estimated DOA corresponding to θ is $\left\{\hat{\theta}_i\right\}^I_{i=1}$. In clean environment, all the estimated DOA values are distinguishable, since the arrivals are from different source locations. Whereas in spoofing attack, the estimated DOA values are in-distinguishable due to all the signals arrive from same direction and the same source location.

$$\zeta = \begin{cases} 0 & ; \quad \hat{\theta}_i \neq \hat{\theta}_j \quad \forall \quad i,j = 1,2,\ldots N \quad \text{where} \quad i \neq j \\ 1 & ; \quad \text{else} \end{cases} \tag{2.71}$$

2.5 Results and Discussions

To evaluate the proposed distributed spoofing, a single target - distributed spoofers scenario is simulated. The initial position of the target is considered at Paris, France (48 degree 51 min 24 sec north, 02 deg 21 min 03 sec east). The simulations are carried out by converting these coordinates into navigation frame.

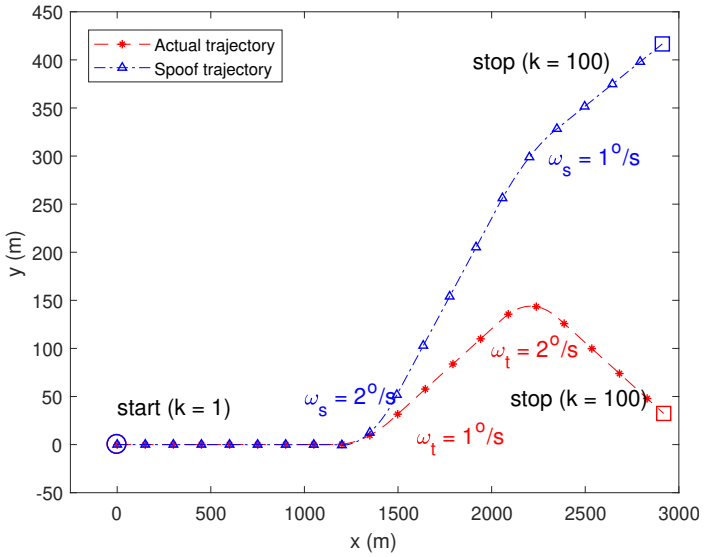

Figure 2.5: Target actual trajectory and spoofer imposed spoof trajectory

2.5.1 True Target Trajectory

We simulated a position pull-off target trajectory which follows CV and CT models. The target state is given by X^t. At initial time $t = 0$s, the target state is

$$\begin{aligned} \mathbf{x}^r(0) &= \begin{bmatrix} x & y & z & \dot{x} & \dot{y} & \dot{z} \end{bmatrix} \\ &= \begin{bmatrix} 0\text{m} & 0\text{m} & 2\text{m} & 30\text{m/s} & 0\text{m/s} & 0\text{m/s} \end{bmatrix} \end{aligned} \tag{2.72}$$

where x, y, and z represents the coordinates of the navigation frame. Initially the target moves with CV of 30m/s in x direction in the 3-D plane. At 40s discrete time instant, it takes 1^o/s left coordinate turn for 10s, then it continues in straight line until $t = 69$s. Then it takes 2^o/s right coordinate turn for 10s, and continues in straight line until $t = 100$s as shown in Figure 2.5. The sampling time of the scenario is $t_s = 1$s. The actual motion of the target is combination of above trajectory and random turbulence noise. The random turbulence is modeled as process noise with zero mean Gaussian noise. The process noise covariance is given by $\mathbf{Q}^r(k)$.

$$\begin{aligned} \mathbf{Q}^r(k) &= \text{diag}\{(\sigma_x^r)^2, (\sigma_y^r)^2, (\sigma_z^r)^2\} \\ &= \text{diag}\{0.001^2, 0.001^2, 0\} \end{aligned} \tag{2.73}$$

Since we assumed that GPS receiver is mounted on top of a vehicle, the altitude is raised to 2m and process noise along the altitude is zero. During the coordinated turn, the process noise variance corresponds to the turn rate is $(\sigma_\omega^r)^2 = 0.001^2$.

2.5.2 Spoof Target Trajectory

The spoof trajectory is an offline trajectory planned and projected by the spoofer onto the target. The initial time $t = 0$s, the spoof state is

$$\mathbf{x}^f(0) = \begin{bmatrix} 0\text{m} & 0\text{m} & 2\text{m} & 30\text{m/s} & 0\text{m/s} & 0\text{m/s} \end{bmatrix} \tag{2.74}$$

the spoof target moves with CV of 30m/s in x-direction. At 40s, it starts a 2^o/s left coordinate turn for 10s, then it follows CV 30m/s until $t = 69$s. Then it starts 1^o/s right coordinate turn for 10s, and continues in straight line till $t = 100$s as shown in Figure 2.5. This motion is superimposition of spoof trajectory and process noise. The process noise covariance is given by Q_k^s and the noise variance of coordinate turn is $(\sigma_\omega^s)^2 = 0.001^2$

$$\begin{aligned} \mathbf{Q}^f(k) &= \text{diag}\{(\sigma_x^f)^2, (\sigma_y^f)^2, (\sigma_z^f)^2\} \\ &= \text{diag}\{0.001^2, 0.001^2, 0\} \end{aligned} \tag{2.75}$$

2.5.3 Authentic Satellites and Spoofers Spatial Deployment

The authentic satellite positions are simulated based on Section-1.1.8 with an assumption that satellite trajectories follows WGS-84 model. The spoofers are deployed using (2.63) with optimized parameter $\alpha = 10^{-3}$ and handles the received pseudorange p_i^s from the respective satellite ID. The pseudorange measurement noise follows WGN distribution with zero mean and standard deviation $\sigma_i^s = 1$m.

2.5.4 Target Tracker

The spoofers are equipped with synchronous radars with a sampling time $t_s = 1$s. The measurement vector consists of range, azimuth and elevation with standard deviation $\sigma_\rho = 10$m, $\sigma_{\phi_a} = 0.1$rad and $\sigma_{\phi_e} = 0.1$rad respectively. The maximum range of the target $R_{\max}$ is 5000m, bearings [-180 − 180] and elevation [-90 − 0]. The false alarm rate follows poison distribution with clutter $\lambda = 1e^{-7}\text{m}^{-2}$ and probability of detection of a target is P_D. The single point track initialization (Yeom et al. 2004, Musicki and Song 2013) is used with maximum velocity $V_{max} = 40$m/s and the maximum turn rate $\omega_{max} = 2^o$/s with IMM filter and 2D-assignment. The IMM filter consists of CV and CT models. The tracking of the target starts at $t = 0$s and tracks till the destination at

$t = 100$s. Three different scenarios are considered by varying the detection probability $P_D = 0.9$, 0.7 and 0.5. The track initialization and termination follows 3/5 logic for all the above three cases. Moreover, the local estimates of the trackers are fused to obtain the global estimate.

2.5.5 Comparison Work - Simulator based Spoofing

For comparison of the proposed distributed spoofer model, we consider a simulator-based spoofing as given in (Kerns et al. 2014). The simulator is generating the spoofed GPS signals based on the characteristics of GPS signal from the single valid constellation. The simulator is static in position and range between simulator and target initial position is 1.5Km with an assumption that spoofer is located on the drone at an altitude of 200m. Since the simulator transmits the spoofed signals using the same channel, the spatial location of the simulator is (41.70^o, 27.11^o) from the targeted GPS receiver. The simulator transmitting power is constant during the simulation time. Besides, it is assumed that simulator contains the tracker module to track the target with the same tracking performance as given in Section 2.5.4.

2.5.6 Counter-countermeasures Evaluation

Constellation, power, and spatial distribution based anti-spoofing algorithms are analyzed for three different cases: clean environment, simulator-based spoofing, and proposed repeater based distributed spoofing.

Time synchronization is achieved in the proposed repeater based distributed spoofing method, since the current satellite signals are received by the repeater and retransmits these signals by modifying the delays. Due to repeater based spoofer configuration, constellation based anti-spoofing techniques fails to detect the spoofing activity.

Based on the received power of the signals, the spoofing attack was detected in (Wesson et al. 2013). During the simulation of no-spoofing scenario, the losses due to FSL, AL, and MM are considered. Whereas, in the simulator-based spoofing, the simulator is placed at 1.5Km away from targeted GPS receiver, the transmitted power of all the generated spoofed signals is constant, as they are transmitting from the same source and same location. The transmitting power of the simulator is calculated in

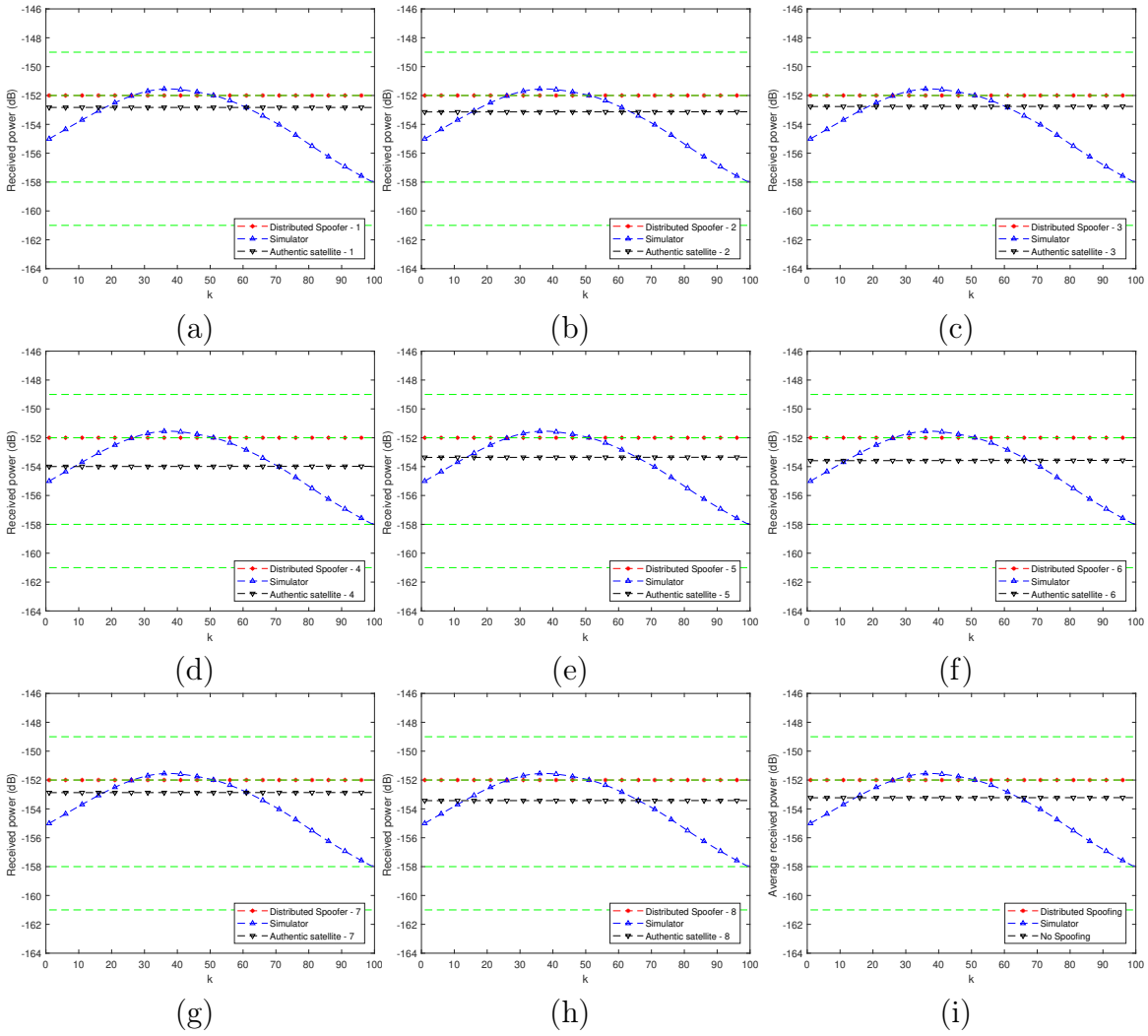

Figure 2.6: (a–h) Received power of 8 individual GPS signals for no spoofing, spoofing by simulator, and spoofing by proposed distributed spoofer and (i) average received power corresponding to all the received signals

such a way that the received power at the GPS receiver is equal to the critical value to avoid the unnecessary locking issues with signals at $t = 0$s. The simulator is static in location throughout the simulation, and hence the trajectory of the target only influence the range between them. Here, no external losses are incorporated during the transmission of a signal from the simulator to the target and the power calculations were done using inverse square law relation (Günther 2014). In distributed spoofing scenario, the spoofers location is calculated by (2.63) and spatially deployed in the ranges of $1 - 5$Km away from the target and all the spoofers are dynamic in location. All the spoofers are at various ranges and driven with different transmitted powers.

Figure 2.6(a–h) shows the individual signal received power (dBW) for three different cases of no-spoofing, spoofing with the simulator, and proposed repeater based

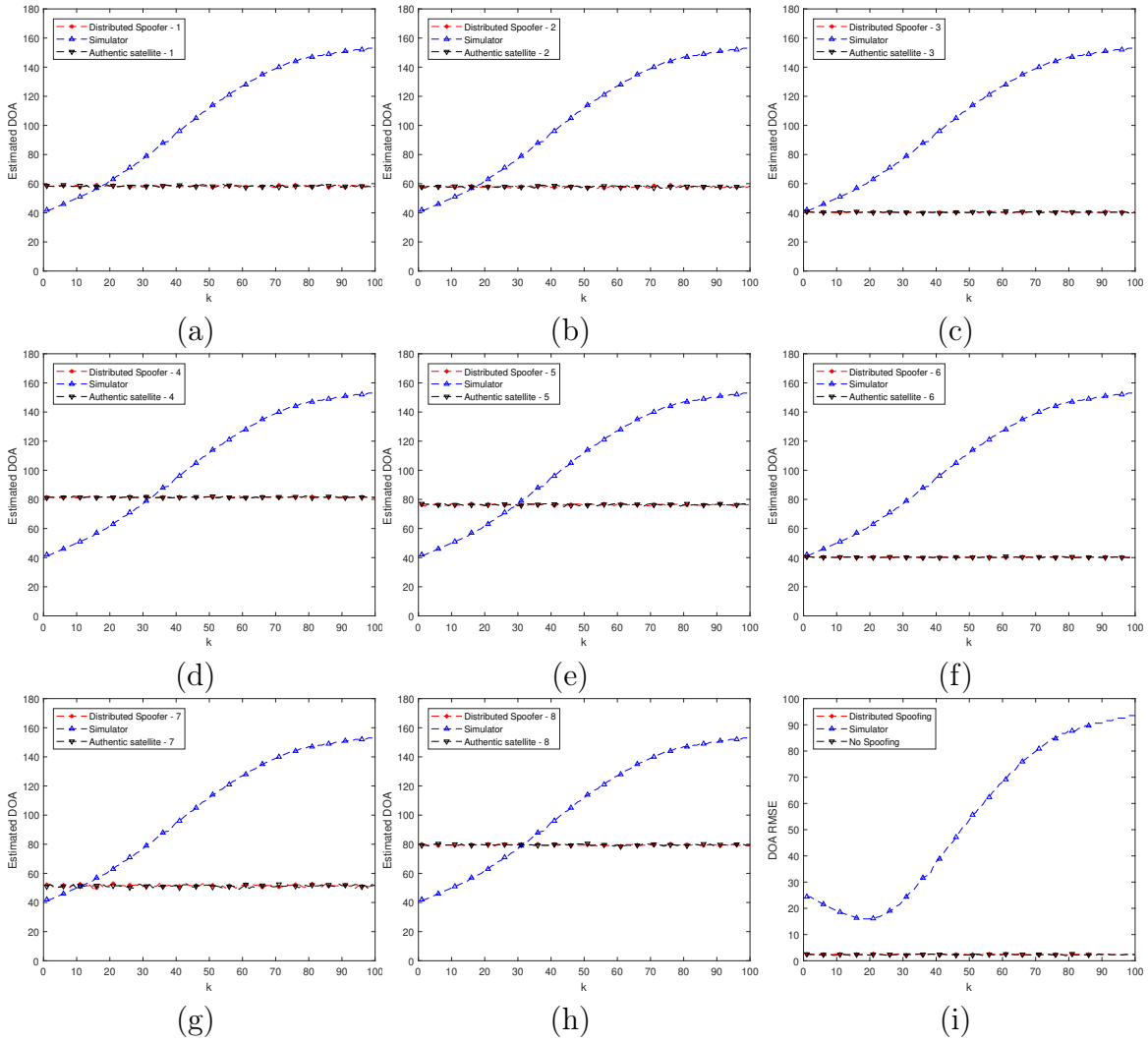

Figure 2.7: DOA estimation of signals using SS-MUSIC algorithm (Pal and Vaidyanathan 2010) (eight satellite signals, six linear antennas, 3200 snaps,and 100 Monto carlo runs) : (a – h) Estimated DOA for individual signal at SNR = 0dB.

distributed spoofing. As the power and distances are inversely related, the variation in distance (20,000Km) between GPS receiver to authentic satellite transmitter is insignificant, and it is observed in the figures that the power of the authentic satellite signals are almost equal with a maximum deviation of ±1dBW. However in simulator case, the received power varies drastically with the time varying behavior of the target. As spoofers posses tunable power gain, the transmitted power changes in accordance with the target kinematics and maintains almost a constant value. However, there is a small deviation in the received power due to estimation error of the tracker. The proposed algorithm provides improved results for power, as we observe insignificant deviation from upper and lower bounds (±6dBW) from critical value.

On the other hand, the simulator-based method also provides the individual signal power with in the boundaries due to higher distance between target and simulator. Further, all spoofer are in LOS and higher power results in stealthy spoofing, and the signals are locked onto the targeted GPS receiver. In addition, all the received power levels of the signals from the simulator are in-distinguishable and therefore ζ equals to one as given in (2.69). However, in the proposed repeater based distributed spoofing case, all the power levels are distinguishable and hence ζ is zero. Therefore proposed distributed spoofing is more stealthy and targeted GPS receiver is highly vulnerable for spoofing attacks. Furthermore, for all the three test cases, the average power is within the boundaries and therefore ζ is zero.

Based on the DOA of signals, the spoofing attack is detected in (Kang et al. 2017). For no-spoofing scenario, the trajectory of the satellites over the time is simulated by using (2.61)–(2.62) with an assumption of circular orbits. Whereas in simulator-based spoofing, the spatial location of the spoofer is static. In the proposed method, the spatial location of spoofers is in occlusion to the LOS of the satellite to target with $m = 10^{-3}$ and remains dynamic to maintain LOS throughout the simulation. The DOA of the received signals are estimated using SS-MUSIC algorithm (Pal and Vaidyanathan 2010) with a linear array of 6 sensors by considering 3200 snaps and SNR at 0dB. Figure 2.7(a–h) shows the DOA estimation of signals over time corresponding to the no-spoofing scenario, spoofing with a simulator and proposed repeater-based distributed spoofing. The proposed method provides improved performance compared to the simulator based spoofing. This is because, the spoofers are deployed in various locations and yields distinguishable DOA's. Whereas, in the simulator-based spoofing, the spoofing activity is detected ζ is one since all the signal sources are arriving from the same direction. Estimated DOA's in the proposed method are unique and unable to detect the presence of spoofing. Due to LOS of the spoofers, it is hard to detect spoofing by the target even though there is any prior information regarding the angle of arrivals from satellites.

2.5.7 Spoofing Accuracy Evaluation

Track breakages while tracking the target is one of the reasons for failure of spoofing activity. Track breakages are very common in target tracking due to target maneuver,

Table 2.1: Effectiveness of spoofing; $\zeta = 1$ (spoofing attack detected by anti-spoofing algorithm) and $\zeta = 0$ (spoofing attack not detected by anti-spoofing algorithm)

anti-spoofing algorithm	Simulator ζ	Proposed ζ
Satellite constellation	1	0
Distinguishable power levels (2.69)	1	0
Average power (2.70)	0	0
Distinguishable DOA (2.71)	1	0
Overall DOA	1	0

low detection probability, associating the track with a false alarm, and large measurement error. During track breakages, it is not possible to compute the external delay to be incorporated by the spoofer. Since the delay is a dependent parameter on the position estimate of a target as given in (2.42). Hence the spoof pseudorange cannot be generated by the spoofer. Since tracking is performed with IMM, less likely that track breakages occur around the turning interval for higher P_D. Whereas for lower P_D, track breakages are highly likely. The percentage of continuous tracks are shown in Table - 2.2. Only for continuous tracks, the spoof attack is successful. It can be seen that the proposed repeater-based distributed spoofing technique outperformed the simulator based spoofing due to the fusion of tracks. In high P_D case, when a track gets terminated, it is highly likely that a corresponding new track gets initiated within next few scans or ever before the termination of the old track. Consequently, the simulator based method shows inferior results to the proposed technique in lesser P_D case. In the proposed method, as a result of fusing the local state estimates, the tracking efficiency increases.

Table 2.2: % of continuous tracks by the tracker

		Simulator	Distributed spoofing
P_D	0.9	92	100
	0.7	83	97
	0.5	47	80

Here to quantify the spoofing, two different RMSE values are given. First, the $RMSE_{s-p}$ is defined as the root mean square error corresponding to spoof target

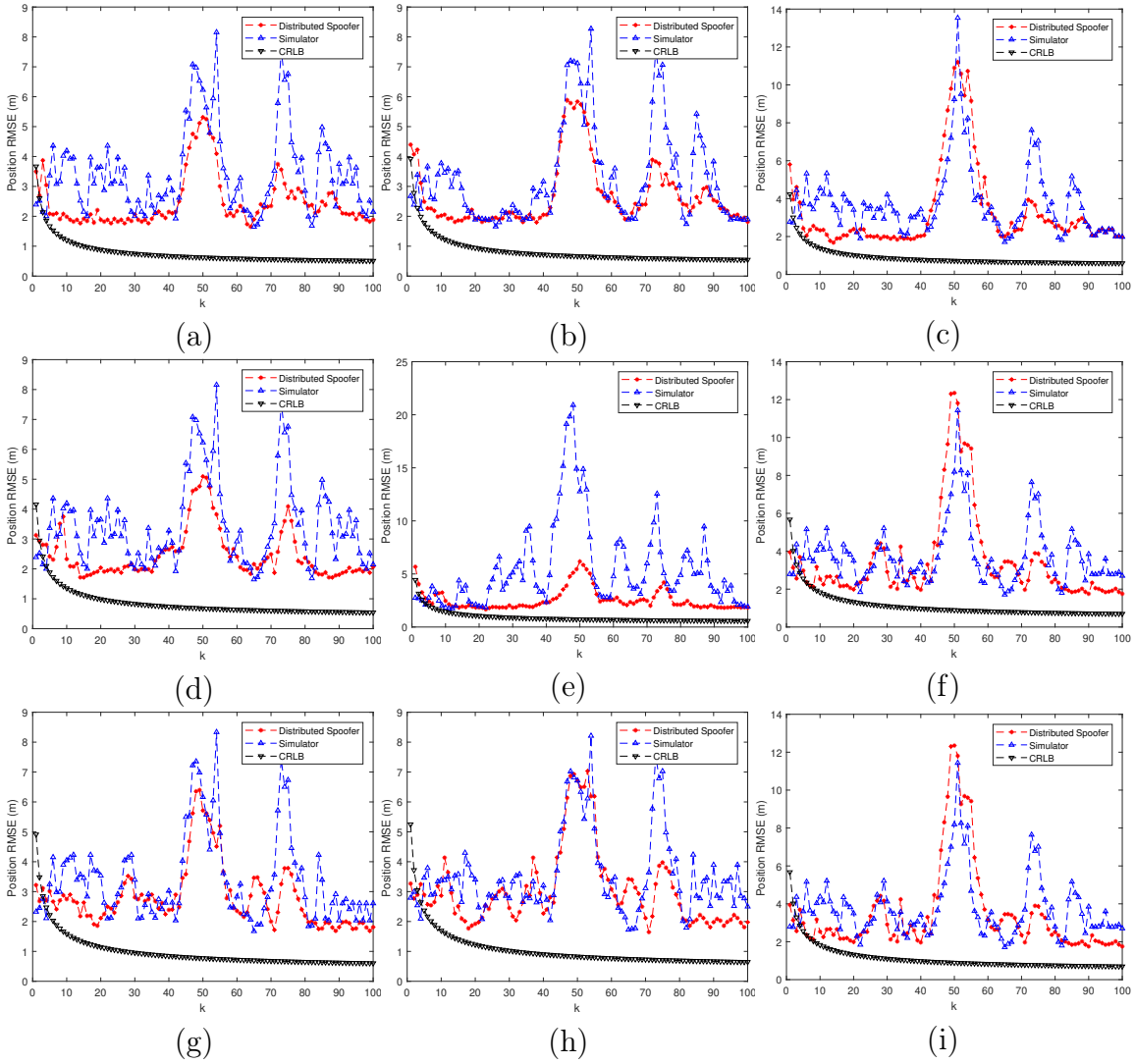

Figure 2.8: Position RMSE corresponding to spoof target trajectory to perception of target trajectory ($RMSE_{s-p}$) for ideal spoofing, spoofing by simulator and spoofing by proposed distributed spoofing case: ($\lambda = 1e^{-7}\text{m}^{-2}$ and Monto carlo runs = 100) (a) $P_D = 0.9$ and $N = 8$, (b) $P_D = 0.9$ and $N = 7$, (c) $P_D = 0.9$, and $N = 6$, (d) $P_D = 0.7$ and $N = 8$, (e) $P_D = 0.7$ and $N = 7$, (f) $P_D = 0.7$, and $N = 6$, (g) $P_D = 0.5$ and $N = 8$, (h) $P_D = 0.5$ and $N = 7$, (i) $P_D = 0.5$, and $N = 6$.

trajectory to target perception, which is useful to quantify how efficiently spoofing is carried out. Secondly, $RMSE_{t-p}$ is defined as the RMSE corresponding to true target trajectory to target perception to quantify whether the spoofing attack is carried out or not. The $RMSE_{t-p}$ values are plotted for $k \in$ [20–60] for better visualization. Two coordinate turns are considered in the trajectory $k \in [40 - 50]$ and $k \in [70 - 80]$. Figure 2.8 shows $RMSE_{s-p}$ for $P_D = 0.9$ with variation of number of satellites for spoofing with simulator and spoofing with proposed distributed spoofer case. We can clearly observe that, the RMSE increases as the number of satellites decreases.

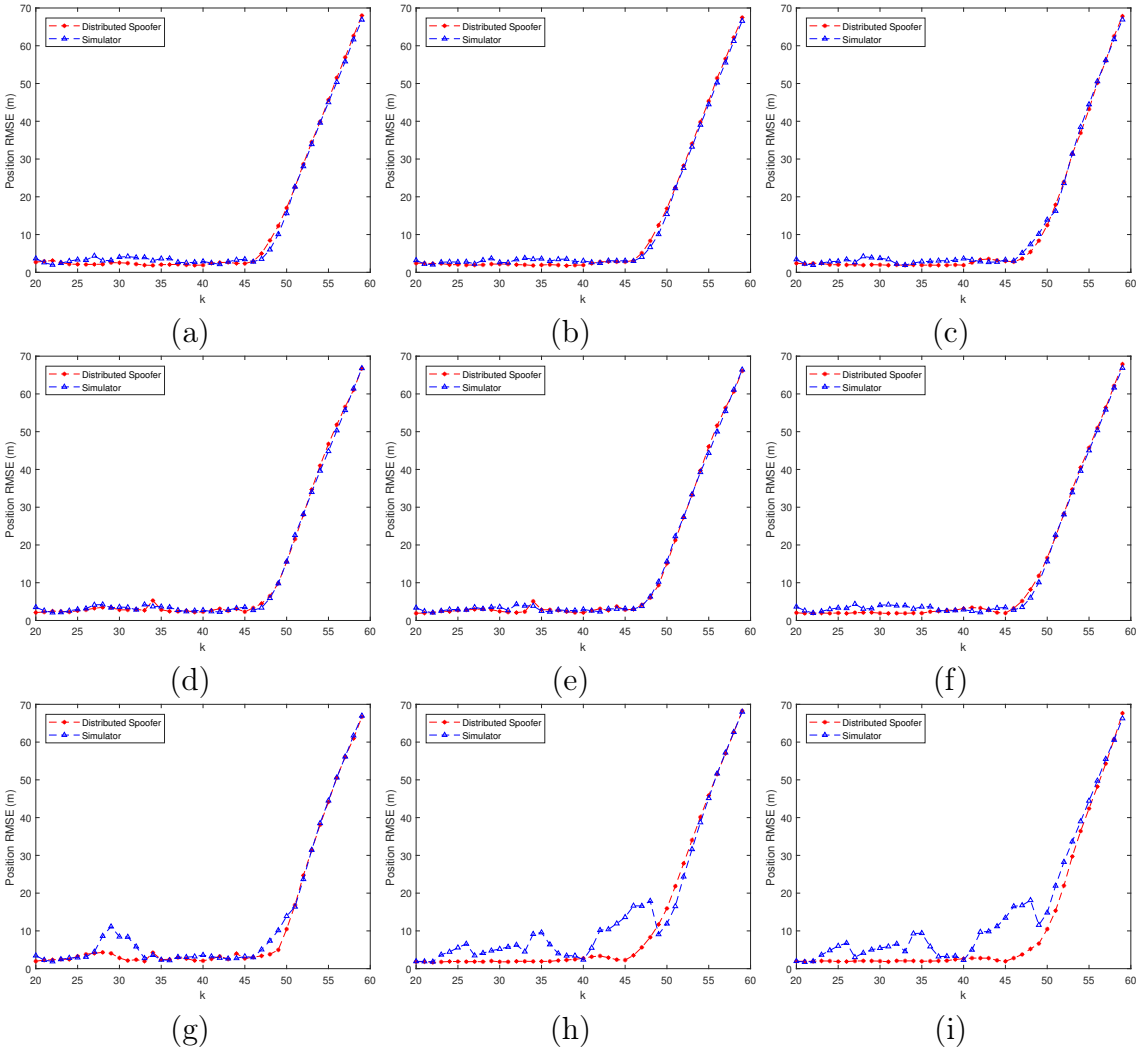

Figure 2.9: Position RMSE corresponding to actual target trajectory to perception of target trajectory ($RMSE_{t-p}$) for spoofing by simulator and spoofing by proposed distributed spoofer case: ($\lambda = 1e^{-7}\text{m}^{-2}$ and Monto carlo runs = 100) (a) $P_D = 0.9$ and $N = 8$, (b) $P_D = 0.9$ and $N = 7$, (c) $P_D = 0.9$, and $N = 6$, (d) $P_D = 0.7$ and $N = 8$, (e) $P_D = 0.7$ and $N = 7$, (f) $P_D = 0.7$, and $N = 6$, (g) $P_D = 0.5$ and $N = 8$, (h) $P_D = 0.5$ and $N = 7$, (i) $P_D = 0.5$, and $N = 6$.

Whereas once the satellite number reaches to seven, the $RMSE_{s-p}$ is nearly constant.

During the turning intervals, it can be seen that proposed distributed spoofing provides improved RMSE compared to simulator-based spoofing. This is because, the proposed distributed spoofing algorithm utilizes the advantage of IMM filtering and fusion of local estimates to achieve a global estimate. This leads to an increase in performance of spoofing even in the presence of clutter density and low detection probability.

Chapter 3

Stealthy GPS Spoofing in Multi-spoofer Multi-target Scenario: Spoofer-to-target Association

3.1 Mathematical Model for GPS Spoofing scenario

In this section, a generalized mathematical model is derived by assuming that multiple spoofers and multiple targets are present. The spoofing signals generation, transmission, and reception by the GPS receiver are modeled in this section. In GPS spoofing, the spoofer (s) transmits mimic GPS signals either by playback of previously captured signals or simulate the GPS signals. Let M 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 $\mathcal{S}$ is

$$\mathcal{S} = \{\mathbf{x}_m^s\}_{m=1}^{M};\ \mathbf{x}_m^s \in \mathbb{R}^3 \tag{3.1}$$

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

$$\mathcal{T} = \left\{\mathbf{x}_j^r\right\}_{j=1}^{J};\ \mathbf{x}_j^r \in \mathbb{R}^3 \tag{3.2}$$

Here, The superscript r represents the real position or the physical position of the GPS receiver. The spoofer m intends to create a fake-position $\mathbf{x}_{m,j}^f$ for the target j which is being located at $\mathbf{x}_j^r \in \mathbb{R}^3$ as shown in Figure 3.1. The superscript f represents the fake or spoofed, or false position. The subscript $\{m, j\}$ indicates the spoofer-to-target pre-association, which is defined as spoofer-to-target mapping before the spoofing process begins.

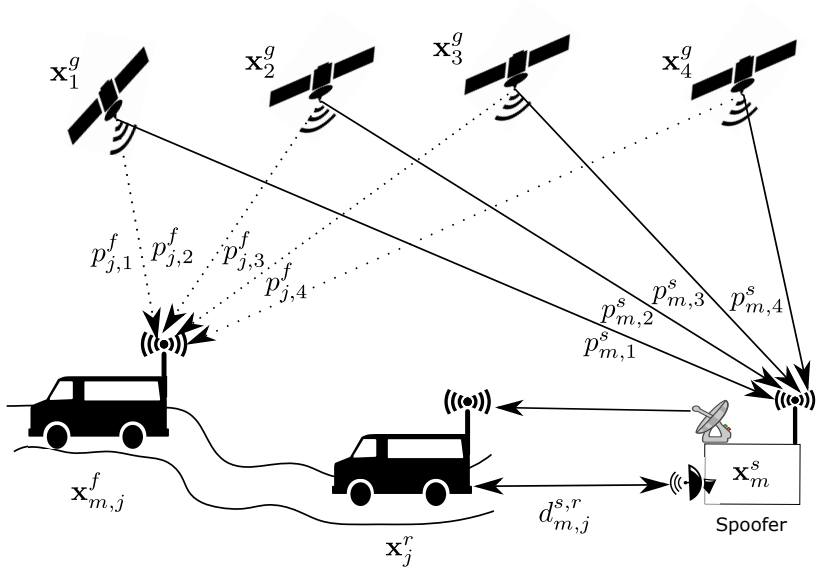

Figure 3.1: Illustration of location spoofing of a truck on a road scenario. The physical location of the truck is $\mathbf{x}_j^r$ and its spoofed location is $\mathbf{x}_{m,j}^f$, the spoofing achieved by using a spoofer which is being located at $\mathbf{x}_m^s$. (The dark lines from satellite-to-target represent the authentic signals. The dotted lines from satellite-to-target are due to transmission of spoofed signals from spoofer)

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 $\mathbf{x}_i^g$, 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 I satellite. The positions of the satellite are given by

$$\mathcal{X} = \{\mathbf{x}_i^g\}_{i=1}^I \,;\; \mathbf{X}_i \in \mathbb{R}^3 \tag{3.3}$$

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 Figure 3.1 for proper visualization. In the working principle of Figure 3.1, the spoofer located at $\mathbf{x}_m^s$ is having a receiver module to receive I authentic satellite signals; the received signals gets modify by the spoofer according to the intended spoof location $\mathbf{x}_{m,j}^f$ and transmit onto the target located at $\mathbf{x}_j^r$.

3.1.1 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 (Günther 2014). The spoofer located at $\mathbf{x}_m^s$ receives all authentic satellite signals in the range as

$$\psi\left(\mathbf{x}_m^s, t\right) = \sum_{i=1}^{I} A_{i,m}\psi_{i,m}\left(t - \frac{\mid \mathbf{x}_m^s - \mathbf{x}_i^g \mid}{c}\right) + n\left(\mathbf{x}_m^s, t\right), \tag{3.4}$$

where $A_{i,m}$ is signal attenuation due to transmission from $\mathbf{x}_i^g$ to $\mathbf{x}_m^s$. Whereas, $\mid \mathbf{x}_m^s - \mathbf{x}_i^g \mid$ and $n\left(\mathbf{x}_m^s, t\right)$ 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

$$\psi\left(\mathbf{x}_m^s, t'\right) = \sum_{i=1}^{I} A_{i,m}\psi_{i,m}\left(t - \delta_{i,m}^s\right) + n\left(\mathbf{x}_m^s, t'\right). \tag{3.5}$$

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

$$p_{i,m}^s = \sqrt{(x_m^s - x_i^g)^2 + (y_m^s - y_i^g)^2 + (z_m^s - z_i^g)^2} + b. \tag{3.6}$$

Where $\mathbf{x}_i^g = [x_i^g, y_i^g, z_i^g]'$, $\mathbf{x}_m^s = [x_m^s, y_m^s, z_m^s]'$, 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 (Malyshev et al. 2018). The spoofer m 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

$$\psi\left(\mathbf{x}_m^s, t'\right) = \sum_{i=1}^{I} A_{i,m}\psi_{i,m}\left(t - \delta_{i,m}^s - \delta_{i,m,j}\right) + n\left(\mathbf{x}_m^s, t'\right). \tag{3.7}$$

The external time delay offered to the i^{th} satellite signal by the m^{th} spoofer to the j^{th} target is given by $\delta_{m,j,i}$. This external delay being offered in MSMT is analogous to derivation of single-target single-spoofer external delay calculation as given in (Kerns et al. 2014). By following the geometrical derivation as given in (Kerns et al. 2014), the calculated external delay by the spoofer m for target j pertaining to signal i is $\delta_{i,m,j}$, given by

$$\delta_{i,m,j} = \frac{p_{i,j}^f - p_{i,m}^s - d_{m,j}^{s,r}}{c}. \tag{3.8}$$

Here $p^f_{i,j}$ is the spoofed pseudorange between $\mathbf{x}^g_i$ and $\mathbf{x}^f_{m,j}$ and is given by

$$p^f_{i,j} = \sqrt{(x^f_j - x^g_i)^2 + (y^f_j - y^g_i)^2 + (z^r_f - z^g_i)^2} + b \tag{3.9}$$

Whereas $\mathbf{x}^r_j = [x^r_j, y^r_j, z^r_j]'$, and $p_{i,m}$ is the pseudorange between $\mathbf{x}^g_i$ and $\mathbf{x}^s_j$, as shown in Figure 3.1. The distance between spoofer k to the target j is $d^{s,r}_{m,j}$. In practice, this distance calculation is carried out by using any range measuring devices like radar, visual sensor, and lidar, etc. But, to simplify this problem, we assumed that the distance between spoofer and target is known precisely. The $d^{s,r}_{m,j}$ is the euclidean distance or the range between spoofer and target, is represented as

$$d^{s,r}_{m,j} = \sqrt{(x^s_m - x^r_j)^2 + (y^s_m - y^r_j)^2 + (z^s_m - z^r_j)^2}. \tag{3.10}$$

3.1.2 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 Figure 3.2, where the target of interest is $\mathbf{x}^r_j$, but the near by target is $\mathbf{x}^r_l$. The simulated repeater signals for target $\mathbf{x}^r_j$ locked onto the target $\mathbf{x}^r_l$. So the generalized receiving signal is modeled for any target in the surveillance. Therefore, in general the target located at $\mathbf{x}^r_l$ receives the composite signal as

$$\psi\left(\mathbf{x}^r_l, t'\right) = \sum_{i=1}^{I} A_{i,l}\psi_{i,l}\left(t - \delta^s_{i,l} - \delta_{i,m,j} - \frac{d^{s,r}_{m,l}}{c}\right) + n\left(\mathbf{x}^r_l, t'\right). \tag{3.11}$$

Here $l \in \{1, \ldots, J\}$. For $l = j$, the above equation states that all the signals transmitted by spoofer m 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 m are locked onto l^{th} target, which is not a target of interest. That is, the pre-association

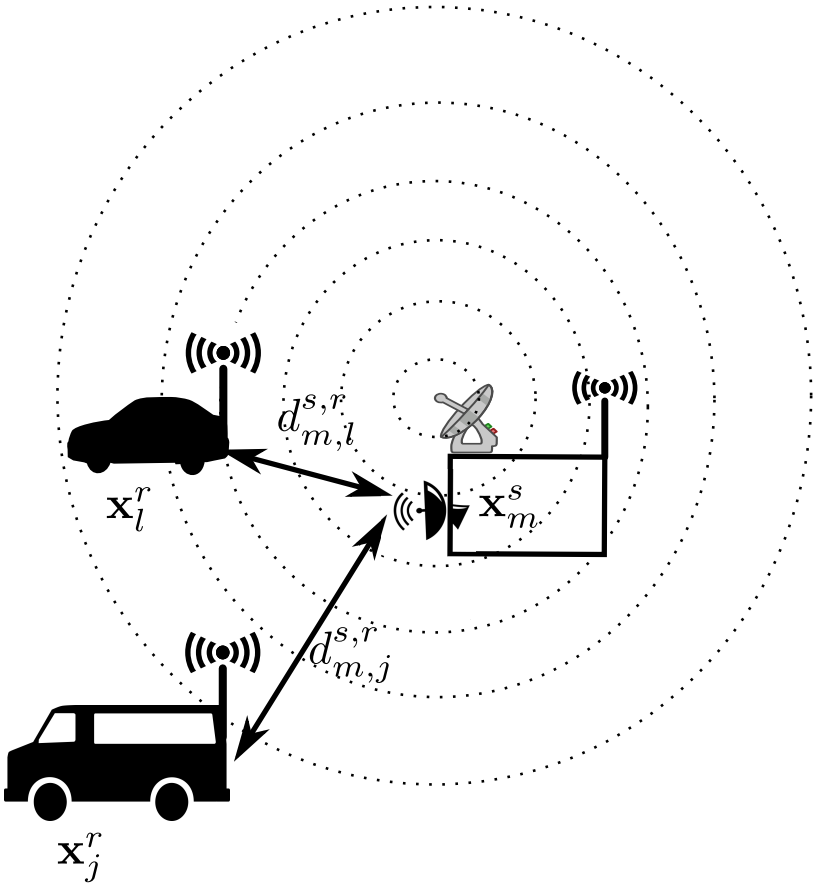

Figure 3.2: Illustration of multiple targets and single omni-directional spoofer scenario (The dotted circle represents the direction of the spoofed signals generated by the spoofer).

and post-associations are different; this is considered as unsuccessful spoofing. After processing the $\psi(\mathbf{x}^r_l, t')$ signals, the pseudorange measurements obtained are given by

$$p^{s,r}_{i,m,l} = c\left(\delta^s_{i,m} + \delta_{i,m,j} + \frac{d^{s,r}_{m,l}}{c}\right). \tag{3.12}$$

Substituting $\delta^s_{i,m} = \frac{z^s_{i,m}}{c}$ and (3.8) in (3.12) yields

$$p^{s,r}_{i,m,l} = c\left(\frac{p^s_{i,m}}{c} + \frac{p^f_{i,j} - p^s_{i,m} - d^{s,r}_{m,j}}{c} + \frac{d^{s,r}_{m,l}}{c}\right). \tag{3.13}$$

Solving the above (3.13) gives

$$p^{s,r}_{i,m,l} = p^f_{i,j} - d^{s,r}_{m,j} + d^{s,r}_{m,l}. \tag{3.14}$$

Here $\{m, j\}$ is the pre-association and $\{m, l\}$ is the post-association. If this pre-association and post-association are equal, then the spoofing is successful, else unsuccessful. The (3.14) 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 m is $\left\{p_{m,l,i}^{s,r}\right\}_{i=1}^{I} = \{p_i\}_{i=1}^{I}$. Now, we are removing the superscripts and subscripts to avoid further confusion in the mathematical equations in the following Subsections. However, we use the actual terms whenever required without loosing the generality.

3.1.3 Iterative Least Squares Framework for GPS positioning

The generalized form of pseudorange measurement p_i is given by

$$p_i = \sqrt{(x_i^g - x)^2 + (y_i^g - y)^2 + (z_i^g - z)^2} + c(dt_i - dt) + w_i \tag{3.15}$$

where $c(dt_i\text{-}dt)$ is the bias term equivalent to b.
The geometrical range is $\sqrt{(x_i^g - x)^2 + (y_i^g - y)^2 + (z_i^g - z)^2}$. Here $\mathbf{x}$ is an unknown position $[x, y, z]'$, and w_i represents zero-mean white Gaussian noise with covariance $\mathbf{R}$. 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 I. 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 (Abel and Chaffee 1991).

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 u be the iteration number and U be the total number of iterations i.e., $u = 1, 2, ..., U$. The position estimate improves iteratively. Generalizing, the nominal state for u^{th} iteration is $\hat{\mathbf{x}}_u = [x_u, y_u, z_u, dt_u]'$. The approximate pseudorange that is computed from the satellite position $\mathbf{x}_i$ to nominal position $\mathbf{x}_u$ is given by $\rho_{i,u}$. Where $\rho_{i,u} = \sqrt{(x_i^g - x_u)^2 + (y_i^g - y_u)^2 + (z_i^g - z_u)^2}$ 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 $[\Delta x_u, \Delta y_u, \Delta z_u]'$ is added to the approximate receiver

position $[x_u, y_u, z_u]$ to update the receiver position as

$$\begin{aligned} x_{u+1} &= x_u + \Delta x_u, \\ y_{u+1} &= y_u + \Delta y_u, \\ z_{u+1} &= z_u + \Delta z_u. \end{aligned} \tag{3.16}$$

Based on the relation, the right hand sided of (4.10) is linearized using the first order Taylor series expansion. whereas the Taylor series expansion for $\rho_{i,u+1}$ is

$$\rho_{i,u+1} = \rho_{i,u} + \frac{\partial \rho_{i,u}}{\partial x_u}\Delta x_u + \frac{\partial \rho_{i,u}}{\partial y_u}\Delta y_u + \frac{\partial \rho_{i,u}}{\partial z_u}\Delta z_u. \tag{3.17}$$

The partial derivatives are given by

$$\begin{aligned} \frac{\partial \rho_{i,u}}{\partial x_u}\Delta x_u &= \frac{x_i^g - x_u}{\rho_{i,u}}, \\ \frac{\partial \rho_{i,u}}{\partial y_u}\Delta y_u &= \frac{y_i^g - y_u}{\rho_{i,u}}, \text{ and} \\ \frac{\partial \rho_{i,u}}{\partial z_u}\Delta z_u &= \frac{z_i^g - z_u}{\rho_{i,u}}. \end{aligned} \tag{3.18}$$

The first ordered linearized form of observation equation is

$$\begin{aligned} p_{i,u} &= \rho_{i,u} - \frac{x_i^g - x_u}{\rho_{i,u}}\Delta x_u - \frac{y_i^g - y_u}{\rho_{i,u}}\Delta y_u \\ &\quad - \frac{z_i^g - z_u}{\rho_{i,u}}\Delta z_u + c(dt_u - dt) + w_i, \end{aligned} \tag{3.19}$$

where b_u is the estimated clock error at the receiver. Re-arranging the above equation yields

$$\begin{bmatrix} -\frac{x_i^g - x_u}{\rho_{i,u}} & -\frac{y_i^g - y_u}{\rho_{i,u}} & -\frac{z_i^g - z_u}{\rho_{i,u}} & 1 \end{bmatrix} \begin{bmatrix} \Delta x_u \\ \Delta y_u \\ \Delta z_u \\ cdt_i \end{bmatrix} = b_{i,u}, \tag{3.20}$$

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

$$\min \| \mathbf{H}_u \hat{\mathbf{x}}_u - \mathbf{b}_u \|, \tag{3.21}$$

where

$$\mathbf{H}_u = \begin{bmatrix} -\frac{x_1^g - x_u}{\rho_{1,u}} & -\frac{y_1^g - x_u}{\rho_{1,u}} & -\frac{z_1^g - x_u}{\rho_{1,u}} & 1 \\ -\frac{x_2^g - x_u}{\rho_{2,u}} & -\frac{y_2^g - x_u}{\rho_{2,u}} & -\frac{z_2^g - x_u}{\rho_{2,u}} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ -\frac{x_I^g - x_u}{\rho_{I,u}} & -\frac{y_I^g - x_u}{\rho_{I,u}} & -\frac{z_I^g - x_u}{\rho_{I,u}} & 1 \end{bmatrix}, \tag{3.22}$$

and $\mathbf{x}_u = [\Delta x_u, \Delta y_u, \Delta z_u, cdt_u]$. The approximate receiver position is updated for every iteration. This iteration process continues until the solution reaches to desired accuracy or till U. Here from (4.15), we can observe that $\hat{\mathbf{x}}$ minimizes the length of the error vector $\hat{\mathbf{e}}_u$. The sum of squares of I separate errors is given by

$$|| \mathbf{e}_u ||^2 = (\mathbf{b}_u - \mathbf{H}_u \mathbf{x}_u)'(\mathbf{b}_u - \mathbf{H}_u \mathbf{x}_u). \tag{3.23}$$

By minimizing the quadratic form (4.17) gives

$$\hat{\mathbf{x}}_u = (\mathbf{H}_u' \mathbf{H}_u)^{-1} \mathbf{H}_u' \mathbf{b}_u. \tag{3.24}$$

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 $(\mathbf{H}'\mathbf{H})^{-1}$.

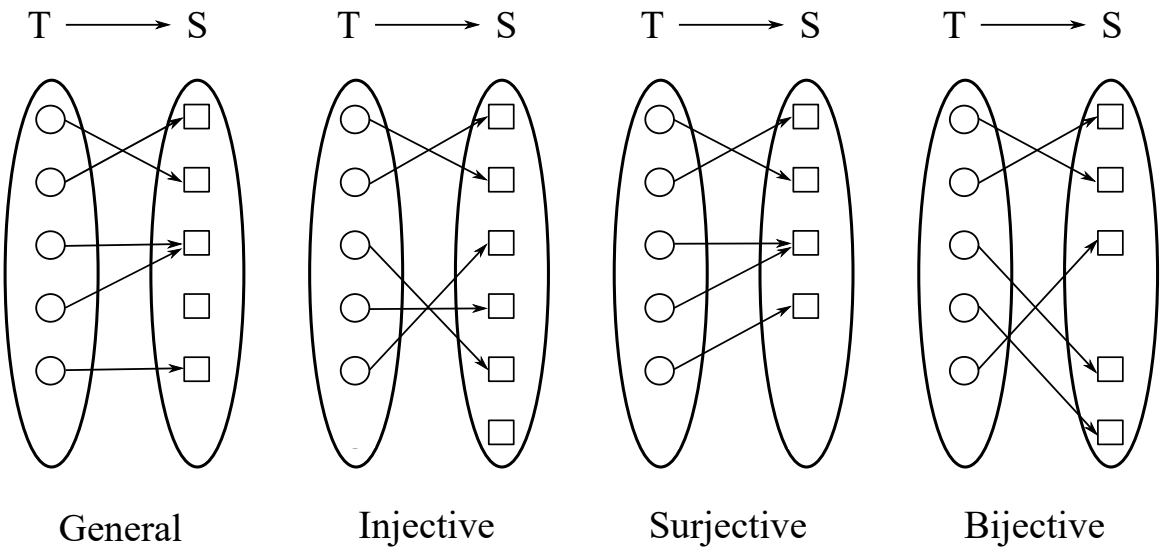

Figure 3.3: Different types of assignments involved in multi-spoofer multi-target scenario.

3.2 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 $\mathcal{S}$ and set of targets $\mathcal{T}$ are present. Where, $\mathcal{T}$ is the set of targets given by $\{T_j\}_{j=1}^{J}$ and $\mathcal{S}$ be the set of spoofers represented as $\{S_m\}_{m=1}^{M}$. Here T_j and S_m are target-ID and spoofer-ID respectively. Traditionally, the transmitting power of the spoofers is a constant value and equal to p_m^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 m is given by

$$P_{m,j}^{s,r} = \frac{P_m^s}{4\pi \left(d_{m,j}^{s,r}\right)^2}. \tag{3.25}$$

The $d_{m,j}^{s,r}$ is the euclidean distance as given in (3.10). 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.

3.2.1 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 ($J = M$). Therefore, M spoofers are governing M targets in the given surveillance region. The pre-association between $\mathcal{T}$ and $\mathcal{S}$ 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 $\mho_{BS} : \mathcal{T} \to \mathcal{S}$ is a bijective as shown in Figure 3.3. The bijective assignment states that every element in $\mathcal{T}$ has $\mathcal{S}$, and every

element has a unique mapping, and no element is left out in these sets.

$$\begin{aligned}\mho_{BS} =&\{(T_j, S_m) \mid j, m \in \mathbb{R};\ j, m = 1, \cdots, M \\ &\text{Association is bijective}\}\end{aligned} \tag{3.26}$$

After spoofing, there is a likelihood that multiple targets are associated with the same spoofer, and the relation between $\mathcal{T}$ and $\mathcal{S}$ becomes general, as shown in Figure 3.3. A general assignment where $\mathcal{S}$ can have many elements from $\mathcal{T}$ and few elements in $\mathcal{S}$ may/may not be assigned. The association after spoofing is represented as $\mho_{AS}$. Where $\mho_{AS} : \mathcal{T} \rightarrow \mathcal{S}$ is a general assignment. The modified mapping after spoofing is

$$\begin{aligned}\mho_{AS} =&\{(T_j, S_m) \mid j, m \in \mathbb{R};\ j, m = 1, \ldots, M \\ &\text{Association is a general}\}\end{aligned} \tag{3.27}$$

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

$$D = \begin{bmatrix} d^{s,r}_{1,1} & \cdots & d^{s,r}_{1,j} & \cdots & d^{s,r}_{1,M} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ d^{s,r}_{m,1} & \cdots & d^{s,r}_{m,j} & \cdots & d^{s,r}_{m,M} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ d^{s,r}_{M,1} & \cdots & d^{s,r}_{M,j} & \cdots & d^{s,r}_{M,M} \end{bmatrix} \tag{3.28}$$

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

$$D_{NN} = \min_{m,j} \sum_{m}^{M} \sum_{j}^{M} d^{s,r}_{m,j} \xi_{m,j} \tag{3.29}$$

subjected to

$$\sum_{j}^{M} \xi_{m,j} = 1 \ \forall m$$

where $\xi_{m,j}$ is binary association variable such that $\xi_{m,j} = 1$, 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.

3.2.2 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 (3.28) is solved as following

$$D_{GNN} = \min_{m,j} \sum_{m}^{M} \sum_{j}^{M} d_{m,j}^{s,r} \xi_{m,j} \tag{3.30}$$

subjected to

$$\sum_{j}^{M} \xi_{m,j} = 1 \ \forall m$$

$$\sum_{m}^{M} \xi_{m,j} = 1 \ \forall j$$

Where $\psi_{m,j}$ is a binary association variable such that $\psi_{m,j} = 1$ if the spoofer is associated with a particular target. Otherwise, it is set to zero. By optimizing the above problem, the pre-association is $\mho_{BS} : \mathcal{T} \rightarrow \mathcal{S}$ is bijective as shown in Figure 3.3. 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 $\mho_{AS} : \mathcal{T} \rightarrow \mathcal{S}$ 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.

3.2.3 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

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 $d_{m,j}^{s,r}; m = 1, \ldots, M, j = 1, \ldots, M+i$
    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 {m,j}, 100% hit ratio not possible and exit
    end if
  end for
end procedure

a centralized node to make pre-association. Let K additional spoofers be included in the set $\mathcal{S}$ and existing $\mathcal{M}$ spoofers to complete the set $\mathcal{S}$. Now, the total number of spoofers in the set $\mathcal{S}$ be $L = M + K$. The extra spoofers are included in the existing spoofers set $\mathcal{S}$ to form a new post-association as

$$D_{NN}^* = \min_{m,j} \sum_{m}^{L} \sum_{j}^{M} d_{m,j}^{s,r} \xi_{m,j} \tag{3.31}$$

subjected to

$$\sum_{j}^{M} \xi_{m,j} = 1 \ \forall m$$

Similarly, the GNN association for the new S is

$$D_{GNN}^* = \min_{m,j} \sum_{m}^{M} \sum_{j}^{L} d_{m,j}^{s,r} \xi_{m,j} \tag{3.32}$$

subjected to

$$\sum_{j}^{M} \xi_{m,j} \leq 1 \ \forall m$$

$$\sum_{m}^{M} \xi_{m,j} = 1 \ \forall j$$

Where $\xi_{m,j}$ is a binary association variable such that $\xi_{m,j} = 1$ 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 $\mho_{BS} : \mathcal{T} \rightarrow \mathcal{S}$ is injective as shown in Figure 3.3. Injective is a class of sets, where all the elements in $\mathcal{T}$ are uniquely

mapped onto $\mathcal{S}$ and few elements of $\mathcal{S}$ are empty, i.e., not mapped to any element in $\mathcal{T}$.

$$\begin{aligned}\mho_{BS} =&\{(T_j, S_m) \mid j, m \in \mathbb{R};\ j = 1, \ldots, M \text{and } m = 1, \cdots L \\ &\text{Association is injective}\}\end{aligned} \tag{3.33}$$

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 $\mho_{BS} : \mathcal{T} \to \mathcal{S}$ is bijective and is represented as

$$\begin{aligned}\mho_{BS} =&\{(T_j, S_m) \mid j, m \in \mathbb{R};\ j, m = 1, \cdots M - P \\ &\text{Association is bijective}\}\end{aligned} \tag{3.34}$$

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

$$\begin{aligned}\mho_{AS} =&\{(T_j, S_m) \mid j, m \in \mathbb{R};\ m = 1, \cdots J - P, j = 1, \ldots J \\ &\text{Association is surjective}\}\end{aligned} \tag{3.35}$$

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

3.2.4 Centralized Spoofing with Tunable Power based GNN Association

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

$$P = \begin{bmatrix} p_{1,1}^{s,r} & \cdots & p_{1,j}^{s,r} & \cdots & p_{1,M}^{s,r} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ p_{m,1}^{s,r} & \cdots & p_{m,j}^{s,r} & \cdots & p_{m,M}^{s,r} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ p_{L,1}^{s,r} & \cdots & p_{L,j}^{s,r} & \cdots & p_{L,M}^{s,r} \end{bmatrix} \tag{3.36}$$

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

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

The above cost matrix is formulated as

$$P_{GNN}^* = \max_{m,j} \sum_{m}^{L} \sum_{j}^{M} p_{m,j}^{s,r} \xi_{m,j} \tag{3.37}$$

subjected to

$$\sum_{j}^{M} \xi_{m,j} \leq 1 \ \forall m$$

$$\sum_{m}^{L} \xi_{m,j} = 1 \ \forall j$$

where $\xi_{m,j}$ is a binary association variable such that $\xi_{m,j} = 1$ 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

$$P_{NN}^* = \max_{m,j} \sum_{m}^{L} \sum_{j}^{M} p_{m,j}^{s,r} \xi_{m,j} \tag{3.38}$$

subjected to

$$\sum_{j}^{M} \xi_{m,j} = 1 \ \forall m$$

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 m^{th} spoofer is p_m^*. Hence, the received power by r^{th} target is p_{mj}^*. The selection of modified transmitting powers is calculated by using the Algorithm-II

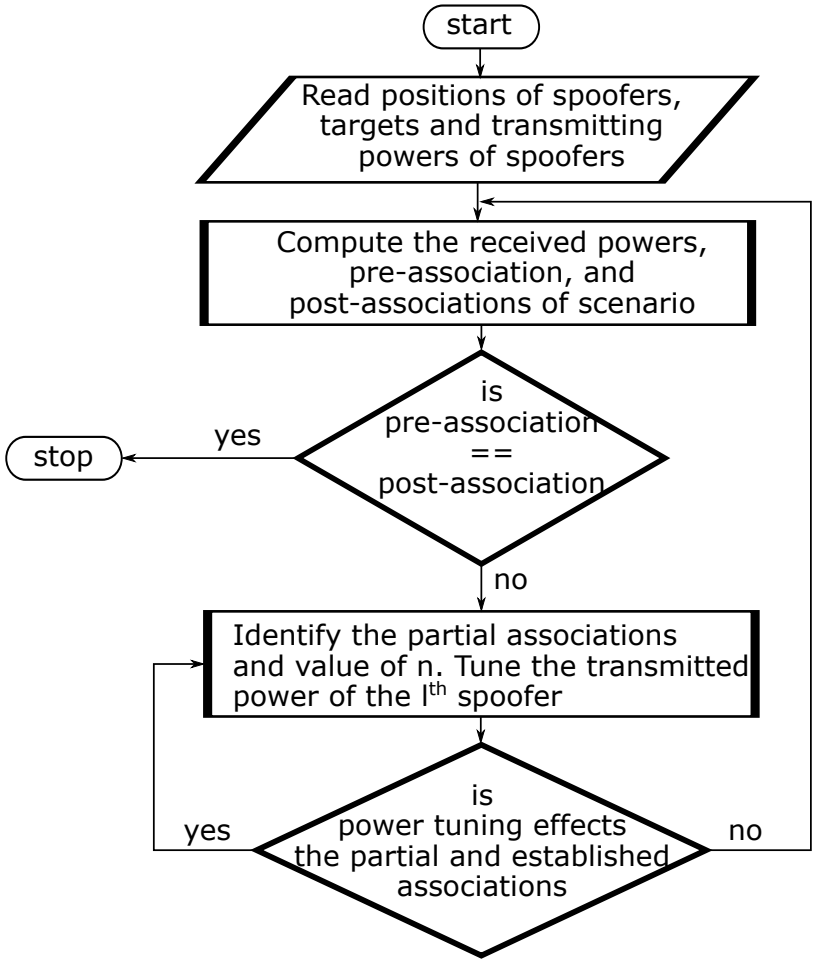

Figure 3.4: Flow chart for Algorithm-2.

3.3 Results and Discussions

3.3.1 Scenario Generation

The satellite location set $\{\mathbf{x}_i\}_{i=1}^{I}$ is modeled using WGS-84 model and follows the assumption of circular orbits as given in Section-1.1.8. 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 frame are shown in Table. 3.1. In Table. 3.1, the indexes m and j indicates the spoofer-ID and target-ID

Table 3.1: The spoofer-to-target mapping and its respective positions in local coordinates

m	$\mathbf{x}_m^s$	j	$\mathbf{x}_j^r$	$\mathbf{x}_{m,j}^f$
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]	-	-	-

respectively. The $\mathbf{x}_m^s$ and $\mathbf{x}_j^r$ are physical locations of spoofer-ID m 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 $\mathbf{x}_{m,j}^f$.

3.3.2 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.

A 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 $T_j \rightarrow S_m$ denotes that the target-ID T_j is to be locked with the sensor-ID S_m. The visualization of the spoofers individual locations and target physical locations and projected fake locations are represented in Figure 3.5. Moreover, the pre-association is also depicted in the Figure 3.5 as (T_j, S_m).

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

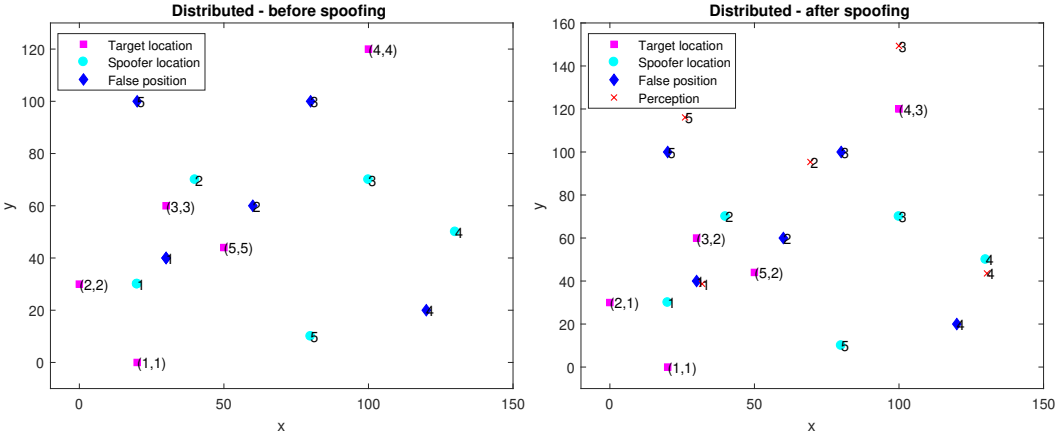

Figure 3.5: The pre-association and post association in distributed spoofing

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. 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 Figure 3.5. 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

$$\text{Hit ratio (HR)} = \frac{\text{Number of correct associations}}{\text{Total number of associations}} \tag{3.39}$$

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.

B 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 (3.30), the pre-associations are presented in Figure 3.6.

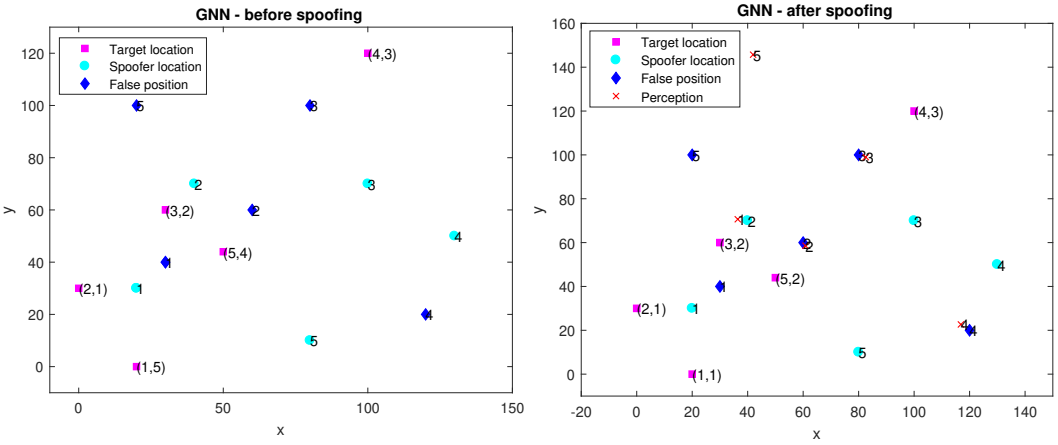

Figure 3.6: The pre-association and post association in centralized GNN spoofing

Therefore, the spoofer-to-target pre-association after solving the minimization problem (3.30) 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 Figure 3.6 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.

C 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., ${}^{8}C_{5}$ 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 Figure 3.7 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.

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

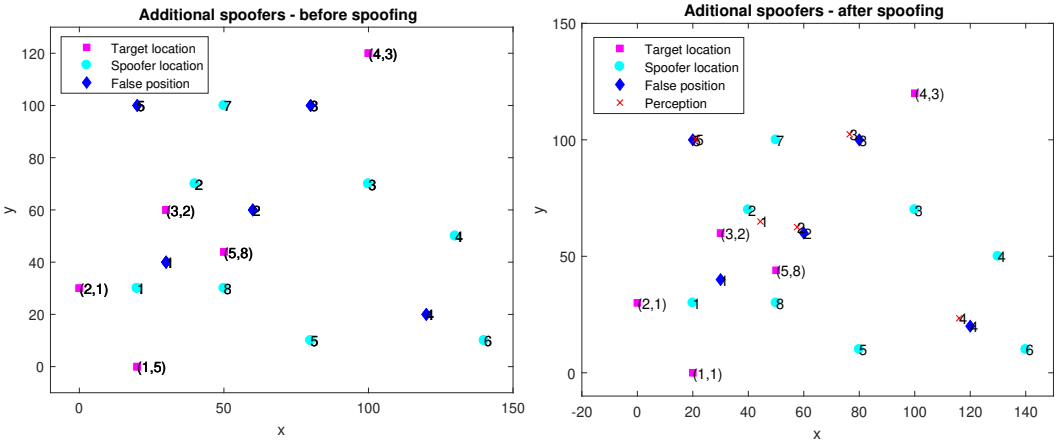

Figure 3.7: The pre-association and post association in opportunistic GNN spoofing

to the new association of $(5, 8)$, the target-5 is in successful spoofing and is observed in Figure 3.7. From Figure 3.7, 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 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.

D 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 (3.37) is shown in Figure 3.8. 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 $\mho_{BS} : \{1 \to 5, 2 \to 1, 3 \to 2, 4 \to 3, 5 \to 4\}$.

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 Figure 3.8. 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

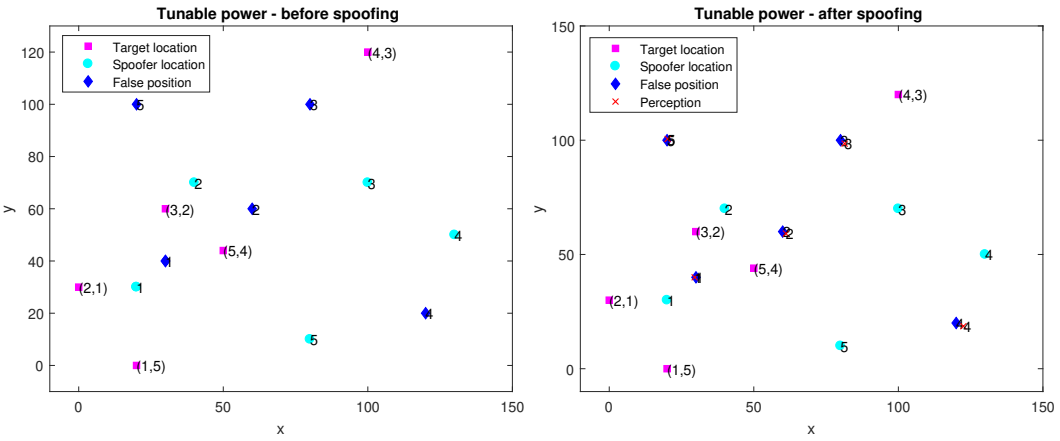

Figure 3.8: The pre-association and post association in tunable power of spoofers

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.

3.3.3 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.

Figure 3.9(a) 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

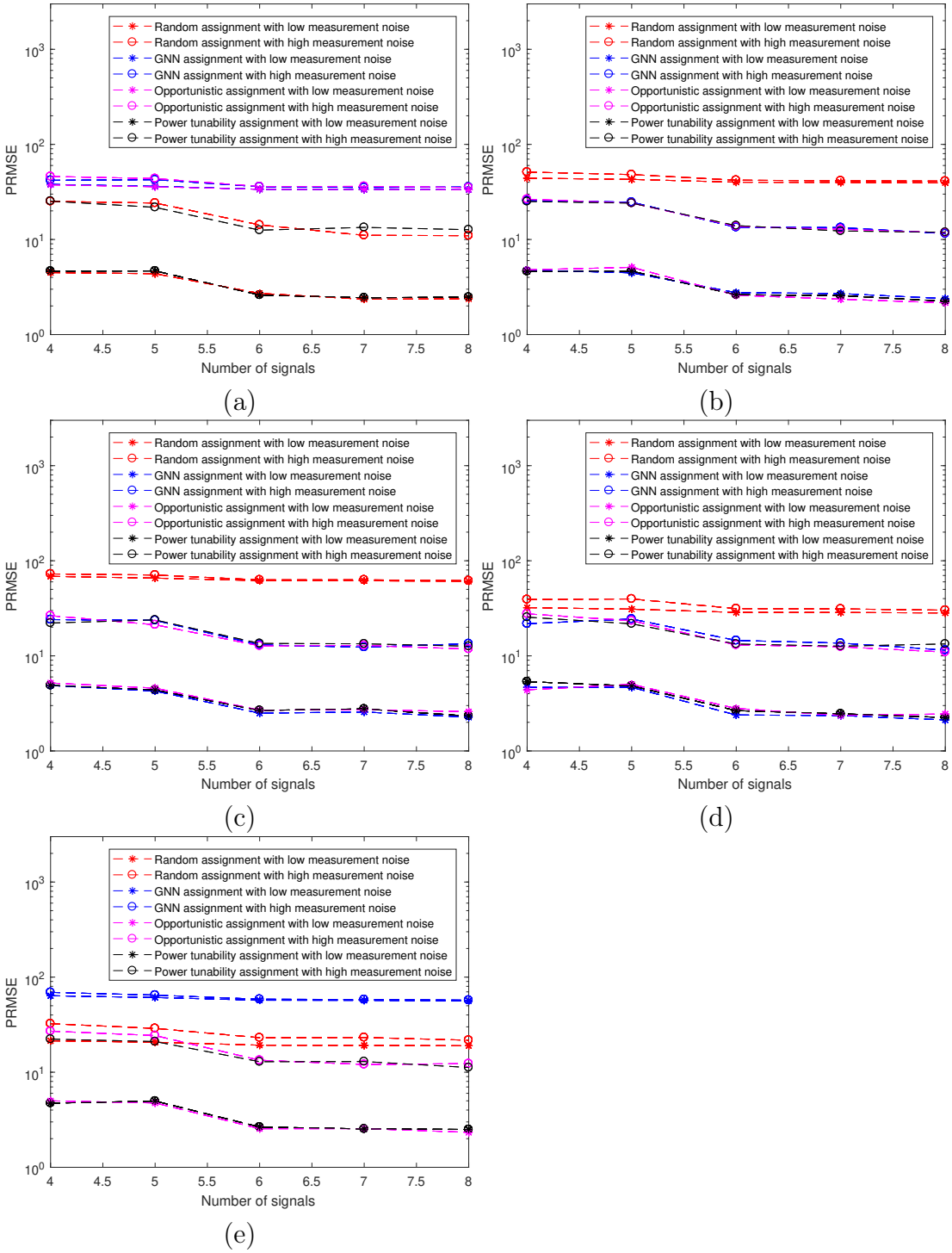

Figure 3.9: The PRMSE for various scenarios (a) target-1, (b) target-2, (c) target-3, (d) target-4, and (e) target-5

by using the ILS algorithm. From Figure 3.9(a), 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 Figure 3.9(b) and Figure 3.9(c) 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 Figure 3.9(d) and Figure 3.9(e) 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 Figure 3.9(d) 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.

Chapter 4

Anti-spoofing in Single-spoofer Single-target Scenario: M-best Association

4.1 Problem Formulation

This section describes GPS receiver in a clean environment, GPS receiver in spoofer only environment, and GPS receiver with an authentic and spoofed environment.

4.1.1 GPS Receiver in Clean Environment

The GPS receiver uses satellite transmitters located at $\mathbf{X}_i^r \in \mathbb{R}^3$. The satellite-based transmitted signals are $\{\psi_i^r(t)\}_{i=1}^I$, where I represents the number of satellites governing in the range. Here, we assumed that all the satellite transmitters are equipped with synchronized clock with no clock offset among them to extract the exact system time t' as given in (Tippenhauer et al. 2011). However, this assumption is not valid in reality due to presence of clock offset in the satellites. In practice, this offset is transmitted in the navigation message, the receiver decodes the navigation message and uses the information to remove the clock offset from the measurement. The navigation signal $\psi_i^r(t)$ consists of satellite position, transmission timestamp, satellite health, and satellite trajectory deviation information. These satellite signals are propagated with the speed of light c and received by the GPS receiver, located at $\mathbf{x}^r \in \mathbb{R}^3$ to estimate its position. The received combined signals of all satellites in the range are

$$\psi^r(\mathbf{x}^r, t) = \sum_{i=1}^{I} A_i \psi_i^r \left(t - \frac{\mid \mathbf{X}_i^r - \mathbf{x}^r \mid}{c} \right) + n^r(\mathbf{x}^r, t). \tag{4.1}$$

A_i is the signal's attenuation due to the propagation of the signal from the satellite location to the target receiver. $n^r(\mathbf{x}^r, t)$ is the background noise. Due to the properties of the navigation signal $\psi_i(t)$, the receiver separates individual terms and extract the satellite ID, relative spreading code phase using replica of the used spreading code. Highly stable clocks like cesium oscillators are costly to employ in civilian GPS receivers. The GPS receivers cannot have two-way clock synchronization, 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

$$\psi^r(\mathbf{x}^r, t') = \sum_{i=1}^{I} A_i \psi_i^r \left(t - \frac{\mid \mathbf{X}_i^r - \mathbf{x}^r \mid}{c} - \delta \right) + n^r(\mathbf{x}^r, t'). \tag{4.2}$$

The true pseudorange measurements, corresponding to received authentic satellite signals, are given by

$$p_i^r = \sqrt{(x^r - X_i^r)^2 + (y^r - Y_i^r)^2 + (z^r - Z_i^r)^2} + c\delta + w_i^r. \tag{4.3}$$

The received pseudorange measurement set is denoted by $\{p_i^r\}_{i=1}^I$. Here $\mathbf{x}^r = [x^r, y^r, z^r]'$, $\mathbf{X}_i^r = [X_i^r, Y_i^r, Z_i^r]'$, and w_i^r is the measurement noise with zero mean Gaussian probability density function with variance $(\sigma^r)^2$. Since the pseudorange measurement consists of four unknowns, at-least four authentic satellite measurements are required to estimate three dimensional GPS receiver's location.

4.1.2 GPS Receiver in Spoofer only Environment

The simulation of fake constellation and exact satellite time is hard. But, one can achieve this by using a meaconing technique as given in (Coulon et al. 2020). Spoofer is a device that transmits mimic GPS signals $\left\{\psi^f(t)\right\}_{j=1}^J$ onto the target receiver with higher power than the authentic satellite signals, to achieve easy locking into the receiver and thereby forcing the GPS receiver to wrong positioning. Let us assume that a stealthy spoofer simulates J mimic satellite signals and project them towards the target, and one cannot mitigate it using clock bias based detection technique as given in (Marnach et al. 2013). The composite signal representation of all the signals due to the presence of spoofer (fake signals) in the range is

$$\psi^f(\mathbf{x}^f, t') = \sum_{j=1}^{J} A_j s \psi_j^f \left(t - \frac{\mid \mathbf{X}_j^f - \mathbf{x}^f \mid}{c} - \delta \right) + n^f(\mathbf{x}^f, t'). \tag{4.4}$$

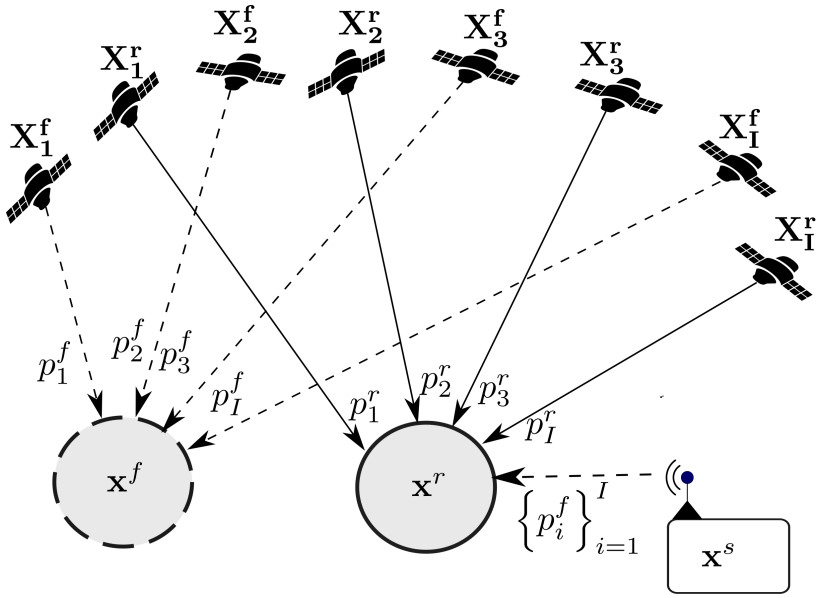

Figure 4.1: Geometry of the spoofing scenario (dotted lines represent the authentic satellite signals, dotted circle represent the true location of the target, dark lines represent the fake satellite signals, dark circle represent the fake location of the target, and the hacker).

Here A_j is the attenuation of the signal due to propagation from spoofer to the target and $n^f(\mathbf{x}^f, t')$ is the background noise. Here $\left\{\mathbf{X}_j^f\right\}_{j=1}^{J}$ are the set of fake satellite positions. This fake satellite position set is different from the true satellite position set due to the simulated signals, or they have captured signals at some other place or time. $\mathbf{X}^f$ is the fake location projected by the spoofer. The spoofed pseudorange measurement is given by

$$p_j^f = \sqrt{(x^f - X_j^f)^2 + (y^f - Y_j^f)^2 + (z^f - Z_j^f)^2} + c\delta + w_j^f. \tag{4.5}$$

The received fake pseudorange measurement set is $\left\{p_j^f\right\}_{j=1}^{J}$. Here $\mathbf{x}^f = \left[x^f, y^f, z^f\right]'$ and $\mathbf{X}_i^f = \left[X_i^f, Y_i^f, Z_i^f\right]'$. Due to locking of fake signals into the target receiver, the position estimation with these processed fake measurements results in spoofed locations. Even though the target is physically present at $\mathbf{x}^r$, the position estimate on account of fake pseudoranges results in $\mathbf{x}^f$ as shown in Figure 4.1. The noise statistics of the spoofed pseudoranges are considered the same as true measurements, w_j^f follows white Gaussian distribution with mean zero and variance $(\sigma^f)^2$; assuming that the spoofer is ideal, and the spoofing attack cannot be detected by the signal processing techniques, like power thresholding, satellite observations, power across the individual signals, and clock bias analysis. The attenuation A_i, bias δ and noise

w are same in (4.1) and (4.4) owing to ideal spoofer assumption.

4.1.3 GPS Receiver in Authentic and Spoofing Environment

Based on the correlation of signals, the receiver receives all the available signals, and few measurements are considered for the position estimation. Here it is assumed that, the GPS receiver is receiving all the authentic and spoofed signals. The received signals in the range are expressed as a composed signal of true and spoofed signals as

$$\psi(t') = \sum_{l=1}^{K} \psi_l(t). \tag{4.6}$$

Here, (4.6) is composite form of (4.2) and (4.4). However, to avoid the ambiguity, we represented (4.6) in the simplified form. Here $\psi_l(t) \in \left\{ \{\psi_i^r(t)\}_{i=1}^{I}, \left\{\psi_j^f(t)\right\}_{j=1}^{J} \right\}$. The total number of independent signals available in the composite signal is $K = I + J$. The extraction of navigation signal components from the composite signal can be obtained by spread spectrum techniques (Polydoros and Weber 1984, Malyshev et al. 2018). For the above (4.6), the equivalent measurement equation is given by

$$p_l = h_l(\mathbf{x}) + w_l;\ l = 1, \ldots, K. \tag{4.7}$$

Where

$$\begin{aligned} p_l &\in \left\{ \{p_i^r\}_{i=1}^{I}, \left\{p_j^f\right\}_{j=1}^{J} \right\}, \\ \mathbf{X}_l &\in \left\{ \{\mathbf{X}_i^r\}_{i=1}^{I}, \left\{\mathbf{X}_j^f\right\}_{j=1}^{J} \right\}, \text{ and} \\ \mathbf{x} &\in \left\{ \mathbf{x}^r, \mathbf{x}^f \right\}. \end{aligned}$$

The function h has a real and non linear relation between $\mathbf{x}$ and $\mathbf{X}$. The non-linear geometry matrix is $h(\mathbf{x}) = [h_1(\mathbf{x}), \ldots h_K(\mathbf{x})]'$. Here $\mathbf{x}$ can be real position or fake position. The measurement noise vector is $w = [w_1, w_2, \ldots w_K]'$.

From K measurements, only four measurements are involved in the correlation to compute the 3D positioning. However, for 2D positioning, three measurements are adequate. Out of K measurements, I measurements are from authentic, and J measurements from the spoofer. For a given measurement, suppose the fake pseudorange probability is p, and true pseudorange probability is q. Accordingly, sum of probabilities $p + q = 1$. If L measurements are selected randomly out of available K

measurements, the probability of correct solution by selecting authentic measurements from the set of received measurements is

$$\text{Probability} = \frac{{}^{I}C_{L}}{{}^{K}C_{L}}. \tag{4.8}$$

For example, the number of authentic measurements $I = 6$, the number of spoofed measurements in the range $J = 4$, the probability of a correct solution by selecting $L = 4$ measurements is 0.0714, which is very low. Therefore, there is a strong need to develop robust algorithms to compute all possible combinations or at least M-best combinations of measurements, and to eliminate unwanted positions to increase detection probability.

4.2 Robust Positioning

This section deals with the problem of position spoofing of a true target by imposing fake measurements, as shown in Figure 4.1. In this section, the robust positioning algorithm is described, and the M-best position estimates algorithm is proposed to reduce the complexity at a particular epoch.

4.2.1 ILS Framework for Robust Positioning

Least squares is the most popular technique in determined and overdetermined systems. Usually, in GPS positioning, the number of pseudorange equations are more than the unknowns to be estimated or some times equal. LS usually solves the whole set to offer a solution that minimizes the sum of squared errors. In LS estimation, linear LS and non-linear LS solutions exist. The closed-form of the solution is linear LS, and iterative refinement of the solution is non-linear LS. Considering the user position $\mathbf{x} = [x, y, z]'$, the position $\mathbf{x} \in \left\{\mathbf{x}^r, \mathbf{x}^f\right\}$ depends on the tuple of measurements considered from all possible pseudoranges, arrived due to true and spoofed measurements. The generalized form of pseudorange measurement p_i is given by

$$p_i = \sqrt{(x_i^g - x)^2 + (y_i^g - y)^2 + (z_i^g - z)^2} + c(dt_i - dt) + w_i \tag{4.9}$$

where $c(dt_i\text{-}dt)$ is the bias term equivalent to b.

The geometrical range is $\sqrt{(x_i^g - x)^2 + (y_i^g - y)^2 + (z_i^g - z)^2}$. 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 I. 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 (Abel and Chaffee 1991).

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 u be the iteration number and U be the total number of iterations i.e., $u = 1, 2, ..., U$. The position estimate improves iteratively. Generalizing, the nominal state for u^{th} iteration is $\hat{\mathbf{x}}_u = [x_u, y_u, z_u, dt_u]'$. The approximate pseudorange that is computed from the satellite position $\mathbf{x}_i$ to nominal position $\mathbf{x}_u$ is given by $\rho_{i,u}$. Where $\rho_{i,u} = \sqrt{(x_i^g - x_u)^2 + (y_i^g - y_u)^2 + (z_i^g - z_u)^2}$ 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 $[\Delta x_u, \Delta y_u, \Delta z_u]'$ is added to the approximate receiver position $[x_u, y_u, z_u]$ to update the receiver position as

$$\begin{aligned} x_{u+1} &= x_u + \Delta x_u, \\ y_{u+1} &= y_u + \Delta y_u, \\ z_{u+1} &= z_u + \Delta z_u. \end{aligned} \tag{4.10}$$

Based on the relation, the right hand sided of (4.10) is linearized using the first order Taylor series expansion. whereas the Taylor series expansion for $\rho_{i,u+1}$ is

$$\rho_{i,u+1} = \rho_{i,u} + \frac{\partial \rho_{i,u}}{\partial x_u}\Delta x_u + \frac{\partial \rho_{i,u}}{\partial y_u}\Delta y_u + \frac{\partial \rho_{i,u}}{\partial z_u}\Delta z_u. \tag{4.11}$$

The partial derivatives are given by

$$\begin{aligned} \frac{\partial \rho_{i,u}}{\partial x_u}\Delta x_u &= \frac{x_i^g - x_u}{\rho_{i,u}}, \\ \frac{\partial \rho_{i,u}}{\partial y_u}\Delta y_u &= \frac{y_i^g - y_u}{\rho_{i,u}}, \text{ and} \\ \frac{\partial \rho_{i,u}}{\partial z_u}\Delta z_u &= \frac{z_i^g - z_u}{\rho_{i,u}}. \end{aligned} \tag{4.12}$$

The first ordered linearized form of observation equation is

$$\begin{aligned} p_{i,u} &= \rho_{i,u} - \frac{x_i^g - x_u}{\rho_{i,u}}\Delta x_u - \frac{y_i^g - y_u}{\rho_{i,u}}\Delta y_u \\ &\quad -\frac{z_i^g - z_u}{\rho_{i,u}}\Delta z_u + c(dt_u - dt) + w_i, \end{aligned} \tag{4.13}$$

where b_u is the estimated clock error at the receiver. Re-arranging the above equation yields

$$\begin{bmatrix} -\frac{x_i^g - x_u}{\rho_{i,u}} & -\frac{y_i^g - y_u}{\rho_{i,u}} & -\frac{z_i^g - z_u}{\rho_{i,u}} & 1 \end{bmatrix} \begin{bmatrix} \Delta x_u \\ \Delta y_u \\ \Delta z_u \\ cdt_i \end{bmatrix} = b_{i,u}, \tag{4.14}$$

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

$$\min \mid\mid \mathbf{H}_u \hat{\mathbf{x}}_u - \mathbf{b}_u \mid\mid, \tag{4.15}$$

where

$$\mathbf{H}_u = \begin{bmatrix} -\frac{x_1^g - x_u}{\rho_{1,u}} & -\frac{y_1^g - x_u}{\rho_{1,u}} & -\frac{z_1^g - x_u}{\rho_{1,u}} & 1 \\ -\frac{x_2^g - x_u}{\rho_{2,u}} & -\frac{y_2^g - x_u}{\rho_{2,u}} & -\frac{z_2^g - x_u}{\rho_{2,u}} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ -\frac{x_I^g - x_u}{\rho_{I,u}} & -\frac{y_I^g - x_u}{\rho_{I,u}} & -\frac{z_I^g - x_u}{\rho_{I,u}} & 1 \end{bmatrix}, \tag{4.16}$$

and $\mathbf{x}_u = [\Delta x_u, \Delta y_u, \Delta z_u, cdt_u]$. The approximate receiver position is updated for every iteration. This iteration process continues until the solution reaches to desired accuracy or till U. Here from (4.15), we can observe that $\hat{\mathbf{x}}$ minimizes the length of the error vector $\hat{\mathbf{e}}_u$. The sum of squares of I separate errors is given by

$$\mid\mid \mathbf{e}_u \mid\mid^2 = (\mathbf{b}_u - \mathbf{H}_u\mathbf{x}_u)'(\mathbf{b}_u - \mathbf{H}_u\mathbf{x}_u). \tag{4.17}$$

By minimizing the quadratic form (4.17) gives

$$\hat{\mathbf{x}}_u = (\mathbf{H}_u'\mathbf{H}_u)^{-1}\mathbf{H}_u'\mathbf{b}_u. \tag{4.18}$$

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 $(\mathbf{H}'\mathbf{H})^{-1}$. At

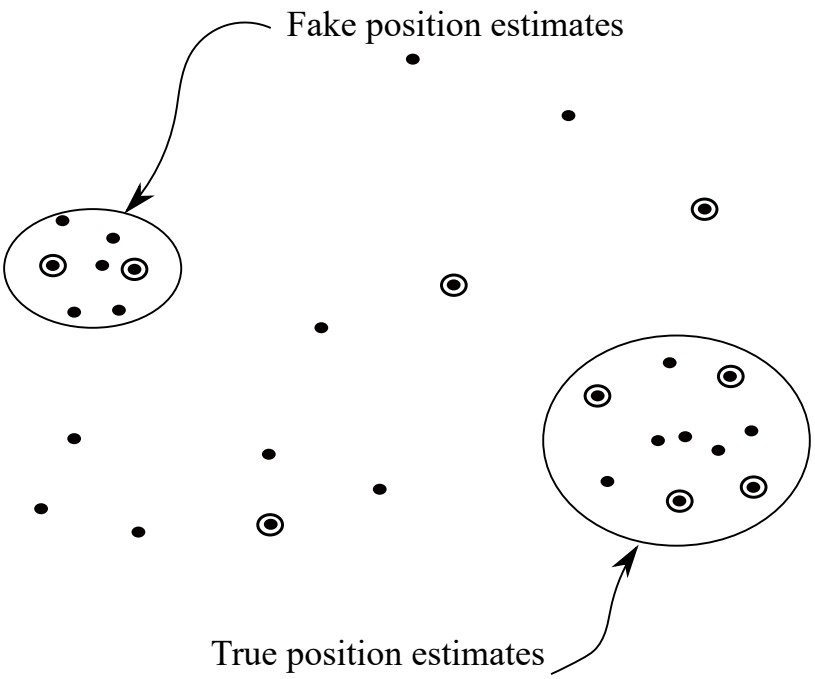

Figure 4.2: Robust positioning by considering all possible solutions and M-best solutions at a given epoch in GPS spoofing scenario (Black dots are the position estimates due to robust positioning and circles are the position estimates due to M-best estimation algorithm).

a given epoch with K pseudoranges (true and spoofed), this ILS runs ${}^{K}C_{L}$ times to produce ${}^{K}C_{L}$ position estimates, in which ${}^{I}C_{L}$ are true position estimates and rest are spoofed position estimates as shown in the Figure 4.2. Here in the given Figure 4.2, The bottlenecks of this robust algorithm are complexity and decision making. The complexity of the robust algorithm increases exponentially with every single injection of spoofed pseudorange. we can clearly see that the true position estimates are forming a cluster and similarly fake position estimates creating another cluster. Consider an example with $I = 5$ and $J = 5$ to understand the problem clearly. In this case, ${}^{I}C_{4}$ true position estimates are available in true cluster and ${}^{J}C_{4}$ position estimates are present in fake cluster. The remaining number of ${}^{K}C_{4} - ({}^{I}C_{4} + {}^{J}C_{4})$ estimates are biased estimates neither fall in true cluster nor fake cluster. So, the algorithm should be intelligent enough to compute M-best pseudorange sets from the given scan of measurements rather than finding all the posible combinations. After that, for the best sets, the ILS algorithm computes position estimates as presented in Section 4.2.2. It is very hard to decide which cluster of positions belong to true positions. Hence, there is a need to discard unwanted position estimates from the given estimates.

4.2.2 M-Best Positioning Algorithm

In a given scan of measurements (true and spoofed), the spoofer simulated measurements are totally different from the authentic satellite measurements by satellite ID, or few spoofer simulated signals match with the authentic satellite signals, thus the measurement set is given as

$$\begin{Bmatrix} p_1^r, & \cdots, & p_i^r, & \cdots, & p_j^r, & \cdots, & p_I^t, & 0, & 0, & 0 \\ 0, & 0, & p_i^f, & \cdots, & p_j^f, & 0, & 0, & p_1^f, & \cdots, & p_J^f \end{Bmatrix}$$

Here, the measurement index i to j have the same satellite ID. Hence there exist total of S active satellites, where $S \leq K$ and $s = 1, 2, \cdots, S$. We wish to associate the observations from S lists of n_s measurements. For a single spoofed signal case, $n_s = 3$, since $\{p_{i_s}^r, p_{i_s}^f, 0\}$, here zero is the dummy variable. The index $i_s = 1, 2, \cdots, n_s$. The measurement corresponding to every index i_s is with detection probability either one or zero.

$$PD_{\zeta(i_s)} = \begin{cases} 0, & \text{if} \quad p_{i_s} = 0, \\ 1, & \text{otherwise.} \end{cases} \tag{4.19}$$

Here, the source may be an authentic satellite, then the true measurements are assumed to be a function of the true state and the additive measurement noise is as given in (4.3). Whereas, in case the source is a spoofer, the spoofed measurements are assumed to be a function of the spoofed state and the additive measurement noise is as given in (4.5). The problem is formulated as a multi-sensor state estimation problem with association and estimation. Association is the process of linking the measurements, and the linked measurements are filtered with estimation. Thus, the measurements have been selected in such a way that one measurement is selected from each index. The measurement index is appended to the dummy variable of zero. This problem is commonly seen in assignment problem formulations in multi-sensor multi-target scenarios (Deb et al. 1997). Here estimation refers to position estimate by using pseudorange algorithms. The target state uniquely determines as a true position or spoofed position. For convenience, the target state is given by $\mathbf{x} \in \{\mathbf{x}^r, \mathbf{x}^f\}$. To associate the list of measurements obtained for sources $\zeta(s) \in [1, 2, \ldots S]$, where $\zeta(i_s)$ is the source of measurement either generated by satellite or spoofer. Let the selection of measurement from i_s index be p_{i_s}. Where $p_{i_s} \in \{p_{i_s}^r, p_{i_s}^f, p_o\}$. The measurement p_{i_s} either originated from satellite or spoofer or missed detection (zero measurement),

in which case, weather true or fake it is taken as $H(\mathbf{x}, \mathbf{X}_{i_s})$ plus some additive white Gaussian noise. Besides, each $\zeta(i_s)$ has a known detection probability $PD_{\zeta(i_s)}$ and it depends on the characteristics of the signal as given in (4.19).

The likelihood of S-tuple of measurements $\mathbf{z} = \{p_1, \ldots, p_L\}$ originating from target $\mathbf{x}$ is

$$\Lambda(p_{i_1}, \ldots, p_{i_S} \mid \mathbf{x}) = \prod_{s=1}^{S} [1 - PD_{\zeta(i_s)}]^{1-u(i_s)} \\ [PD_{\zeta(i_s)} p\left(p_{i_s} \mid \mathbf{x}\right)]^{u(i_s)}. \tag{4.20}$$

The likelihood of set of measurements are spurious with $\psi_{\zeta(i_s)}$ as a field of view for sensor $\zeta(i_s)$ is given by

$$\Lambda(p_{i_1}, \ldots, p_{i_S} \mid \mathbf{x} = \phi) = \prod_{s=1}^{S} \left[\frac{1}{\psi_{\zeta(i_s)}}\right]^{u(i_s)}. \tag{4.21}$$

$u(i_s)$ is a indicator function, given by

$$u(i_s) = \begin{cases} 0, & \text{if} \quad p_{i_s} = 0, \\ 1, & \text{otherwise.} \end{cases} \tag{4.22}$$

The cost of associating the set of measurements to target $\mathbf{x}$ is defined with negative log likelihood ratio

$$C_{i_1,\ldots,i_S} = -\ln \frac{\Lambda(p_{i_1}, \ldots, p_{i_S} \mid \mathbf{x})}{\Lambda(p_{i_1}, \ldots, p_{i_S} \mid \mathbf{x} = \phi)}. \tag{4.23}$$

However, $\mathbf{x}$ is unknown and replaced by maximum likelihood estimate $\hat{\mathbf{x}}^{ML}$. The likelihood can be written as

$$\begin{aligned} \Lambda(\mathbf{z} \mid \mathbf{x}) &= \Lambda(p_{i_1}, \ldots, p_{i_S} \mid \mathbf{x}), \\ &= \left(\frac{1}{\sqrt{2\pi\sigma}}\right)^{S} \exp\left(\frac{-1}{2\sigma^2} \sum_{s=1}^{S} [\mathbf{z} - h][\mathbf{z} - h]'\right), \end{aligned} \tag{4.24}$$

where $\sigma = \sigma^t = \sigma^f$ from ideal spoofer assumption. Here $\mathbf{z} = [p_{i_1}, \ldots, p_{i_S}]'$ and $h = [h_{i_1}, \ldots, h_{i_S}]$. Similarly the log likelihood is written as

$$\ln \Lambda(\mathbf{z} \mid \mathbf{x}) = \left[\frac{-1}{2\sigma^2} \sum_{s=1}^{S} [\mathbf{z} - h][\mathbf{z} - h]'\right]. \tag{4.25}$$

Therefore maximizing the log likelihood is given by

$$\begin{aligned} \hat{\mathbf{x}}^{ML} &= \arg\max \left[\frac{-1}{2\sigma^2} \sum_{s=1}^{S} [\mathbf{z} - h][\mathbf{z} - h]'\right], \\ &= \arg\min \left[\sum_{s=1}^{S} [\mathbf{z} - h][\mathbf{z} - h]'\right]. \end{aligned} \tag{4.26}$$

Therefore, the cost of associating the measurements to target $\mathbf{x}$ is

$$\begin{aligned} C_{i_1,\ldots,i_S} = & \sum_{s=1}^{S}[u(i_s)-1]\ln[1-PD_{\zeta(i_s)}] \\ & - u(i_s)\ln\left(\frac{PD_{\zeta(i_s)}\psi_{\zeta(i_s)}}{\sqrt{2\pi\Sigma_{\zeta(i_s)}}}\right) \\ & + u(i_s)\times\frac{1}{2}\left[p_{i_s}-h_{i_s}\left(\hat{\mathbf{x}}^{ML}\right)\right]^{'}\Sigma_{\zeta(i_s)}^{-1} \\ & \times\left[p_{i_s}-h_{i_s}\left(\hat{\mathbf{x}}^{ML}\right)\right]. \end{aligned} \tag{4.27}$$

The main goal of this formulation is to get most likely set of S-tuples such that either the measurement assigned to target or declared as false by taking at most one measurement from each list. This can be reformulated as a well known optimization problem of S-D assignment in multi-sensor multi-target as

$$\min_{\xi_{i_1 i_2\cdots i_S}} \sum_{i_1=1}^{n_s}\sum_{i_2=1}^{n_s}\cdots\sum_{i_S=1}^{n_s} C_{i_1 i_2\cdots i_S}\xi_{i_1 i_2\cdots i_S} \tag{4.28}$$

subjected to

$$\begin{aligned} \sum_{i_2=1}^{n_s}\cdots\sum_{i_S=1}^{n_s}\xi_{i_1 i_2\cdots i_S} &= 1; \quad i_1 = 1,\cdots n_s \\ \sum_{i_1=1}^{n_s}\cdots\sum_{i_S=1}^{n_s}\xi_{i_1 i_2\cdots i_S} &= 1; \quad i_2 = 1,\cdots n_s \\ &\vdots \qquad\quad \vdots \\ \sum_{i_1=1}^{n_s}\cdots\sum_{i_{S-1}=1}^{n_s}\xi_{i_1 i_2\cdots i_S} &= 1; \quad i_S = 1,\cdots n_s \end{aligned}$$

where, $\xi_{i_1 i_2\cdots i_S}$ are binary association variables such that $\xi_{i_1 i_2\cdots i_S} = 1$ if the S-tuple is associated with true target or spoof target. Otherwise, it is set to zero. The above assignment problem (4.27) solved using the murthy assignment algorithm (Miller et al. 1997, Danchick and Newnam 2006), and M-best costs are selected in this algorithm which in turn results in M-best positions.

Now the position estimates $\{\hat{\mathbf{x}}_l\}_{l=1}^{M}$ evolved at a given epoch are the observations to the KF based estimator. Hence, these position estimates are being redefined, as observations to avoid the confusion in the next section, i.e., $\mathbf{y} = \{\mathbf{y}_l\}_{l=1}^{M} = \{\hat{\mathbf{x}}_l\}_{l=1}^{M}$. This M-best gives results of robust positioning by giving value of M equals to ${}^{K}C_{L}$.

4.3 Kalman Filtering and Data Association

In this section, trajectory spoofing problem is presented. Initially, how the spoofer misleads the true trajectory of the target is explored and then the navigation filter solution is presented.

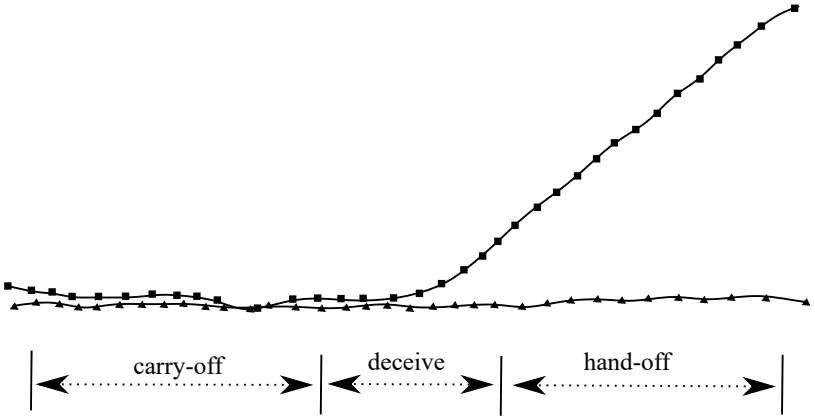

Figure 4.3: Different stages of spoofing attack to deceive the navigation track

4.3.1 Trajectory Spoofing

The final goal of spoofer in trajectory spoofing is to mislead the true target trajectory by continuously imposing the false measurements and change the destination of the target. An abrupt positioning by the spoofing effect can be easily detected by using a normalized innovation square test (NIS) or gating technique. So the ideal spoofer must possess a strategy to mislead the target. Here, we are dealing with the spoofing technique namely position gate pull-off. The stealthy trajectory spoofing involves three phases, i.e., carry-off, deceive, and hand-off. In the carry-off phase, the projected spoofed location and the true location of the target almost coincide with each other for a certain duration of the time. The spoofing starts at $t(o)$, replicates the target position for the time duration of T, as shown in Figure 4.3. During this interval, the spoofer boosts the spoofed signal to capture the receiver. Once the target is captured by the spoofer, the second phase of spoofing is called as deceiving starts. Deceiving is slightly moving the spoofed location from the actual true location with lower turn rates. After a time duration of T, the spoofer generates measurements in such a fashion so as to separate the target from the planned path with any realistic

trajectory models. During this phase, if the autonomous vehicles are more reliable on the inertial navigation system (INS) rather than the GPS, one can move the spoofed trajectory with very small deviations because the IMU sensors are incapable of detecting the lower turn rates for successful spoofing in such cases (Tanil et al. 2018). Once the target totally relies on the spoofed trajectory, the target can lead to a phase called hand-off, as shown in Figure 4.3. The algorithms should be intelligent enough to resolve the issue during this deception phase.

The dynamics of the state consists of state transition and noise gain. $\mathbf{F}$ is a state transition matrix and Γ is a noise gain matrix. The $\mathbf{F}$ can follow constant velocity (CV) model F_{CV} or constant turn (CT) model F_{CT} as given in (Bar-Shalom et al. 2011). The noise $\mathbf{u}$ follows Gaussian with zero mean and covariance $\mathbf{Q}$.

$$F_{CV} = \begin{bmatrix} 1 & 0 & 0 & \Delta t & 0 & 0 \\ 0 & 1 & 0 & 0 & \Delta t & 0 \\ 0 & 0 & 1 & 0 & 0 & \Delta t \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

where Δt is the sampling time.

$$F_{CT} = \begin{bmatrix} 1 & 0 & \frac{\sin \omega \Delta t}{\omega} & -\frac{1-\cos \omega \Delta t}{\omega} & 0 \\ 0 & 1 & -\frac{1-\cos \omega \Delta t}{\omega} & \frac{\sin \omega \Delta t}{\omega} & 0 \\ 0 & 0 & \cos \omega \Delta t & -\sin \omega \Delta t & 0 \\ 0 & 0 & \sin \omega \Delta t & \cos \omega \Delta t & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

where ω is the turn rate. The noise gain matrix is given by

$$\Gamma = \begin{bmatrix} \frac{\Delta t^2}{2} & 0 & 0 \\ 0 & \frac{\Delta t^2}{2} & 0 \\ 0 & 0 & \frac{\Delta t^2}{2} \\ \Delta t & 0 & 0 \\ 0 & \Delta t & 0 \\ 0 & 0 & \Delta t \end{bmatrix},$$

the covariance corresponding to this noise gain matrix is $\mathbf{Q} = \Gamma'\sigma^2\Gamma$. For a discrete time linear dynamic system the plant equation is consider as

$$\mathbf{x}(k) = \mathbf{F}(k')\mathbf{x}(k') + \Gamma\mathbf{u}(k'). \tag{4.29}$$

The observations is given by

$$\mathbf{y}(k) = \begin{cases} \mathbf{H}(k)\mathbf{x}(k) + \mathbf{w}(0, \mathbf{R}(k)), & \text{true origin,} \\ \{FA_l(k)\}_{l=1}^{M-1}, & \text{spoofed.} \end{cases} \tag{4.30}$$

Where $\mathbf{y}(k)$ consists of positions related to true, spoofed, and bias. FA is false alarms representing the spoofed positions. The kalman filter is implemented as given Algorithm. All the above equations in the Algorithm are the same as in standard KF

Algorithm 3 Kalman filter workhorse

1: **procedure** KF($\mathbf{F}(k'), \mathbf{H}(k), \mathbf{Q}(k'), \mathbf{R}(k), \hat{\mathbf{x}}(k' \mid k'), \hat{\mathbf{P}}(k' \mid k'), \mathbf{y}(k)$)

2: The predicted state, predicted covariance and predicted measurement calculated as

$$\hat{\mathbf{x}}(k|k') = \mathbf{F}(k')\hat{\mathbf{x}}(k'|k'), \tag{4.31}$$

$$\hat{\mathbf{P}}(k|k') = \mathbf{F}(k')\hat{\mathbf{P}}_j(k'|k')\mathbf{F}(k')' + \mathbf{Q}(k') \tag{4.32}$$

$$\hat{\mathbf{y}}(k|k') = \mathbf{H}(k)\hat{\mathbf{x}}(k|k'). \tag{4.33}$$

3: The residual and residual covariance are calculated as

$$\mathbf{r}(k|k') = \mathbf{y}(k) - \hat{\mathbf{y}}(k|k'), \tag{4.34}$$

$$\mathbf{S}(k) = \mathbf{H}(k)\hat{\mathbf{P}}(k|k')\mathbf{H}(k)' + \mathbf{R}(k) \tag{4.35}$$

4: The filter gain is given by

$$\mathbf{G}(k) = \mathbf{P}(k|k')\mathbf{H}(k)'\mathbf{S}(k)^{-1}. \tag{4.36}$$

5: The updated state and its associated covariance are designated as

$$\hat{\mathbf{x}}(k|k) = \hat{\mathbf{x}}(k|k') + \mathbf{G}(k)\mathbf{r}(k), \tag{4.37}$$

$$\hat{\mathbf{P}}(k|k) = \hat{\mathbf{P}}(k|k') - \mathbf{G}(k)\mathbf{S}(k)\mathbf{G}(k)'. \tag{4.38}$$

6: **end procedure**

used in navigation. Nevertheless, in navigation, only one measurement is available to update the state and covariance. Either all possible positions or M-best positions are

calculated; in both cases, a large number of observations are evolved, as is the case of a typical tracking scenario. Consider a scenario with four authentic measurements, four spoofed measurements, and four appended dummy variables. Evaluating the combinations (based on four authentic, four spoofed measurements, and four appended dummy variables) yields to eighty-one combinations. Out of these, only fifteen best positions are taken and plotted as seen in Figure 4.4.

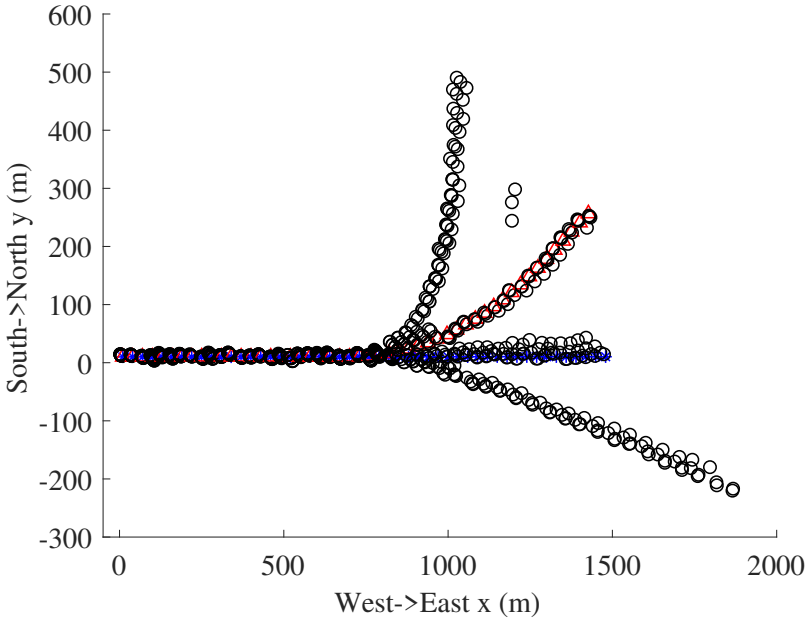

Figure 4.4: Navigation tracks in spoofing (I=4, J=4, K=4, and M-best=15).

In the initial phase of carry-off, all the M-best estimates forms a single cluster, hence there is no ambiguity for measurement-to-track association. Whereas, it is clearly evident that evolved M-best estimates during the deceiving phase are not forming a single cluster, which leads to ambiguity of measurement-to-track association. Further, once the track is associated with wrong measurements, true trajectory follows the fake estimate and carried away by the spoofer. A gating technique is performed with in the filter framework to resolve this issue of selecting few estimates from the M-best estimates. The validation region (gate) is ellipsoid given by

$$\mathcal{V}(m+1) = \left\{ \mathbf{y} : \mathbf{v}(k)' \mathbf{S}(k)^{-1} \mathbf{v}(k) \leq \varsigma_{n_y}^2 \right\}, \tag{4.39}$$

where ς is the gate threshold determined by the chosen gate probability P_G. The ς follows a chi-square distribution with a n_y degree of freedom and given tail probability. For 2D and 3D case n_y is equal to two and three respectively. The valid

measurements falling within the gate are $\{\mathbf{y}_l\}_{l=1}^{L^*}$. In a given M observations, only L^* observations falling within the gate, at the given discrete time instant. The innovation corresponding to the l^{th} validated measurement is used in the KF.

4.3.2 Position to Track Association

The data associations employed in this KF is the nearest neighbor (NN) and probabilistic data association (PDA) (Bar-Shalom et al. 2011). In NN, the nearest observation to the predicted track is considered, and the innovation is carried out using this observation. Whereas, in PDA probability of l^{th} validated measurements considered, to find the correct one be

$$\beta_l(k) = \begin{cases} \frac{\Lambda_l}{1-P_D P_G+\sum_{l=1}^{L^*(k)} \Lambda_l}, & l = 1, \ldots, L^*(k), \\ \frac{1-P_D P_G}{1-P_D P_G+\sum_{l=1}^{L^*(k)} \Lambda_l}, & l = 0. \end{cases} \tag{4.40}$$

$\beta_0(k)$ is association probability, which shows that none of the measurement is correct. The likelihood ratio Λ_l is given by

$$\Lambda_l \triangleq \exp\left(-\frac{1}{2}\mathbf{v}_l(k)' \mathbf{S}(k)^{-1} \mathbf{v}_l(k)\right). \tag{4.41}$$

whereas P_D is the probability of detection and P_G is the gating probability. The updated state is given by

$$\hat{\mathbf{x}}(k|k) = \hat{\mathbf{x}}(k|k') + \mathbf{G}(k)\mathbf{v}(k). \tag{4.42}$$

with the combined innovation as

$$\mathbf{v}(k) \triangleq \sum_{i=1}^{L^*(k)} \beta_i(k)\mathbf{v}_i(k). \tag{4.43}$$

The Updated covariance is given as

$$\begin{aligned} \mathbf{P}(k|k) =& \mathbf{P}(k|k') - [1-\beta_0(k)] \\ & \mathbf{G}(k)\mathbf{S}(k)\mathbf{G}(k)'. \end{aligned} \tag{4.44}$$

4.4 Results and discussions

This section presents scenario generation, design parameters, and robustness of the proposed algorithm. To illustrate the robustness of the proposed algorithm, different scenarios like open space (LOS measurements with $I = 4$ to $I = 6$) and a multi-path environment (Non-LOS measurements with $I = 4$) are examined.

4.4.1 Scenario Generation

The satellite trajectories are modeled using WGS-84, and follows an assumption of circular orbits as given in Section-1.1.8. We consider a position pull-off spoofing

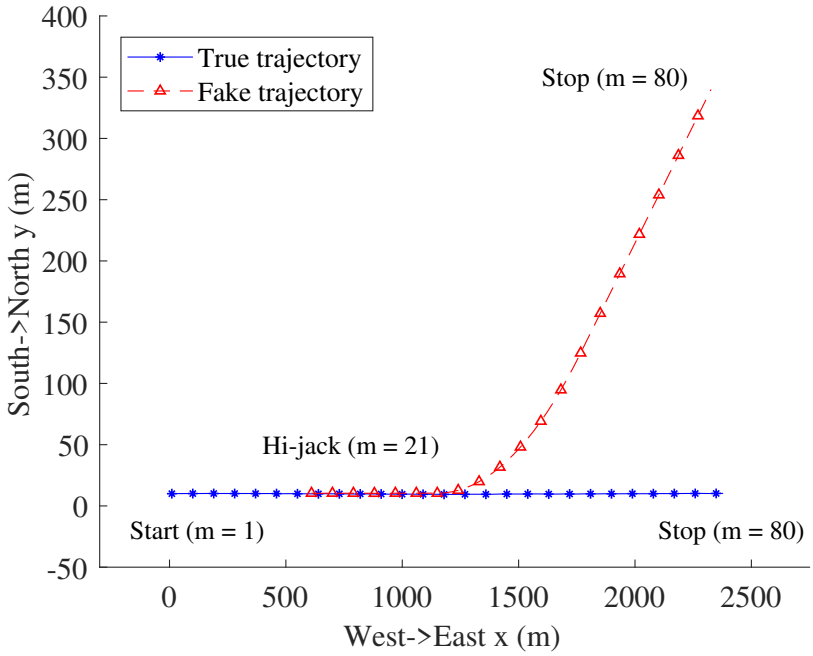

Figure 4.5: True and fake trajectory generation (True - target planned trajectory, fake - Spoofer imposing trajectory on target).

technique test bench trajectory to evaluate the proposed algorithm. The initial state vector of the true target is $\mathbf{x}^r(0) = [10, 10, 10]'$ and its velocity vector $\dot{\mathbf{x}}^r(0) = [30, 0, 0]'$. The target moves towards the east (x) throughout the simulation with 30 m/s for 80 s with a CV model. The target trajectory consists of ideal trajectory and turbulence; the turbulence is modeled as process noise, follows Gaussian with zero mean and the standard deviation vector is given by $[0.05, 0.05, 0, 0.02, 0.02, 0]'$. The first three elements of the standard deviation vector represent the position, and the other three elements correspond to velocity. The process noise exists along x and y directions, and absent in z direction due to the ground moving target assumption.

The spoofing process starts at $t = 21$ s and follows till the end. Since the target is not being influenced until $t = 21$ s, the standard navigation solution exists during this non-spoofing phase. The spoofed trajectory follows both CV and CT models, as presented in critical examples (Liu et al. 2019). From 21 s, the carry-off phase starts with CV model and carried out for a further duration of 20 s. After that, the

deceiving phase starts and lasts for 20 s, by taking left CT with $\omega = 1^o/\text{s}$. Thereafter, the hand-off phase is carried out with the CV model for another 20 s duration as shown in Figure 4.5.

4.4.2 Design Parameters

Since the ideal spoofer is considered in this paper, spoofer can process the spoofed pseudorange measurements with the same noise as of true pseudoranges. Both the pseudorange measurements are corrupted by white Gaussian noise with standard deviation, i.e., $\sigma_i^t = \sigma_j^f = 1$ m. The sampling time of KF is $\Delta t = 1$ s. Two-point initialization method (Bar-Shalom et al. 2011) is used to initialize the filter. If the spoofing is carried out from the initial timestamp, the same two-point initialization method can be applied with the values of means of a cluster. The means of the cluster of positions formed at $t(0)$ and $t(1)$ epoch are $\mathbf{x}_\mu^r(0)$ and $\mathbf{x}_\mu^r(1)$ respectively. The state vector is

$$\begin{aligned} X(1) &= \left[\hat{x},\ \hat{y},\ \hat{z},\ \dot{\hat{x}},\ \dot{\hat{y}},\ \dot{\hat{z}}\right]' \\ &= \left[\mathbf{x}_\mu^r(1),\ \frac{\mathbf{x}_\mu^r(1) - \mathbf{x}_\mu^r(0)}{t(1) - t(0)}\right]'. \end{aligned} \tag{4.45}$$

The state transition matrix in the filter design is F_{CV} and the noise gain is Γ. The measurement transition matrix is given by $\mathbf{H} = [\mathbf{I}_3\ \mathbf{0}_3]$, where $\mathbf{I}_3$ represents the identity matrix and $\mathbf{0}_3$ is the zero matrix with dimension three. Moreover, the process noise covariance of the filter is initialized using the CRLB as given in (Xiangdong Lin et al. 2001). To resolve the ambiguity of observation to track, NN and PDA techniques are deployed.

4.4.3 Robustness of Algorithm

The robustness of the algorithm is verified by varying the number of authentic signals and spoofed signals available at the receiver. Here, the robustness is evaluated for open space environment and urban environment. Open space environment implies that there are no multi-path measurements in the received set. Whereas, the urban environment introduces multi-path measurements in the authentic set. The position root mean square error (PRMSE) and track swap (TS) are the two quantifying mea-

sures considered in this paper. The TS is defined as the deceiving of navigation track from the true trajectory.

A Open space environment

Assuming that the GPS receiver is located in low visibility scenario with $I = 4$ authentic satellite signals. Here all the signals are LOS with the receiver without any multi-path. In this case, a determined solution (number of unknowns to be estimated, equal to the number of available pseudoranges) exists for navigation. In the presence of spoofing, in addition to four true satellite signals, the spoofed signals are introduced with a variable number of $J = 1, \ldots, 6$. Here, during the initial phase of trajectory $k \in [1, 20]$, the navigation filter follows a true trajectory without any spoofing. Due to the lack of initial velocity of the filter, two-point initialization is used, a decrease is seen in PRMSE of navigation filter after initialization, till $k = 20$ s. Thereafter, the carry-off phase is implemented for $k \in [21, 40]$, in which both true and spoofed trajectories follow the same path. Even though huge measurement-to-measurement associations occur in this interval, insignificant deflection in PRMSE is observed, as depicted in Figure 4.6(a) (since trajectories are aligned to each other). Whereas, in the interval of deceiving $k \in [41, 60]$, numerous observations are generated. M-best algorithm produces only M limited observations. From these M observations, selecting a single measurement for measurement-to-track association is a difficult process. Hence, this problem is addressed by deploying NN data association technique. Since NN is employed, the filter selects the nearest observation and updates the filter. In this process, as the number of spoofed injections increases, PRMSE and TS values increases as shown in Figures. 4.6(a–c). This is because, as number of spoofed injections increases, the measurement-to-track association ambiguity increases. As NN is a hard decision, once the track is decepted with the false measurement, it is hard to get back to the true trajectory path, and estimated path would continue to be with false measurements. Therefore, the increase in ambiguity of measurement-to-track association with number of spoof injections can be intuitively related with the increase in PRMSE value during the deception phase In this deceiving phase, the navigation filter chooses either the true trajectory or the spoofed trajectory depending on the data association. If the target tends to follow the spoofed trajectory, it follows until

the end, which is considered as TS. During the hand-off phase $k \in [61, 80]$, the clusters of observations are totally separable and the filter follows any one of the track, and hence PRMSE settles down as illustrated in Figures. 4.6(a–c). The selection of M value in the algorithm is very crucial. So always the value of M set to number of available satellite signals. However one can vary the value of M and see the overall performance of the algorithm.

In another scenario, the GPS receiver receives $I = 5, 6$ authentic satellite signals. The available true ranges are greater than the number of parameters to be estimated, and the solution becomes over-determined. The spoofed signal injections vary as $J = 1, \cdots, 6$. During the carry-off phase, we can observe improved PRMSE compared to the $I = 4$ case. This is due to the total number of ranges being involved in the position estimation and also because of the dummy variable assignment in the algorithm, the M-best solution gives positions related to all authentic satellite measurements. Due to the increase of measurements, there is a huge measurement-to-measurement association in this phase compared to the $I = 4$ scenario, and is computationally expensive. In the Figure 4.6(b) and Figure 4.6(c), an improved PRMSE is observed in the deceiving phase, compared to that of Figure 4.6(a). The improved PRMSE is due to more number of authentic satellite signals involved in the ILS solution, compared to the $I = 4$ case. During the deception phase, the TS is decreased in comparison to four authentic satellite cases; this is because of either an increase in the position integrity or lesser ambiguity of selecting an observation within the gate. The TS is reported in Table 4.1; an increase in true measurements improves the navigation filter to choose the true trajectory rather than fake trajectory. The TS rate increases as the number of injections increase, as shown in Table 4.1. Similar to the previous case, the clusters are well separated in the interval of hold off, and the PRMSE settles down as shown in Figure 4.6(c). The simulations are carried out for five authentic measurements and its corresponding spoofed measurement injection, and the TS are depicted in Table 4.1.

The drawback of the NN is its hard decision towards measurement-to-track association, by considering the nearest observation. So, the probabilistic data association is used for the above-stated problem. Interestingly, owing to PDA, the TS is decreasing compared to NN technique. If wrong measurement-to-track association is

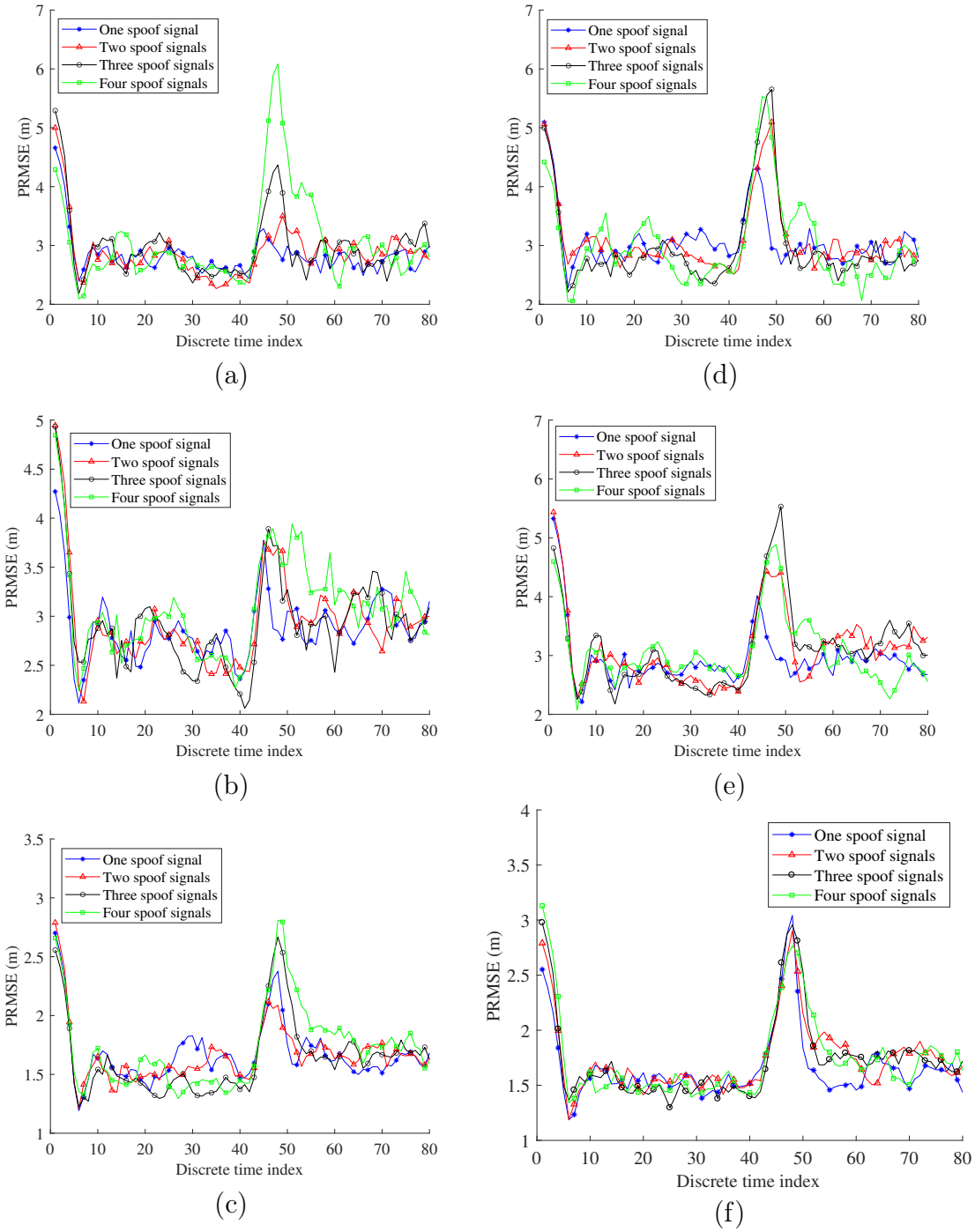

Figure 4.6: PRMSE for variable authentic satellite signals and variable number of spoofed signal injections for 100 MC runs. (a) NN association with N=4 (b) PDA association with N=4 (c) NN association with N=5 (d) PDA association with N=5 (e) NN association with N=6 (f) PDA association with N=6

taken place in the initial stage of deception, there is a highly likelihood that it will get corrected, since PDA evaluate all weighted measurements within the gate to form the innovation. The number of TS by varying the authentic and spoofed signals is

presented in Table 4.1. But, during the interval of carry-off phase, a little raise is seen in PRMSE, by using PDA technique. Since true and spoofed follow the same path in the carry-off, the evolved M-best position estimates correspond to the same ground truth, and hence, we observe this raise in PRMSE as in Figures 4.6(d–f). The calculated weighted innovation, by considering the observations within the gating region is different from the actual innovation seen in the NN technique. However, in the deceiving interval, a degraded PRMSE is observed with PDA as compared to that of the NN technique. Due to the probabilistic decision during the deceiving period, the navigation track to follow spoof track decreases. In Table 4.1, the algorithm's TS is presented, where we can observe that the PDA outperforms NN even as the number of spoofed measurements injection increases. Furthermore, the overall computational load of the algorithm depends on the M-best positions and the total number of measurements being involved in the ILS. However, due to advancement in computational algorithms and hardware realizations, it is possible to achieve a high-speed processing hardware in a compact form.

Table 4.1: Track swap number for varied true and spoofed measurements

	I / J	1	2	3	4	5	6
NN	4	3	7	28	29	74	79
NN	5	2	8	14	28	42	48
NN	6	0	0	4	7	31	33
PDA	4	1	2	9	21	43	61
PDA	5	1	4	14	21	31	34
PDA	6	0	0	3	7	19	22

B Urban environment

If the available authentic measurements are greater than or equal to number of unknowns in the pseudomeasurement equation. Then unique solution exists and it is clearly depicted in the open space environment case in Section-V-C1.

To evaluate the urban environment, we assumed that the available authentic mea-

surement set consists of four measurements, in which multi-path measurements are also present. The multi-path measurement usually differs from the actual measurement by the phase and distance between source and receiver. Since this paper dealt with the distance as a measurement to the estimator, the phase component is ignored. In the first case, one multi-path measurement exists and and it is deflecting with 150 m range, whereas the rest of the three measuremets are LOS to the receiver. The simulations are carried out for this case and the PRMSE is depicted in Figure 4.7(a).

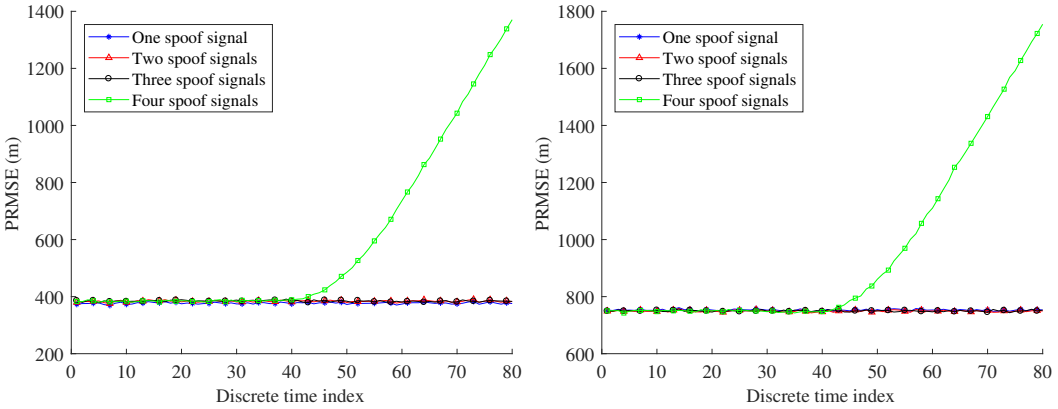

Figure 4.7: PRMSE for fixed four authentic measurements and variable number of spoofed measurement injections with nearest neighbor data association for 100 MC (a) three LOS measurements and one multi-path measurement (b) two LOS measurements and one multi-path measurement

In this case, we can observe that the M-best assignment solution is minimum for the authentic measurement set even though it contains one multi-path measurement. Here, out of four measurements, one multi-path measurement exist and as a result of that the PRMSE is increased to 380 m. We can observe that the cost minimization function is able to mitigate the effect of spoofing upto three spoof measurements. On the other hand, the M-best cost minimization provides the spoof location as the best location rather than the true location for the case of four spoof measurements, which is clearly shown in Figure 4.7(a).

However, further investigation of multi-path effect in the spoofing environment, is performed with increased number of multi-path signals. In this case, out of four measurements in the authentic set, two LOS signals and two multi-path signals are

considered. The multi-path measurements are deflected by 150 m and 250 m in range respectively, and PRMSE is plotted in Figure 4.7(b). From the Figure 4.7(b), it is observed that the average PRMSE is raised to 750 m for the spoof injections of $J = 1, 2, \&3$. Whereas, for $J = 4$, the M-best cost minimization function is getting minimized for the spoof measurement set and eventually following the spoof trajectory. It is also observed that, in very few monto carlo runs, the measurement-to-track association is carried out for true rather than the spoof(only 7 runs out of 100 runs possess correct measurement-to-track association). Hence the TS is not tabulated for this special case.

From the results obtained, it is apparent that, the algorithm has a limitation to mitigate more than four spoof signals in the urban environment. Even though, the NN and PDA data associations are deployed, we observe insignificant improvement in the PRMSE value. There is a future scope to formulate a research problem by using the attributes of the signal (i.e., amplitude, phase, power) and solve the constrained optimization problem to address spoofing problem in urban scenario.

Chapter 5

GNSS Spoofing Detection and Mitigation in Multi-receiver configuration via Tracklets and Spoofer Localization

5.1 Problem Formulation

In a given clean environment, a GNSS sensor located at $\mathbf{x}^r$, estimates its location as $\hat{\mathbf{x}}^r$ by using the available satellite set $\{\mathbf{x}_i^g\}_{i=1}^N$. Minimum of four visible satellites are required out of twenty four satellite constellation to estimate any unknown $3D$ location on the earth. Let the problem be in $2D$ scenario, i.e., $\mathbf{x}^r = [x^r, y^r]'$ and $\mathbf{x}_i^g = [x_i^g, y_i^g]'$. The direction of arrivals from N satellites is given by $\{\theta_i^t\}_{i=1}^N$ as shown in the Figure 5.1. where

$$\theta_i^t = \arctan\left(\frac{y_i^g - y^r}{x_i^g - x^r}\right). \tag{5.1}$$

In a spoofing scenario, a spoofer is located at $\mathbf{x}^s$ and transmits mimic GNSS signals with higher power onto the receiver to create a fake location of $\mathbf{x}^f$. Once the receiver locked onto the generated spurious signals originated from the spoofer, then the receiver estimates its location as $\mathbf{x}^f$ even though the target is physically located at $\mathbf{x}^r$ as shown in Figure 5.1. Where, $\mathbf{x}^s = [x^s, y^s]'$ and $\mathbf{x}^f = [x^f, y^f]$. The direction of arrivals corresponding to the spoofer signals is $\left\{\theta_i^f\right\}_{i=1}^N$, and all signals arrive in the same direction. The bearing of the spoofing scenario is given by

$$\theta_i^f = \arctan\left(\frac{y^s - y^r}{x^s - x^r}\right). \tag{5.2}$$

From (5.1) and (5.2), we can observe that the angle of arrival is dependent on the

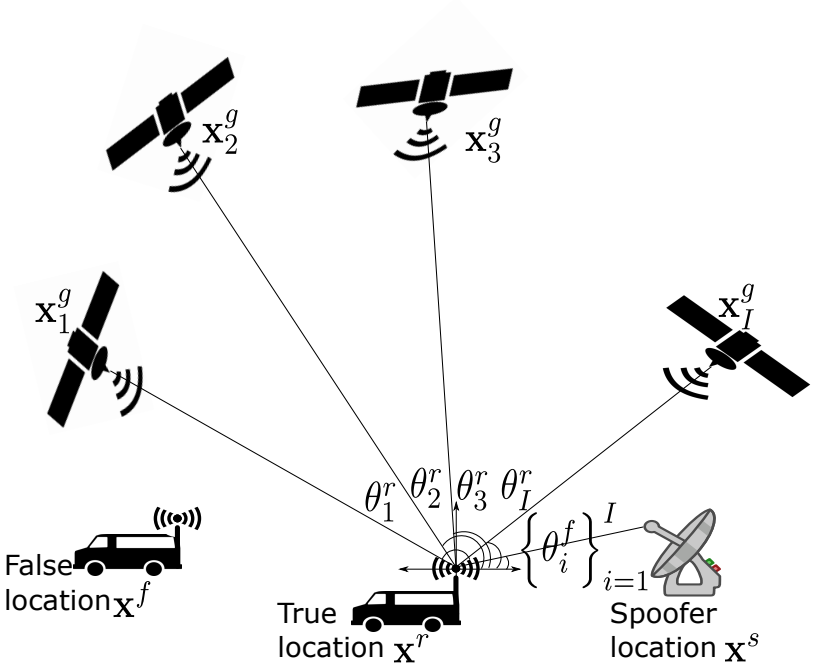

Figure 5.1: Spoofing scenario geometry and measurements

physical state $\mathbf{x}^r$ and the source location $\mathbf{x}_i^g$ or $\mathbf{x}^s$. In a non-intentional interference case, in (5.1), the satellite locations are known since the received signal by the GPS receiver consists of the timestamp of signal transmission and satellite location information. Due to multiple satellites, the GNSS receiver estimates its location as $\hat{\mathbf{x}}^r$. However, in (5.2), both the physical location of the GNSS receiver $\mathbf{x}^r$ and the spoofer location $\mathbf{x}^s$ are unknowns in the received bearings measurement. Interestingly, in spoofing activity, the position information related to the sensor is appeared to be $\mathbf{x}^f$ rather than $\mathbf{x}^r$. Hence, solving the bearings-only localization problem with multiple wrong positions of sensors results in an incorrect estimate of the source. Therefore, the following observations can be made.

- A generalized mathematical framework for spoofing effect on multiple GNSS receivers explores how the multiple sensors behave in the environment.

- Once the spoofer attacks the GNSS receivers in the vicinity, there should be a mechanism to detect the spoofing attack using the falsified position information from multiple sensors.

- Soon after the spoofing attack is detected, the false position $\mathbf{x}^f$ reported by the GNSS receiver at that discrete instant should be discarded, and need to

establish an approximate physical location concerning to $\mathbf{x}^r$.

- Localization of the spoofer using bearings information from multiple sensors and counter-attack the intensional interference source.

5.2 GNSS Positioning and Spoofing Attack Detection

This section models the mathematical model for repeater-based spoofer and its influence on multiple GNSS receivers. Further, the pseudo-measurements calculation for the multiple GNSS sensors using tracklets is presenting. After that, a GLRT is derivation to detect the spoofing attack.

5.2.1 Repeater based Spoofer Measurements

The GPS spoofing considered here is a repeater, in which the spoofer (s) consists of a receiver, process unit, and transmitter module. The receiver module receives signals from the authentic satellites, separated into different channels based on the satellite ID. A repeater-based spoofer system, in which the processing unit calculates the external delays for each navigation signal before re-transmission. Once the delays add to the received signals, the transmitter module transmits the spurious satellite signals ψ onto the targeted GNSS. This spoofer analyzes the target's actual location (physical location), spoof location (wrong location intended to create) and accordingly calculates the delays to be incorporated by the spoofer. The spoofer is operating in escort/ stand-in mode to the target to carry out stealthy spoofing. The spoofer intends to create a fake-position $\mathbf{x}_j^f$ for the target j which is being physically located at $\mathbf{x}_j$ as shown in Figure 5.2.

Here, M GNSS sensors are installed on the target platform at $\left\{\mathbf{x}_j^r\right\}_{j=1}^M$ positions. In this process, not only does the target j gets into spoofed activity, but also all the GNSS receivers in the vicinity get into spoofing attack as stated in (Tippenhauer et al. 2011). In Figure 5.2, the dark lines from satellite-to-spoofer represent the reception of the original signal by the spoofer. These authentic signals are captured by the spoofer located at $\mathbf{x}^s$, process and re-transmits onto target j located at $\mathbf{x}_j^r$ to create a fake location of $\mathbf{x}_j^f$. We can observe that the GNSS sensors are installing on the platform.

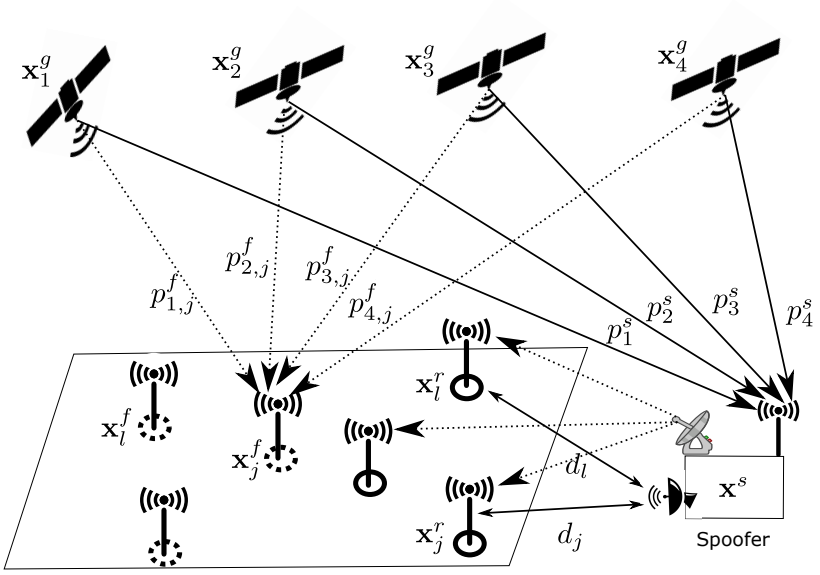

Figure 5.2: The geometry of a single-spoofer multi-receiver spoofing scenario. The dark circle and the dotted circle represent the GNSS sensor's physical location and fake location, respectively. The dark lines and dotted lines represent the authentic pseudoranges and spoofer-generated pseudoranges, respectively. The authentic pseudoranges for the target are not drawn; however, they exist in reality.

Since the spoofer is Omnidirectional, the transmitted signal is receiving by all GNSS receivers within the vicinity of the spoofer. The spoofers use boosted power compared to the authentic signals. Hence all the GNSS receivers get into spoof activity for the same signals. Therefore, we can observe that three spoof locations corresponding to three GNSS receivers are as depicted in Figure 5.2.

The spoofer located at $\mathbf{x}^s$ receives the authentic combined signal of all satellites in the range as

$$\psi\left(\mathbf{x}^s, t'\right) = \sum_{i=1}^{N} A_i \psi_i\left(t - \delta_i^s\right) + n\left(\mathbf{x}^s, t'\right), \tag{5.3}$$

where A_i is signal attenuation due to transmission from $\mathbf{x}_i^g$ to $\mathbf{x}^s$. Whereas t' is the global satellite time or system time, δ_i^s is the time-delay corresponding to the pseudorange measurement p_i^s. Spoofer modifies the time delays of individual satellite signals, then re-transmitted signal onto GNSS sensor j is represented as

$$\psi\left(\mathbf{x}^s, t'\right) = \sum_{i=1}^{N} A_i \psi_i\left(t - \delta_i^s - \delta_{i,j}\right) + n\left(\mathbf{x}^s, t'\right). \tag{5.4}$$

The external time delay offered to the i^{th} satellite signal by the spoofer for target j is given by $\delta_{j,i}$. The external delay calculation (Kerns et al. 2014) is given by

$$\delta_{i,j} = \frac{p_{i,j}^f - p_i^s - d_j}{c}. \tag{5.5}$$

The spoofer-to-target distance for j is d_j. In practice, range measuring devices and trackers are employed for the distance calculation. To simplify the problem, we assumed that the distance between the spoofer and target was known precisely.

The re-transmitted signals propagate with velocity of light (c) in open space and are then receiving by the GNSS receiver. As shown in Figure 5.2, the GNSS receiver located at $\mathbf{x}_l$ receives the combined signal as

$$\psi\left(\mathbf{x}_l, t'\right) = \sum_{i=1}^{N} A_{i,l}\psi_{i,l}\left(t - \delta_{i,l}^{s} - \delta_{i,j} - \frac{d_l}{c}\right) + n\left(\mathbf{x}_l, t'\right). \tag{5.6}$$

Here $l \in \{1, \ldots, M\}$. For $l = j$, the above equation states that all the signals transmitted by the spoofer are locking onto the GNSS receiver j. Whereas for $l \neq j$, the signals transmitted by spoofer are locking onto l^{th} target even though the measurements are generated for j. After processing the received signals, the pseudorange measurements obtained are given by

$$p_{i,l}^{s} = c\left(\delta_i^s + \delta_{i,j} + \frac{d_l^s}{c}\right). \tag{5.7}$$

Substituting $\delta_i^s = \frac{z_i^s}{c}$ and (5.5) in the above (5.7) yields

$$p_{i,l}^{s} = c\left(\frac{p_i^s}{c} + \frac{p_{i,j}^{f} - p_i^s - d_j^s}{c} + \frac{d_l^s}{c}\right). \tag{5.8}$$

Simplifying the (5.8) yields

$$p_{i,l}^{s} = p_{i,j}^{f} - d_j^s + d_l^s. \tag{5.9}$$

The representation in (5.9) is the compact form to generate GPS measurements for single-spoofer multiple GNSS receivers spoofing case. In spoofing process, the pseudorange measurement set obtained at the target l due to spoofer is $\left\{p_{i,l}^{f}\right\}_{i=1}^{N} = \{p_i\}_{i=1}^{N}$. Here, we are ignoring the index of the GNSS receiver j to avoid the ambiguity in equations. Whereas in non-spoofing case, the pseudorange measurement set obtained for the target j is $\{p_i^r\}_{i=1}^{N} = \{p_i\}_{i=1}^{N}$.

5.2.2 Extended Kalman Filter Framework for GPS positioning

For the sensor j, the extended KF is used. The generalized version of the KF is presented here without mentioning the index j. The pseudo measurement is given by

$$\begin{aligned} p_i &= \rho_i + c\Delta t + w_i \\ &= h_i(\mathbf{x}) + w_i \end{aligned} \tag{5.10}$$

where ρ_i is the true range or geometrical range from satellite $\mathbf{x}_i^g$ to GNSS receiver located at $\mathbf{x}$ which is equal to $\sqrt{(x_i^g - x^r)^2 + (y_i^g - y^r)^2 + (z_i^g - z^r)^2}$. where $c\Delta t$ and w_i are bias due to offset and pseudorange measurement error for satellite i respectively. The measurement noise follows the white Gaussian noise with mean zero and variance σ. The stacking of I pseudorange measurements is taken, and one can write

$$\begin{aligned}\mathbf{p}(k) &= h[\mathbf{x}(k)] + \mathbf{w}(k) \\ &= \mathbf{H}(k)\mathbf{x}(k) + \mathbf{w}(k)\end{aligned} \tag{5.11}$$

where

$$\begin{aligned}\mathbf{p}(k) &= [p_1(k), \cdots, p_I(k)]' \\ \mathbf{h}(k) &= [h_1, \cdots, h_I]' \\ \mathbf{w}(k) &= [w_1, \cdots, w_I]'\end{aligned}$$

and $\mathbf{H}(k)$ is the linearized measurement transition matrix represented as

$$\mathbf{H} = \frac{\partial \mathbf{h}}{\partial \mathbf{x}} \mid_{\mathbf{x}=\hat{\mathbf{x}}} = \begin{bmatrix} -h_1^x & 0 & -h_1^y & 0 & -h_1^z & 0 & c \\ \vdots & 0 & \vdots & 0 & \vdots & 0 & c \\ -h_I^x & 0 & -h_I^y & 0 & -h_I^z & 0 & c \end{bmatrix} \tag{5.12}$$

and the state is $\mathbf{x} = [x, \dot{x}, y, \dot{y}, z, \dot{z}, \delta t]$. Here

$$\begin{aligned} h_i^x &= -\frac{\partial h_i}{\partial x} = \frac{(x_i^g - x)}{\sqrt{(x_i^g - x)^2 + (y_i^g - y)^2 + (z_i^g - z)^2}} \\ h_i^y &= -\frac{\partial h_i}{\partial y} = \frac{(y_i^g - y)}{\sqrt{(x_i^g - x)^2 + (y_i^g - y)^2 + (z_i^g - z)^2}} \\ h_i^z &= -\frac{\partial h_i}{\partial z} = \frac{(z_i^g - z)}{\sqrt{(x_i^g - x)^2 + (y_i^g - y)^2 + (z_i^g - z)^2}} \end{aligned}$$

The filter relaying on pseudo measurements at k and its last updates($\hat{\mathbf{x}}_i(k'|k')$ and $\hat{\mathbf{P}}_i(k'|k')$) to estimate state and covariance update at k. Here k' is the last epoch or last updated time. Hence, the target state dynamics is

$$\mathbf{x}(k) = \mathbf{F}(k')\mathbf{x}(k') + \mathbf{v}(k') \tag{5.13}$$

where $\mathbf{F}(k')$ is the state transition matrix and $\mathbf{v}(k')$ is process noise vector, follows zero mean additive WGN with covariance $\mathbf{Q}(k')$. Whereas $\mathbf{R}(k)$ is the measurement

Algorithm 4 Kalman filter workhorse

1: **procedure** KF($\mathbf{F}(k'), \mathbf{H}(k), \mathbf{Q}(k'), \mathbf{R}(k), \hat{\mathbf{x}}(k' \mid k'), \hat{\mathbf{P}}(k' \mid k'), \mathbf{z}(k)$)

2: The predicted state, predicted covariance and predicted measurement calculated as

$$\hat{\mathbf{x}}(k|k') = \mathbf{F}(k')\hat{\mathbf{x}}(k'|k'),$$

$$\hat{\mathbf{P}}(k|k') = \mathbf{F}(k')\hat{\mathbf{P}}_j(k'|k')\mathbf{F}(k')' + \mathbf{Q}(k')$$

$$\hat{\mathbf{z}}(k|k') = \mathbf{H}(k)\hat{\mathbf{x}}(k|k').$$

3: The residual and residual covariance are calculated as

$$\mathbf{r}(k|k') = \mathbf{z}(k) - \hat{\mathbf{z}}(k|k'),$$

$$\mathbf{S}(k) = \mathbf{H}(k)\hat{\mathbf{P}}(k|k')\mathbf{H}(k)' + \mathbf{R}(k)$$

4: The filter gain is given by

$$\mathbf{G}(k) = \mathbf{P}(k|k')\mathbf{H}(k)'\mathbf{S}(k)^{-1}.$$

5: The updated state and its associated covariance are designated as

$$\hat{\mathbf{x}}(k|k) = \hat{\mathbf{x}}(k|k') + \mathbf{G}(k)\mathbf{r}(k),$$

$$\hat{\mathbf{P}}(k|k) = \hat{\mathbf{P}}(k|k') - \mathbf{G}(k)\mathbf{S}(k)\mathbf{G}(k)'.$$

6: **end procedure**

covariance matrix corresponding to the $\mathbf{p}(k)$. Here, the pseudorange measurement set $\mathbf{p}(k)$ is fed as $\mathbf{z}(k)$ to Algorithm .

We are constructing the equivalent measurements in Cartesian space using the updated and predicted states of the filter.

5.2.3 Tracklet Computation

This tracklet method provides approximate equivalent measurements of the reported tracks without any additional assumptions. Moreover, it is not mandatory to have synchronous updates from all the filters. Tracklets can be computed between any two updates from the same GNSS sensor. Here, "inverse Kalman filter based" tracklet computation method (Drummond 2002) is applied. Based on this method, the equivalent measurement for GNSS sensor j using the filtered output at k' and k is $\mathbf{m}_j(k, k')$. The timestamp information at these two instants should be available to compute

equivalent measurements at a given epoch. Therefore, the equivalent measurement is

$$\mathbf{m}_j(k,k') = \hat{\mathbf{x}}_j(k|k') + \mathbf{A}_j(k|k')\left[\hat{\mathbf{x}}_j(k|k) - \hat{\mathbf{x}}_j(k|k')\right] \tag{5.14}$$

where

$$\mathbf{m}_j(k,k') = \mathbf{x}_j(k) + \tilde{\mathbf{m}}_j(k,k) \tag{5.15}$$

and

$$\mathbb{E}\left[\tilde{\mathbf{m}}_j(k,k) \mid \mathbf{z}_j^{k'}\right] = 0 \tag{5.16}$$

where $\mathbb{E}[\cdot]$ is an expectation operator. Here $\mathbf{z}^{k'}$ is represents that measurements upto k' time instant, that is $\mathbf{z}^{k'} = \{p_j(1), \cdots, p_j(k')\}$. The equivalent measurement error covariance matrix corresponding to $\mathbf{m}_j(k,k')$ is $\mathbf{M}_j(k,k')$ designated as

$$\mathbf{M}_j(k,k') = \left[\mathbf{A}_j(k|k') - \mathbf{I}\right]\mathbf{P}_j(k,k') \tag{5.17}$$

where

$$\mathbf{A}_j(k,k') = \mathbf{P}_j(k,k')\left[\mathbf{P}_j(k,k') - \mathbf{P}_j(k,k)\right]^{-1} \tag{5.18}$$

Only the final equation of the equivalent measurement covariance is presented in (5.17), for detailed derivation, refer (Drummond 2002). To compute tracklet at any k, one should have $\hat{\mathbf{x}}_j(k|k)$ and $\mathbf{P}_j(k,k)$. The tracklets can be computed for any number of lags. Because of this feasibility, if the filter update rate is different, it will not create any issues in the algorithm. However, to compute tracklet at k, the matrix $[\mathbf{P}_j(k,k') - \mathbf{P}_j(k,k)]^{-1}$ has to be non-singular. The detailed derivation of the tracklet, its sub-optimality conditions, and non-singularity issues are presented in (Huang et al. 2012). The equivalent measurement corresponding to the position of the GNSS sensor is representing as

$$\mathbf{z}_{\mathbf{x}_j}(k) = \mathbb{F}\mathbf{m}_j(k,k') \tag{5.19}$$

where $\mathbb{F} = \text{diag}\{1,0,1,0,0\}$. Similar to that of state, the equivalent measurement covariance is given by

$$\mathbf{R}_{\mathbf{x}_j}(k) = \mathbb{F}\mathbf{M}_j(k,k')\mathbb{F}' \tag{5.20}$$

Here, $\mathbb{F}$ is to extract the position information from the equivalent measurement vector. It is worth noting that the state vector and the equivalent measurement vector are of the exact dimensions.

5.2.4 Platform Positioning

We consider M GNSS sensors spatially deployed at $\{\mathbf{x}_j\}_{j=1}^{M}$ on a given target as shown in Figure 5.3. The target platform location is $\mathbf{x}$, which can be the arbitrary location on the target (not necessarily GNSS receiver present in that location). Since the installation of sensors is predefined, one can define the location of the GNSS sensors relative to the platform location as illustrated in Figure 5.3. Here, δ_j^x and δ_j^y are the relative distances of $\mathbf{x}_j$ with respect to $\mathbf{x}$. The relation between relative distance-vector, installed sensor location, and platform location is given by

$$\mathbf{x} = \mathbf{x}_j + \begin{bmatrix} \delta x_j \\ \delta y_j \end{bmatrix}. \tag{5.21}$$

The equivalent measurement obtained for the GNSS sensors j is

$$\mathbf{z}_{\mathbf{x}_j} = \mathbf{H}_j \mathbf{x}_j + \mathbf{w}_j, \tag{5.22}$$

where $\mathbf{H}_j = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\mathbf{w}_j$ follows zero mean white Gaussian noise with covariance equal to $\mathbf{R}_{\mathbf{x}_j}$. The measurements are translated with respect to the platform location using the relative position information which is readily available. The modified measurements are designated as

$$\mathbf{z}^t_{\mathbf{x}_j} = \mathbf{H}_j \mathbf{x}_j + \mathbf{H}_j \begin{bmatrix} \delta x_j \\ \delta y_j \end{bmatrix} + \mathbf{w}_j \tag{5.23}$$

$$= \mathbf{H}_j \mathbf{x} + \mathbf{w}_j. \tag{5.24}$$

The (5.24) is obtained by substituting the (5.21) in (5.23). Considering all the N measurements to form a batch least squares solution to estimate the state of interest $\mathbf{x}$. The measurement transition matrix and the measurement noise covariance matrix for batch LS is given by

$$\mathbf{H}^N = \begin{bmatrix} \mathbf{H}_1 \\ \vdots \\ \mathbf{H}_N \end{bmatrix}, \mathbf{R}^N = \text{diag}(\mathbf{R}_{\mathbf{x}_1}, \cdots, \mathbf{R}_{\mathbf{x}_N}). \tag{5.25}$$

The LS estimate is given by (Bar-Shalom et al. 2004) as

$$\hat{\mathbf{x}} = \left[\left(\mathbf{H}^N\right)' \left(\mathbf{R}^N\right)^{-1} \left(\mathbf{H}^N\right) \right]^{-1} \left(\mathbf{H}^N\right)' \left(\mathbf{R}^N\right)^{-1} \left(\mathbf{z}^t_{\mathbf{x}_j}\right)^N \tag{5.26}$$

Substituting the (5.25) in (5.26) provides

$$\hat{\mathbf{x}} = \frac{1}{N}\sum_{j=1}^{N} \mathbf{z}^{t}_{\mathbf{x}_j} \tag{5.27}$$

The above result in (5.27) using batch LS is equal to the sample mean of all the N observations.

In the given environment, a spoofer is located at $\mathbf{x}^s$ and trying to spoof any one of the GNSS sensors installed on the target. In a crowded GNSS sensors case, the influence of spoofing is not limited to one receiver, and it corrupts all the position information of GNSS receivers in the vicinity (Tippenhauer et al. 2011). Besides, due to the spoofing activity of the spoofer, GNSS sensor j is spoofed by a distance of $\Delta\mathbf{x}_j$. Where $\Delta\mathbf{x}_j = [\Delta x, \Delta y]'$. The relation between relative distance-vector, installed sensor location, and spoofed distance is given by

$$\mathbf{x} = \mathbf{x}_j + \Delta\mathbf{x}_j + \begin{bmatrix} \delta x_j \\ \delta y_j \end{bmatrix}. \tag{5.28}$$

The translated measurement for the sensor j using the relative distance vector is represented as

$$\mathbf{z}^{f}_{\mathbf{x}_j} = H_j\mathbf{x}_j + \Delta\mathbf{x}_j + \begin{bmatrix} \delta x_j \\ \delta y_j \end{bmatrix} + \mathbf{w}_j. \tag{5.29}$$

here, the measurement contain two unknown vectors $\mathbf{x}_j$ and $\Delta\mathbf{x}_j$. The (5.29) is subjected to the batch LS frame work as shown in the clean environment, and the estimate is given by

$$\hat{\mathbf{x}}^f = \frac{1}{N}\sum_{j=1}^{N} \mathbf{z}^{f}_{\mathbf{x}_j} \tag{5.30}$$

By observing the (5.27) and (5.30), we can infer that the objectives of the proposed investigation are to detect the spoofing effect, localize the spoofer location $\mathbf{x}^s$ and mitigate the effect of spoofing.

5.2.5 Detection of a Spoofing Attack with Tracklets

To detect the spoofing effect, we are establishing a binary hypothesis test using the obtained translated measurements. In no spoofing case, the hypothesis $\mathcal{H}_0$ is assuming

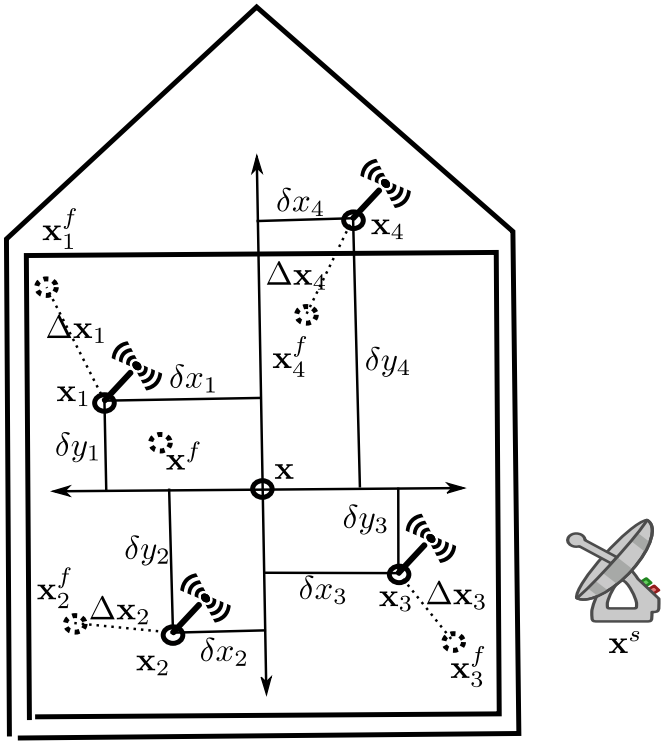

Figure 5.3: The geometry of multiple GNSS receivers installation on a target (ship). The dark circle represents the actual position of the GNSS receiver, and the dotted circle represents the false position of the GNSS receiver in spoofing activity.

that estimated positions of the GNSS receivers are owing to authentic measurements. Whereas the hypothesis $\mathcal{H}_1$ is for the spoofing case, in which the estimated position estimates are false due to the spoofing. That is

$$\mathcal{H}_0 : \mathbf{z}_{\mathbf{x}_j} = \mathbf{x}_j + \begin{bmatrix} \delta x_i \\ \delta y_i \end{bmatrix} + \mathbf{w}_j; j = 1, \cdots, N \tag{5.31}$$

$$\mathcal{H}_1 : \mathbf{z}_{\mathbf{x}_j} = \mathbf{x}_j + \Delta\mathbf{x}_j + \begin{bmatrix} \delta x_i \\ \delta y_i \end{bmatrix} + \mathbf{w}_j; j = 1, \cdots, N \tag{5.32}$$

The observations in (5.31) and (5.32) follow a normal distribution and the noise samples are independent of each other. The pdf of likelihood of observations under the given hypothesis $\mathcal{H}_0$ is

$$p\left(\mathbf{z}_{\mathbf{x}_j}; \mathbf{x}_j, \begin{bmatrix} \delta x_i \\ \delta y_i \end{bmatrix}, \mathcal{H}_0\right) = \prod_{j=1}^{N} p\left(\mathbf{z}_{\mathbf{x}_j}^r \mid \mathbf{x}\right) \tag{5.33}$$

Similarly, the pdf of likelihood of observations under the given hypothesis $\mathcal{H}_1$ is

$$p\left(\mathbf{z}_{\mathbf{x}_j}; \mathbf{x}_j, \begin{bmatrix} \delta x_i \\ \delta y_i \end{bmatrix}, \Delta\mathbf{x}_j, \mathcal{H}_1\right) = \prod_{j=1}^{N} p\left(\mathbf{z}_{\mathbf{x}_j}^f \mid \mathbf{x}\right) \tag{5.34}$$

The generalized likelihood ratio test (GLRT) of the above two hypothesis is given by

$$\frac{p\left(\mathbf{z}_{\mathbf{x}_j};\mathbf{x}_j,\begin{bmatrix}\delta x_i\\ \delta y_i\end{bmatrix},\Delta\mathbf{x}_j,\mathcal{H}_1\right)}{p\left(\mathbf{z}_{\mathbf{x}_j};\mathbf{x}_j,\begin{bmatrix}\delta x_i\\ \delta y_i\end{bmatrix},\mathcal{H}_0\right)}=\frac{\prod_{j=1}^{N}p\left(\mathbf{z}^f_{\mathbf{x}_j}\mid\mathbf{x}\right)}{\prod_{j=1}^{N}p\left(\mathbf{z}^t_{\mathbf{x}_j}\mid\mathbf{x}\right)}\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}\gamma \tag{5.35}$$

At time index k, the GLRT is evaluated to distinguish between a spoofing attack is present or not. Therefore

$$\zeta(k)=\begin{cases}1; & \text{GNSS attack presence}\\ 0; & \text{else.}\end{cases} \tag{5.36}$$

Here, ζ is a flag signal to know the spoofing presence. For GNSS spoofing attack presence flag $\zeta=1$, else $\zeta=0$.

5.2.6 Spoofing Attack Detection with Bearings

The GLRT based spoofing attack detection is presented in Section 5.2.5. Along with this GLRT, another spoofing attack detection is also considering by using the bearings information. In clean environment, all the DOA $\{\theta^t_i\}_{i=1}^{M}$ are distinguishable, since the arrivals are from different source locations. Whereas in spoofing attack, the DOA $\left\{\theta^f_i\right\}_{i=1}^{M}$ are in-distinguishable due to all the signals arrive from same direction and the same source location (Kang et al. 2018). Therefore at time k, the detector is

$$\eta(k)=\begin{cases}0; & \theta_i\neq\theta_j \quad \forall \quad i,j=1,2,\ldots M \quad \text{where} \quad i\neq j\\ 1; & \text{else}\end{cases} \tag{5.37}$$

Here, η is a flag signal to distinguish the spoofing attack or not.

5.3 Pseudo-track and Spoofer Localization

Once the spoofing attack is confirmed using the GLRT, the spoofer localization or tracking is essential to mitigate the spoofing effect. However, during the spoofing attack, the position integrity of the GNSS sensors is not preserving. Hence, we propose a pseudo track updation technique to preserve the platform positioning. These pseudo track updates are used in the bearings-only information framework to localize the intensional interference source.

5.3.1 Pseudo Track of the Platform

At discrete time index k, the spoofer attack is detected by using the GLRT and DOA. Hence, the estimated position at k using batch LS results in $\hat{\mathbf{x}}^f(k)$ rather than $\hat{\mathbf{x}}(k)$. Therefore, an approximate position of the GNSS physical sensor location is required to perform localization using bearings-only information. The updated position can be approximated by using the pseudo-position method. At a given discrete time instant k, the failure of measurement (spoofing) or unavailability of measurement (jamming) results in a lack of updated state at k^{th} instant. However, one can assume the updated state as predicted state in the intensional interference case as suggested in (Bar-Shalom et al. 2004)

$$X_j(k) = F_j(k')\hat{X}_j(k') \tag{5.38}$$

The above is KF pseudo-update step at k, which uses the last update state available at k' and the state transition matrix.

5.3.2 Source Localization with Bearings only Information

The source localization is performed at a given k using the pseudo-position and observed bearings. The spoofer is located at $\mathbf{x}^s$ and transmitting the spurious signals onto the target. If the GNSS cannot generate the bearings due to the packaging, the bearing can also be retrieved by placing nearby bearings sensors. A low cost and area bearings only sensor modules are readily available for limited range applications. Hence, each GNSS sensor platform is also providing with a bearing sensor. The localization problem can be formulated as LS, ILS, and newtons methods. However, the ILS outperforms other methods. Hence, we are formulating the ILS to localize the spoofing source; since this method iteratively improves the current estimate using the measurements until the desired accuracy accomplishes.

The measurement model for the bearings corresponding to the sensor j is

$$\begin{aligned}\theta_j &= h\left(\mathbf{x}^s, \mathbf{x}_j\right) + v_j \\ &= \arctan\left(\frac{y^s - y_j}{x^s - x_j}\right) + v_j; j = 1, \cdots, N\end{aligned} \tag{5.39}$$

where v_j is the zero mean white Gaussian measurement noise with variance σ_θ^2. In (5.39), x_j and y_j are the pseudo-positions obtained by using the prediction of the

previous state. The stacked vector Θ of all the available bearings is given by

$$\begin{aligned}\Theta &= \begin{bmatrix}\theta_1 \\ \vdots \\ \theta_N\end{bmatrix} \\ &= \mathbf{h}\left(\mathbf{x}^s, \mathbf{x}_j\right) + \mathbf{v}\end{aligned} \tag{5.40}$$

where

$$\mathbf{h}(\mathbf{x}^s) = \begin{bmatrix}h\left(\mathbf{x}^s, \mathbf{x}_1\right) \\ \vdots \\ h\left(\mathbf{x}^s, \mathbf{x}_N\right)\end{bmatrix}, \quad \mathbf{v} = \begin{bmatrix}v_1 \\ \vdots \\ v_N\end{bmatrix} \tag{5.41}$$

Using the estimate $\hat{\mathbf{x}}_n^s$ at the end of iteration n, one can update the ILS estimate as $\hat{\mathbf{x}}_{n+1}^s$ using (Bar-Shalom et al. 2004)

$$\hat{\mathbf{x}}_{n+1}^s = \hat{\mathbf{x}}_n^s + \left(J_n' \mathcal{R}^{-1} J_n\right)^{-1} J_n' \mathcal{R}^{-1} \left[\Theta - \mathbf{h}\left(\hat{\mathbf{x}}_n^s, \mathbf{x}_j\right)\right] \tag{5.42}$$

where J_n is the Jacobian matrix represented as

$$J_n = \begin{bmatrix}\frac{\partial h(\mathbf{x^s}, \mathbf{x_1})}{\partial x} & \frac{\partial h(\mathbf{x^s}, \mathbf{x_1})}{\partial y} \\ \vdots & \vdots \\ \frac{\partial h(\mathbf{x^s}, \mathbf{x_N})}{\partial x} & \frac{\partial h(\mathbf{x^s}, \mathbf{x_N})}{\partial y}\end{bmatrix}_{\mathbf{x^s} = \hat{\mathbf{x}}_\mathbf{n}^\mathbf{s}} \tag{5.43}$$

with

$$\begin{aligned}\frac{\partial h\left(\mathbf{x^s}, \mathbf{x_j}\right)}{\partial x^s} &= -\frac{y^s - y_j}{\left(x^s - x_j\right)^2 + \left(y^s - y_j\right)^2} \\ \frac{\partial h\left(\mathbf{x^s}, \mathbf{x_j}\right)}{\partial y^s} &= \frac{x^s - x_j}{\left(x^s - x_j\right)^2 + \left(y^s - y_j\right)^2}\end{aligned}$$

Convergence criteria is decided with the number of iterations or the achievable accuracy. Moreover, the initialization of the position is done by taking any two intersections from the given bearings only measurements.

5.3.3 Spoofing Mitigation

In spoofing activity, all the spoof signals arriving in the same direction. Hence, by placing a null beam in the direction of spurce mitigates the spoofing (Daneshmand et al. 2012). However, to steer the null beam in that direction, one need to calculate the spoofer location and which is being carried out by using bearings information.

When ever the flags ζ and η sets to one, it confirms spoofing activity and it enables the flag f, which is given by

$$f(k) = \begin{cases} 1; \ (\zeta(k) == 1)\&\&(\eta(k) == 1) \\ 0; \ \text{else} \end{cases} . \tag{5.44}$$

However, the flag $f(k)$ sometimes can be a false positive. So, we formulated a management module to study the flags over the time which is similar to track management in target tracking application (Bar-Shalom et al. 2011). We adopted m/n rule to make a decision about spoofing. In a given n scans of data, if flags are unity for m scans, it confirms spoofing activity. The quantifying metric to launch counter-measure against the spoofing activity is given from a decision metric

$$f_n = \sum_{i=0}^{n} f(k-i), \tag{5.45}$$

whenever this metric $f_n > m$, the counter measure launches. This mitigation is possible by launching an counter-attack like null beam projection towards the direction of spoofer or shooting the spoofer as a anti-spoofing measure as in defense applications. The overall algorithm flow corresponding to detection and mitigation are given in Algorithm 1.

5.4 Results and discussions

5.4.1 Simulation scenario

WGS-84 with circular orbit assumption is used to simulate the satellite trajectories in both spoofing case and non-spoofing cases. The positions of the satellite are simulated using Section-1.1.8. Superyachts to mega yachts usually vary from 24m long to 100m long. Hence we consider a yacht in our simulation scenario on which four GNSS receivers are installed. The center of the yacht (platform) is considered as the position estimate of the whole yacht. At the initial time $k = 1$, the position vector of the yacht is $\mathbf{x} = [0, 0]'$, and the yacht moving with a constant velocity of 10m/s in the east and 20m/s in north directions throughout the simulation. The simulation time is 50s, and the sampling time is 1s. However, rather than installing the sensor at the center of the yacht, four GNSS receivers are deployed at different locations. The RPV of the GNSS sensors concerning the platform is tabulated in Table 5.1. The location of

Algorithm 5 Algorithm overview for GNSS spoofing detection and mitigation

procedure DETECTION AND MITIGATION
  for $k = 1 :$ scans **do**
    for $j = 1 : M$ **do**
      Compute updated state $\hat{\mathbf{x}}_j(k|k)$ and updated covariance $\hat{\mathbf{P}}_j(k|k)$ by using pseudorange measurements $\{p_{i,j}\}_{i=1}^{I}$. ▷ EKF framework
      Compute equivalent measurement $\mathbf{z}_{\mathbf{x}_j}(k)$ and equivalent measurement covariance $\mathbf{R}_{\mathbf{x}_j}$ by using prediction $\hat{\mathbf{x}}_j(k|k')$, $\hat{\mathbf{P}}_j(k|k')$ and updated information $\hat{\mathbf{x}}_j(k|k)$, $\hat{\mathbf{P}}_j(k|k)$. ▷ Tracklet framework
      Compute translated equivalent measurement $\mathbf{z}^t_{\mathbf{x}_j}(k)$ by using equivalent measurement $\mathbf{z}_{\mathbf{x}_j}(k)$ and RPV $\delta x_j, \delta y_j$. ▷ Translation
    end for
    Compute ζ by using translated equivalent measurement $z^t_{\mathbf{x}_j}(k)$. ▷ Spoofing test with tracklets
    Compute η by using the bearings information Θ. ▷ Spoofing test with Bearings
    if $(\zeta == 1)\&\&(\eta == 1)$ **then**
      for $j = 1 : M$ **do**
        Compute pseudo track update $\hat{\mathbf{x}}^p_j(k|k)$ using predicted states $\hat{\mathbf{x}}_j(k \mid k')$, $\hat{\mathbf{x}}_j(k' \mid k'')$ and updated state $\hat{\mathbf{x}}_j(k'|k')$. ▷ Pseudo track updation
      end for
      Compute platform position $\hat{\mathbf{x}}(k)$ by using pseudo track updates $\left\{\hat{\mathbf{x}}^p_j(k|k)\right\}_{j=1}^{M}$ ▷ batch LS framework
      Set flag $f(k) = 1$
      Compute spoofer state $\mathbf{x}^s$ using $\Theta(k)$ ▷ ILS framework
    else
      Compute platform location $\hat{\mathbf{x}}(k)$ using updated states $\left\{\hat{X}_j(k|k)\right\}_{j=1}^{M}$ ▷ batch LS framework
    end if
    Compute $f_{\sum}$ ▷ Windowing
    if $f_n > 3$ **then**
      Null beam projection towards $\mathbf{x}^s$ ▷ Spoofing mitigation
    end if
  end for
end procedure

spoofer concerning platform location is also presented in Table 5.1, and is as shown in Figure 5.3. We consider a false trajectory walking test bench to evaluate the proposed algorithm. That is, consistently the receiver is misled by constant distance, and the trajectory follows the constant velocity (CV) model as shown in Figure 5.3. The spoofing process is carried out using a repeater-based spoofer. It is always advisable to maintain a constant distance between the spoofer and target to avoid anti-spoofing algorithms like power thresholding (Wesson et al. 2017). Therefore, the spoofer is 300m away from the platform and traveling parallel to the yacht throughout the simulation scenario. The yacht turbulence modeled as a process noise. The process

Table 5.1: The relative position vector from the center of the yacht

	receiver-1	receiver-2	receiver-3	receiver-4	spoofer
δ_x	-20	-15	45	35	0
δ_y	20	-30	-10	50	300

noise components along the east and north follows the white Gaussian with standard deviations of 1m and 1m respectively. The state vector is $[x\ y\ \dot{x}\ \dot{y}]'$ and the state transition is given by

$$F_j = \begin{bmatrix} 1 & 0 & \delta t & 0 \\ 0 & 1 & 0 & \delta t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{5.46}$$

In which the δt is the sampling time and equal to 1s. All the GNSS sensors are synchronous for the given sampling time and report the updated state by processing the received pseudorange measurements. The spoofing process starts at k=20; the simulation scenario of GNSS sensors and spoofer is as shown in Figure 5.4. The true pseudorange measurements are corrupted with WGN noise with mean zero and standard deviation of 3m. Due to the ideal spoofer assumption, the repeater-based spoofer also processes with the same noise statistics, i.e., the spoofed pseudorange measurements are also corrupted with WGN noise with zero mean and standard deviation of 3m.

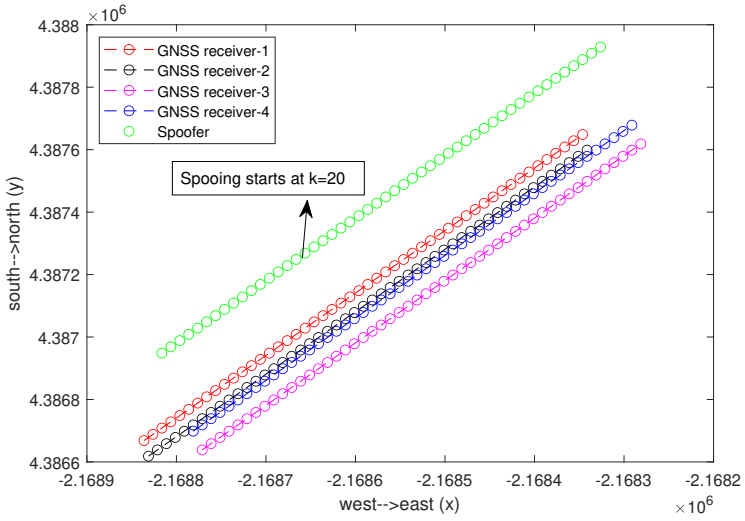

Figure 5.4: Positions of multiple GNSS receivers installed on a target (ship) and spoofer

5.4.2 GNSS tracks accuracy

The position estimate of the each GNSS receiver is obtained by using pseudorange measurements in EKF framework. The tunable parameters of the filter are its process noise covariance $\mathbf{Q}$ and measurement noise covariance $\mathbf{R}$. All the GNSS sensors are given with

$$\mathbf{Q} = q_\sigma \begin{bmatrix} \frac{\delta t^3}{3} & 0 & & 0 \\ 0 & \frac{\delta t^3}{3} & 0 & \frac{\delta t^2}{2} \\ \frac{\delta t^2}{2} & 0 & \delta t & 0 \\ 0 & \frac{\delta t^2}{2} & 0 & \delta t \end{bmatrix}, \mathbf{R} = \text{diag}(3^2, \cdots, 3^2). \tag{5.47}$$

Two point initialization method (Bar-Shalom et al. 2011) is adopted to initialize the GNSS tracks at $k = 1$. The two point initialization uses the position estimates provided at $t(0)$ and $t(1)$ as

$$\mathbf{x}(1) = \left[\mathbf{x}(1), \ \frac{\mathbf{x}(1) - \mathbf{x}(0)}{\delta t}\right]'. \tag{5.48}$$

Till $k = 20$, the GNSS receivers estimate the PVT correctly due to the reception of authentic measurements. At $k = 20$, spurious signals are locking onto the receiver, and the GNSS receiver estimates a false position owing to false pseudoranges. So in the absence of anti-spoofing algorithms, the position root means square error (PRMSE) increases during the attack. Even though the spoofer intended to spoof the GNSS-1, all the four GNSS receivers spoofed to different locations. Here, all the four GNSS

receivers are involved in spoofing attacks due to the Omni-directional behavior of the spoofer (Tippenhauer et al. 2011). Hence, in the spoofing activity, the PRMSE of the GNSS receivers is different under spoofer-to-receiver distance as given in (5.9). Therefore, throughout the spoofing attack, the PRMSE raises in the absence of anti-spoofing algorithms. The EKF estimation accuracy for all the GNSS receivers are depicted in Figure 5.5 with four spoofed measurements.

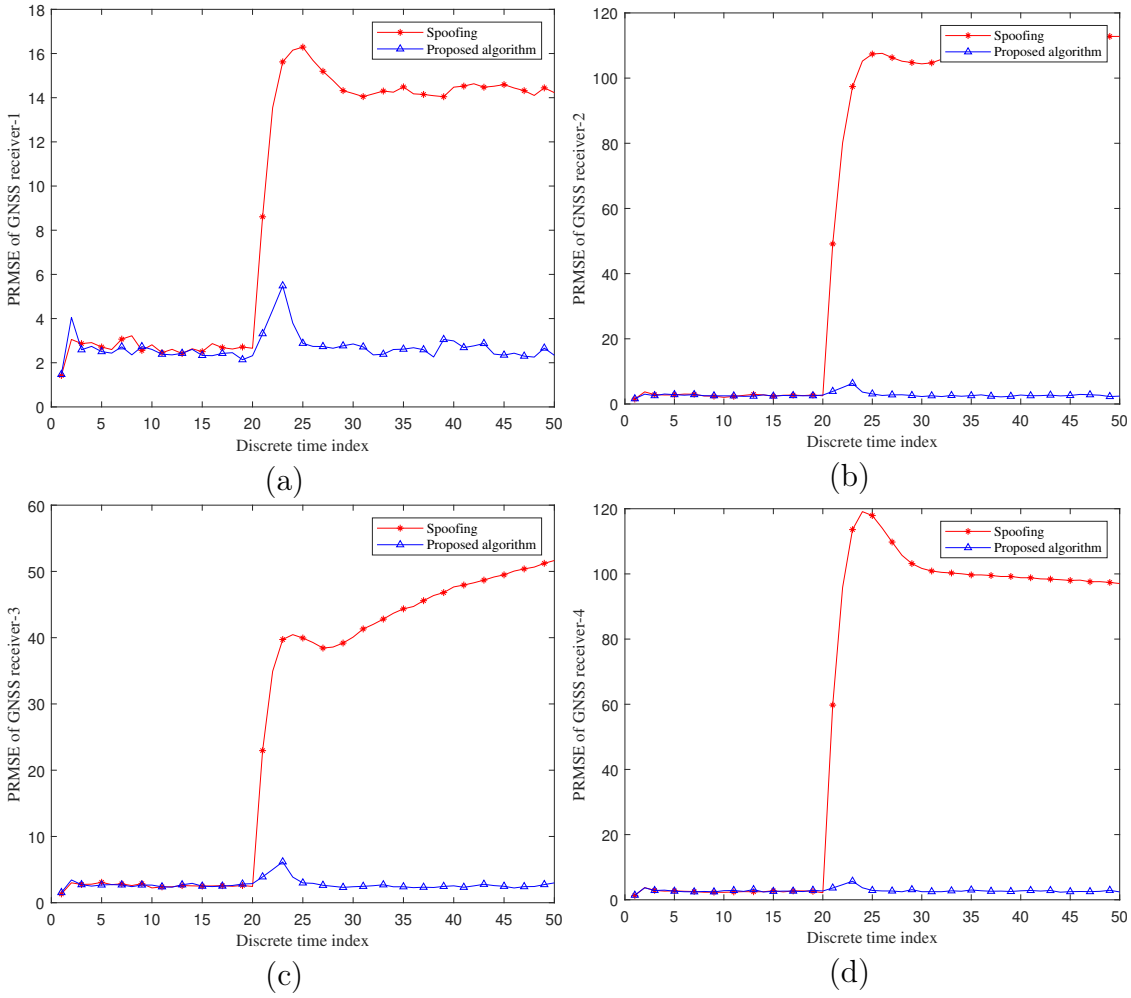

Figure 5.5: PRMSE of installed GNSS receivers with four satellite measurements (a) GNSS receiver-1, (b) GNSS receiver-2, (c) GNSS receiver-3, and (d) GNSS receiver-4

In Figure 5.5(a), we can see that the spoofing attack leads to a rise in PRMSE to 16m since the spoofer intended to spoof GNSS-1 by 10m along east and north. This implication of position spoofing does not imply equality on all the GNSS receivers. Because the spatial distance of GNSS receivers is different, hence we can observe that the GNSS-2, GNSS-3, GNSS-4 receivers are spoofing to different locations, and

PRMSE is 40m, 100m, 100m, respectively. In the initial phase of spoofing attack, i.e., at $k \in [21-23]$, the PRMSE is rising because the filter gives more weight to measurement rather than prediction. In this process, the gain changes and tunes to the spoofed measurements. The sudden deflection in the measurement is considered the outlier, and the filter cannot mitigate such outliers. The filter estimates the updated state based on the prediction and the available measurement at that instant. In this process, the filter took four samples to reach the worst spoofing case (max value of spoofing deflection). We adopted the 1/3 rule to make pseudo track updation and the 4/7 rule to mitigate the effect. Therefore, as given in (5.38), the pseudo track is considered for the GNSS during the period of $k \in [21-24]$. Hence after four samples of data, i.e., at $k = 25$, the signals are not considered from the spoofer localized direction as mitigation. Once this mitigation performs, the actual measurements getting locked into the receivers. Therefore, the actual measurements are considered from $k = 25$ to perform the position estimate.

In the Figure 5.5, it is worth noting that the PRMSE raises during the interval of $k \in [21-24]$. This is due to the prediction state rather than the updated state. Hence, if a filter runs with the prediction, it cannot accommodate the turbulence, and an error is seen. The rise in PRMSE during this interval is around $2-4$m. Since the target is moving with the CV model, this error is less, and else we can see more error for turn and acceleration models. Therefore, this pseudo track updation is a suitable candidate for navigation in an intensional interference case for a lesser duration. Once the attack is detected, the target can rely on the prediction of the track or inertial measurement units. Soon after the attack is mitigating, the filter again acquires the authentic measurements and computes the GNSS state. After mitigation, the filter again tunes to these measurements, and PRMSE starts decreasing. This can be seen in the results that the PRMSE comes down from $k = 24$ and again settles.

5.4.3 Platform Positioning

The platform positioning is the resultant of constructed equivalent measurements. Here, the equivalent measurements are translated and processed in batch LS framework to get the platform position. In this process, the estimate improves compared to the GNSS track due to batch LS. The platform position PRMSE is depicting in

Figure 5.6 with four GNSS receivers, and each receiver gets four pseudoranges. Here, we observe that in the spoofing case, the PRMSE increase and proposed method can maintain the continuity in the track with the help of pseudo-track update. In the absence of anti-spoofing, the PRMSE comes around 15–20m. Whereas, by the proposed method, the platform can maintain the PRMSE in the range of 2–4m, agreeing with the civilian GNSS receiver estimate.

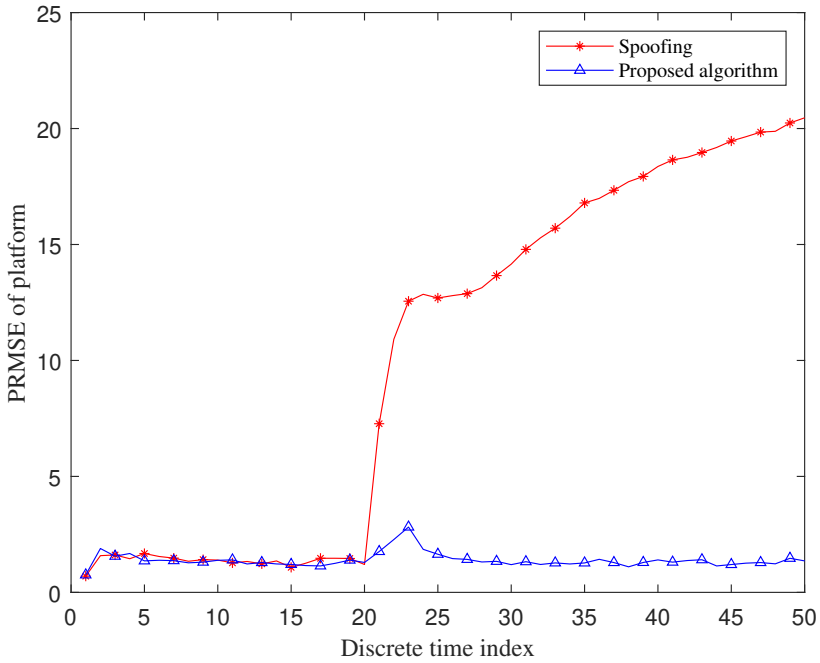

Figure 5.6: PRMSE of the platform by fusing all the pseudo-positions obtained by tracklet framework (four satellites are in range to GNSS receivers)

Moreover, this batch LS gives an improved estimate, and it is shown in the Figure 5.7 concerning PRMSE. It is observed that computing the platform position using batch LS gives an improved estimate. The individual GNSS sensors offer the PRMSE around 2.5–6m, whereas the platform offers 1.5–3m accuracy, almost twofold improvement. This proposed method can work for spoofing detection and is a suitable candidate to process the multiple sensors data to get the overall estimate of the platform.

5.4.4 Impact of Number of Satellites

The number of available satellites is an essential parameter in pseudorange to position estimation. Here, the state of the GNSS consists of three parameters of interest.

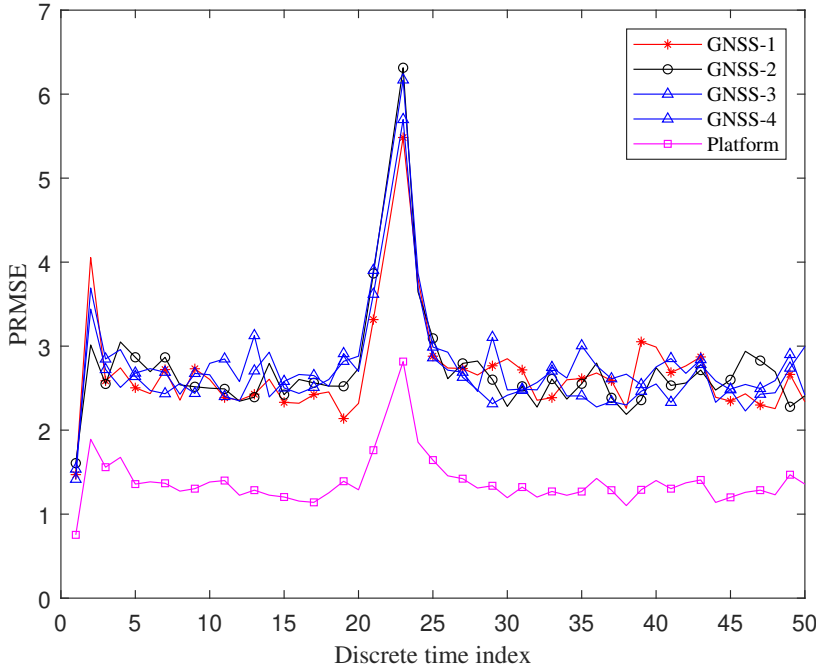

Figure 5.7: PRMSE of the platform by batch LS on equivalent measurements.

Hence, to estimate a position in 2D, one needs at least three pseudorange measurements. For satellite number is lesser than the parameters to be estimated, the solution is underdetermined. Whereas in the case of more satellites, the solution is overdetermined. Hence, the number of satellites increases the position accuracy. Therefore, in this simulation, we varied the number of satellites $N \in \{4, 5, 6\}$. By varying the number of satellites, the PRMSE of the GNSS receiver-1 is depicted in Figure 5.8, where we can observe that the increase in satellite number increases the position estimate. The other GNSS receivers also behave the same as given in Figure 5.8. Further, the platform PRMSE is also computed and visualized in Figure 5.9, and is observed the improved performance by increasing the satellite number.

5.4.5 Accuracy of Localization and Mitigation

The localization of the spoofer helps to mitigate the spoofing attack. The localization of the spoofer is achieved by using bearings to position estimates in the ILS framework. Here, the bearings are corrupted with WGN with mean zero and standard deviation of 1m rad. While performing the localization, the initial estimate of the spoofer's location is an intersection of two bearings. After that, we performed the ILS with the obtained bearings information. The number of iterations is stopped based on the achieved accuracy over the time frames and is limited to 3m. In another case, the

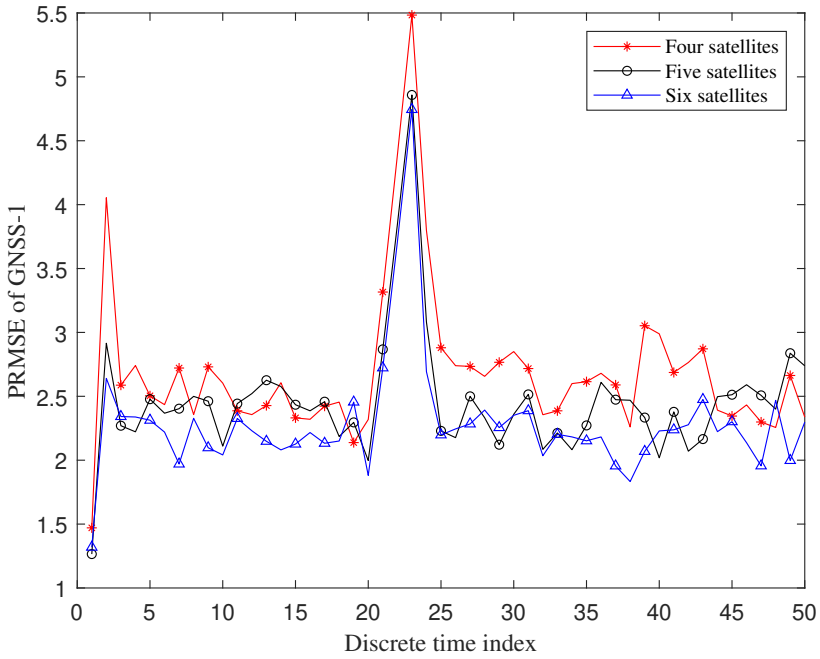

Figure 5.8: Comparison of PRMSE of GNSS-1 for various number of satellite signals.

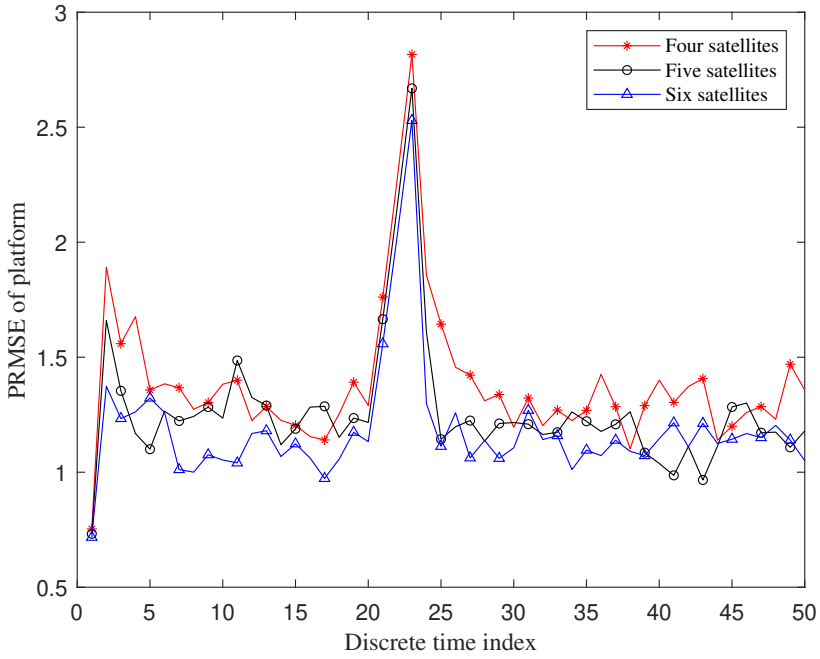

Figure 5.9: Comparison of PRMSE of platform for various number of satellite signals.

maximum number of iterations is 20. Even though the position information of the GNSS sensors is calculated using the pseudo update, we achieved a good performance. For a time-varying target, the localization problem is extended to the target tracking problem and achieved lower PRMSE in both cases. The PRMSE of the spoofer is depicted in Figure 5.10.

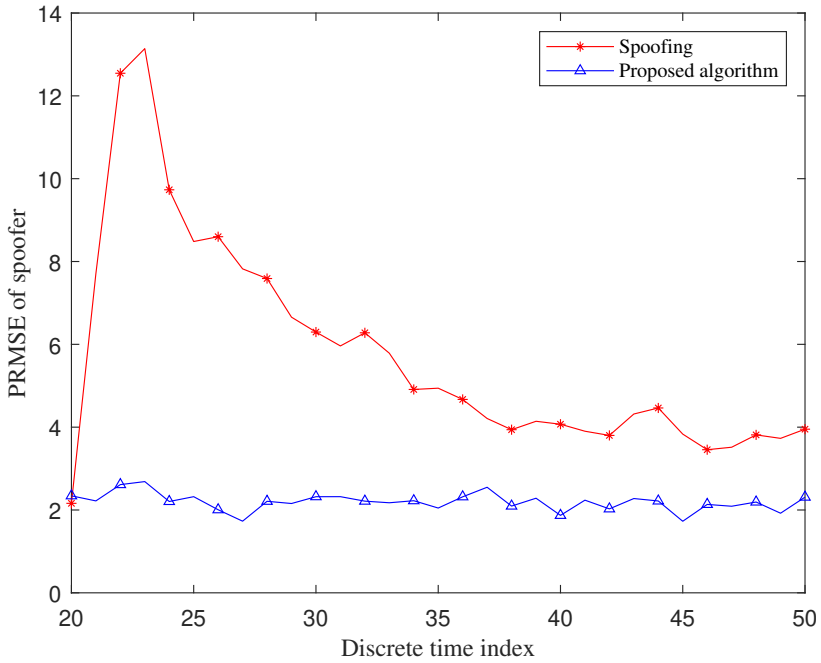

Figure 5.10: PRMSE of the spoofer (four satellites are in range to GNSS receivers)

The decision of mitigation is carried out by observing the spoofing attack detection over time. The m/n rule is adapted to make a decision. Here, for larger m, the target tracking performance can be improved, but in the same duration, the GNSS track may attain higher PRMSE due to pseudo track update. Hence, to demonstrate the effect of the decision on several scans, we varied the value of m as 4,6,8. The PRMSE corresponding to GNSS-1 for the variable number of scans is presented in Figure 5.11. This analogy is equally adapted to all the other GNSS receivers. We can observe a rise in PRMSE after $k = 20$ and before applying the mitigation. During this duration, the PRMSE only increases because of the prediction state rather than the updated state. Here, it is essential to note that this algorithm gives poor performance for a higher value of scan number to mitigate. In Figure 5.11, as the number of scans increases, the PRMSE increases. Moreover, the same impact of scans is also seen in platform positioning. In Figure 5.12, the platform position accuracy can be seen, and it is also in agreement with the sensors. This rise in the PRMSE is owing to the batch estimate of the installed GNSS sensors. Even though the PRMSE increases, it is lower compared to the installed GNSS receivers. Hence, this algorithm is equally deployable for larger scans to decide mitigation.

Further, it is worth mentioning that this algorithm works for any number of GNSS sensors. As the number of installed GNSS sensors increases, the position estimate of

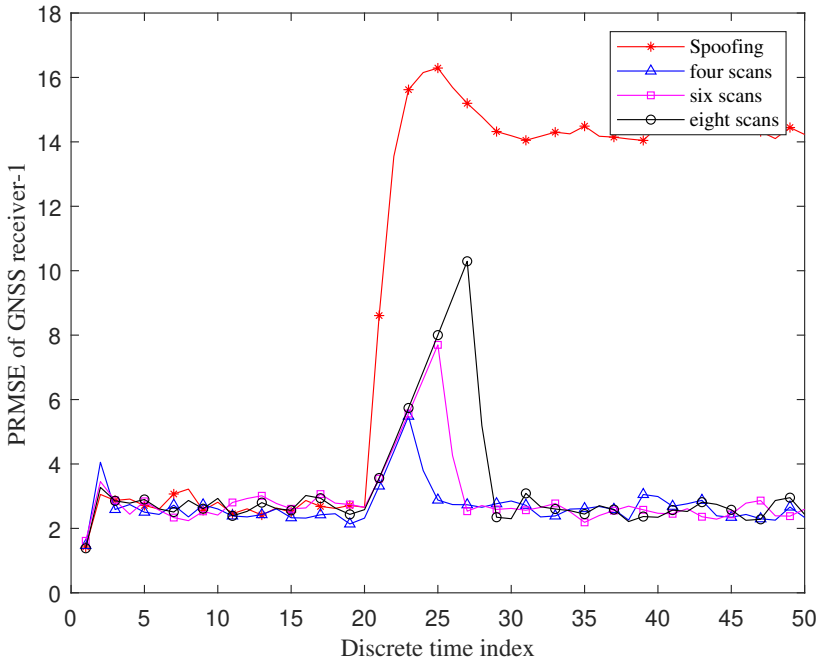

Figure 5.11: PRMSE of GNSS receiver -1 for variable number of decision on mitigation (four satellites are in range to GNSS receivers)

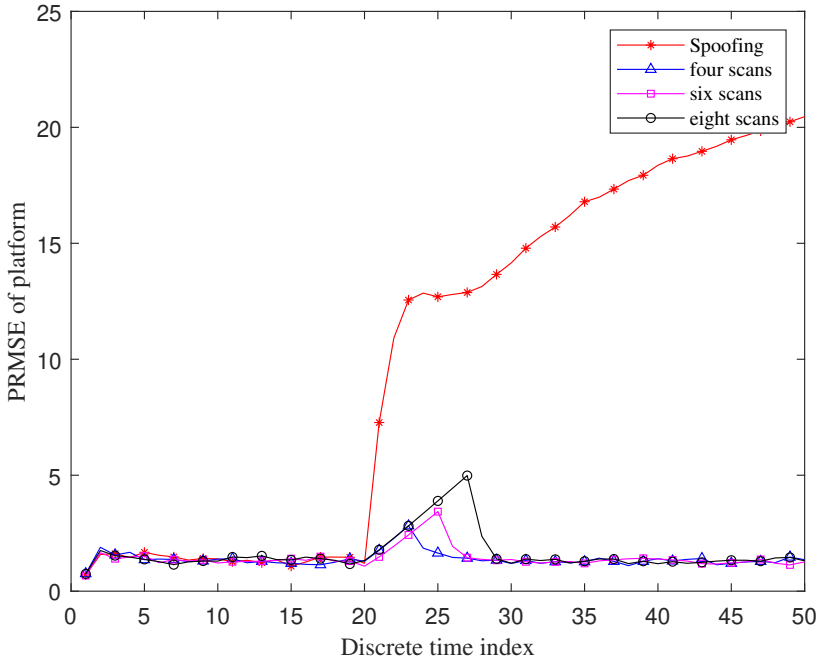

Figure 5.12: PRMSE of platform for variable number of decision on mitigation (four satellites are in range to GNSS receivers)

the platform increases. This algorithm is evaluated on a target, but this can be equally applied in the surveillance, and it is easy to know the RPV while installing.

Chapter 6

Conclusions and Future Directions

6.1 Conclusion

This thesis delt GPS spoofing and anti-spoofing techniques by using estimation theory and optimization techniques. The results obtained in this research work accomplished superior performance when compared with existing techniques. Further it added significant domain knowledge in the area of spoofing techniques with the following major contributations.

This research work primary focus is on development of stealthy GPS spoofer and spoofing mechanism. In this single-spoofer single-target (SSST)work, we present stealthy spoofer design which can counter-countermeasure the anti-spoofing state of arts like constillation check, power thresholding, and DOA estimation. The proposed repeater based distributed spoofer simulates the spoofed trajectory with the current constellation information to counter-countermeasure the anti-spoofing techniques like time synchronization and constellation check. Unlike the traditional spoofers, the proposed spoofer contains the tracker module to estimate the state of the target on which the GPS receiver is mounted, and accordingly transmit the spoofed signals with tunable transmitting power to counter-countermeasure the anti-spoofing techniques like received power threshold, received power of individual GPS signals. Further, proposed distributed spoofer configuration is spatially stealthy in deployment to counter-countermeasure the DOA based anti-spoofing technique, spoofers capable of operating in any location. Furthermore, proposed the distributed spoofer configuration with tracking and fusion is explored to enrich the quality of spoofing for low detection probability targets. further, As part of multi-spoofer multi-target (MSMT)

environment, we derived a generalized mathematical model for transmission and reception of GPS spoofed signals in MSMT scenario. Formulated the spoofer-to-target association as an optimization problem by subjected to constrains of unique mapping between spoofer and target, no spoofer and target conflicts. 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. The simulation results it is evident that only lower hit ratios are possible with this approach. Secondly the spoofers of opportunity-based centralized spoofing with GNN association is proposed to resolve the spoofer-to-target association and observed the improvement in hit-ratio as the number of spoofer of opportunity increases. 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. 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. It is evident from the PRMSE analysis, that the proposed algorithms are very stealthy to spoof both high precision and low precession GPS receivers.

This research work secondary focus is on development of Anti-spoofing algorithms for single receiver and multi receiver configurations. This work proposes an efficient alleviating method for GPS spoofing by using M-best likelihood-based optimization and a Kalman filter with data association. A novel technique of accepting all the authentic GPS signals and spoofed signals into the robust positioning algorithm, at every epoch, is presented in this paper. The robust positioning algorithm computes all possible combinations of pseudoranges, using the ILS solution. M-best position algorithm is successfully deployed to decrease the computational complexity of the robust positioning algorithm. To further accomplish the performance of the proposed method, Kalman filter followed by data association, is given and a lower track swapping rate with probabilistic data association is achieved. Simulations demonstrate that the proposed methodology is efficiently working for higher to lower satellite visibility, even

with the increase in spoofed signal injections. As a part of multi-receiver configuration, we proposed the method of installing multiple GNSS sensors on a target and assumes that the installed sensors' relative position vector (RPV) concerning the target platform center is known precisely. The generalized mathematical framework is derived for the multiple GNSS sensors in a spoofing environment. The pseudo-range measurements of either authentic satellites or the spoofer are considered to estimate the receiver's state using the extended Kalman filter (EKF) framework. Once the states are available, an equivalent measurement in the cartesian domain is derived with the help of tracklets, and these tracklets are translated using RPV. The platform location is calculated using the translated equivalent measurements in the batch least square (LS) framework. The generalized likelihood ratio test is derived based on the translated equivalent measurements to distinguish the spoofing and non-spoofing attacks. Soon after the threat is detected, an iterative least square (ILS) based localization framework is employed to localize the spoofer using the bearings-only information. However, due to the spoofing location at that epoch, the estimated GNSS location is falsified. Hence, we employed a pseudo track update to calculate the receiver's position at that epoch. The results reveal that the installation of a number of GNSS sensors is not only valid for the detection of the spoofing attack but also increasing the platform position estimate. It is also observed that as the number of satellite signals increases, the algorithms give better PRMSE of GNSS sensors, platform, and spoofer location.

It is concluded that, the above listed contributions have generated significant research interest in this domain for the future research works to be carried out. The following section provides brief summery of future research works that can be carried out based on the contributions of this thesis work.

6.2 Future Work

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 a novel algorithms which will equally 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 carry-out the spoofing process during the sensor failures.

4. One can address the non-ideal spoofer scenario, selection of positioning algorithm for non-Gaussian measurement noise, development of navigation track for the non-Gaussian case, development of data association, and low computation algorithms.

5. Furthermore, one can carry out the problem of spoofing effect mitigation in urban environment using the signal attributes and constrained optimization.

6. This research assumed that the spoofer-to-target line of sight exists and accordingly derived the cost functions. One can relax this constrain and develop a novel algorithms which will equally adaptable to urban scenario.

7. This research 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. Existing wireless sensor network algorithms can be adapted to effectively carryout the spoofing process during the sensor failures.

Bibliography

J. S. Abel and J. W. Chaffee. Existence and uniqueness of GPS solutions. *IEEE Transactions on Aerospace and Electronic Systems*, 27(6):952–956, November 1991. ISSN 0018-9251. doi: 10.1109/7.104271.

Yaakov Bar-Shalom, X Rong Li, and Thiagalingam Kirubarajan. *Estimation with applications to tracking and navigation: theory algorithms and software*. John Wiley & Sons, 2004.

Yaakov Bar-Shalom, Peter K Willett, and Xin Tian. *Tracking and data fusion*. YBS publishing Storrs, CT, USA:, 2011.

Sriramya Bhamidipati and Grace Xingxin Gao. Locating multiple GPS jammers using networked UAVs. *IEEE Internet of Things Journal*, 6(2):1816–1828, 2019.

Jahshan Bhatti and Todd E Humphreys. Hostile control of ships via false GPS signals: Demonstration and detection. *NAVIGATION: Journal of the Institute of Navigation*, 64(1):51–66, May 2017.

Jahshan A Bhatti, Todd E Humphreys, and Brent M Ledvina. Development and demonstration of a TDOA-based GNSS interference signal localization system. In *Proceedings of IEEE/ION PLANS 2012*, pages 455–469, 2012.

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)*, pages 1430–1434, July 2017. doi: 10.1109/AIM.2017.8014219.

C. Bonebrake and L. Ross O'Neil. Attacks on GPS time reliability. *IEEE Security Privacy*, 12(3):82–84, May 2014. ISSN 1540-7993. doi: 10.1109/MSP.2014.40.

Maxandre Coulon, Alexandre Chabory, Axel Garcia-Pena, Jeremy Vezinet, Christophe Macabiau, Philippe Estival, Pierre Ladoux, and Benoit Roturier. Characterization of meaconing and its impact on gnss receivers. In *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, pages 3713–3737, 2020.

R Danchick and GE Newnam. Reformulating reid's MHT method with generalised murty K-best ranked linear assignment algorithm. *IEE Proceedings-Radar, Sonar and Navigation*, 153(1):13–22, 2006.

Saeed Daneshmand, Ali Jafarnia-Jahromi, Ali Broumandan, and Gérard 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*, 2:1233–1243, September 2012.

Somnath Deb, Murali Yeddanapudi, Krishna Pattipati, and Yaakov Bar-Shalom. A generalized S-D assignment algorithm for multisensor-multitarget state estimation. *IEEE Transactions on Aerospace and Electronic systems*, 33(2):523–538, 1997.

Fontanella Diana, Bauernfeind Roland, Essfellar Bernd, and Dr Henn Gunten. In car GNSS jammer localization using vehicular ad-hoc network. *Inside GNSS Research Society*, 2013.

Oliver E Drummond. Track and tracklet fusion filtering. In *Signal and Data Processing of Small Targets 2002*, volume 4728, pages 176–195. International Society for Optics and Photonics, 2002.

Xiaoyuan Fan, Liang Du, and Dongliang Duan. Synchrophasor data correction under GPS spoofing attack: A state estimation-based approach. *IEEE Transactions on Smart Grid*, 9(5):4538–4546, 2017.

Rachel Foote. Cybersecurity in the marine transportation sector: Protecting intellectual property to keep our ports, facilities, and vessels safe from cyber threats. *Cybaris®*, 8(2):3, 2017.

Diego Galar, Uday Kumar, and Dammika Seneviratne. *Robots, Drones, UAVs and UGVs for Operation and Maintenance*. CRC Press, 2020.

Christoph Günther. A survey of spoofing and counter-measures. *NAVIGATION: Journal of The Institute of Navigation*, 61(3):159–177, June 2014.

Y. Hu, S. Bian, B. Li, and L. Zhou. A novel array-based spoofing and jamming suppression method for GNSS receiver. *IEEE Sensors Journal*, 18(7):2952–2958, April 2018. ISSN 1530-437X. doi: 10.1109/JSEN.2018.2797309.

Dongliang Huang, Henry Leung, and Eloi Bosse. A pseudo-measurement approach to simultaneous registration and track fusion. *IEEE Transactions on Aerospace and Electronic Systems*, 48(3):2315–2331, 2012.

T. E. Humphreys. Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Transactions on Aerospace and Electronic Systems*, 49(2):1073–1090, April 2013. ISSN 0018-9251. doi: 10.1109/TAES.2013.6494400.

Todd E Humphreys, Brent M Ledvina, Mark L Psiaki, Brady W O'Hanlon, and Paul M Kintner. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Radionavigation laboratory conference proceedings*, 2008.

Louis J Ippolito. *Satellite communications systems engineering*. Wiley Online Library, 2017.

Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle. GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, 2012(127072):1–16, July 2012.

Kai Jansen, Matthias Schäfer, Vincent Lenders, Christina Pöpper, and Jens Schmitt. Localization of spoofing devices using a large-scale air traffic surveillance system. In *Proceedings of the 2017 ACM on Asia conference on computer and communications security*, pages 914–916, 2017.

Zhiyang Ju, Hui Zhang, and Ying Tan. Distributed deception attack detection in platoon-based connected vehicle systems. *IEEE Transactions on Vehicular Technology*, 69:4609–4620, 2020.

Chang Ho Kang, Sun Young Kim, and Chan Gook Park. Adaptive complex EKF based DOA estimation for GPS spoofing detection. *IET Signal Processing*, 12(2): 174–181, September 2017.

Chang Ho Kang, Sun Young Kim, and Chan Gook Park. Adaptive complex-ekf-based doa estimation for gps spoofing detection. *IET Signal Processing*, 12(2):174–181, 2018.

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*, pages 262–269, May 2014. doi: 10.1109/PLANS.2014.6851385.

Andrew J Kerns, Daniel P Shepard, Jahshan A Bhatti, and Todd E Humphreys. Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, 31(4):617–636, April 2014.

T. Kirubarajan, Y. Bar-Shalom, K. R. Pattipati, and I. Kadar. Ground target tracking with variable structure IMM estimator. *IEEE Transactions on Aerospace and Electronic Systems*, 36(1):26–46, January 2000. ISSN 0018-9251. doi: 10.1109/7.826310.

T Kirubarajan, Huimin Chen, and Yaakov Bar-Shalom. Parameter estimation and the CRLB with uncertain origin measurements. *Methodology and Computing in Applied Probability*, 3(4):387–410, 2001.

Brent M Ledvina, William J Bencze, Brian Galusha, and Issac Miller. An in-line anti-spoofing module for legacy civil GPS receivers. *Proceedings of the ION ITM, San Diego, CA*, pages 698–712, January 2010.

Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou. Analysis of kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system. *IEEE Sensors Journal*, 19(13):5167–5178, July 2019. ISSN 1530-437X. doi: 10.1109/JSEN.2019.2902178.

Yang Liu, Sihai Li, Qiangwen Fu, Zhenbo Liu, and Qi Zhou. Analysis of kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system. *IEEE Sensors Journal*, 19:5167–5178, 2019.

Mohammad Majidi, Alireza Erfanian, and Hamid Khaloozadeh. Prediction-discrepancy based on innovative particle filter for estimating UAV true position in the presence of the GPS spoofing attacks. *IET Radar Sonar and Navigation*, 14: 887–897, 2020.

Alexey Malyshev, Ivan Malay, and Mikhail Ozerov. Algorithm for separating GNSS signals into components. In *2018 IEEE East-West Design & Test Symposium (EWDTS)*, pages 1–4. IEEE, 2018.

Esteban Garbin Manfredini. *Signal processing techniques for GNSS anti-spoofing algorithms*. PhD thesis, Doctoral Dissertation, Politecnico di Torino, 2017.

Daniel Marnach, Sjouke Mauw, Miguel Martins, and Carlo Harpes. Detecting meaconing attacks by analysing the clock bias of gnss receivers. *Artificial Satellites*, 48 (2):63–83, 2013.

Michael Meurer, Andriy Konovaltsev, Manuel Cuntz, and Christian 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*, pages 3007–3016, September 2012.

Fahad Ali Milaat and Hang Liu. Decentralized detection of GPS spoofing in vehicular Ad Hoc networks. *IEEE Communications Letters*, 22:1256–1259, 2018.

Matt L Miller, Harold S Stone, and Ingemar J Cox. Optimizing murty's ranked assignment method. *IEEE Transactions on Aerospace and Electronic Systems*, 33 (3):851–862, 1997.

D. Musicki and T. L. Song. Track initialization: Prior target velocity and acceleration moments. *IEEE Transactions on Aerospace and Electronic Systems*, 49(1):665–670, January 2013. ISSN 0018-9251. doi: 10.1109/TAES.2013.6404131.

Piya Pal and Palghat P Vaidyanathan. Nested arrays: A novel approach to array processing with enhanced degrees of freedom. *IEEE Transactions on Signal Processing*, 58(8):4167–4181, April 2010.

Adrien Perkins, Louis Dressel, Sherman Lo, and Per Enge. Antenna characterization for UAV based GPS jammer localization. In *Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, pages 1684–1695, 2015.

Scott Peterson and Payam Faramarzi. Iran hijacked us drone, says iranian engineer. *Christian Science Monitor*, 15, 2011.

Andreas Polydoros and Charlesl Weber. A unified approach to serial search spread-spectrum code acquisition-part i: General theory. *IEEE Transactions on communications*, 32(5):542–549, 1984.

Mark L Psiaki and Todd E Humphreys. GNSS spoofing and detection. *Proceedings of the IEEE*, 104(6):1258–1270, June 2016.

Mark L. Psiaki, Brady W. O'Hanlon, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys. GPS spoofing detection via dual-receiver correlation of military signals. *IEEE Transactions on Aerospace and Electronic Systems*, 49:2250–2267, 2013.

Juha Saarinen. Students hijack luxury yacht with gps spoofing. *Secure Business Intelligence Magazine*, 2013.

Christian Sanders and Yongqiang Wang. Localizing spoofing attacks on vehicular gps using vehicle-to-vehicle communications. *IEEE Transactions on Vehicular Technology*, 2020.

Desmond Schmidt, Kenneth Radke, Seyit Camtepe, Ernest Foo, and Michał Ren. A survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Computing Surveys (CSUR)*, 48(4):64, May 2016.

Shunshun Shang, Hong Li, Chenxi Peng, and Mingquan Lu. A novel method for gnss meaconer localization based on a space–time double-difference model. *IEEE Transactions on Aerospace and Electronic Systems*, 56(5):3432–3449, 2020.

Peter F Swaszek, Scott A Pratz, Benjamin N Arocho, Kelly C Seals, and Richard 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, pages 745–758, September 2014.

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*, 54(1):131–143, February 2018. ISSN 0018-9251. doi: 10.1109/TAES.2017.2739924.

Shahab Tayeb, Matin Pirouz, Gabriel Esguerra, Kimiya Ghobadi, Jimson Huang, Robin Hill, Derwin Lawson, Stone Li, Tiffany Zhan, Justin Zhijun Zhan, and Shahram Latifi. Securing the positioning signals of autonomous vehicles. *2017 IEEE International Conference on Big Data*, pages 4522–4528, 2017.

Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 75–86, 2011.

J. Sterling Warner, Roger G. Johnston, and CPP Los Alamos. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *The Journal of Security Administration*, 25(10):19–28, 2002.

K. D. Wesson, B. L. Evans, and T. E. Humphreys. A combined symmetric difference and power monitoring GNSS anti-spoofing technique. In *IEEE Global Conference on Signal and Information Processing*, pages 217–220, December 2013. doi: 10.1109/GlobalSIP.2013.6736854.

Kyle Wesson, Mark Rothlisberger, and Todd Humphreys. Practical cryptographic civil GPS signal authentication. *NAVIGATION: Journal of the Institute of Navigation*, 59(3):177–193, 2012.

Kyle D Wesson, Jason N Gross, Todd E Humphreys, and Brian L Evans. GNSS signal authentication via power and distortion monitoring. *IEEE Transactions on Aerospace and Electronic Systems*, 54(2):739–754, 2017.

Xiangdong Lin, T. Kirubarajan, Y. Bar-Shalom, and Xiaorong Li. Enhanced accuracy GPS navigation using the interacting multiple model estimator. In *2001 IEEE*

Aerospace Conference Proceedings (Cat. No.01TH8542), volume 4, pages 1911–1923, March 2001. doi: 10.1109/AERO.2001.931509.

S. . Yeom, T. Kirubarajan, and Y. Bar-Shalom. Track segment association, fine-step IMM and initialization with doppler for improved track performance. *IEEE Transactions on Aerospace and Electronic Systems*, 40(1):293–309, January 2004. ISSN 0018-9251. doi: 10.1109/TAES.2004.1292161.

Zhenjun Zhang and Xingqun Zhan. GNSS spoofing network monitoring based on differential pseudorange. *Sensors*, 16(10):1771, 2016.

List of Publications

Journal Publications

1. Pardhasaradhi Bethi, Pathipati Srihari, and P. Aparna. "**Navigation in GPS spoofed environment using m-best positioning algorithm and data association.**" IEEE Access, vol. 9, pp. 51536-51549, 2021, doi: 10.1109/ACCESS.2021.3064383.

2. Pardhasaradhi Bethi, Pathipati Srihari, and P. Aparna. "**Spoofer-to-target association in multi-spoofer multi-target scenario for stealthy GPS spoofing.**" IEEE Access, vol. 9, pp. 108675-108688, 2021, doi: 10.1109/ACCESS.2021.3099968.

3. Pardhasaradhi Bethi, Pathipati Srihari, and P. Aparna. "**GNSS Spoofing Detection and Spoofer Localization using DOA and Pseudo State Updation.**" in IEEE Access, vol. 10, pp. 42014-42028, 2022, doi: 10.1109/ACCESS.2022.3160047.

4. Pardhasaradhi Bethi, Pathipati Srihari, P. Aparna, R. Tharmarasa, and T. Kirubarajan. "**Distributed Stealthy GPS Spoofing with Target Tracking and Sensor Fusion.**" (communicating to IEEE transactions on AES).

Conference Publications

1. Bethi Pardhasaradhi, Srihari Pathipati, and P. Aparna. "**Stealthy GPS Spoofing: Spoofer Systems, Spoofing Techniques and Strategies.**" 2020 IEEE 17th India Council International Conference (INDICON). IEEE, 2020.

2. Bethi Pardhasaradhi, Srihari Pathipati, and P. Aparna. "**Impact of Target Tracking Module in GPS Spoofer Design for Stealthy GPS Spoofing.**" 2020 IEEE 17th India Council International Conference (INDICON). IEEE, 2020.

3. Bethi Pardhasaradhi, Srihari Pathipati, and P. Aparna. "**GNSS Intentional Interference Mitigation via Average KF Innovation and Pseudo Track**

Updation." 2020 IEEE 17th India Council International Conference (INDICON). IEEE, 2020.

4. Bethi Pardhasaradhi, Srihari Pathipati. "**Stealthy GPS Spoofer Design by Incorporating Processing Time and Clock Offsets.**" 2021 IEEE 18th India Council International Conference (INDICON).