ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Μελέτη αναμετάδοσης σημάτων GPS σε κλειστούς χώρους

Διπλωματική Εργασία

Θεόδωρος Β. Σταμπουλής

Επιβλέπων: Νικόλαος Ουζούνογλου
Καθηγητής Ε.Μ.Π.

ΑΘΗΝΑ, Ιούνιος 2016

Η σελίδα αυτή είναι σκόπιμα λευκή.

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Μελέτη αναμετάδοσης σημάτων GPS σε κλειστούς χώρους

Διπλωματική Εργασία

Θεόδωρος Β. Σταμπουλής

Επιβλέπων: Νικόλαος Ουζούνογλου
Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 30η Ιουνίου 2016.

(Υπογραφή)	(Υπογραφή)	(Υπογραφή)
…….	…….	……..
Ουζούνογλου	Δ. Κακλαμάνη	Ρ. Μακρή
Καθηγητής Ε.Μ.Π	Καθηγήτρια Ε.Μ.Π	Ερευνήτρια ΕΠΙΣΕΥ

ΑΘΗΝΑ, Ιούνιος 2016

(Υπογραφή)

_____

Θεόδωρος Β. Σταμπουλής

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Θα ήθελα να ευχαριστήσω τον καθηγητή κ. Νικόλαο Ουζούνογλου για την εμπιστοσύνη που έδειξε να μου αναθέσει την συγγραφή της διπλωματικής αυτής εργασίας. Επιπλέον θα ήθελα να εκφράσω τις ευχαριστίες μου στην κυρία Ροδούλα Μακρή για τις υποδείξεις της κατά τη διάρκεια του πειραματικού σκέλους. Τέλος θα ήθελα να ευχαριστήσω την οικογένειά μου για την συνεχή υποστήριξη κατά τη διάρκεια των σπουδών μου.

Η σελίδα αυτή είναι σκόπιμα λευκή.

Περίληψη

Σκοπός της παρούσας διπλωματικής είναι η θεωρητική μελέτη για την κατασκευή διάταξης αναμετάδοσης του σήματος GPS σε κλειστούς χώρους. Αρχικά γίνεται μια ανασκόπηση του συστήματος του GPS και παρουσιάζονται συνοπτικά τα υποσυστήματά του. Ιδιαίτερη έμφαση δίνεται στους αλγόριθμους με τους οποίους οι δέκτες υπολογίζουν την θέση τους.

Εκτός από τον τρόπο λειτουργίας του συστήματος εξετάζονται οι επίθεσεις που μπορεί να δεχτεί. Δίνεται ο ορισμός της επιτυχημένης επίθεσης GPS spoofing. Ειδικότερα μελετώνται οι συνθήκες που θα πρέπει να πληρούνται για μια επιτυχημένη επίθεση.

Στη συνέχεια προτείνεται απλή διάταξη για την εισαγωγή καθυστερήσεων και την αναμετάδοση του σήματος GPS. Επιχειρείται μοντελοποίηση του συστήματος με χρήση του λογισμικού Matlab, ώστε να εξαχθούν χρήσιμα συμπεράσματα για τον τρόπο λειτουργία της διάταξης.

Τέλος γίνεται αξιολόγηση των αποτελεσμάτων και εξάγονται τα τελικά συμπεράσματα.

Λέξεις-κλειδιά: GPS, GNSS, ψευδοτυχαίοι κώδικες, GPS spoofing, GPS jamming.

Η σελίδα αυτή είναι σκόπιμα λευκή.

Abstract

The purpose of the current thesis is the theoretical study and design of a retransmission system for use inside buildings. A comprehensive presentation of the GPS system is Initially attempted and its subsystem are briefly presented. The algorithms that calculate the user's position are extensively presented.

Besides the GPS system mode of operation, the GPS attacks are also summarized. The successful GPS spoofing attack is defined, and the conditions tht must be met for a successful attack are thoroughly analyzed.

Subsequently, a simple layout for the introduction of time offset and the retransmission of the GPS signal is recommended, and a simulation of the system, using Matlab software, is attempted, in order to extract useful deductions regarding the layout's modus operendi.

Finally, the results are evaluated and the final conclusions are drawn.

Key words: GPS, GNSS, PRN, GPS spoofing, GPS jamming.

Η σελίδα αυτή είναι σκόπιμα λευκή.

Περιεχόμενα

1. Εισαγωγή

1.1 Πρόλογος

Το σύστημα GPS ή NAVSTAR GPS (NAVigation Satellite Timing And Ranging, Global Positioning System) όπως είναι η πλήρη ονομασία του, είναι ένα παγκόσμιο δορυφορικό σύστημα προσδιορισμού θέσης, χρόνου και ταχύτητας. Ανήκει στην κατηγορία των συστημάτων GNSS (Global Navigation Satellite System), δηλαδή των παγκοσμίων συστημάτων πλοήγησης, στην οποία περιλαμβάνονται το Ρωσικό σύστημα GLONASS και το καθαρά πολιτικό Ευρωπαϊκό σύστημα GALILAIO.

Παρόλο που η αρχική σχεδίαση του GPS ήταν για καθαρά στρατιωτικούς σκοπούς, η χρήση του επεκτάθηκε ταχέως στον πολιτικό κλάδο των εφαρμογών. Την τάση αυτή έχει ενισχύσει η ολοένα αυξανόμενη χρήση φορητών ηλεκτρονικών συσκευών, όπως τα smartphones, η οποία έχει προκαλέσει μια πληθώρα νέων αναγκών και ευκολιών. Πέραν όμως της καλόβουλης χρήσης του συστήματος εντοπισμού θέσης, υπάρχουν και οι κακόβουλες εφαρμογές. Χαρακτηριστικό είναι το παράδειγμα μιας γυναίκας στις ΗΠΑ, η οποία αναγκάστηκε να αποταθεί σε τεχνολογικό ίδρυμα της χώρας της, για να αποτρέψει τον πρώην σύζυγο της από το να εντοπίζει συνεχώς την τοποθεσία στην οποία βρίσκεται. Ο εντοπισμός της θέσης της γίνονταν μέσω ενός μικροσκοπικού δέκτη GPS, που είχει τοποθετήσει ο σύζυγός της στο αυτοκίνητό της. Απαραίτητη λοιπόν είναι η ανάπτυξη αντιμέτρων, ώστε να αποτραπεί η χρήση της υπάρχουσας τεχνολογίας από τρίτους με σκοπό τον περιορισμό της ιδιωτικότητας του ατόμου.

Οι δύο βασικοί τρόποι με τους οποίους δρουν τα αντίμετρα αυτά είναι:

α. Η παρακώλυση του σήματος των GNSS (jamming).

β. Η παραπλάνηση του δέκτη GNSS με ψεύτικα σήματα (spoofing).

Η πρώτη μέθοδος είναι η πιο απλή και εύκολα εφαρμόσιμη, καθώς απαιτείται απλά η παρεμβολή του σήματος με ένα πιο ισχυρό σήμα θορύβου. Η δεύτερη μέθοδος είναι πολύ περισσότερο περίπλοκη και δύσκολη στην εφαρμογή, καθώς απαιτείται η αναπαραγωγή ενός σήματος το οποίο θα πρέπει να καλύπτει κάποιες πολύ συγκεκριμένες προϋποθέσεις. Προφανώς οι εφαρμογές

της δεύτερης μεθόδου είναι πολύ περισσότερο «εκλεπτυσμένες» και αποτελεσματικές.

1.2 Δομή της διπλωματικής εργασίας

Στο 2ο κεφάλαιο γίνεται μια συνοπτική παρουσίαση του συστήματος GPS. Δίδονται τα επιμέρους υποσυστήματα από τα οποία αποτελείται και η λειτουργία τους. Με ιδιαίτερη έμφαση παρουσιάζονται οι ψευδοτυχαίες ακολουθίες (PRN) και ο αλγόριθμος για τον υπολογισμό θέσης από τον δέκτη.

Το 3ο κεφάλαιο αφιερώνεται στις επιθέσεις που είναι δυνατό να λάβουν χώρα στο σύστημα. Για την θεωρητική μελέτη αυτού του αντικειμένου είναι αναγκαίο να δωθούν το πλήρες μοντέλο μιας επίθεσης, καθώς και ο ακριβής προσδιορισμός του συστήματος. Με σχεδόν μαθηματική τυποποίηση δίδεται και ο ορισμός μια επίθεσης spoofing σε έναν μοναδικό δέκτη ή και σε ομάδα δεκτών. Τέλος στο κεφάλαιο αυτό σχηματίζονται οι εξισώσεις που θα πρέπει να λυθούν από τον επιτιθέμενο, για να προσδιορίσει τις τιμές που θα πρέπει να δώσει στις παραμέτρους του συστήματος.

Το 4ο κεφάλαιο αφιερώνεται στην περιγραφή διάταξης αναμετάδοσης του σήματος GPS, η οποία μπορεί να εισάγει συγκεκριμένη καθυστέρηση στα σήματα των δορυφόρων. Γίνεται θεωρητική μελέτη της συσκευής, καθώς και μοντελοποίηση του συστήματος με χρήση του λογισμικού MATLAB. Η μοντελοποίηση περιορίζεται στον υπολογισμό των ψευδοαποστάσεων με δεδομένη τη γεωμετρία του συστήματος (θέσεις δορυφόρων, δέκτη και συσκευής) και λύση των εξισώσεων θέσης από τη πλευρά του δέκτη, ώστε να υπολογιστεί η μετατόπιση, που μπορεί να προκαλέσει η διάταξη στην υπολογισθέντα θέση του δέκτη. Η προσομοίωση πραγματοποιείται για δύο διαφορετικούς αλγόριθμους λύσης των εξισώσεων θέσης από τη πλευρά του χρήστη. Ο πρώτος αλγόριθμος είναι αυτός των ελαχίστων τετραγώνων, ενώ ο δεύτερος είναι ο «βελτιωμένος» αλγόριθμος ελαχίστων τετραγώνων με βάρη.

Τέλος στο 5ο κεφάλαιο δίδονται συμπεράσματα για τη λειτουργία της συσκευής. Τα συμπεράσματα αυτά προκύπτουν από την θεωρητική ανάλυση και μοντελοποίηση που προηγήθηκε.

2. Το σύστημα GPS

2.1 Επισκόπηση του συστήματος

Το σύστημα GPS παρέχει συνεχή, παγκόσμιας κάλυψης, τριών διαστάσεων και με ακρίβεια, πληροφορία για τη θέση και την ταχύτητα των χρηστών που έχουν τον κατάλληλο εξοπλισμό (δέκτη GPS). Εκτός από τα παραπάνω μπορεί να χρησιμοποιηθεί και για τον ακριβή προσδιορισμό του χρόνου, μέσω της αποστολής του χρόνου UTC (Coordinated Universal Time), που χρησιμοποιείται στο συγχρονισμό της λειτουργίας του .

Αποτελείται από τρία ξεχωριστά τμήματα, το δορυφορικό τμήμα, το τμήμα ελέγχου και το τμήμα χρηστών. Τα δύο πρώτα ανταλλάσσουν συνεχώς πληροφορίες για την εύρυθμη λειτουργία του συστήματος.

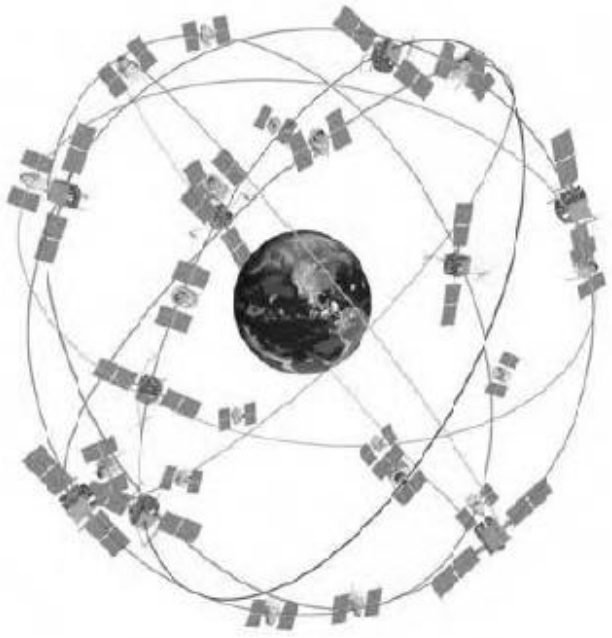
Επιπλέον παρέχει δύο διαφορετικά επίπεδα υπηρεσιών, ανάλογα με τον τύπο του δέκτη που χρησιμοποιεί ο χρήστης. Η πρώτη υπηρεσία είναι η τυπική υπηρεσία προσδιορισμού θέσης SPS (Standard Positioning Service) και προορίζεται για κοινή πολιτική χρήση, ενώ η δεύτερη είναι η ακριβής υπηρεσία προσδιορισμού PPS (Precise Positioning Service), η οποία προορίζεται για στρατιωτική χρήση και γεωδαιτικές εφαρμογές.

2.1.1 Δορυφορικό τμήμα

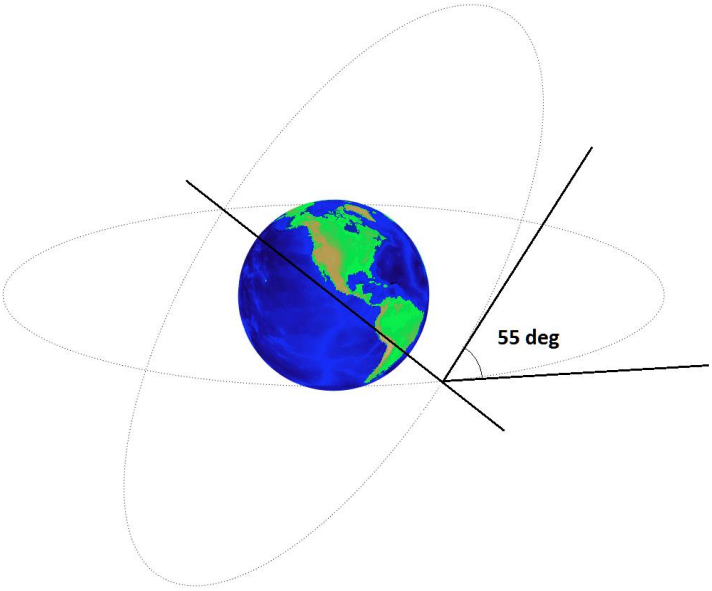
Το δορυφορικό τμήμα αποτελείται από τους δορυφόρους του συστήματος GPS, οι οποίοι πετούν σε συγκεκριμένες τροχιές σχηματίζοντας έναν «αστερισμό». Ο υπολογισμός της θέσης από τους χρήστες πραγματοποιείται μετρώντας την απόσταση που απέχουν από τους δορυφόρους με τους οποίους έχουν οπτική επαφή. Κάθε δορυφόρος εκπέμπει ένα σήμα διαμορφωμένο από έναν μοναδικό, χαρακτηριστικό για τον καθένα, ψευδοτυχαίο κώδικα PRN (Pseudo-random Noise). Μέσω αυτού του κώδικα γίνεται και η μέτρηση των αποστάσεων από τον χρήστη. Εκτός από τις ψευδοτυχαίες ακολουθίες, το δορυφορικό σήμα διαμορφώνεται και από μια ακολουθία δεδομένων, η οποία παρέχει πληροφορίες για την τρέχουσα θέση των δορυφόρων.

Οι δορυφόροι πετάνε σε μέσες γήινες τροχιές MEO (medium Earth orbit) με προσεγγιστικό ύψος 22.200km. Συγκριτικά η ακτίνα της γής είναι 6.371km. Ένα σημαντικό πρόβλημα που προκύπτει είναι ο σωστός σχεδιασμός των

δορυφορικών τροχιών και η κατάλληλη επιλογή του αριθμού των δορυφόρων, ώστε να παρέχεται συνεχή και παγκόσμια κάλυψη. Ο τρέχων αστερισμός που χρησιμοποιείται αποτελείται από έξι ελλειπτικές τροχιές, οι οποίες σχηματίζουν δίεδρη γωνία περίπου 55^{o}, σχήμα 2.2, με το επίπεδο του ισημερινού και τοποθετούνται σε ίσες γωνιακές αποστάσεις των 60^{o} κατά μήκος του ισημερινού. Στο σχήμα 2.1 απεικονίζονται οι τροχιές των δορυφόρων.



Σχήμα 2.1 Δορυφορικός αστερισμός του GPS [1]



Σχήμα 2.2 Απεικόνιση της δίεδρης γωνίας 55^{o}, που σχηματίζει η τροχιά με το επίπεδο του ισημερινού.

2.1.2 Τμήμα Ελέγχου

Το τμήμα ελέγχου CS (Control Segment) είναι υπεύθυνο για την σωστή λειτουργία του δορυφορικού τμήματος. Αυτό περιλαμβάνει την διατήρηση των δορυφόρων στις κατάλληλες θέσεις, εντός της τροχιάς τους και τον έλεγχο των διαφόρων υποσυστημάτων των δορυφόρων. Επιπλέον το τμήμα ελέγχου είναι υπεύθυνο για την ενημέρωση του μηνύματος δεδομένων ή μηνύματος πλοήγησης, το οποίο εκπέμπουν οι δορυφόροι.

Αποτελείται από δεκαέξι μόνιμους σταθμούς παρακολούθησης με γνωστές συντεταγμένες κατανεμημένους σε όλη τη γη, τέσσερις σταθμούς τηλεπικοινωνών και έναν κεντρικό σταθμό ελέγχου MCS (Master Control Station).

2.1.3 Τμήμα Χρηστών

Το τμήμα χρηστών είναι οι δέκτες GPS και η λειτουργία του είναι παθητική, δηλαδή περιορίζεται στη λήψη των δορυφορικών σημάτων. Εκτός από το RF κομμάτι για τη λήψη του σήματος, απαιτείται και η ύπαρξη ενσωματωμένου ψηφιακού συστήματος για την περαιτέρω επεξεργασία του μηνύματος πλοήγησης και τον προσδιορισμό της θέσης. Εκτός όμως από την κύρια λειτουργία της πλοήγησης, οι δέκτες μπορούν να δώσουν πληροφορία για την ταχύτητα του χρήστη και τον ακριβή χρόνο.

2.1.4 SPS

Η υπηρεσία τυπικού προσδιορισμού θέσης SPS είναι διαθέσιμη σε όλους τους χρήστες παγκοσμίως, χωρίς να απαιτείται κάποιου είδους συνδρομή. Η ακρίβεια στον εντοπισμό θέσης που παρέχεται είναι κατά προσέγγιση καλύτερη από 13m κατά μήκος του οριζόντιου επίπεδου και καλύτερη από 22m στον κάθετο άξονα, στο 95% των χρηστών για τις δύο περιπτώσεις. Η τυπική ακρίβεια του χρόνου που παρέχεται είναι της τάξης των 40ns.

2.1.5 PPS

Η υπηρεσία ακριβούς προσδιορισμού θέσης PPS είναι σχεδιασμένη κυρίως για στρατιωτικές εφαρμογές. Στο χώρο του διαστήματος, όταν δηλαδή τα σήματα κινούνται σε χώρο χωρίς ατμόσφαιρα, οι δύο υπηρεσίες παρέχουν ίση ακρίβεια. Η PPS όμως παρέχει δυνατότητα διόρθωσης του ιονοσφαιρικού σφάλματος από τους χρήστες, με αποτέλεσμα βελτιωμένη ακρίβεια. Αυτό είναι δυνατό καθώς για την υπηρεσία αυτή διατίθενται δύο φέρουσες συχνότητες. Το ιονοσφαιρικό σφάλμα στις δύο αυτές φέρουσες είναι ίσο κατά απόλυτη τιμή αλλά έχει αντίθετο πρόσημο. Επομένως η συνδυασμένη εκτίμηση εξαλείφει το συνολικό σφάλμα.

2.2 Δομή Δορυφορικού Σήματος

Το δορυφορικό σήμα του GPS είναι εξαιρετικά σύνθετο. Ο αρχικός σχεδιασμός του συστήματος που βρίσκεται σε πλήρη ισχύ σήμερα προβλέπει τις παρακάτω δύο φέρουσες συχνότητες:

α. Τη συχνότητα L1 = 1575.42 MHz με μήκος κύματος λ_1 = 19.03 cm.

β. Τη συχνότητα L2 = 1227.6 MHz με μήκος κύμταος λ_2 = 24.42 cm.

Για τη μέτρηση της απόστασης μεταξύ δορυφόρου και δέκτη που απαιτείται για τον προσδιορισμό σε πραγματικό χρόνο της θέσης, οι φέρουσες διαμορφώνονται από δύο μετρητικούς κώδικες, οι οποίοι είναι οι παρακάτω:

α. Ο κώδικας C/A (Coarse/Acquisition), ο οποίος είναι σε ελεύθερη χρήση και διαμορφώνει μόνο τη συχνότητα L1.

β. Ο κώδικας P (Precise), ο οποίος μεταδίδεται κρυπτογραφημένα ως P(Y) και διαμορφώνει και τις δύο φέρουσες.

Οι μετρητικοί κώδικες ανήκουν στους κώδικες ψευδοτυχαίου θορύβου PRN (Pseudo Random Noise). Η συχνότητα παραγωγής των PRN ακολουθιών ονομάζεται ψηφιακός ρυθμός και μετριέται σε cps (chips per second). Η χρησιμοποίηση του όρου των chips αντι των bits, δεν είναι τυχαία καθώς δεν υπάρχει μεταφορά πληροφορίας (data).

Εκτός του ψευδοτυχαίου κώδικα μεταφέρονται στον δέκτη πληροφορίες για τον υπολογισμό της θέσης του δορυφόρου στον ουράνιο θόλο, παράμετροι

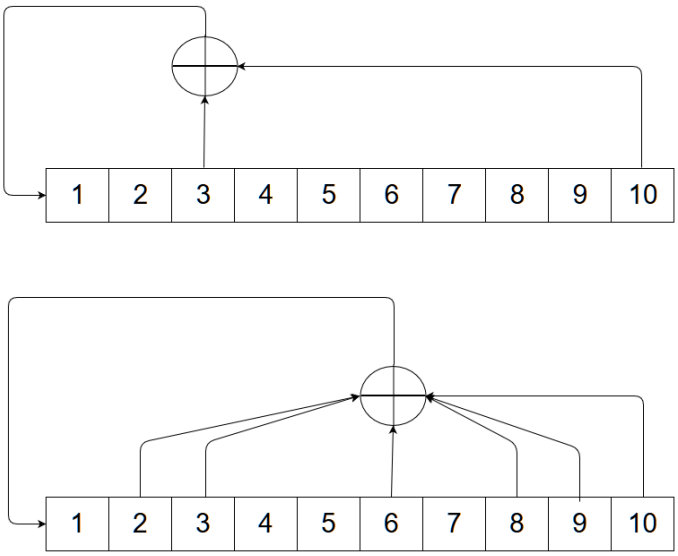
για τον συγχρονισμό των ρολογιών και την διόρθωση του ιονοσφαιρικού σφάλματος. Τα δεδομένα αυτά αποτελούν το μήνυμα πλοήγησης.

2.2.1 PRN

Ο ψευδοτυχαίος θόρυβος PRN είναι ένα σήμα το οποίο ικανοποιεί κάποια συγκεκριμένα στατιστικά κριτήρια τυχαιότητας, με αποτελέσμα να φαίνεται σαν τελείως τυχαίο σε έναν «ανυποψίαστο» παρατηρητή. Στην πραγματικότητα είναι ένα απόλυτα ντετερμινιστικό σήμα, που μιμείται τις στατιστικές ιδιότητες του τυχαίου θορύβου. Το πλεονέκτημα αυτών των τυχαίων ακολουθιών είναι ότι υλοποιούνται εξαιρετικά αποδοτικά από ψηφιακά ηλεκτρονικά κυκλώματα. Μια γεννήτρια PRN θορύβού αποτελείται από μια σειρά καταχωρητών εφοδιασμένων με μια πράξη XOR.

Για την κατασκευή του κώδια C/A χρησιμοποιούνται οι λεγόμενοι Gold Codes οι οποίοι είναι περιοδικοί κώδικες. Το χαρακτηριστικό τους γνώρισμα είναι ότι έχουν το μέγιστο δυνατό μήκος ακολουθίας. Αυτό σημαίνει ότι αν το κύκλωμα παραγωγής τους υλοποιείται με συνολικά n καταχωρητές, η ακολουθία επαναλαμβάνεται περιοδικά ανα $2^n - 1$ chips, που είναι και το μέγιστο μήκος που μπορεί να επιτευχθεί με τον συγκεκριμένο αριθμό καταχωρητών. Επιπλέον έχουν πολύ καλές ιδιότητες αυτοσυσχέτισης και πολύ μικρή συσχέτιση μεταξύ τους (cross-correlation).

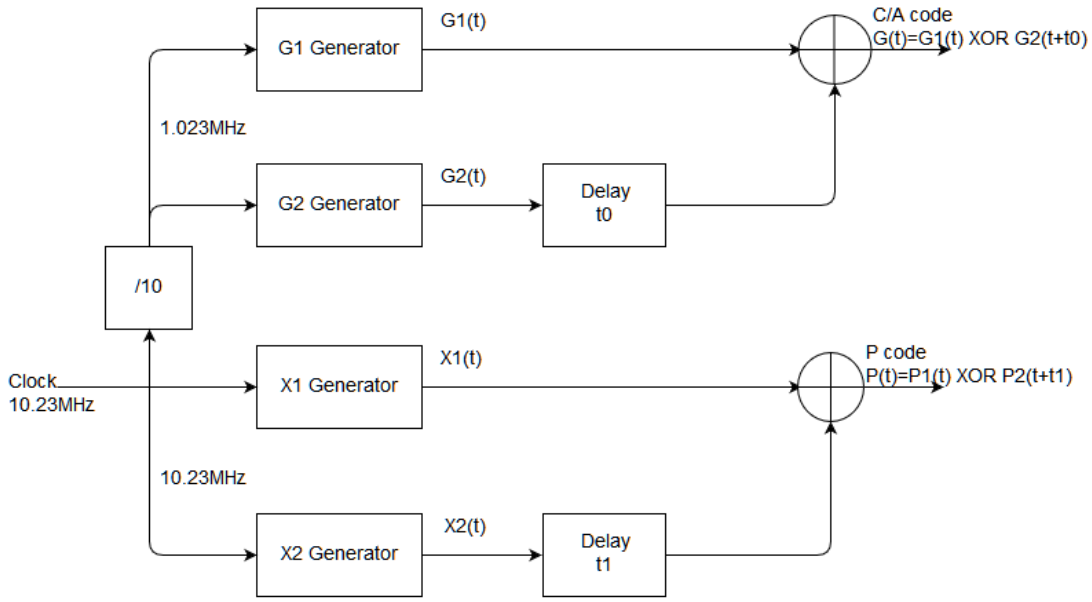
Το μήκος των Cold Codes που χρησιμοποιούνται για τον κώδικα C/A είναι 1023 chips. Καθώς το chip rate είναι 1023 MHz ο κώδικας επαναλαμβάνεται ανά 1 μs. Το κύκλωμα του PRN generator που χρησιμοποιείται διαθέτει 10 καταχωρητές. Για τη περιγραφή των κυκλωμάτων χρησιμοποιούνται συνήθως πολυώνημα της μορφής $1 + \sum X^i$, όπου X^i σημαίνει ότι η έξοδος του i-οστού καταχωρητή χρησιμοποιείται ως είσοδος στην πύλη XOR και το 1 ότι η έξοδος της πύλης XOR τροφοδοτείται στον πρώτο καταχωρητή. Η αρχική κατάσταση όλων των καταχωρητών είναι το λογικό 1. Στο σχήμα 2.3 φαίνοναι οι δύο PRN generators που χρησιμοποιούνται για την δημιουργία του C/A code.



Σχήμα 2.3 Οι δύο PRN generators με χαρακτηριστικά πολυώνυμα $1 + x^3 + x^{10}$ και $1 + x^2 + x^3 + x^6 + x^8 + x^9 + x^{10}$.

Ο τελικός κώδικας είναι το αποτέλεσμα άθροισης XOR του 10ου καταχωρητή του πρώτου κυκλώματος με μια καθυστερημένη εκδοχή του κώδικα που παράγεται από το δεύτερο κύκλωμα. Ανάλογα με τη καθυστέρηση που εισάγεται προκύπτει μια διαφορετική ακολουθία, η οποία αντιστοιχεί σε συγκεκριμένο δορυφόρο.

Ο κώδικας P είναι αρκετά πιο περίπλοκος μολονότι τα κυκλώματα που τον παράγουν είναι της ίδιας λογικής με του C/A κώδικα. Παράγεται από την άθροιση XOR δύο επιμέρους PRN κωδίκων με μήκος 15345000 και 15345037 ψηφίων ο καθένας. Το αποτέλεσμα είναι μια τεράστια ακολουθία μήκους περίπου $2{,}3547 \times 10^{14}$. Ο ψηφιακός ρυθμός του κώδικα P είναι δεκαπλάσιος από αυτόν του C/A (10.23MHz). Για την εξολοκλήρου παραγωγή του απαιτούνται 266,4 μέρες ή 38 εβδομάδες. Στην πράξη ο κώδικας χωρίζεται σε 38 τμήματα μήκους μίας εβδομάδας και κάθε δορυφόρος εκπέμπει ένα συγκεκριμένο τμήμα. Το σχήμα 2.4 παριστάνει σε επίπεδο λειτουργικών μονάδων τα κυκλώματα παραγωγής των κωδίκων P και C/A.

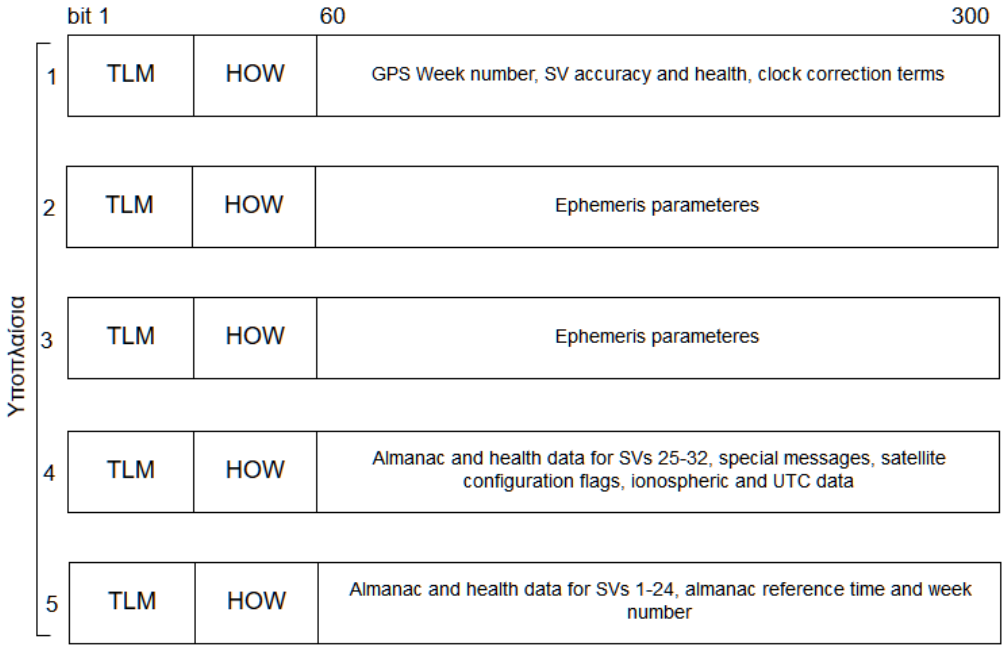


Σχήμα 2.4 Σχηματικό PRN generator για τους κώδικες P και C/A.

2.2.2 Το μήνυμα δεδομένων-πλοήγησης

Για να υπολογιστεί η θέση του δέκτη σε πραγματικό χρονο απαιτείται, εκτός από τη μέτρηση της απόστασης του δέκτη από τους δορυφόρους και η γνώση των θέσεων των δορυφόρων. Την πληροφορία αυτήν προσφέρει το μήνυμα δεδομένων ή μήνυμα πλοήγησης. Εκτός από στοιχεία για τις τροχιές των δορυφόρων, με το μήνυμα μεταβιβάζονται πληροφορίες που βοηθούν τον δέκτη να μεταφράσει τον χρόνο του συστήματος σε UTC και να διορθώσει σφάλματα που επηρεάζουν την μέτρηση των αποστάσεων.

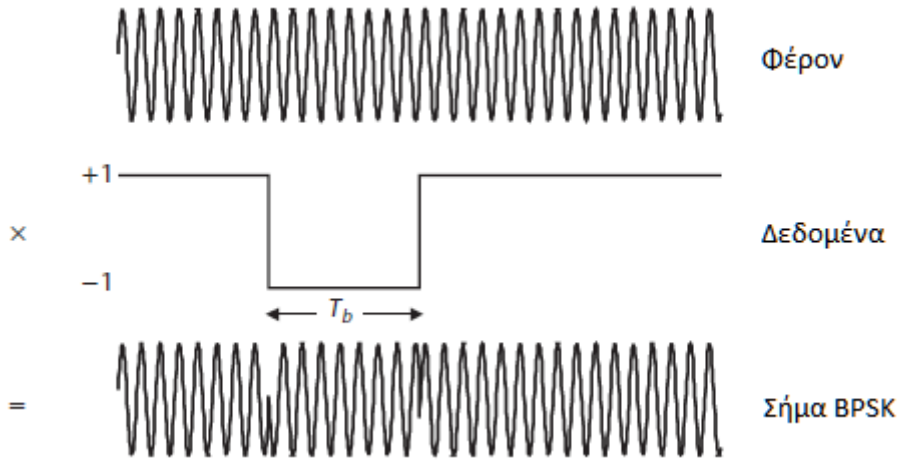
Το μήνυμα δεδομένων είναι και αυτό μια δυαδική ακολουθία με ψηφιακό ρυθμό παραγωγής 50 bps. Αυτό σημαίνει ότι η διάρκεια κάθε ψηφίου δεδομένων είναι 20 ms, επομένως περιέχει ακριβώς 20 C/A κώδικες. Αποστέλνεται σε πέντε υποτμήματα των 300 bit. Κάθε υποτμήμα αποτελείται από λέξεις των 30 bit. Τα τελευταία 6 bit κάθε λέξης διατίθενται ως ελεγκτές ισοτιμίας για διόρθωση λαθών. Στο σχήμα 2.5 παρατίθεται η δομή του μηνύματος πλοήγησης.



Σχήμα 2.5 Δομή μηνύματος πλοήγησης [1].

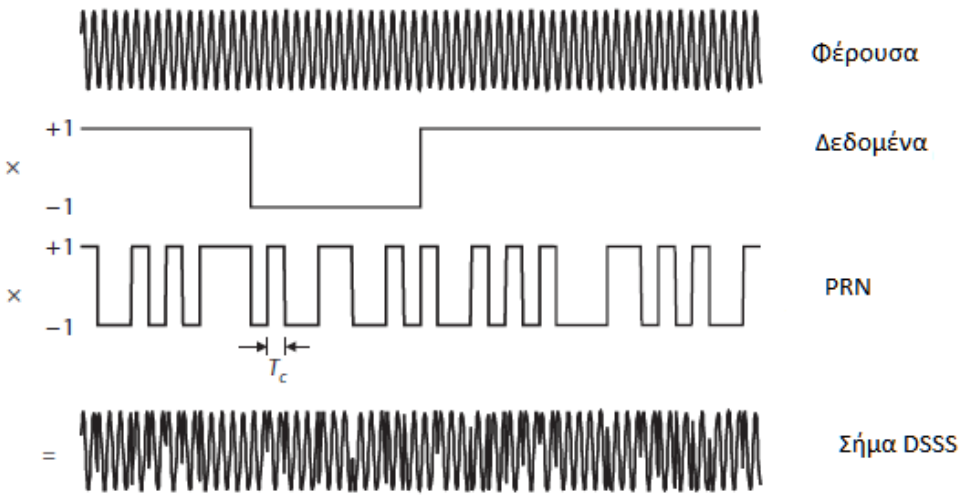
2.2.3 Διαμόρφωση δορυφορικού σήματος.

Για τη διαμόρφωση του δορυφορικού σήματος χρησιμοποιείται η τεχνική direct sequence spread spectrum (DSSS) η οποία είναι μια επέκταση της τεχνικής της δυαδικής διφασικής διαμόρφωσης BPSK (Binary phase-shift keying). Η BPSK είναι μια απλή μέθοδος διαμόρφωσης ψηφιακού σήματος κατά την οποία η φέρουσα συχνότητα μεταδίδεται είτε όπως είναι είτε με μετατόπιση φάσης 180^{o}, η οποία αντιστοιχεί σε πολλαπλασιασμό του φέροντος με -1. Σχήμα 2.6.



Σχήμα 2.6 Διαμόρφωση BPSK [1]

Στην DSSS το σήμα δεδομένων πολλαπλασιάζεται πρώτα με την ακολουθία PRN και η ακολουθία που προκύπτει διαμορφώνει τη φέρουσα συχνότητα. Σχήμα 2.7.



Σχήμα 2.7 Διαμόρφωση DSSS [1]

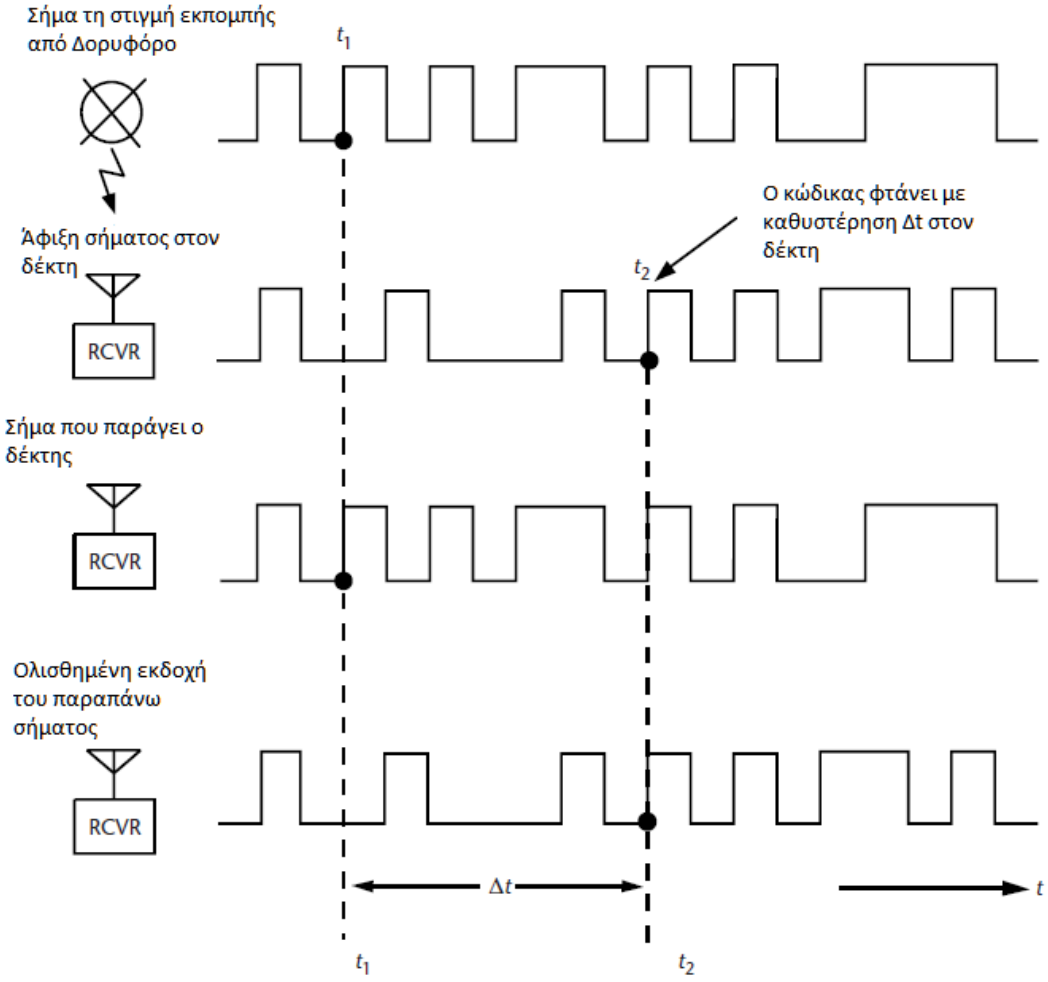
Η φέρουσα συχνότητα L1 διαμόρφώνεται και από τους δύο κώδικες, τον C/A και τον P(Y). Για τον λόγο αυτό αρχικά η φέρουσα χωρίζεται σε δύο συνιστώσες-φορείς με διαφορά φάσης 90^o. Η συνιστώσα που προηγείται κατά 90^o διαμορφώνεται με το αποτέλεσμα του πολλαπλασιασμού του σήματος δεδομένων με τον C/A ενώ η άλλη με το αποτέλεσμα του πολλαπλασιασμού των δεδομένω με τον P(Y). Τέλος οι δύο συνιστώσες συντίθενται πριν την εκπομπή. Η φέρουσα συχνότητα L2 διαμορφώνεται μόνο από τον πολλαπλασιασμό των δεδομένων με τον P(Y) κώδικα.

2.3 Υπολογισμός θέσης

Ο υπολογισμός της θέσης του χρήστη γίνεται ξεκινώντας με τον προσδιορισμό του χρόνου ταξιδιού του σήματος από τον δορυφόρο στον δέκτη. Οι PRN κώδικες παίζουν το σημαντικότερο ρόλο σε αυτήν τη διαδικασία.

Ο δέκτης συγκρίνει την ακολουθία που λαμβάνει από τον δορυφόρο με την ακολουθία που αναπαράγει ο ίδιος. Οι κοινοί δέκτες αναπαράγουν μόνο τον

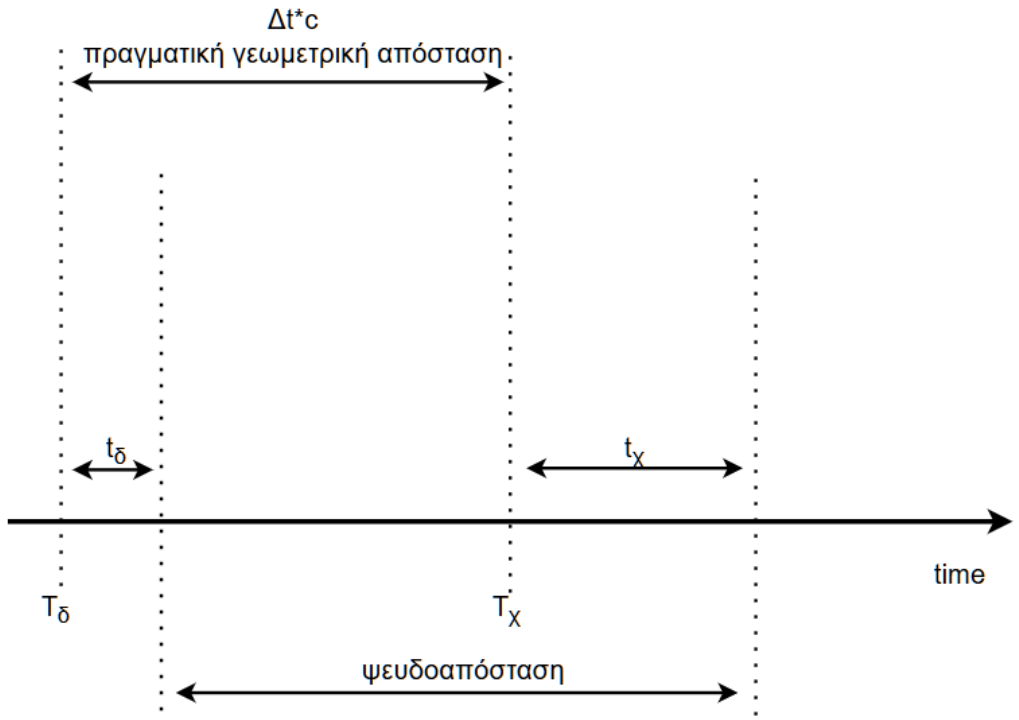
C/A κώδικα ένώ οι στρατιωτικοί και τους δύο. Ουσιαστικά συσχετίζει τα δύο σήματα, δηλαδή πολλαπλασιάζει τις δύο ακολουθίες και προσθέτει έναν μεγάλο αριθμό ψηφίων. Όταν έχουμε σύμπτωση των σημάτων, η ισχύς που λαμβάνεται στην έξοδο του συσχετιστή είναι σημαντικά μεγαλύτερη από την περίπτωση μη σύμπτωσης και ο δέκτης διακρίνει το σήμα με μεγάλο ποσοστό επιτυχίας. Ο διαχωρισμός των σημάτων είναι δυνατός, αν και τα σήματα στην επιφάνεια της γης είναι «θαμμένα» στον θόρυβο, λόγω των πολύ καλών ιδιοτήτων συσχέτισης των κωδίκων που χρησιμοποιούνται. Στο σχήμα 2.7 φαίνονται το σήμα που αναπαράγει ο δορυφόρος και η καθυστερημένη εκδοχή που λαμβάνει ο δέκτης, το σήμα που αναπαράγει ο δέκτης και η καθυστερημένη εκδοχή του που συμπίπτει με το λαμβανόμενο σήμα.



Σχήμα 2.7 Αναπαράσταση των σημάτων ως προς το χρόνο [1].

Στη γενικότερη περίπτωση το ρολόι του δέκτη έχει μια μικρή απόκλιση από τον ακριβή χρόνο του συστήματος. Αυτό συμβαίνει, σε πολύ μικρότερο βαθμό, ακόμα και για τα ατομικά ρολόγια που διαθέτουν οι δορυφόροι. Επομένως η χρονική ολίσθηση Δt την οποία μετρούν οι δέκτες, δεν δίνει την πραγματική γεωμετρική απόσταση δορυφόρου-δέκτη, αλλά τη λεγόμενη ψευδοαπόσταση. Στο σχήμα 2.8 φαίνονται οι σχέσεις μεταξύ των διαφόρων χρονικών ποσοτήτων, όπου:

T_δ = Ο χρόνος GPS όταν το σήμα φεύγει από τον δορυφόρο.
T_χ = Ο χρόνος GPS όταν το σήμα φτάνει στον δέκτη του χρήστη.
t_δ = Η απόκλιση του ρολογιού του δορυφόρου από το χρόνο GPS.
t_χ = Η απόκλιση του ρολογιού του χρήστη από το χρόνο GPS.



Σχήμα 2.8 Σχέση μεταξύ χρονικών ποσοτήτων.

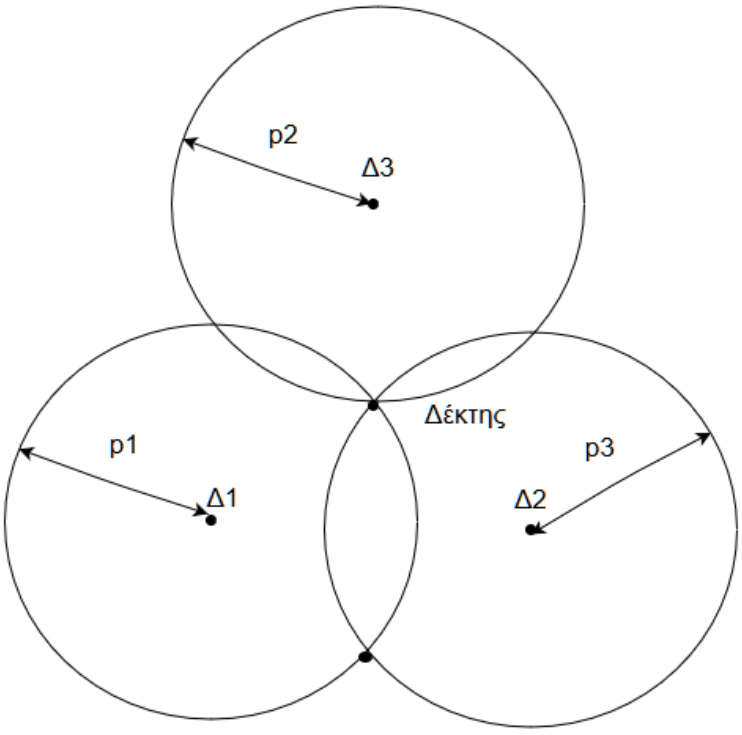
Γεωμετρική απόσταση: $r = c(T_\chi - T_\delta)$ = cΔt (2.1)

Ψευδοαπόσταση: $p = c\left[\left(T_\chi + t_\chi\right) - \left(T_\delta + t_\delta\right)\right] = r + c\left(t_\chi - t_\delta\right) = r + c\delta t$ (2.2)

2.3.1 Γεωμετρική ερμηνεία του προβλήματος προσδιορισμού θέσης

Για την καλύτερη κατανόηση του τρόπου με τον οποίο γίνεται ο προσδιορισμός της θέσης από το GPS, είναι απαραίτητη η γεωμετρική ερμηνεία του προβλήματος. Η ανάλυση γίνεται στις δύο διαστάσεις, όμως η επέκταση στις τρεις είναι σχεδόν τετριμμένη.

Στην υποθετική περίπτωση όπου ο χρόνος που μετρούν οι δέκτες και οι δορυφόροι δεν είχε απόκλιση από τον χρόνο GPS, η ψευδοαπόσταση θα συνέπιπτε με την πραγματική γεωμετρική απόσταση μεταξύ χρήστη και δορυφόρου. Επομένως για τον προσδιορισμό της θέσης του χρήστη θα αρκούσε η μέτρηση της απόστασης από τρεις δορυφόρους σε συνδυασμό με την ακριβή γνώση της θέσης των τριών αυτών δορυφόρων σχήμα 2.9. Η θέση του δέκτη είναι απλώς το σημείο τομής των τριών κύκλων, με κέντρο κάθε κύκλου τους δορυφόρους και ακτίνα τη μετρούμενη για κάθε δορυφόρο ψευδοαπόσταση. Στην πραγματικότητα ο τρίτος δορυφόρος χρειάζεται απλά για να γίνει επιλογή ενός από τα δύο σημεία στα οποία τέμνονται οι δύο από τους τρεις κύκλους.



Σχήμα 2.9 Προσδιορισμός θέσης στο επίπεδο.

Στον πραγματικό κόσμο, όπου υπάρχουν σφάλματα και συστηματική απόκλιση μεταξύ των ρολογιών των δεκτών και των ατομικών ρολογιών των δορυφόρων, η προηγούμενη ανάλυση δεν ισχύει. Θέτοντας με P_i και R_i την ψευδοαπόσταση και την πραγματική-γεωμετρική απόσταση αντίστοιχα, μεταξύ i-οστού δορυφόρου και δέκτη έχουμε το παρακάτω σύστημα εξισώσεων, όπου δt είναι η χρονική απόκλιση του ρολογιού του δέκτη από τον χρόνο GPS.

$$\begin{aligned} p_1 &= r_2 + c\delta t \\ p_2 &= r_2 + c\delta t \\ p_3 &= r_3 + c\delta t \end{aligned} \tag{2.3}$$

Για την απαλοιφή του χρόνου δt αφαιρείται η πρώτη από τη δεύτερη και την τρίτη εξίσωση, οπότε προκύπτει το παρακάτω σύστημα το οποίο περιγράφει δύο υπερβολές με εστίες τους δορυφόρους Δ2 και Δ3. Το σημείο τομής των δύο υπερβολών είναι και η θέση του δέκτη. Σχήμα 2.10.

$$\begin{aligned} p_2 - p_1 &= r_2 - r_1 \\ p_3 - p_1 &= r_2 - r_1 \end{aligned} \tag{2.4}$$

Σχήμα 2.10 Προσδιορισμός θέσης από σημείο τομής υπερβολών

2.3.2 Λύση των εξισώσεων προσδιορισμού θέσης

Έστω ότι οι συντεταγμένες σε καρτεσιανό σύστημα του χρήστη είναι $\boldsymbol{L_u} = (X_u, Y_u, Z_u)$, ενώ αντίστοιχα του i-οστού δορυφόρου $\boldsymbol{L_i} = (X_i, Y_i, Z_i)$, τότε έχουμε:

$$p_i = \|\boldsymbol{L_i} - \boldsymbol{L_u}\| + c\delta t \tag{2.1}$$

Στην περίπτωση που ο χρήστης έχει οπτική επαφή με 4 δορυφόρους σχηματίζεται το παρακάτω σύστημα τεσσάρων εξισώσεων, στο οποίο οι άγνωστοι είναι οι $X_u, Y_u, Z_u, \delta t$.

$$\begin{aligned} p_1 &= \sqrt{(X_1 - X_u)^2 + (Y_1 - Y_u)^2 + (Z_1 - Z_u)^2} + c\delta t \\ p_2 &= \sqrt{(X_2 - X_u)^2 + (Y_2 - Y_u)^2 + (Z_2 - Z_u)^2} + c\delta t \\ p_3 &= \sqrt{(X_3 - X_u)^2 + (Y_3 - Y_u)^2 + (Z_3 - Z_u)^2} + c\delta t \\ p_4 &= \sqrt{(X_4 - X_u)^2 + (Y_4 - Y_u)^2 + (Z_4 - Z_u)^2} + c\delta t \end{aligned} \tag{2.2}$$

Η λύση αυτού του μη γραμμικού συστήματος μπορεί να δοθεί είτε σε κλειστή μορφή είτε με γραμμικοποίησή και αριθμητική προσεγγίση με επαναληπτικές μεθόδους.

Για την γραμμικοποίηση του συστήματος χρειάζεται να είναι γνωστή η προσεγγιστική θέση του χρήστη $(\hat{X}_u, \hat{Y}_u, \hat{Z}_u)$. Η πραγματική θέση του χρήστη (X_u, Y_u, Z_u) θα βρεθεί υπολογίζοντας την διαφορά της από την προσεγγιστική $(\Delta X_u, \Delta Y_u, \Delta Z_u)$.

Έστω η i-οστή ψευδοαπόσταση

$$p_{\mathrm{i}} = \sqrt{(X_{\mathrm{i}} - X_u)^2 + (Y_{\mathrm{i}} - Y_u)^2 + (Z_{\mathrm{i}} - Z_u)^2} + c\delta t = f(X_u, Y_u, Z_u, \delta t) \tag{2.3}$$

Αντικαθιστώντας την προσεγγιστική θέση του χρήστη $(\hat{X}_u, \hat{Y}_u, \hat{Z}_u)$ και διαφορά χρόνου $\widehat{\delta t}$ προκύπτει η προσεγγιστική ψευδοαπόσταση $\hat{p}_i$

$$\hat{p}_i = \sqrt{(X_\mathrm{i} - \hat{X}_u)^2 + (Y_\mathrm{i} - \hat{Y}_u)^2 + (Z_\mathrm{i} - \hat{Z}_u)^2} + c\widehat{\delta t} = f(\hat{X}_u, \hat{Y}_u, \hat{Z}_u, \widehat{\delta t}) \qquad (2.4)$$

Επιπλέον ισχύουν οι παρακάτω εξισώσεις:

$$\begin{gathered}(X_u, Y_u, Z_u) = (\hat{X}_u + \Delta X_u, \hat{Y}_u + \Delta Y_u, \hat{Z}_u + \Delta Z_u) \\ \delta t = \widehat{\delta t} + \Delta t\end{gathered} \qquad (2.5)$$

Όπου Δt είναι η διαφορά της προσεγγιστικής με την πραγματική χρονική απόκλιση μεταξύ χρόνου GPS και χρόνου του χρήστη. Επομένως αντικαθιστώντας στη σχέση 2.3 προκύπτει η παρακάτω εξίσωση:

$$f(X_u, Y_u, Z_u, \delta t) = f\left(\hat{X}_u + \Delta X_u, \hat{Y}_u + \Delta Y_u, \hat{Z}_u + \Delta Z_u, \widehat{\delta t} + \Delta t\right) \quad (2.6)$$

Αυτή η σχέση μπορεί να επεκταθεί γύρω από τη προσσεγγιστική θέση με σειρές Taylor όπως παρακάτω:

$$\begin{gathered}f\left(\hat{X}_u + \Delta X_u, \hat{Y}_u + \Delta Y_u, \hat{Z}_u + \Delta Z_u, \widehat{\delta t} + \Delta t\right) = f(X_u, Y_u, Z_u, \delta t) \\ + \frac{\partial f(\hat{X}_u, \hat{Y}_u, \hat{Z}_u, \widehat{\delta t})}{\partial \hat{X}_u}\Delta X_u + \frac{\partial f(\hat{X}_u, \hat{Y}_u, \hat{Z}_u, \widehat{\delta t})}{\partial \hat{Y}_u}\Delta Y_u + \frac{\partial f(\hat{X}_u, \hat{Y}_u, \hat{Z}_u, \widehat{\delta t})}{\partial \hat{Z}_u}\Delta Z_u \\ + \frac{\partial f(\hat{X}_u, \hat{Y}_u, \hat{Z}_u, \widehat{\delta t})}{\partial \widehat{\delta t}}\Delta t + \cdots\end{gathered} \qquad (2.7)$$

Οι μερικές παράγωγοι υπολογίζονται ως εξής:

$$\begin{gathered}\frac{\partial f(\hat{X}_u, \hat{Y}_u, \hat{Z}_u, \widehat{\delta t})}{\partial \hat{X}_u} = -\frac{X_i - \hat{X}_u}{\hat{R}_i} \\ \frac{\partial f(\hat{X}_u, \hat{Y}_u, \hat{Z}_u, \widehat{\delta t})}{\partial \hat{Y}_u} = -\frac{Y_i - \hat{Y}_u}{\hat{R}_i}\end{gathered} \qquad (2.8)$$

$$\frac{\partial f(\hat{X}_u, \hat{Y}_u, \hat{Z}_u, \widehat{\delta t})}{\partial \hat{Z}_u} = -\frac{Z_i - \hat{Z}_u}{\hat{R}_i}$$

$$\frac{\partial f(\hat{X}_u, \hat{Y}_u, \hat{Z}_u, \widehat{\delta t})}{\partial \widehat{\delta t}} = \mathrm{c}$$

Όπου $\hat{R}_i$ είναι η γεωμετρική απόσταση μεταξύ i-οστού δορυφόρου και προσεγγιστικής θέσης του χρήστη

$$\hat{R}_i = \sqrt{\left(X_\mathrm{i} - \hat{X}_u\right)^2 + \left(Y_\mathrm{i} - \hat{Y}_u\right)^2 + \left(Z_\mathrm{i} - \hat{Z}_u\right)^2} \tag{2.9}$$

Αντικαθιστώντας στην αρχική εξίσωση:

$$\hat{p}_i - p_\mathrm{i} = \frac{X_i - \hat{X}_u}{\hat{R}_i}\Delta X_u + \frac{Y_i - \hat{Y}_u}{\hat{R}_i}\Delta Y_u + \frac{Z_i - \hat{Z}_u}{\hat{R}_i}\Delta Z_u - c\Delta t \tag{2.10}$$

Για λόγους απλοποίησης των σχέσεων, είναι απαραίτητο να εισαχθούν οι παρακάτω νέες μεταβλητές:

$$\begin{aligned} \Delta p_i &= \hat{p}_i - p_\mathrm{i} \\ a_{xi} &= \frac{X_i - \hat{X}_u}{\hat{R}_i} \\ a_{yi} &= \frac{Y_i - \hat{Y}_u}{\hat{R}_i} \\ a_{zi} &= \frac{Z_i - \hat{Z}_u}{\hat{R}_i} \end{aligned} \tag{2.11}$$

Οπότε η εξίσωση 2.7 μπορεί να γραφεί σε πιο απλή μορφή

$$\Delta p_i = a_{xi}\Delta X_u + a_{yi}\Delta Y_u + a_{zi}\Delta Z_u - c\Delta t \tag{2.12}$$

Λαμβάνοντας υπόψη τις σχέσεις που προκύπτουν και για τους 4 δορυφόρους σχηματίζεται το παρακάτω σύστημα εξισώσεων σε μορφή πινάκων:

$$\Delta\boldsymbol{\rho} = \begin{bmatrix} \Delta p_1 \\ \Delta p_2 \\ \Delta p_3 \\ \Delta p_4 \end{bmatrix} \quad \boldsymbol{H} = \begin{bmatrix} a_{x1} & a_{y1} & a_{z1} & 1 \\ a_{x2} & a_{y2} & a_{z2} & 1 \\ a_{x3} & a_{y3} & a_{z3} & 1 \\ a_{x4} & a_{y4} & a_{z4} & 1 \end{bmatrix} \quad \Delta\boldsymbol{x} = \begin{bmatrix} \Delta X_\chi \\ \Delta Y_\chi \\ \Delta Z_\chi \\ -c\Delta t \end{bmatrix}$$

$$\Delta\boldsymbol{\rho} = \boldsymbol{H}\Delta\boldsymbol{x} \tag{2.13}$$

Όπου τελικά λύνοντας ως προς Δx προκύπτει το επιθυμητό αποτέλεσμα:

$$\Delta\boldsymbol{x} = \boldsymbol{H^{-1}}\Delta\boldsymbol{p} \tag{2.14}$$

Στη συνήθη περίπτωση όπου υπάρχουν πάνω από τέσσερις δορυφόροι σε οπτική επαφή με τον χρήστη, το σύστημα είναι υπερπροσδιορισμένο και μπορεί να λυθεί με τη χρήση ελαχίστων τετραγώνων. Έστω ότι λαμβάνεται σήμα από n δορυφόρους τότε προκύπτει το παρακάτω σύστημα

$$\Delta\boldsymbol{\rho} = \begin{bmatrix} \Delta p_1 \\ \Delta p_2 \\ \Delta p_3 \\ \Delta p_4 \\ . \\ . \\ \Delta p_n \end{bmatrix} \quad \boldsymbol{H} = \begin{bmatrix} a_{x1} & a_{y1} & a_{z1} & 1 \\ a_{x2} & a_{y2} & a_{z2} & 1 \\ a_{x3} & a_{y3} & a_{z3} & 1 \\ a_{x4} & a_{y4} & a_{z4} & 1 \\ . & . & . & . \\ . & . & . & . \\ a_{xn} & a_{yn} & a_{zn} & 1 \end{bmatrix} \quad \Delta\boldsymbol{x} = \begin{bmatrix} \Delta X_u \\ \Delta Y_u \\ \Delta Z_u \\ -c\Delta t \end{bmatrix}$$

$$\Delta\boldsymbol{\rho} = \boldsymbol{H}\Delta\boldsymbol{x} \tag{2.15}$$

Το οποίο λύνεται όπως παρακάτω:

$$\Delta\boldsymbol{x} = (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\Delta\boldsymbol{x} \tag{2.16}$$

3. Επιθέσεις στο σύστημα GPS

3.1 Εισαγωγικά

Όπως κάθε σύστημα έτσι και το GPS μπορεί να γίνει στόχος επιθέσεων. Οι τακτικές που χρησιμοποιείται για αυτό το σκοπό είναι η παραγωγή από τον επιτιθέμενο τεχνητών σημάτων GPS, τα οποία «μιμούνται» τα αυθεντικά (Spoofing). Για να γίνει όμως μια επιτυχής επίθεση είναι απαραίτητο να πληρούνται κάποιες προϋποθέσεις. Για την θεωρητική ανάλυση του προβλήματος, σε αυτό το κεφάλαιο δίδεται ο πλήρης προσδιορισμός του μοντέλου που το περιγράφει, καθώς και οι ακριβείς στόχοι που τίθενται.

3.1.1 Προσδιορισμός του συστήματος

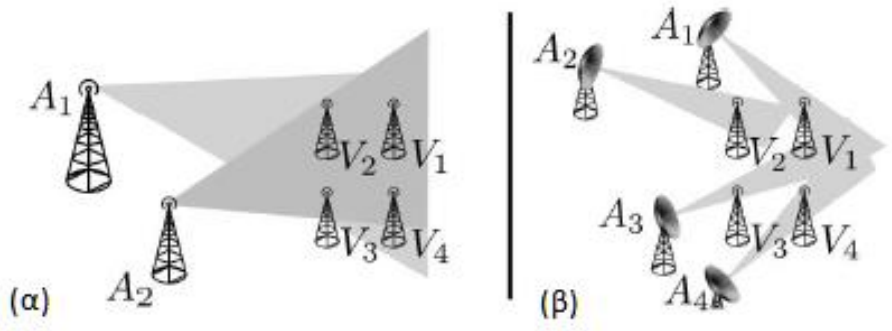
Το σύστημα στο οποίο γίνεται επίθεση αποτελείται από ένα σύνολο δορυφόρων GPS και ένα σύνολο από δέκτες χρηστών που αποτελούν τα «θύματα». Οι δέκτες-θύματα δέχονται ασύρματα σήματα GPS, με τα οποία υπολογίζουν την θέση τους με τους αλγόριθμους που περιγράφηκαν στην παράγραφο 2.3.2.

Η θέση κάθε δέκτη-θύματος V_i δίδεται από τις συντεταγμένες του L_i ενώ η απόκλιση του χρόνου από τον χρόνο του συστήματος δίδεται ως δ_i. Σημειώνεται ότι οι υπολογιζόμενες από το δέκτη συντεταγμένες δεν είναι αναγκαίο να συμπίπτουν με τις πραγματικές συντεταγμένες R_i. Όταν ένας δέκτης-θύμα δέχεται επίθεση spoofing, οι νέες συντεταγμένες που υπολογίζει θα συμβολίζονται με L_i' ενώ αντίστοιχα η απόκλιση του χρόνου θα συμβολίζεται με δ_i'.

3.1.2 Μοντέλο επιθέσεων

Είναι απαραίτητο να προσδιορισθούν οι δυνατότητες του επιτιθέμενου, δηλαδή αν διαθέτει πλήρη γνώση της θέσης του θύματος, κατά πόσο μπορεί να παράγει εξολοκλήρου τα δορυφορικά σήματα ή απλώς να τα επανεκπέμψει και αν στέλνει το ίδιο σήμα σε όλους τους δέκτες θύματα ή μπορεί να στοχεύσει σε κάθε θύμα ξεχωριστά.

Αν ο επιτιθέμενος έχει πλήρη έλεγχο της εισόδου κάθε κεραίας δέκτη, θα μπορεί να στέλνει σήματα και να αλλοιώνει τις συντεταγμένες κάθε δέκτη με διαφορετικό τρόπο. Για να γίνει όμως αυτό θα πρέπει να χρησιμοποιοηθούν κεραίες μεγάλης κατευθυντικότητας από τον επιτιθέμενο, ή να βρίσκεται πολύ κοντά σε κάθε θύμα. Σχήμα 2.9.



Σχήμα 2.9. (α) Το σήμα των επιτιθέμενων A_1, A_2 φτάνει σε όλους τους δέκτες σ (β) Κάθε επιτιθέμενος στέλνει σήμα σε έναν συγκεκριμένο δέκτη [5].

Ο επιτιθέμενος διαθέτει ένα σύνολο πομπών και μπορεί να τους μετακινεί σε κάθε θέση ανεξάρτητα από τους άλλους. Η θέση του i-οστού πομπού, ο οποίος επεμβαίνει στο σήμα του i-οστου δορυφόρου του επιτιθέμενου δηλώνεται με R_i^a. Ένα από τα σενάρια που μπορούν να δοθούν είναι ο επιτιθέμενος να προσθέτει εσκεμένα καθυστέρηση δ_i^a στο σήμα του i-οστού δορυφόρου. Στην ανάλυση που ακολουθεί γίνεται η υπόθεση ότι ο επιτιθέμενος γνωρίζει τις φυσικές συντεταγμένες των θυμάτων και των δορυφόρων από τους οποίους λαμβάνει σήματα.

Με βάση το κατά πόσο μπορεί ο επιτιθέμενος να επέμβει στο δορυφορικό σήμα υπάρχουν δύο κατηγορίες επιθέσεων:

(α) Επίθεση στο πολιτικό σκέλος του συστήματος. Ο επιτιθέμενος έχει τη δυνατότητα να παράγει το δικό του σήμα, καθώς οι κώδικες που χρησιμοποιούνται είναι ανοιχτοί και μη κρυπτογραφημένοι. Επομένως μπορεί να στείλει ένα σήμα με οποιαδήποτε καθυστέρηση ή ακόμα και προπορευόμενο του αυθεντικού. Μπορεί επίσης να επέμβει στα δεδομένα του σήματος που στέλνει αλλάζοντας τις συντεταγμένες των δορυφόρων.

(β) Επίθεση στο κρυπτογραφημένο σκέλος του συστήματος. Ο επιτιθέμενος σε αυτή τη περίπτωση είναι αρκετά πιο δεσμευμένος καθώς δεν έχει τη δυνατότητα να παράγει δικά του σήματα, που να μιμούνται τα πραγματικά λόγω της ισχυρής κρυπτογράφησης. Η μόνη δυνατότητα που έχει είναι η αναμετάδοση πραγματικών σημάτων που λαμβάνει από τη δική του φυσική θέση. Αυτό μπορεί να γίνει λαμβάνοντας ξεχωριστά σήματα με στόχευση κάθε δορυφόρου με μεγάλης κατευθυντικότητας κεραίες. Επομένως η μόνη παράμετρος που μπορεί να επηρεάσει είναι η καθυστέρηση δ_i^a.

3.2 Διατύπωση ορισμών

Σε αυτήν την παράγραφο θέτονται οι ορισμοί του προβλήματος του GPS spoofing.

1ος Ορισμός (Επίθεση GPS spoofing). Έστω ότι το θύμα υπολογίζει την θέση του L, με το σύστημα GPS, χωρίς να παρεμποδίζεται από κάποιον επιτιθέμενο. Στην περίπτωση επίθεσης ο επιτιθέμενος στέλνει σήματα που μιμούνται τα πραγματικά (GPS spoofing attack), με στόχο το θύμα να υπολογίσει τη αλλοιωμένη θέση του $L' \neq L$.

Ο ορισμός αυτός μπορεί να επεκταθεί και για ομάδες δεκτών GPS οι οποίοι επικοινωνούν μεταξύ τους. Με αυτόν τον τρόπο ο κάθε ένας γνωρίζει τη σχετική του θέση ως προς τους άλλους.

2ος Ορισμός (Επίθεση σε ομάδα). Έστω ένα σύνολο δεκτών θυμάτων V_i με πραγματικές θέσεις R_i. Το πρόβλημα της επίθεσης σε ομάδα είναι η δημιουργία του κατάλληλου συνδυασμού σημάτων, τα οποία στέλνονται από τον επιτιθέμενο, ώστε να μετατοπιστούν οι θέσεις τις οποίες υπολογίζουν οι δέκτες θύματα στις $L_i' \neq L_i$.

Στη δεύτερη περίπτωση της επίθεσης σε ομάδα, υπάρχει ο επιπλέον περιορισμός ότι οι αλλοιωμένες θέσεις των θυμάτων μετά την επίθεση, θα πρέπει να διατηρούν αναλλοίωτες τις σχετικές θέσεις μέσα στην ομάδα των δεκτών. Αν συνέβαινε το αντίθετο τα θύματα θα ανίχνευαν τη μεταξύ τους μετατόπιση και επομένως και την επίθεση.

3ος Ορισμός (Πρόβλημα υπολογισμού των παραμέτρων του επιτιθέμενου). Έστω R_j οι συντεταγμένες της πραγματικής θέσης των θυμάτων V_j και $L'_j, \delta t'_j$ είναι η μετατοπισμένη θέση των θυμάτων και η «αλλοιωμένη» μετατόπιση χρόνου (time offset) μετά την επίθεση. Το πρόβλημα υπολογισμού των παραμέτρων του επιτιθέμενου, είναι η επιλογή κατάλληλων παραμέτρων στις οποίες μπορεί να επέμβει ο επιτιθέμενος, όπως η θέση του R_A, η καθυστέρηση δt_aμε την οποία εκπέμπει το σήμα ή τη μετατοπισμένη, σε σχέση με την πραγματική, θέση του δορυφόρου L_i^A την οποία στέλνει με το μήνυμα δεδομένων, ώστε η επίθεση να είναι επιτυχημένη σύμφωνα με τον 1ο ορισμό.

3.3 Διατύπωση εξισώσεων

Η εσφαλμένη θέση L'_j την οποία υπολογίζει το θύμα V_j μετά από μια επιτυχημένη επίθεση είναι συνάρτηση της πραγματικής θέσης του επιτιθέμενου R_A, της καθυστέρησης δt_A και της θέσης του δορυφόρου L_i^A. Η ψευδοαπόσταση P_{ij}^A την οποία θα υπολογίσει το θύμα όταν λάβει το σήμα από τον επιτιθέμενο είναι συνάρτηση της καθυστέρησης δt_i^A και της θέσης του R_A και δίνεται από την παρακάτω εξίσωση:

$$P_{ij}^A = \left|R_j - R_A\right| + \delta t_i^A \cdot c \tag{3.1}$$

Για να υπολογίσει τη θέση του L'_j το θύμα V_j θα λύσει το παρακάτω σύστημα εξισώσεων:

$$P_{ij}^A = \left|L'_j - L_i^A\right| + \delta t'_j \cdot c \tag{3.2}$$

Επομένως εξισώνοντας τα δεξιά μέρη των εξισώσεων, προκύπτει το σύστημα το οποίο θα πρέπει να λύσει ο επιτιθέμενος προκειμένου να προσδιορίσει τις παραμέτρους τις οποίες ο ίδιος μπορεί να μεταβάλει.

$$\left|R_j - R_A\right| + \delta t_i^A \cdot c = \left|L'_j - L_i^A\right| + \delta t'_j \cdot c \tag{3.3}$$

Στην περίπτωση του πολιτικού σήματος, ο επιτιθέμενος μπορεί να διατηρήσει σταθερή την τοποθεσία του και έχοντας επιλέξει την θέση στόχο L'_j να λύσει ως προς την καθυστέρηση δt_A ή ακόμα και την θέση του δορυφόρου L_i^A. Αντίθετα στο στρατιωτικό σκέλος του συστήματος η μόνη παράμετρος που μπορεί να ελεγχθεί είναι η καθυστέρηση δt_A. Ακόμα όμως και η καθυστέρηση υπόκεινται στον περιορισμό ότι δεν μπορεί να είναι μικρότερη από την πραγματική απόσταση επιτιθέμενου-δορυφόρου προς την ταχύτητα του φωτός.

$$\delta t_i^A \geq \left|L'_j - L_i\right|/c \tag{3.4}$$

Αντικαθιστώντας στην εξίσωση … προκύπτει η παρακάτω ισότητα:

$$\left|R_j - R_A\right| + \left|L'_j - L_i\right| \leq \left|L'_j - L_i\right| + \delta t'_j \cdot c \tag{3.5}$$

Εφαρμόζοντας την τριγωνική ανισότητα στο πρώτο μέλος προκύπτει:

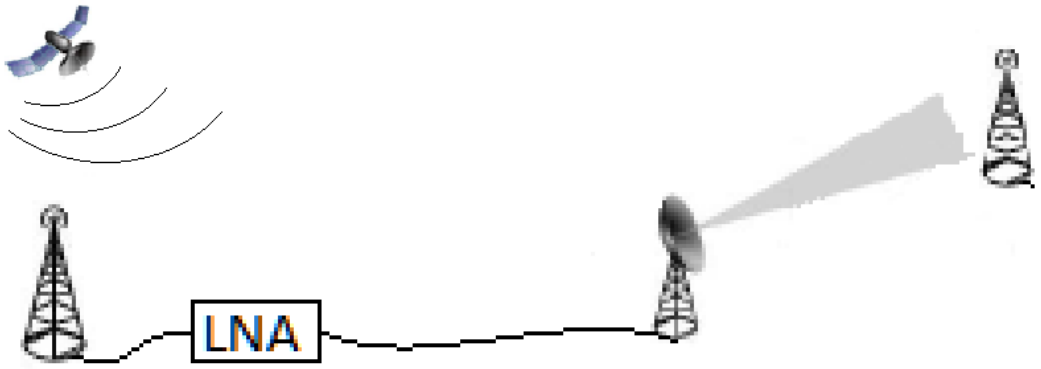
$$\left|R_j - L_i\right| \leq \left|L'_j - L_i\right| + \delta t'_j \cdot c \tag{3.6}$$

Η εξίσωση αυτή δείχνει ότι υπάρχει περιορισμός στην επιλογή της θέσης στόχου L'_j και της χρονικής μετατόπισης $\delta t'_j$.

4. Προτεινόμενη διάταξη

4.1 Περιγραφή της διάταξης

Η διατήρηση της απλότητας έπαιξε σημαντικό ρόλο στην σχεδίαση της προτεινόμενης διάταξης. Το πλεονέκτημα της απλής σχεδίασης είναι ότι διευκολύνει τη θεωρητική περιγραφή της λειτουργίας της. Η γενική ιδέα είναι η λήψη των δορυφορικών σημάτων με μια αρκετά υψηλής κατευθυντικότητας κεραία, ενίσχυσή τους με έναν ενισχυτή χαμηλού θορύβου (LNA), εισαγωγή καθυστέρησης και επανεκπομπή τους προς τον δέκτη στόχο. Σχήμα 4.1



Σχήμα 4.1 Σχηματική αναπαράσταση της προτεινόμενης διάταξης

Η ισχύς του σήματος που λαμβάνεται από την κεραία της διάταξης είναι εύλογο να θεωρηθεί προσεγγιστικά ίση με την ισχύ του σήματος που λαμβάνει ο δέκτης από τον δορυφόρο. Αυτό συμβαίνει γιατί η αναλογία των δύο αποστάσεων είναι περίπου ίση με 1 επομένως οι συντελεστές απωλειών κενού χώρου προσεγγιστικά ίσοι.

Ένα βασικό στοιχείο που χρειάζεται να υπολογιστεί για τη σχεδίαση της διάταξης είναι το κέρδος του ενισχυτή χαμηλού θορύβου. Για να γίνει αυτό θα πρέπει να υπολογιστούν όλες οι απώλειες που εισάγει η διάταξη από τη λήψη του δορυφορικού σήματος, από την κεραία του επιτιθέμενου, έως και την λήψη του καθυστερημένου σήματος από την κεραία του θύματος.

Αρχικά γίνεται υπολογισμός του συντελεστή απωλειών κενού χώρου και για τις δύο φέρουσες συχνότητες του συστήματος, L1 = 1575,42 MHz με μήκος κύματος λ_1 = 19,03 cm και L2 = 1227,60 MHz με μήκος κύματος λ_2 = 24,42 cm. Μια ενδεικτική απόσταση για την ακτίνα που μπορεί να λειτουργήσει η συσκευή είναι τα 100m.

$$20\log\frac{\lambda_1}{4\pi R} = 20\log\frac{0{,}19}{4\pi 100} = -175dB$$
$$20\log\frac{\lambda_1}{4\pi R} = 20\log\frac{0{,}24}{4\pi 100} = -171dB \quad (4.1)$$

Για την εισαγωγή καθυστέρησης χρησιμοποιείται καλώδιο μήκους 100m. Μια αντιπροσωπευτική τιμή απωλειών για αυτό το μήκος καλωδίου είναι τα 15dB.

Οι κεραίες που μπορούν να χρησιμοποιηθούν είναι ελικοειδείς. Για τον υπολογισμό του κέρδους τους χρησιμοποιήθηκε ο παρακάτω τύπος.

$$G = 15N(\frac{C}{\lambda})^2(\frac{S}{\lambda})^2 \quad (4.2)$$

Όπου C είναι η περιφέρεια του κύκλου, S η απόσταση μεταξύ των σπειρωμάτων και N ο αριθμός των σπειρωμάτων. Θέτοντας C=λ, S = 0.25λ και N = 20 το κέρδος της κεραίας μπορεί να δοθεί κατά προσέγγιση στα 30dB. Επομένως για να εξισοροπισθούν οι απώλειες που ισάγονται θα πρέπει το κέρδος του LNA να είναι:

$$175 + 15 - 2 * 30 = 130dB \quad (4.3)$$

Για τις ανάγκες μιας πειραματικής διάταξης προκειμένου να διερευνηθούν οι δυνατότητες της προτεινόμενης σχεδίασης δεν είναι απαραίτητη η χρησιμοποίηση ενισχυτικής διάταξης τόσο μεγάλου κέρδους, καθώς ο δέκτης μπορεί απλά να βρίσκεται σε πολύ μικρή απόσταση από την

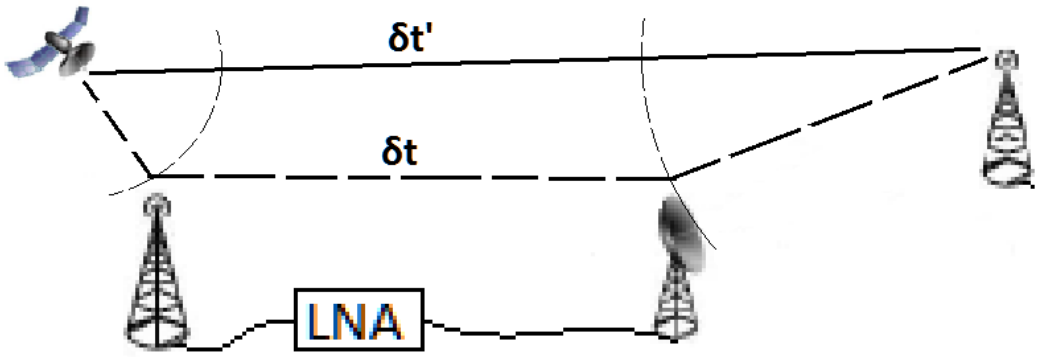
κεραία εκπομπής. Αν στο πείραμα ο δέκτης απέχει απόσταση 1m οι απώλειες κενού χώρου θα ήταν κατά 80 dB λιγότερες και άρα ο ενισχυτής θα πρέπει να έχει κέρδος 50dB. Σε κάθε περίπτωση ένας ενισχυτής με μεταβλητό κέρδος θα ήταν η ιδανικότερη λύση στην περίπτωση που η προς μελέτη διάταξη χρησιμοποιηθεί σε πραγματικές συνθήκες.

4.2 Θεωρητική μελέτη

Για τη πρόβλεψη της συμπεριφοράς της διάταξης σε θεωρητικό επίπεδο αρχικά εξετάζεται η απλούστερη περίπτωση κατά την οποία ο δέκτης-θύμα λαμβάνει σήμα από μόνο τέσσερις δορυφόρους. Αυτή είναι και η αναγκαία συνθήκη που πρέπει να ικανοποιείται για να μπορεί ο χρήστης να υπολογίζει τη θέση του. Το πρόβλημα χωρίζεται σε δύο υποπεριπτώσεις. Στην πρώτη υποπερίπτωση η διάταξη εισάγει καθυστέρηση και επανεκπέμπει τα σήματα και από τους τέσσερις δορυφόρους. Στην δεύτερη υποπερίπτωση η διάταξη εισάγει καθυστέρηση σε ένα, δύο ή και τρία δορυφορικά σήματα αλλά όχι και στα τέσσερα.

4.2.1 Εισαγωγή της ίδιας καθυστέρησης σε όλα τα σήματα

Η περίπτωση αυτή αποδεικνύεται ιδιαίτερα ενδιαφέρουσα καθώς καταλήγει σε ένα εντελώς αναπάντεχο αποτέλεσμα. Για να γίνει επακριβώς κατανοητή η λειτουργία της διάταξης θα πρέπει να διερευνηθεί το πόσο καθυστερημένα λαμβάνονται τα σήματα του επιτιθέμενου από το θύμα, σε σχέση με τα πραγματικά σήματα που θα λάμβανε το θύμα αν δε δέχονταν επίθεση. Η συνολική αυτή καθυστέρηση είναι ίση με το άθροισμα της σταθερής καθυστέρησης δt που εισάγει η διάταξη και της καθυστέρησης δt’ λόγω της μεγαλύτερης διαδρομής που ακολουθεί το σήμα όταν αναμεταδίδεται από τον επιτιθέμενο σχήμα 4.2



Σχήμα 4.2 Αναπαράσταση των διαδρομών που ακολουθεί το σήμα.

Οι εξισώσεις των ψευδοαποστάσεων που προκύπτουν είναι οι παρακάτω:

$$P_i' = S_i A + AV + c\delta T_V + c\delta t \tag{4.4}$$

Όπου i = 1,..4 ο αριθμός των δορυφόρων, $S_i A, AV$ η πραγματική απόσταση μεταξύ επιτιθέμενου Α, δορυφόρου S_i και επιτιθέμενου Α και θύματος V ενώ δT_V η απόκλιση του ρολογιού του δέκτη-θύματος.

Το σύστημα λύνεται εύκολα αφαιρώντας την πρώτη εξίσωση από όλες τις υπόλοιπες οπότε απαλοίφονται οι κοινοί όροι (AV, $c\delta T_V$, $c\delta$t) και προκύπτει το παρακάτω σύστημα τριών υπερβολικών εξισώσεων, στο οποίο οι γνωστοί όροι είναι οι ψευδοαποστάσεις και οι θέσεις Si των δορυφόρων.

$$\begin{aligned} P_2' - P_1' &= S_2 A - S_1 A \\ P_3' - P_1' &= S_3 A - S_1 A \\ P_4' - P_1' &= S_4 A - S_1 A \end{aligned} \tag{4.5}$$

Κάθε εξίσωση περιγράφει μία υπερβολή που προσδιορίζεται πλήρως από τις εστίες της (οι θέσεις των δορυφόρων S_i, S_j) και την σταθερή διαφορά μεταξύ των αποστάσεων που απέχει κάθε σημείο της από τις εστίες. Ο επιτιθέμενος προσδιορίζει και ο ίδιος τη θέση του λύνοντας το παρακάτω σύστημα

εξισώσεων, όπου ο όρος δT_A είναι η σταθερή διαφορά που έχει το ρολόι του δέκτη του από αυτό του συστήματος GPS.

$$P_i^{\mathrm{A}} = S_i A + c\delta T_A \tag{4.6}$$

Όπου i = 1,..4 ο αριθμός των δορυφόρων

Επαναλαμβάνοντας την προηγούμενη διαδικασία λύσης των εξισώσεων προκύπτει το ακόλουθο σύστημα τριών εξισώσεων.

$$\begin{aligned} P_2^{\mathrm{A}} - P_1^{\mathrm{A}} &= S_2 A - S_1 A \\ P_3^{\mathrm{A}} - P_1^{\mathrm{A}} &= S_3 A - S_1 A \\ P_4^{\mathrm{A}} - P_1^{\mathrm{A}} &= S_4 A - S_1 A \end{aligned} \tag{4.7}$$

Κάθε μία από τις υπερβολές που περιγράφονται από τις εξισώσεις αυτές, είναι ταυτόσημη με την αντίστοιχη του συστήματος 4,5 καθώς έχουν κοινές εστίες του δορυφόρους S_i, S_j και ίση διαφορά μεταξύ των αποστάσεων των σημείων τους από τις εστίες. Επομένως η λύση του συστήματος 4,7 είναι ταυτόσημη με αυτή του συστήματος …

Η ερμηνεία αυτού του αποτελέσματος είναι ότι το θύμα GPS υπολογίζει τη θέση του επιτιθέμενου και άρα θεωρεί ότι είναι η δική του θέση.

4.2.2 Εισαγωγή καθυστέρησης σε λιγότερα από 4 σήματα

Στην περίπτωση αυτή έχουμε το παρακάτω σύστημα τεσσάρων εξισώσεων

$$\begin{aligned} P_i' &= S_i A + AV + c\delta T_V \\ P_j' &= S_j A + AV + c\delta T_V + c\delta t \end{aligned} \tag{4.8}$$

Όπου $i \neq j$.

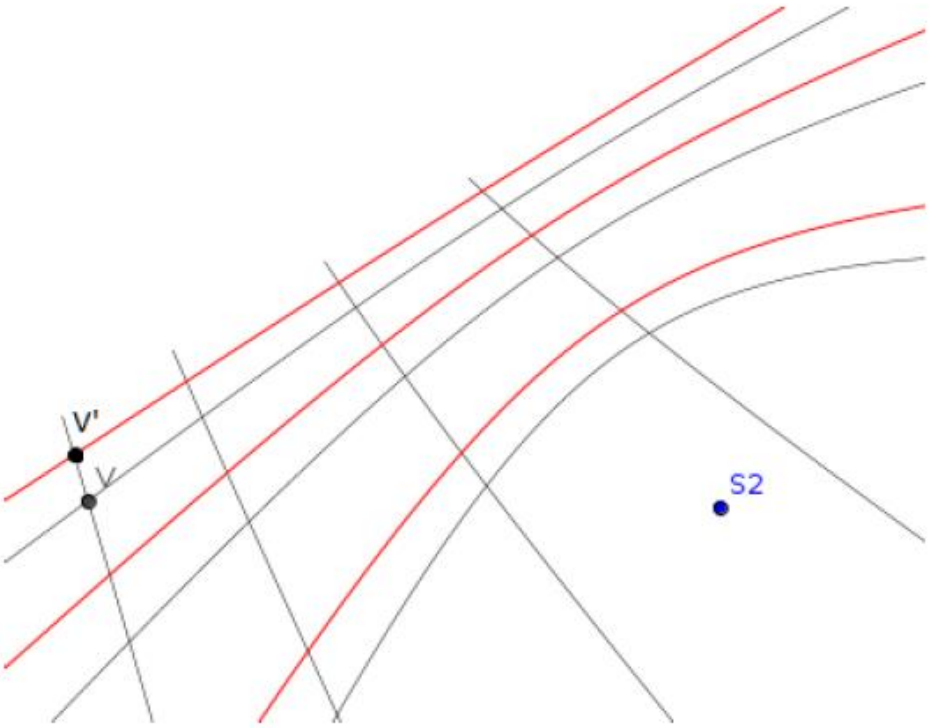
Στην ειδικότερη περίπτωση κατά την οποία εισάγεται καθυστέρηση μόνο σε ένα δορυφόρο έστω στον 2ο έχουμε το παρακάτω σύστημα υπερβολών

$$P_2' - P_1' - c\delta t = S_2A - S_1A$$

$$P_3' - P_1' = S_3A - S_1A \tag{4.9}$$

$$P_4' - P_1' = S_4A - S_1A$$

Επομένως θα μετακινηθεί η μία μόνο υπερβολή, παράλληλα με τον εαυτό της, ενώ οι υπόλοιπες θα μείνουν όπως έχουν. Στο παρακάτω σχήμα … το θύμα υπολογίζει τη θέση του στη θέση V'.



Σχήμα 4.3 Μετακίνηση υπερβολής παράλληλα στον εαυτό της

4.3 Προσομοίωση λειτουργίας με χρήση MATLAB

Για την προσομοίωση του συστήματος αφαιρέθηκαν αρκετά επίπεδα πολυπλοκότητας, καθώς η πλήρη κατασκευή των δορυφορικών σημάτων καθώς και η προσομοίωση της λειτουργίας ενός δέκτη GPS δεν θα προσέφερε στην τελική διατύπωση συμπερασμάτων. Το κυρίως αντικείμενο προς μελέτη είναι η λύση των εξισώσεων προσδιορισμού θέσης και το πως η λύση αυτών μετατοπίζεται με την κατάλληλη χρήση της προτεινόμενης διάταξης. Επομένως το σενάριο της προσομοίωσης περιορίστηκε στη λύση ακριβώς αυτών των εξισώσεων όταν δίδονται οι ψευδοαποστάσεις και η ακριβής θέση των δορυφόρων.

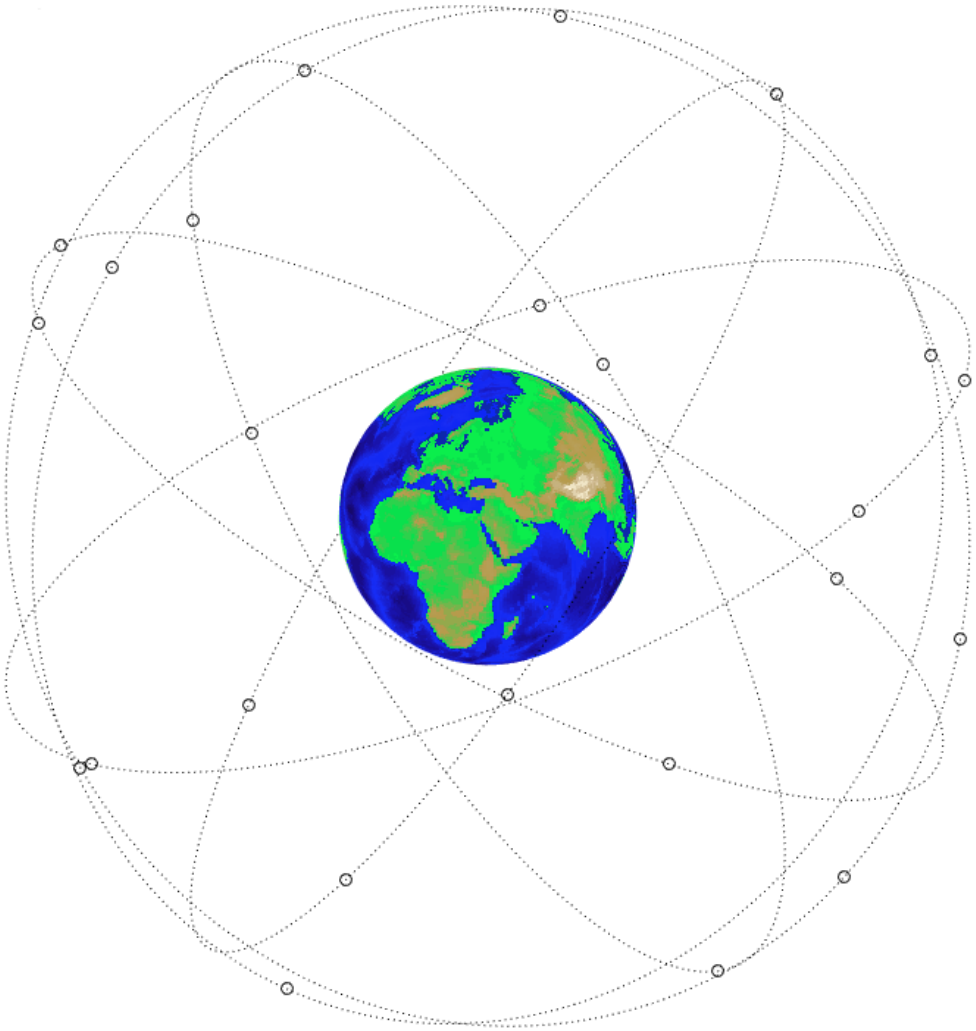
4.3.3 Προσομοίωση δορυφορικών τροχιών

Προκειμένου το σενάριο να πλησιάζει όσο το δυνατόν περισσότερο στον πραγματικό κόσμο χρησιμοποιήθηκαν δεδομένα από πραγματικές δορυφορικές τροχιές. Ο πίνακας 4.1 δίνει τα στοιχεία των δορυφορικών τροχιών τη 1η Ιουλίου 1993, 18 ώρες 36 λεπτά 14,4 δευτερόλεπτα ώρα Greenwich. Η κλίση των τροχιών που χρησιμοποιήθηκε στην προσομοίωση είναι 55ο.

Slot	*RAAN (°)*	*Argument of Latitude (°)*	*Slot*	*RAAN (°)*	*Argument of Latitude (°)*
A1	272.847	268.126	D1	92.847	135.226
A2	272.847	161.786	D2	92.847	265.446
A3	272.847	11.676	D3	92.847	35.136
A4	272.847	41.806	D4	92.847	167.356
B1	332.847	80.956	E1	152.847	197.046
B2	332.847	173.336	E2	152.847	302.596
B3	332.847	309.976	E3	152.847	66.066
B4	332.847	204.376	E4	152.847	333.686
C1	32.847	111.876	F1	212.847	238.886
C2	32.847	11.796	F2	212.847	345.226
C3	32.847	339.666	F3	212.847	105.206
C4	32.847	241.556	F4	212.847	135.346

Πίνακας 4.1 Στοιχεία δορυφορικών τροχιών της 1ης Ιουλίου 1993.

Ο σχηματισμός των δορυφόρων τη συγκεκριμένη στιγμή φαίνεται στο σχήμα 4.4.



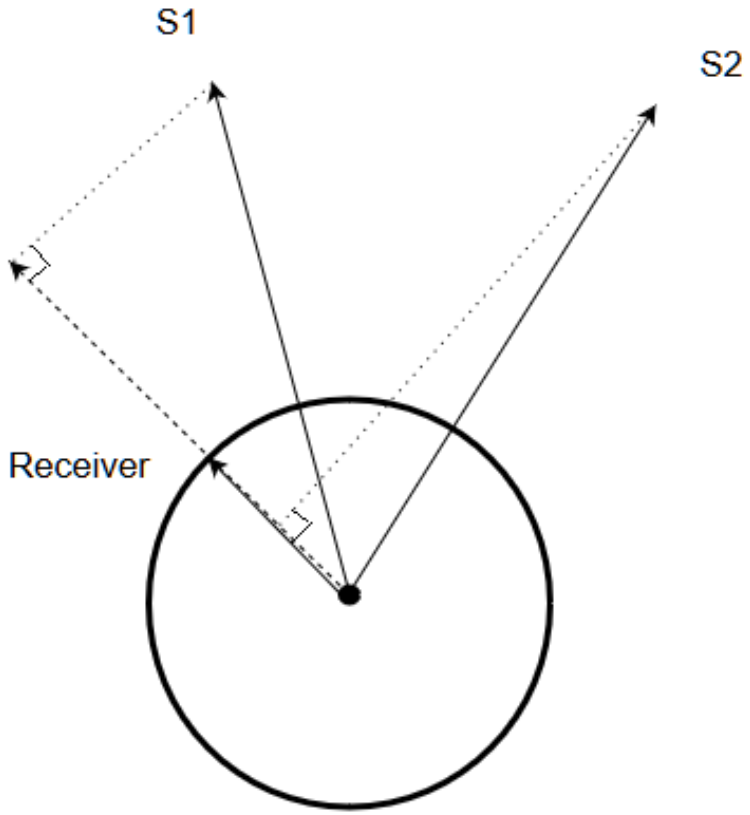
Σχήμα 4.4 Αστερισμός δορυφόρων GPS της 1ης Ιουλίου 1993.

Η θέση του δέκτη επιλέχθηκε για απλότητα να έχει συντεταγμένες (0^o, 0^o) πάνω στην επιφάνεια της γης. Είναι απαραίτητο να διαχωριστούν οι δορυφόροι που έχουν οπτική επαφή με τον δέκτη και οι ψευδοαποστάσεις να υπολογιστούν μόνο για αυτό το σύνολο των δορυφόρων. Για να γίνει αυτό θα πρέπει να εξεταστεί για ποιους δορυφόρους ικανοποιείται η παρακάτω μαθηματική συνθήκη, όπου $\boldsymbol{R} = (X_r, Y_r, Z_r)$ οι συντεταγμένες του δέκτη και $\boldsymbol{S} = (X_s, Y_s, Z_s)$ οι συντεταγμένες του υπό εξέταση δορυφόρου:

$$\|\boldsymbol{R}\| < \frac{\boldsymbol{S} * \boldsymbol{R}}{\|\boldsymbol{R}\|}$$

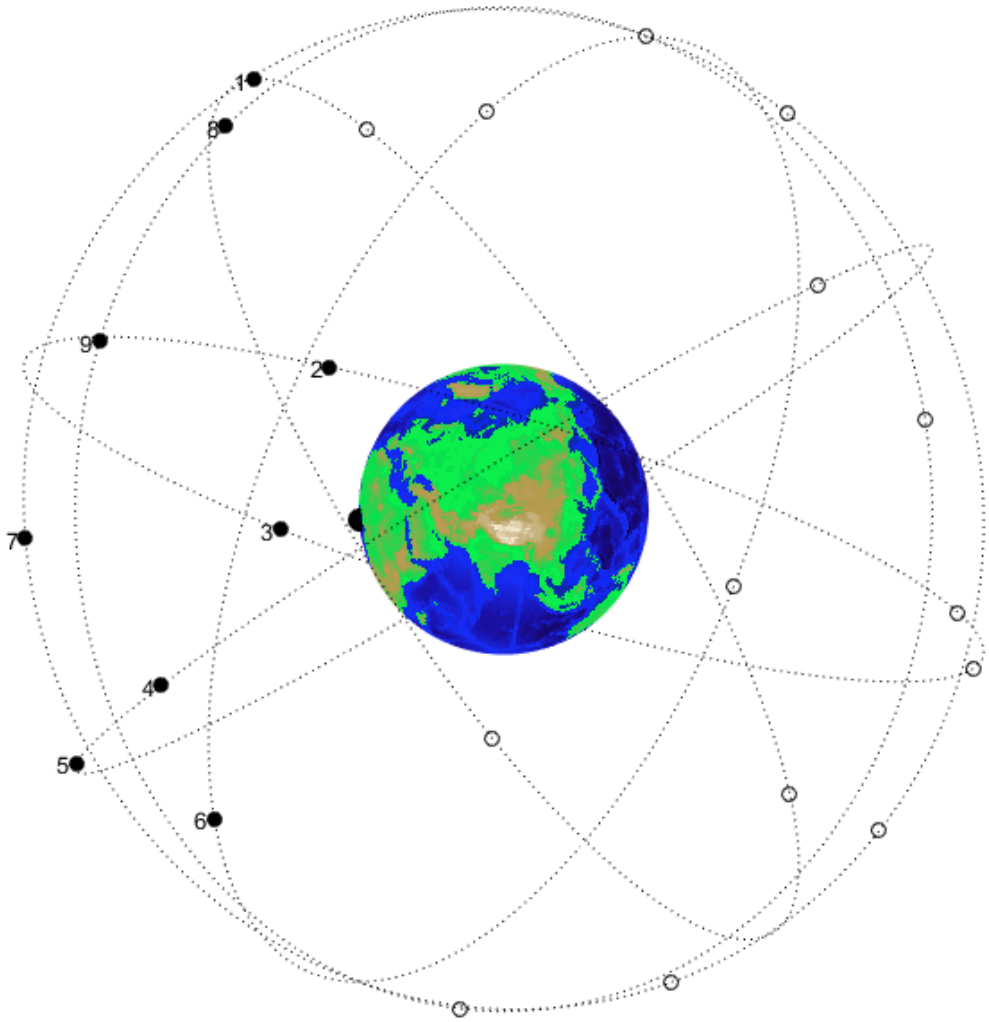
$$(X_r{}^2 + Y_r{}^2 + Z_r{}^2)^2 < \frac{X_r X_s + Y_r Y_s + Z_r Z_s}{(X_s{}^2 + Y_s{}^2 + Z_s{}^2)^2}$$

Ο υπόψιν τύπος ελέγχει αν η προβολή του διανύσματος των καρτεσιανών συντεταγμένων του δορυφόρου επί του διανύσματος των συντεταγμένων του δέκτη, είναι μεγαλύτερη από το μέτρο του διανύσματος των συντεταγμένων του δέκτη. Στο σχήμα 4.5 ο δορυφόρος S1 είναι σε οπτική επαφή με τον δέκτη καθώς πληροί αυτή τη συνθήκη. Αντίθετα η προβολή του S2 είναι μικρότερη από το μέτρο των συντεταγμένων του δέκτη και άρα δε βρίσκεται σε οπτική επαφή.



Σχήμα 4.5 Ο S1 έχει οπτική επαφή με το δέκτη, αντίθετα με τον S2.

Το αποτέλεσμα αυτού του «φιλτραρίσματος» φαίνεται στο σχήμα 4.6 όπου με οι αριθμημένες τελείες είναι οι δορυφόροι που έχουν οπτική επαφή με τον δέκτη, ο οποίος σημειώνεται με μαύρη τελεία πάνω στη γη.



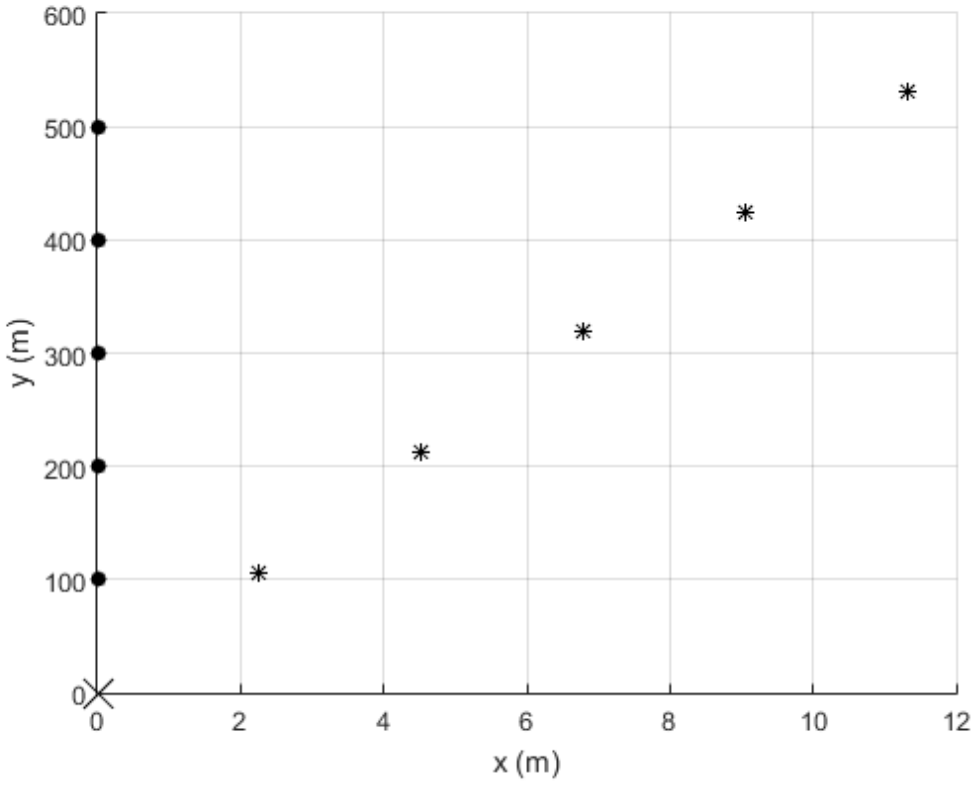
Σχήμα 4.6 Δορυφόροι με οπτική επαφή στον δέκτη.

4.3.2 Αλγόριθμος ελαχίστων τετραγώνων για προσδιορισμό θέσης

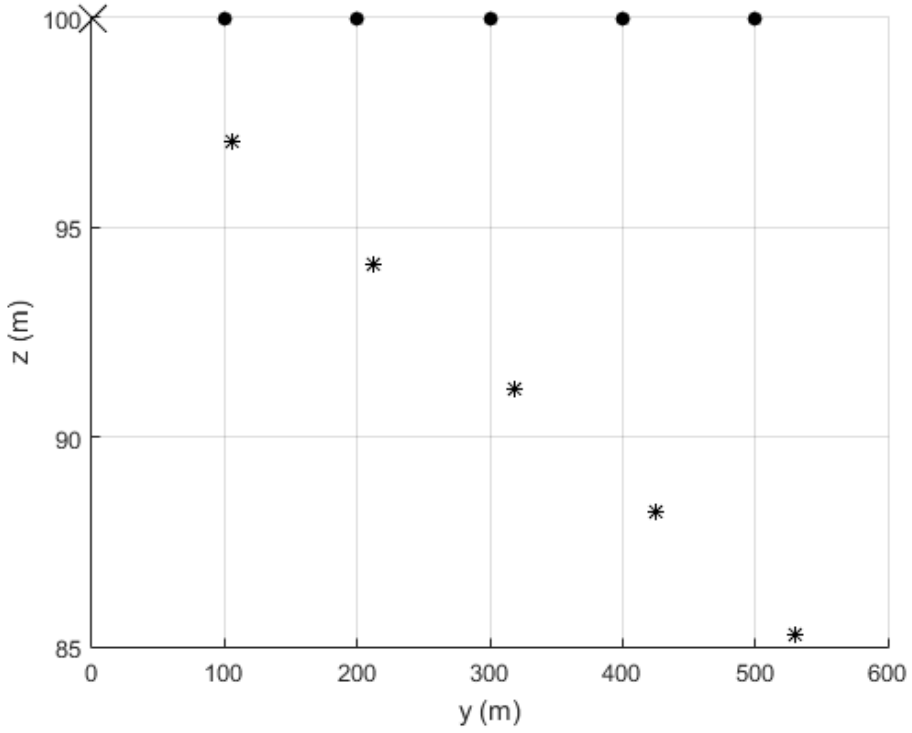
Στην πιο απλή περίπτωση ένας δέκτης προσδιορίζει τη θέση του εφαρμόζοντας τον αλγόριθμό των ελαχίστων τετραγώνων, ο οποίος περιεγράφηκε στη παράγραφο 2.3.2. Με την παραδοχή ότι δε κάνει χρήση κανενός αντίμετρου ο δέκτης αυτός είναι ευάλωτος σε οποιαδήποτε επίθεση.

Η σενάριο της προσομοίωσης περιλαμβάνει πέντε δέκτες, οι οποίοι τοποθετήθηκαν στην ίδια ευθεία ανά 100m ενώ στην αρχή των αξόνων και σε απόσταση 100m από τον πρώτο δέκτη τοποθετήθηκε η διάταξη.

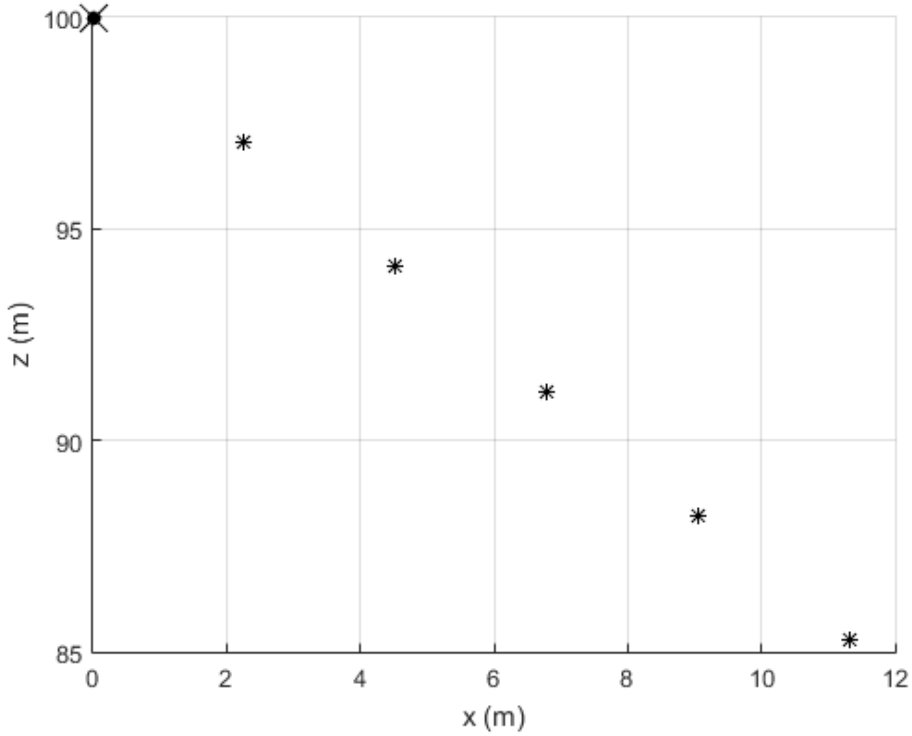
Στο πρώτο πείραμα η καθυστέρηση δt που εισήγαγε η διάταξη τέθηκε μηδενική. Επομένως η καθυστέρηση του σήματος στον δέκτη οφείλονταν μόνο στη διαφορά δρόμου, την διαφορά δηλαδή της διαδρομής που ακολουθεί το πραγματικό σήμα από τον δορυφόρο μέχρι τον δέκτη και της διαδρομής που ακολουθεί το καθυστερημένο σήμα μέσω της αναμετάδοσης που γίνεται από τον επιτιθέμενο. Στόχος της επίθεσης είναι να γίνει αναμετάδοση ενός μόνο δορυφορικού σήματος. Τα αποτελέσματα της προσομοίωσης δίδονται στο σχήμα 4.7, όπου με γεμάτο κύκλο είναι η φυσική θέση των δεκτών και με αστερίσκο σημειώνεται η εσφαλμένη θέση τους. Καθώς οι μετατοπίσεις μπορεί να συμβούν και στις τρεις διαστάσεις για την καλύτερη απεικόνιση χρησιμοποιήθηκαν τρία διαφορετικά διαγράμματα.



(α)



(β)

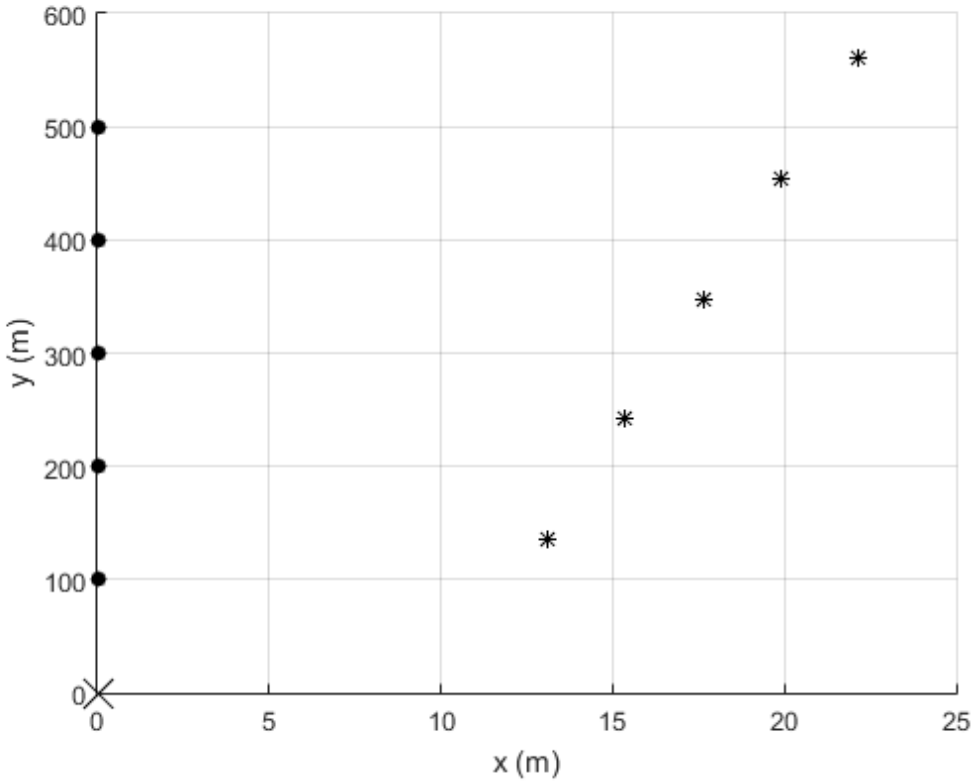


(γ)

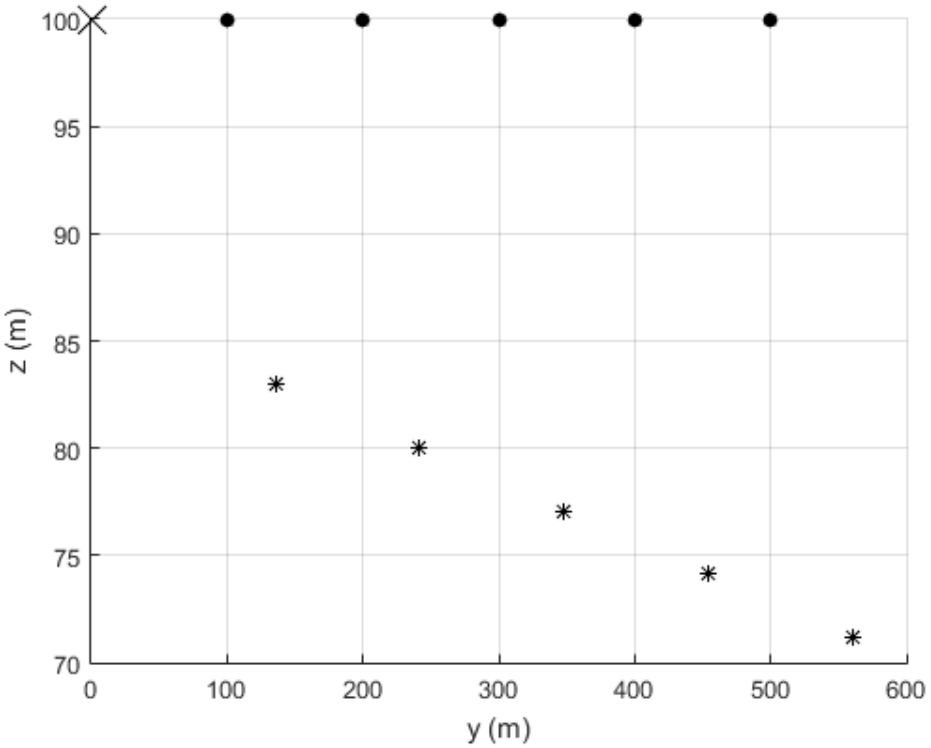
Σχήμα 4.7 (α), (β), (γ) Σχεδιάγραμμα όπου φαίνονται οι φυσικές (κύκλοι) και εσφαλμένες (αστερίσκοι) θέσεις των δεκτών-θυμάτων, με άξονες (χ, y), (y, z) και (x, z) αντίστοιχα.

Η μέγιστη μετατόπιση θέσης που παρατηρείται ανήκει στον πιο απομακρυσμένο δέκτη και είναι της τα 35m. Για τον ποιο κοντινό δέκτη η μετατόπιση δεν ξεπερνά τα 5m. Αυτό είναι αναμενόμενο καθώς όσο ο δέκτης-θύμα απομακρύνεται από τον επιτιθέμενο μεγαλώνει και η διαφορά δρόμων, άρα και η μετατόπιση της εσφαλμένης θέσης από τη φυσική. Η μετατόπιση που παρατηρείται σε κάθε άξονα εξαρτάται ισχυρά από την γεωμετρία του συστήματος, δηλαδή τη θέση του δορυφόρου και του επιτιθέμενου ως προς τον δέκτη.

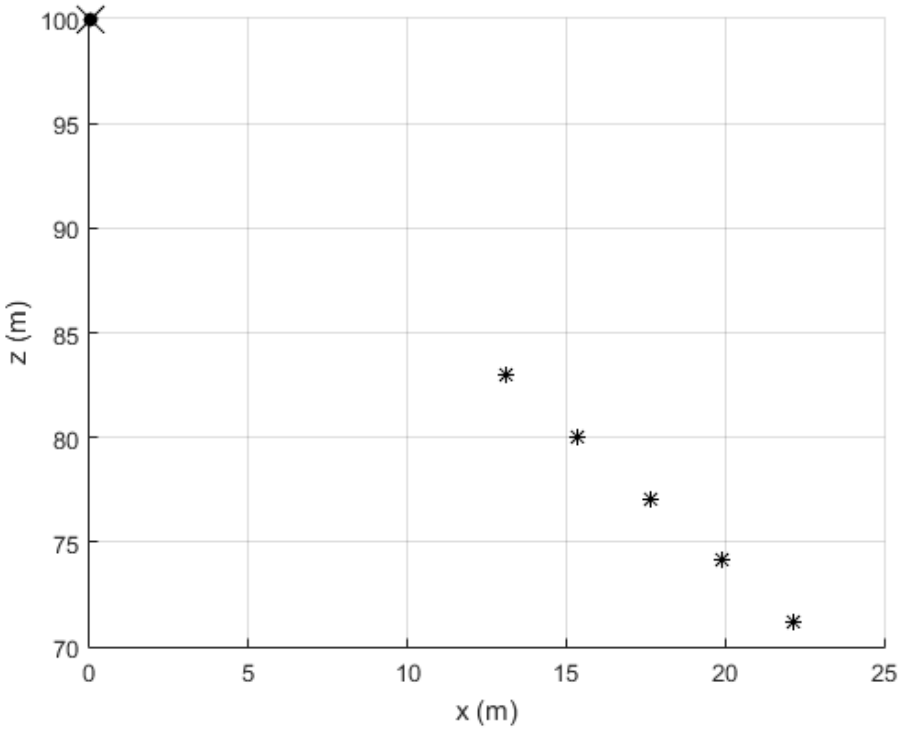
Στη συνέχεια έγινε το ίδιο πείραμα με τη διαφορά ότι η διάταξη εισήγαγε καθυστέρηση 333ns. Το αποτέλεσμα της προσομοίωσης φαίνεται στο σχήμα 4.8.



(α)



(β)

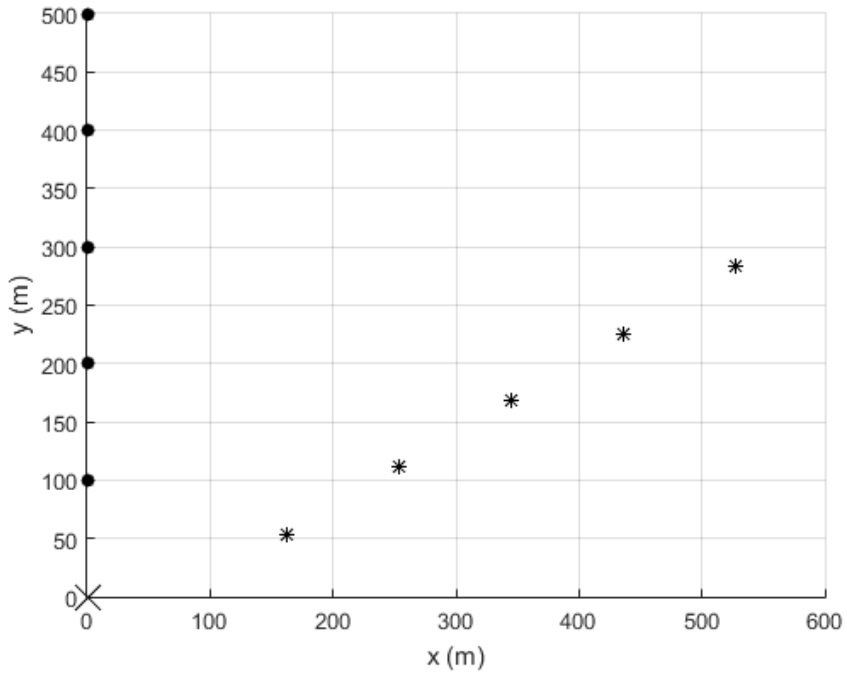


(γ)

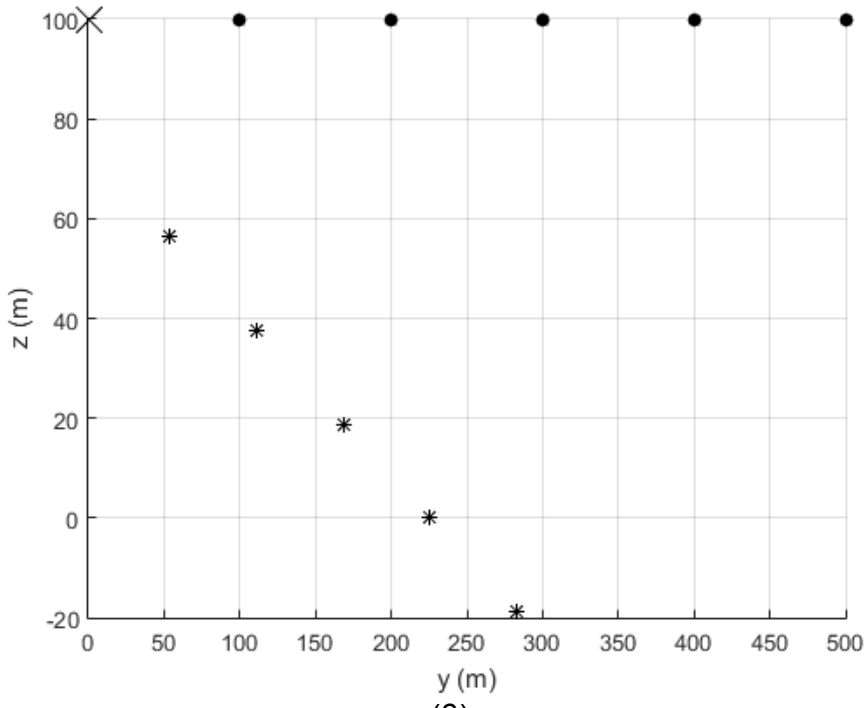
Σχήμα 4.8 (α), (β), (γ) Σχεδιάγραμμα όπου φαίνονται οι φυσικές (κύκλοι) και εσφαλμένες (αστερίσκοι) θέσεις των δεκτών-θυμάτων, με άξονες (χ, y), (y, z) και (x, z) αντίστοιχα.

Η καθυστέρηση των 333ns αντιστοιχεί σε διαφορά δρόμων κατά προσέγγιση 100m. Η μέγιστη μετατόπιση θέσης που παρατηρείται αυτή τη φορά είναι στα 70m για τον πιο απομακρυσμένο παρατηρητή.

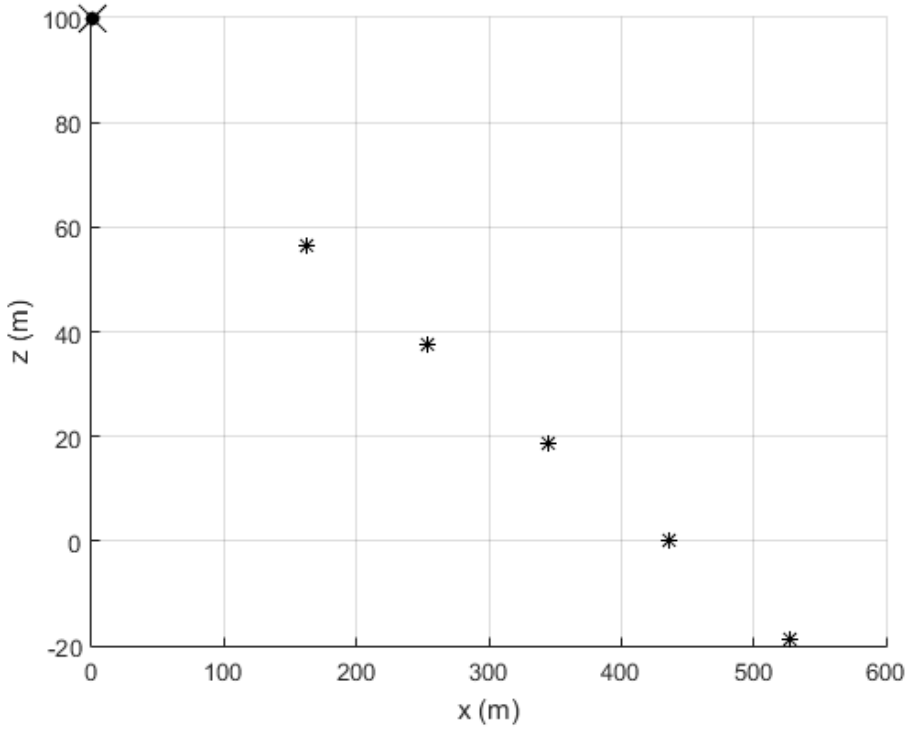
Στη συνέχεια εισήχθη καθυστέρηση 333ns σε σήματα δύο δορυφόρων. Το αποτέλεσμα της προσομοίωσης φαίνεται στο σχήμα 4.9.



(α)



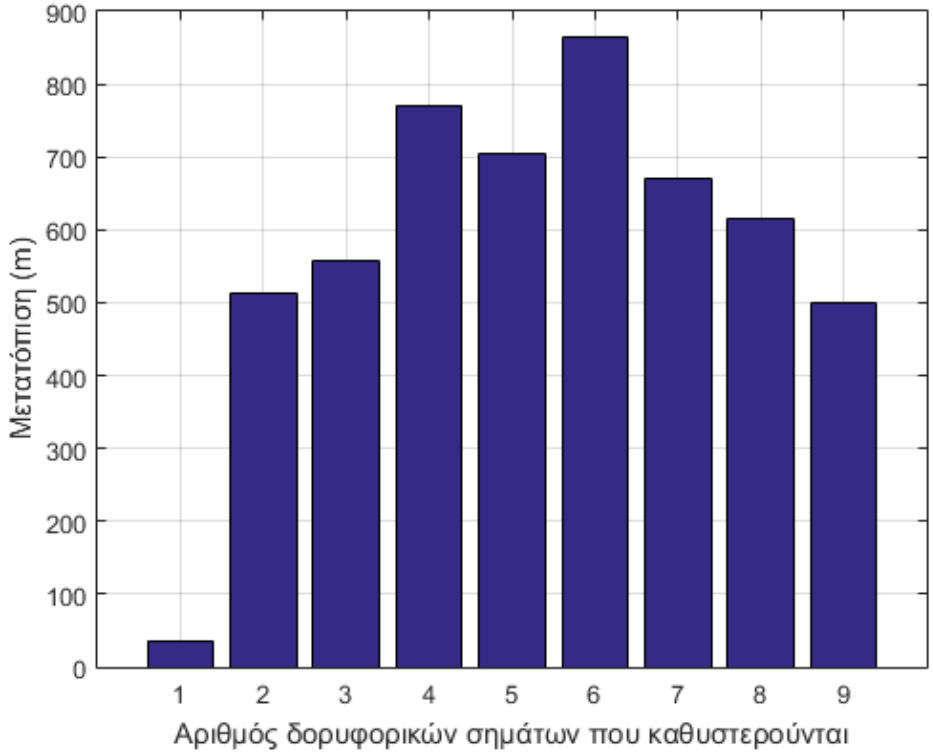
(β)



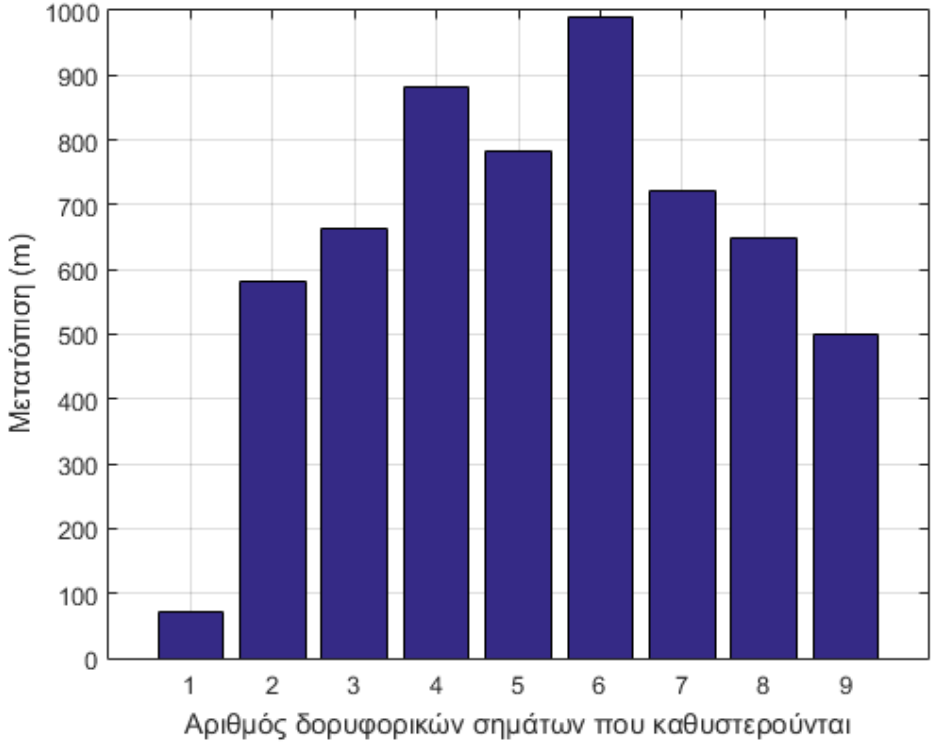
(γ)

Σχήμα 4.9 (α), (β), (γ) Σχεδιάγραμμα όπου φαίνονται οι φυσικές (κύκλοι) και εσφαλμένες (αστερίσκοι) θέσεις των δεκτών-θυμάτων, με άξονες (χ, y), (y, z) και (x, z) αντίστοιχα.

Η μέγιστη μετατόπιση θέσης που αντιστοιχεί στον πιο απομακρυσμένο δέκτη ήταν αυτή τη φορά τα 583m. Για τον ίδιο δέκτη η συνολική μετατόπιση συγκριτικά με τον αριθμό των δορυφορικών σημάτων που καθυστερούνται όταν η διάταξη δεν εισάγει εσωτερική καθυστέρηση, δίδεται στο σχήμα 4.10. Είναι λογικό η μετατόπιση να μη μεταβάλλεται γραμμικά με τον αριθμό των δορυφόρων, καθώς οι θέσεις των δορυφόρων ως προς τον δέκτη δεν είναι ομοιόμορφα κατανεμημένες. Στην τελευταία περίπτωση όπου καθυστερούνται τα σήματα και των εννιά δορυφόρων, η μετατόπιση είναι ακριβώς όση η απόσταση του δέκτη από τη διάταξη. Αυτό συμβαίνει γιατί όπως προβλέφθηκε και θεωρητικά, ο δέκτης σε αυτήν την περίπτωση θα πιστεύει εσφαλμένα ότι βρίσκεται πάνω στη θέση του επιτιθέμενου. Στο σχήμα 4.11 δίδεται η συνολική μετατόπιση συναρτήσει του αριθμού των δορυφόρων όταν η διάταξη εισάγει εσωτερική καθυστέρηση 333ns.



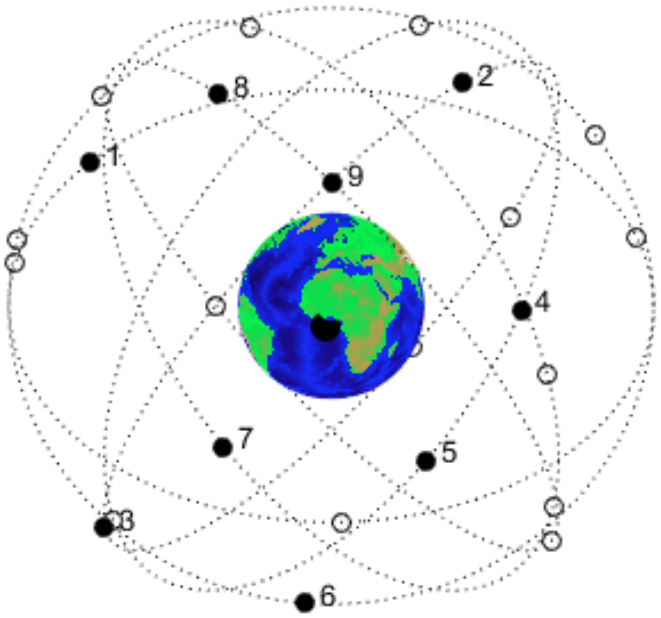
Σχήμα 4.10 Μετατόπιση σε σχέση με τον αριθμό των σημάτων που επηρεάζονται με μηδενική καθυστέρηση.



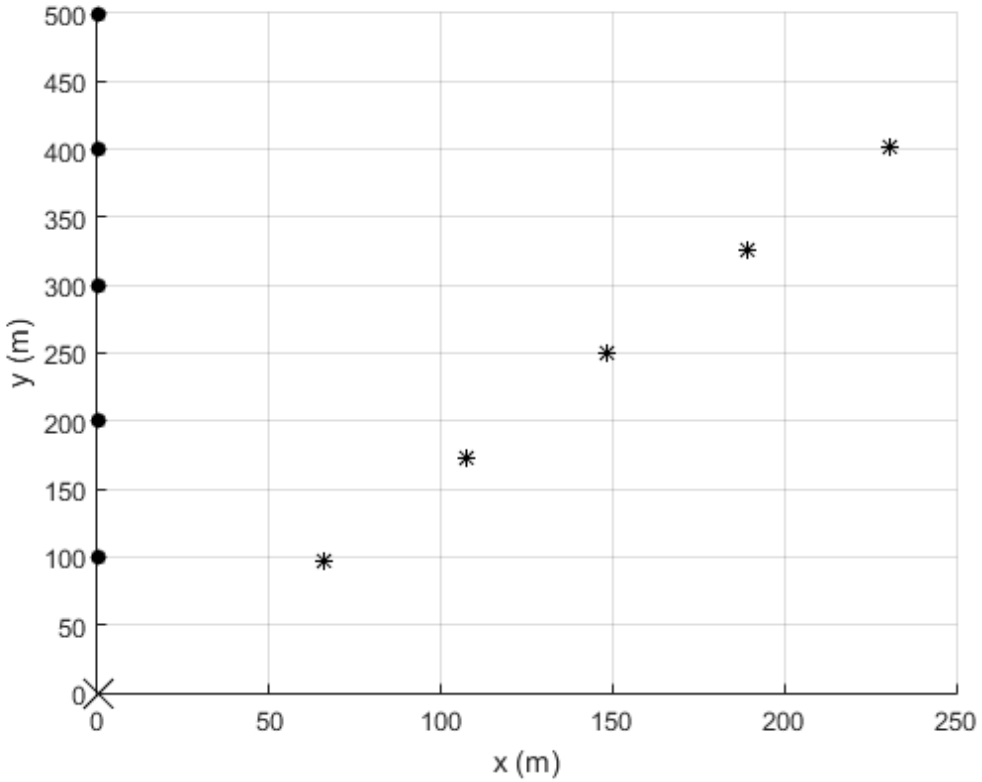
Σχήμα 4.11 Μετατόπιση σε σχέση με τον αριθμό των σημάτων που επηρεάζονται με καθυστέρηση 333ns.

Όλες οι προηγούμενες προσομοιώσεις θεωρούν ότι τα σήματα των δορυφόρων μπορούν να απομονωθούν από τα υπόλοιπα και να επανεκπεμφθούν με την εισαγωγή καθυστέρησης. Αυτό προϋποθέτει την χρησιμοποίηση κεραιών λήψης μεγάλης κατευθυντικότητας ώστε κάθε μία να στοχεύει έναν συγκεκριμένο δορυφόρο. Στη συνέχεια γίνεται μίξη των σημάτων αυτών ενίσχυση και εκπομπή.

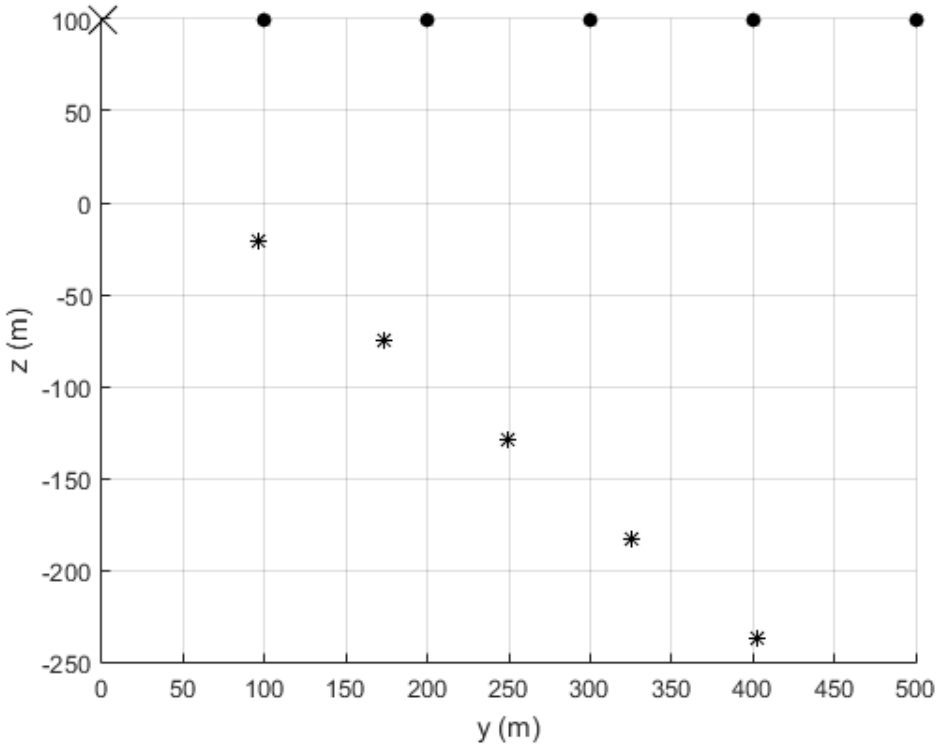
Στην περίπτωση που η κεραία λήψης είναι μια λιγότερο κατευθυντική κεραία η επίθεση θα μπορούσε να πραγματοποιηθεί στοχεύοντας μια ομάδα δορυφόρων. Όπως φαίνεται στο σχήμα 4.12 οι δορυφόροι 1, 2, 8, 9 βρίσκονται σε κοντινές γωνιακές. Στοχεύοντας αυτό το σύνολο δορυφόρων και θεωρώντας ότι η συσκευή εισάγει καθυστέρηση ίση με 333ns προκύπτουν τα παρακάτω διαγράμματα, σχήμα 4.13. Η μέγιστη μετατόπιση που προκύπτει είναι τα 420m.



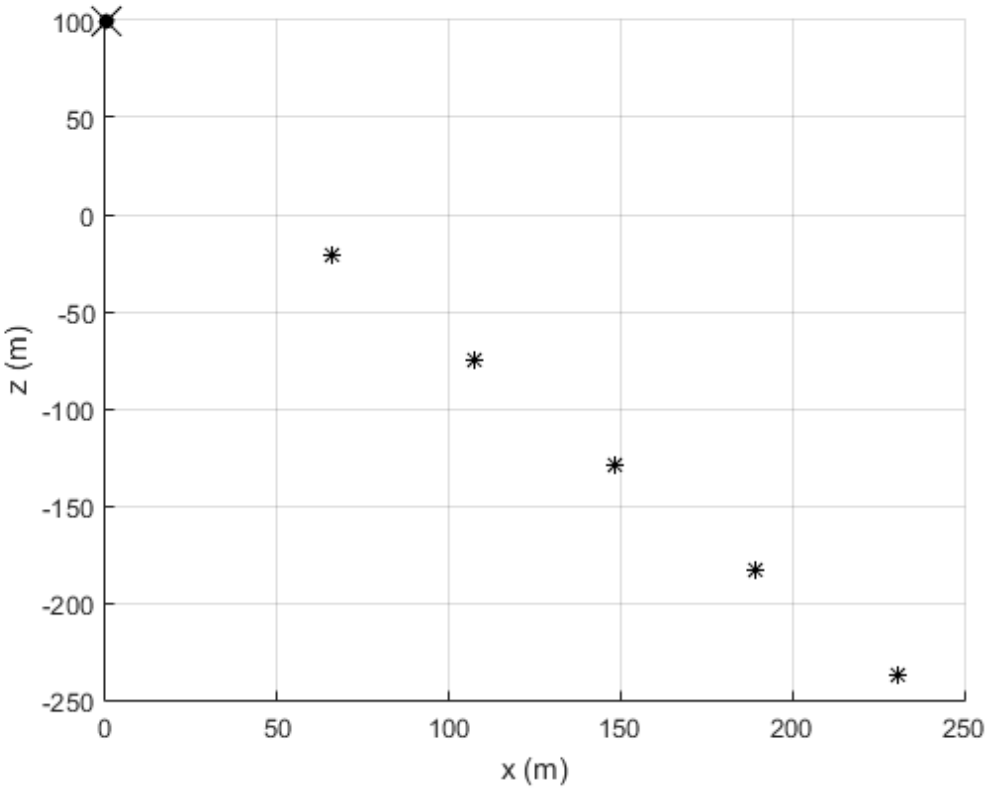
Σχήμα 4.12 Απεικόνιση των δορυφόρων με οπτική επαφή.


500
450
400
350
300
250
200
150
100
50
0
y (m)
0
50
100
150
200
250
x (m)

(α)


100
50
0
-50
-100
-150
-200
-250
z (m)
0
50
100
150
200
250
300
350
400
450
500
y (m)

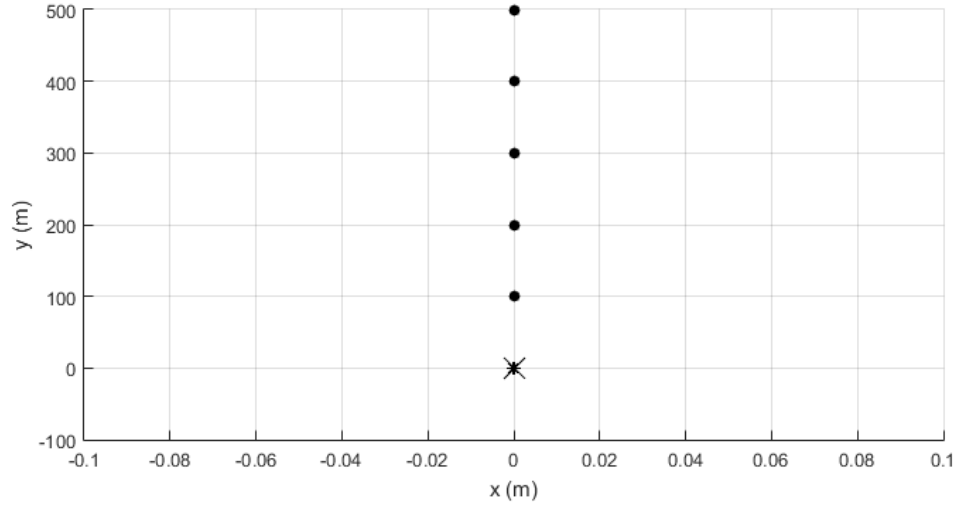
(β)



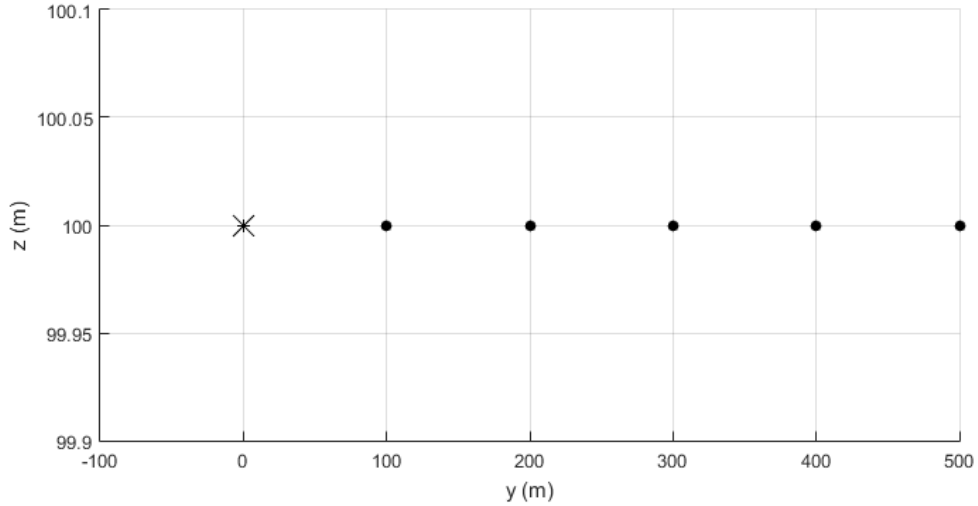
(γ)

Σχήμα 4.13 (α), (β), (γ) Σχεδιάγραμμα όπου φαίνονται οι φυσικές (κύκλοι) και εσφαλμένες (αστερίσκοι) θέσεις των δεκτών-θυμάτων, με άξονες (χ, y), (y, z) και (x, z) αντίστοιχα.

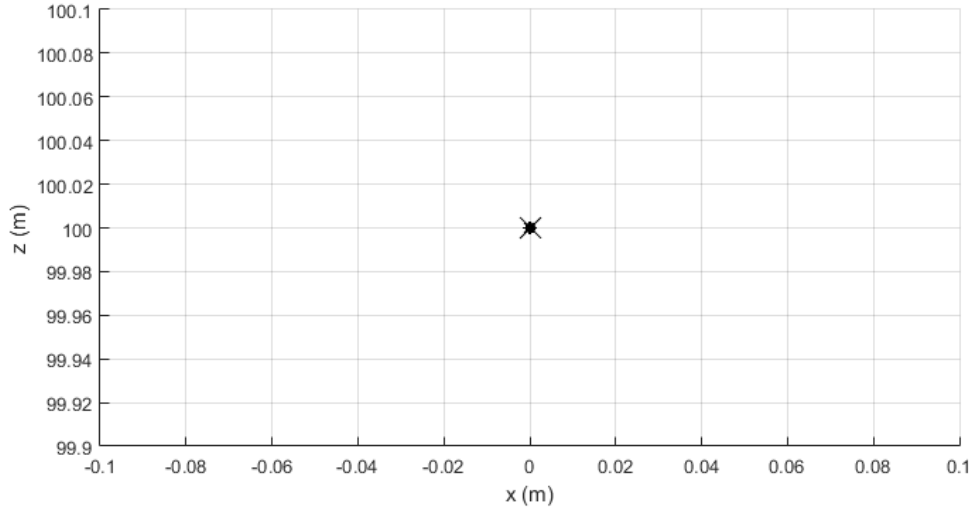
Τέλος εξετάζεται η περίπτωση κατά την οποία όλα τα λαμβανόμενα σήματα επανεκπέμπονται από τη διάταξη με την εισαγωγή καθυστέρησης ίσης με 333ns. Όπως αποδείχθηκε στη παράγραφο 4.2.1 αυτό οδηγεί στο να υπολογίζει ο δέκτης εσφαλμένα ότι βρίσκεται πάνω στη θέση της κεραίας λήψης του επιτιθέμενου σχήμα 4.14.



(α)



(β)



(γ)

Σχήμα 4.14 (α), (β), (γ) Σχεδιάγραμμα όπου φαίνονται οι φυσικές (κύκλοι) και εσφαλμένες (αστερίσκοι) θέσεις των δεκτών-θυμάτων, με άξονες (χ, y), (y, z) και (x, z) αντίστοιχα.

4.3.3 Αλγόριθμος ελαχίστων τετραγώνων με βάρη

Στην προηγούμενη παράγραφο εξετάστηκε η πιο απλή περίπτωση, κατά την οποία ο δέκτης υπολόγιζε τη θέση του με τον αλγόριθμο ελαχίστων τετραγώνων. Ο αλγόριθμος αυτός μπορεί να λειτουργήσει σωστά και να δώσει αξιόπιστη λύση μόνο όταν όλες οι ψευδοαποστάσεις έχουν την ίδια διασπορά. Σε αυτή τη περίπτωση ο πίνακας διασποράς των ψευδοαποστάσεων έχει την παρακάτω μορφή.

$$\boldsymbol{\Sigma_p} = \begin{bmatrix} \sigma^2 & 0 & 0 & 0 \\ 0 & \sigma^2 & .. & 0 \\ : & : & : & 0 \\ 0 & 0 & 0 & \sigma^2 \end{bmatrix}$$

Όπου $\sigma^2 = \sigma_i^2$, $i = 0,1,$ ... και σ_i^2 η διασπορά της ψευδοαπόστασης p_i

Αντικαθιστώντας τη λύση στο σύστημα των ψευδοαποστάσεων η κάθε εξίσωση του συστήματος θα απέχει το ίδιο από το αποτέλεσμα, δηλαδή θα ικανοποιούνται οι παρακάτω συνθήκες.

$$\|\boldsymbol{H_i x} - p_i\| \cong \left\|\boldsymbol{H_j x} - p_j\right\|$$

Όπου $\boldsymbol{H_{i,j}}$ η i, j-οστή γραμμή του πίνακα Η.

Στην περίπτωση όμως όπου επιχειρηθεί να εισαχθεί τεχνητά καθυστέρηση σε κάποιο σήμα δε θα ισχύει η προηγούμενη συνθήκη, καθώς η ψευδοαπόσταση αυτού του σήματος δε θα συμβαδίζει με τις υπόλοιπες ψευδοαποστάσεις.

Για να αντιμετωπιστεί αυτή η κατάσταση μπορεί να υπολογιστεί η λύση με τον αλγόριθμο ελαχίστων τετραγώνων και στη συνέχεια να υπολογιστεί ο παρακάτω πίνακας βαρών

$$\boldsymbol{\Sigma_p} = \begin{bmatrix} \|\boldsymbol{H_1 x} - p_1\| & 0 & 0 & 0 \\ 0 & \|\boldsymbol{H_1 x} - p_1\| & .. & 0 \\ : & : & : & 0 \\ 0 & 0 & 0 & \|\boldsymbol{H_1 x} - p_1\| \end{bmatrix}$$

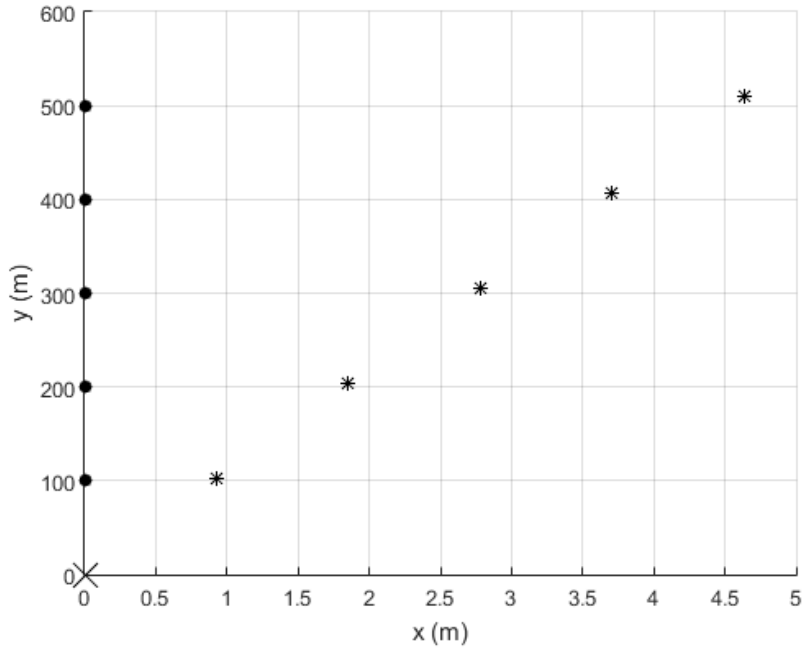
Η βελτιωμένης ακρίβεια λύση θα δοθεί από το παρακάτω σύστημα εξισώσεων

$$\boldsymbol{\Delta x} = \ (H^T C\ H)^{-1} H^T C\ \boldsymbol{\Delta x}$$

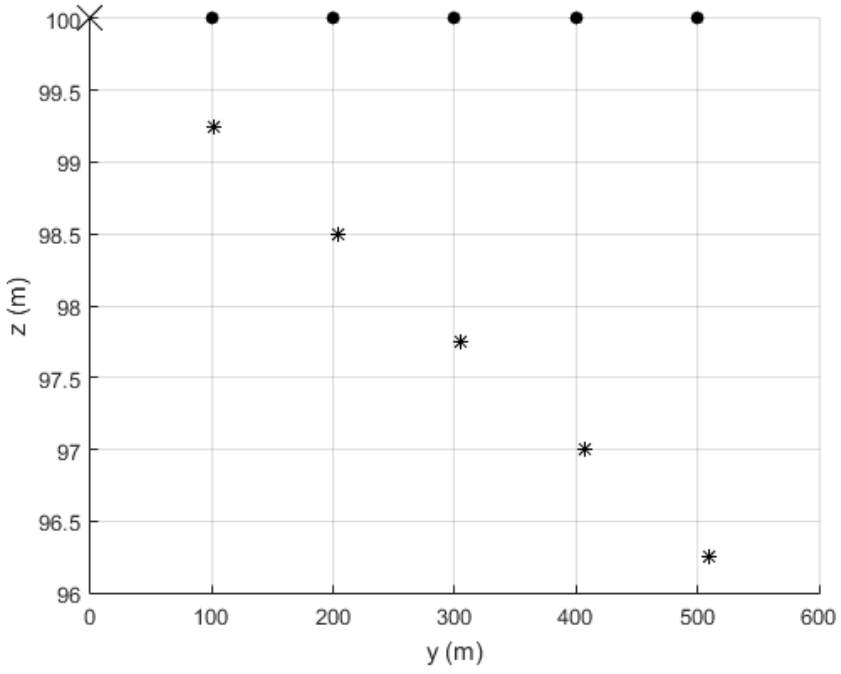
Όπου C είναι ο αντίστροφος πίνακας του πίνακα διασποράς, δηλαδή

$$C = \boldsymbol{\Sigma_p}^{-1}$$

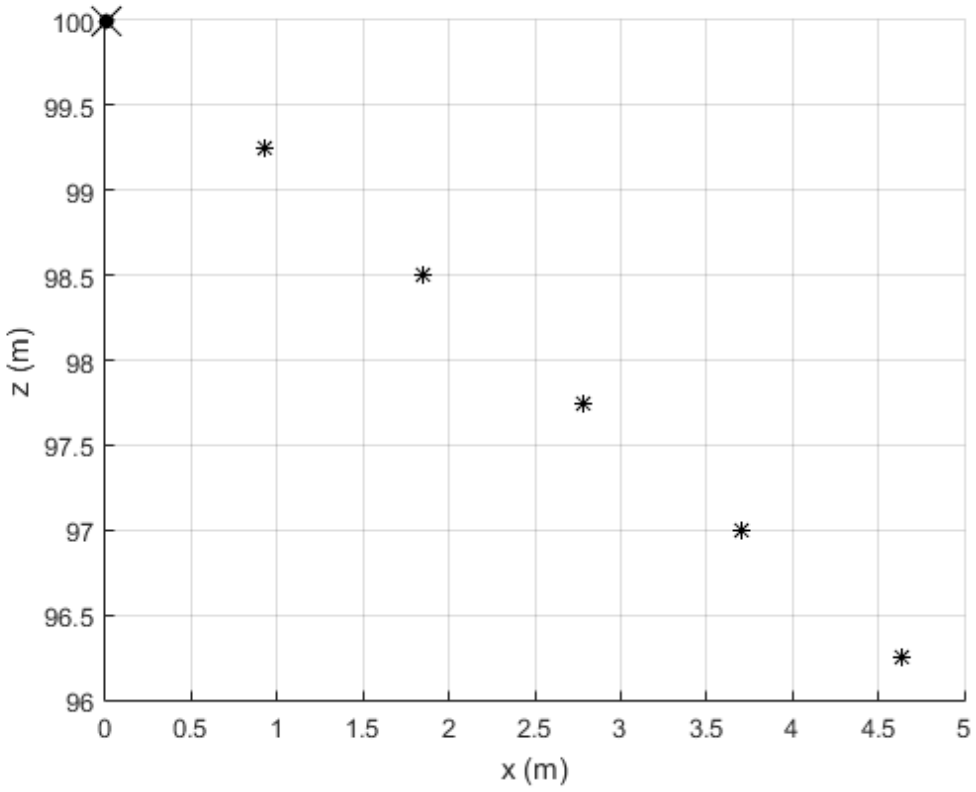
Το σενάριο της προσομοίωσης είναι το ίδιο με αυτό της προηγούμενης παραγράφου. Αρχικά θεωρήθηκε ότι η διάταξη δεν εισάγει εσωτερική καθυστέρηση και αναμεταδίδεται ένα μόνο δορυφορικό σήμα σχήμα 4.15.



(α)



(β)

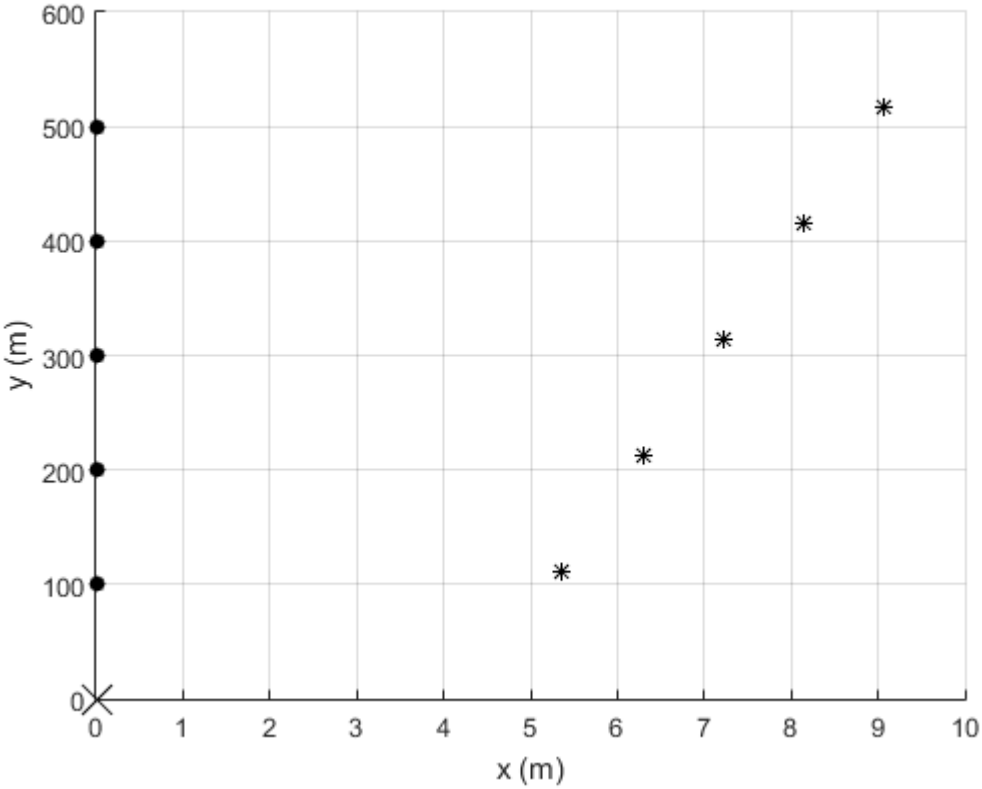


(γ)

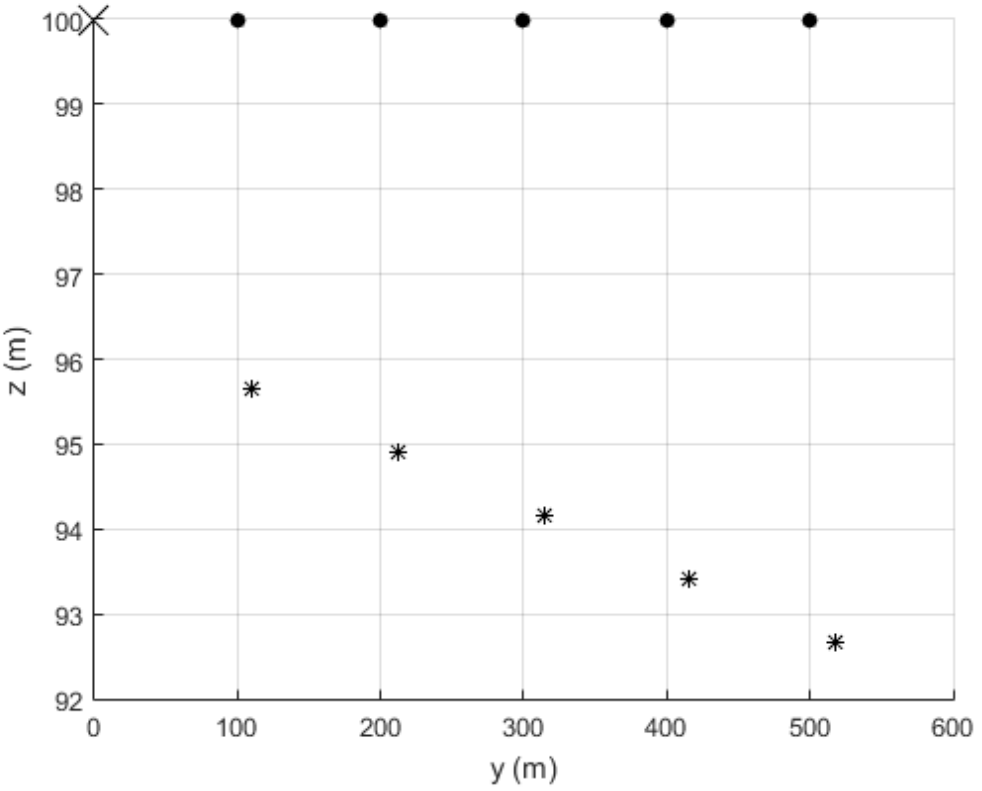
Σχήμα 4.15 (α), (β), (γ) Σχεδιάγραμμα όπου φαίνονται οι φυσικές (κύκλοι) και εσφαλμένες (αστερίσκοι) θέσεις των δεκτών-θυμάτων, με άξονες (χ, y), (y, z) και (x, z) αντίστοιχα.

Η μεγαλύτερη μετατόπιση που προκύπτει από τον αλγόριθμο είναι 10m. Η πρόβλεψη είναι σαφώς βελτιωμένη σε σχέση με αυτή του απλού αλγορίθμου η ο οποία είναι στα 35m.

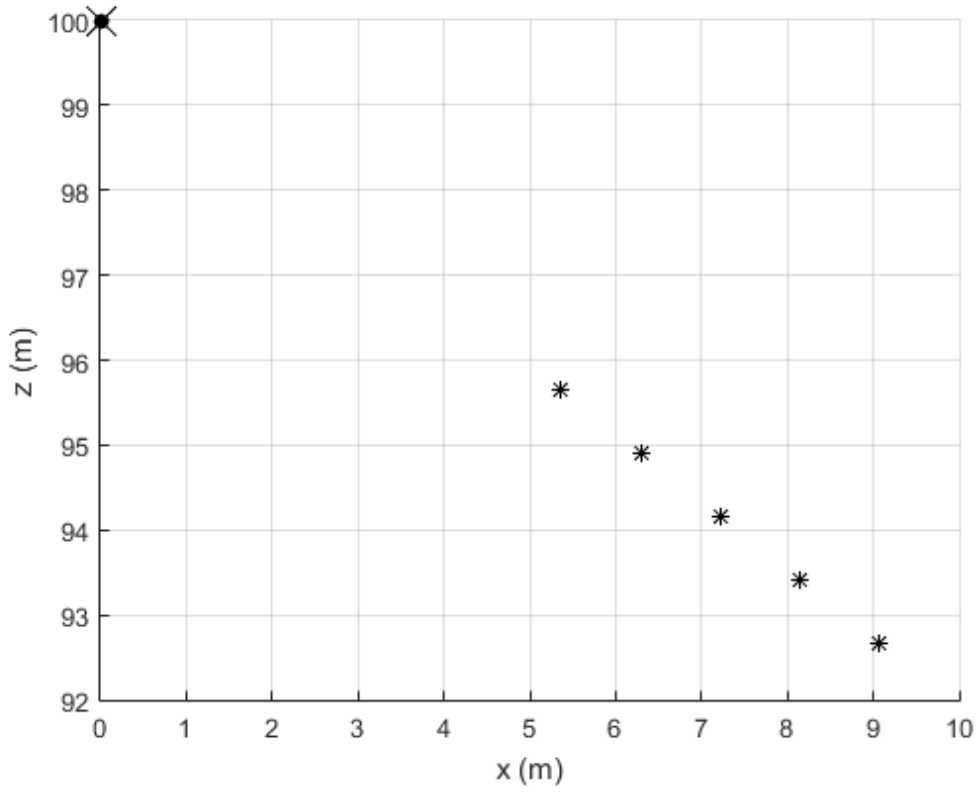
Στη συνέχεια έγινε το ίδιο πείραμα με τη διαφορά ότι η διάταξη εισήγαγε καθυστέρηση 333ns. Το αποτέλεσμα της προσομοίωσης φαίνεται στο σχήμα 4.16.


600
500
400
300
200
100
0
y (m)
0
1
2
3
4
5
6
7
8
9
10
x (m)

(α)


100
99
98
97
96
95
94
93
92
z (m)
0
100
200
300
400
500
600
y (m)

(β)

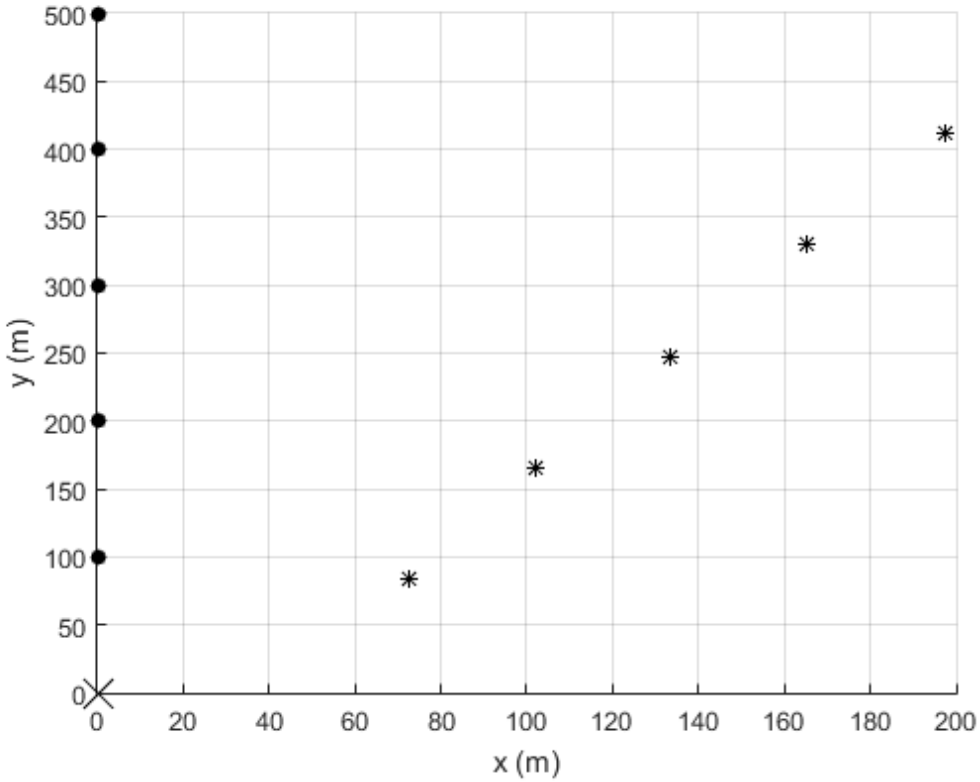


(γ)

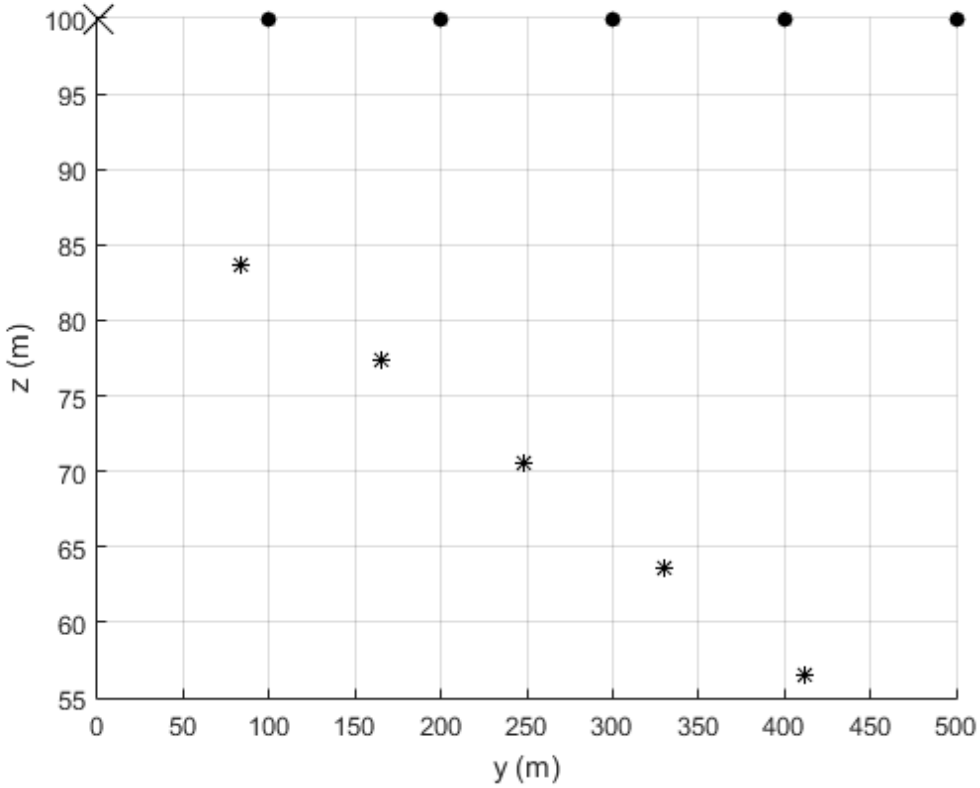
Σχήμα 4.16 (α), (β), (γ) Σχεδιάγραμμα όπου φαίνονται οι φυσικές (κύκλοι) και εσφαλμένες (αστερίσκοι) θέσεις των δεκτών-θυμάτων, με άξονες (χ, y), (y, z) και (x, z) αντίστοιχα.

Η μεγαλύτερη μετατόπιση αυτή τη φορά είναι 21m. Η πρόβλεψη είναι σαφώς βελτιωμένη σε σχέση με αυτή του απλού αλγορίθμου που ήταν στα 70m.

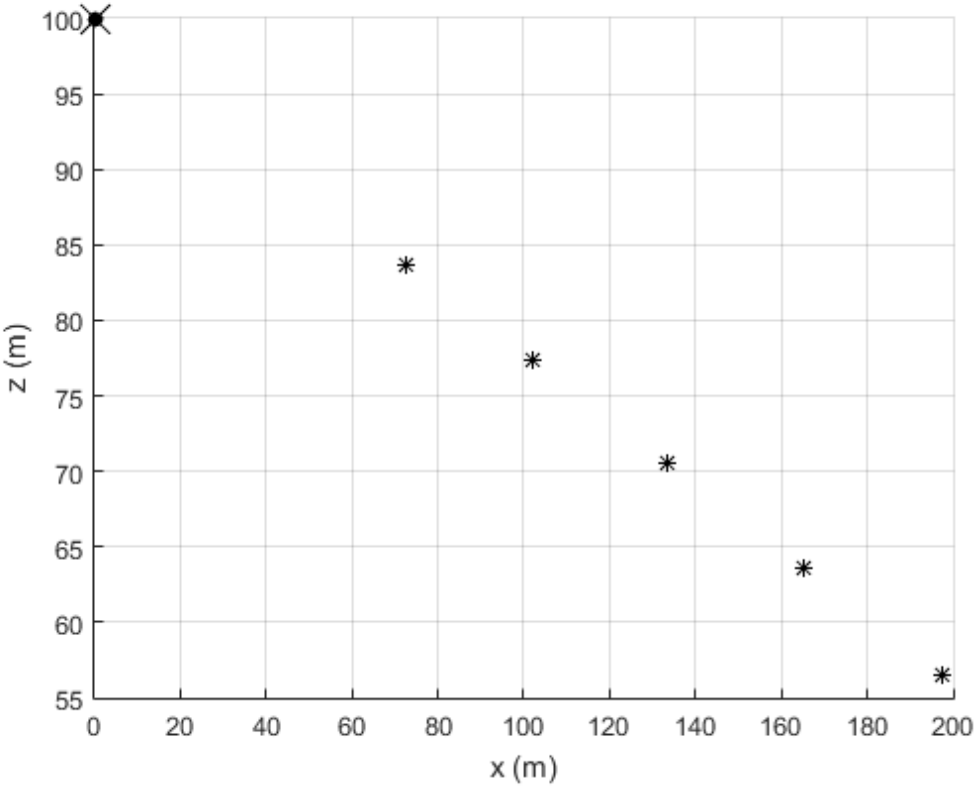
Στη συνέχεια εισήχθη καθυστέρηση 333ns σε σήματα δύο δορυφόρων. Το αποτέλεσμα της προσομοίωσης φαίνεται στο σχήμα 4.17.


y (m)
x (m)
0
50
100
150
200
250
300
350
400
450
500
0
20
40
60
80
100
120
140
160
180
200

(α)


z (m)
y (m)
55
60
65
70
75
80
85
90
95
100
0
50
100
150
200
250
300
350
400
450
500

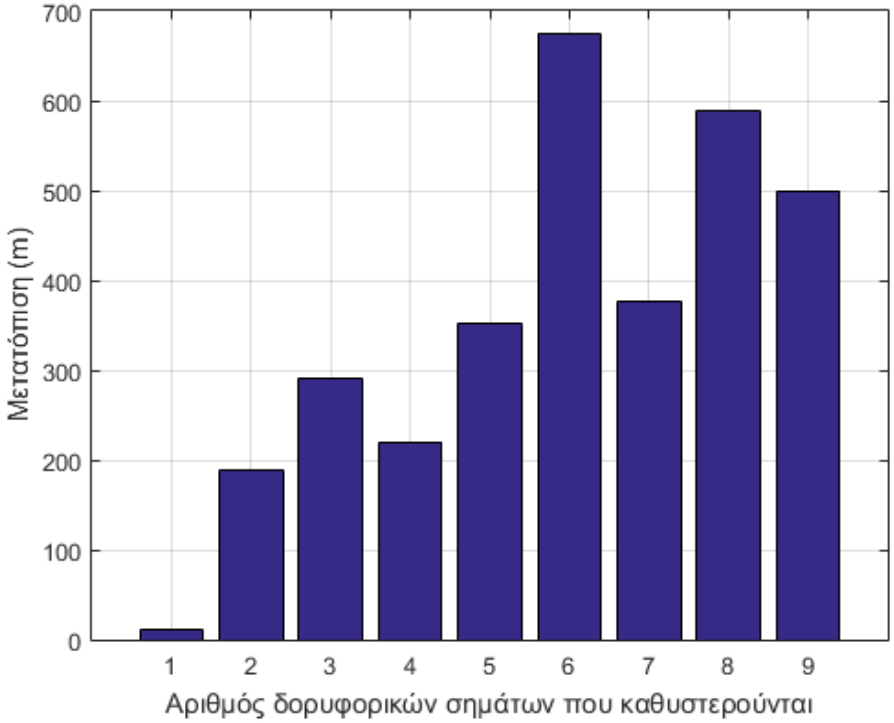
(β)



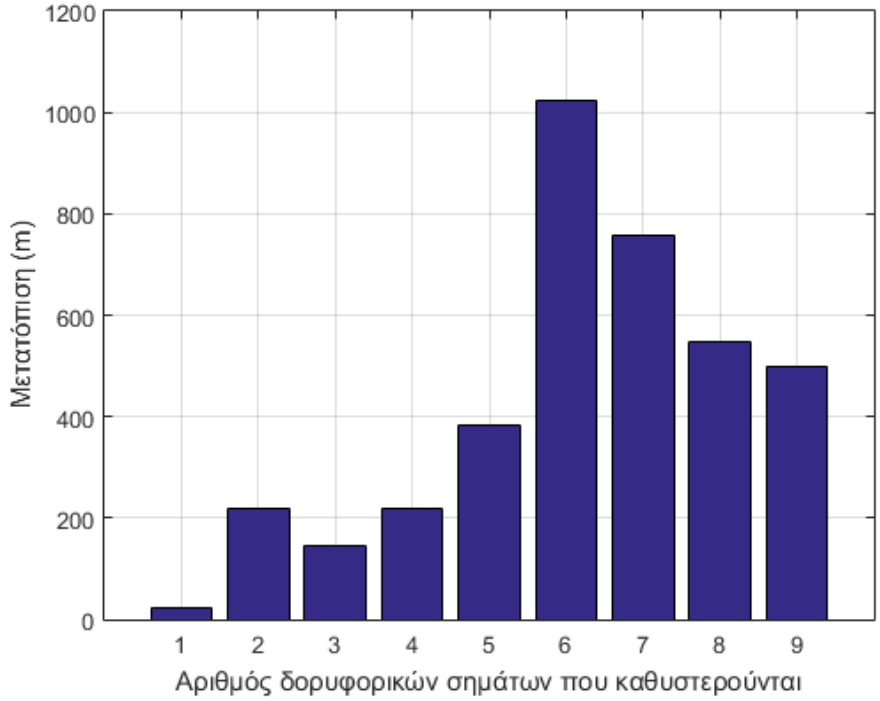
(γ)

Σχήμα 4.17 (α), (β), (γ) Σχεδιάγραμμα όπου φαίνονται οι φυσικές (κύκλοι) και εσφαλμένες (αστερίσκοι) θέσεις των δεκτών-θυμάτων, με άξονες (χ, y), (y, z) και (x, z) αντίστοιχα.

Η μεγαλύτερη μετατόπιση αυτή τη φορά είναι μόλις 22m, έναντί 70m που ήταν η πρόβλεψη του απλού αλγορίθμου. Για τον ίδιο δέκτη η συνολική μετατόπιση συγκριτικά με τον αριθμό των δορυφορικών σημάτων που καθυστερούνται όταν η διάταξη δεν εισάγει εσωτερική καθυστέρηση, δίδεται στο σχήμα 4.18. Είναι λογικό η μετατόπιση να μη μεταβάλλεται γραμμικά με τον αριθμό των δορυφόρων, καθώς οι θέσεις των δορυφόρων ως προς τον δέκτη δεν είναι ομοιόμορφα κατανεμημένες. Στην τελευταία περίπτωση όπου καθυστερούνται τα σήματα και των εννιά δορυφόρων, η μετατόπιση είναι ακριβώς όση η απόσταση του δέκτη από τη διάταξη. Αυτό συμβαίνει γιατί όπως προβλέφθηκε και θεωρητικά ο δέκτης σε αυτήν την περίπτωση θα πιστεύει εσφαλμένα ότι βρίσκεται πάνω στη θέση του επιτιθέμενου. Στο σχήμα 4.19 δίδεται η συνολική μετατόπιση συναρτήσει του αριθμού των δορυφόρων όταν η διάταξη εισάγει εσωτερική καθυστέρηση 333ns.

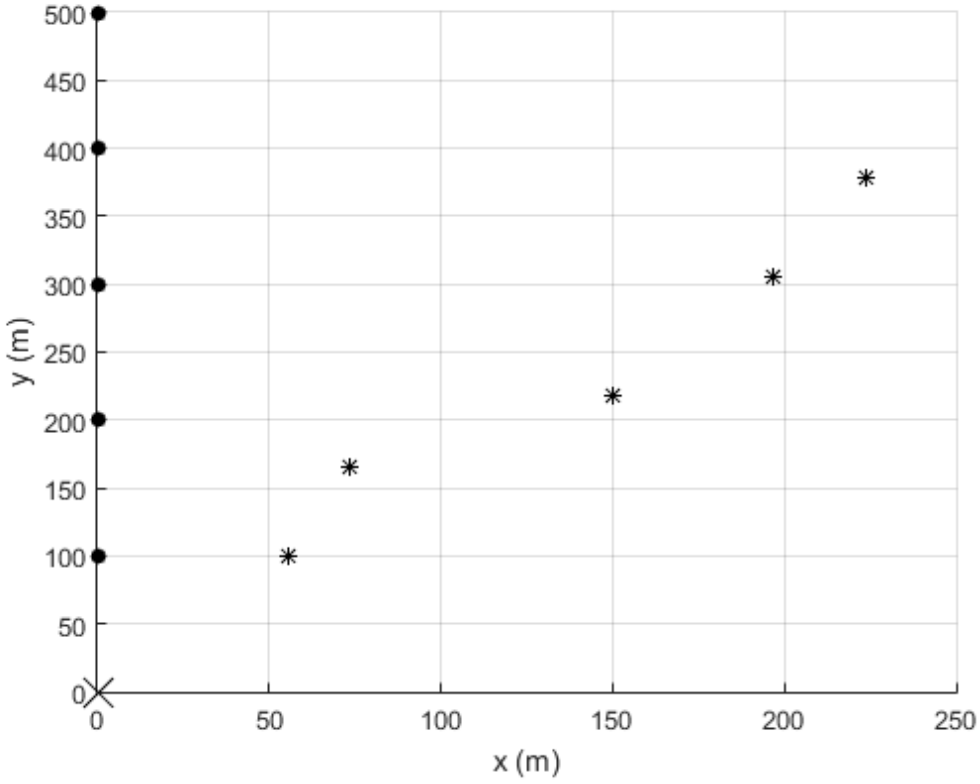


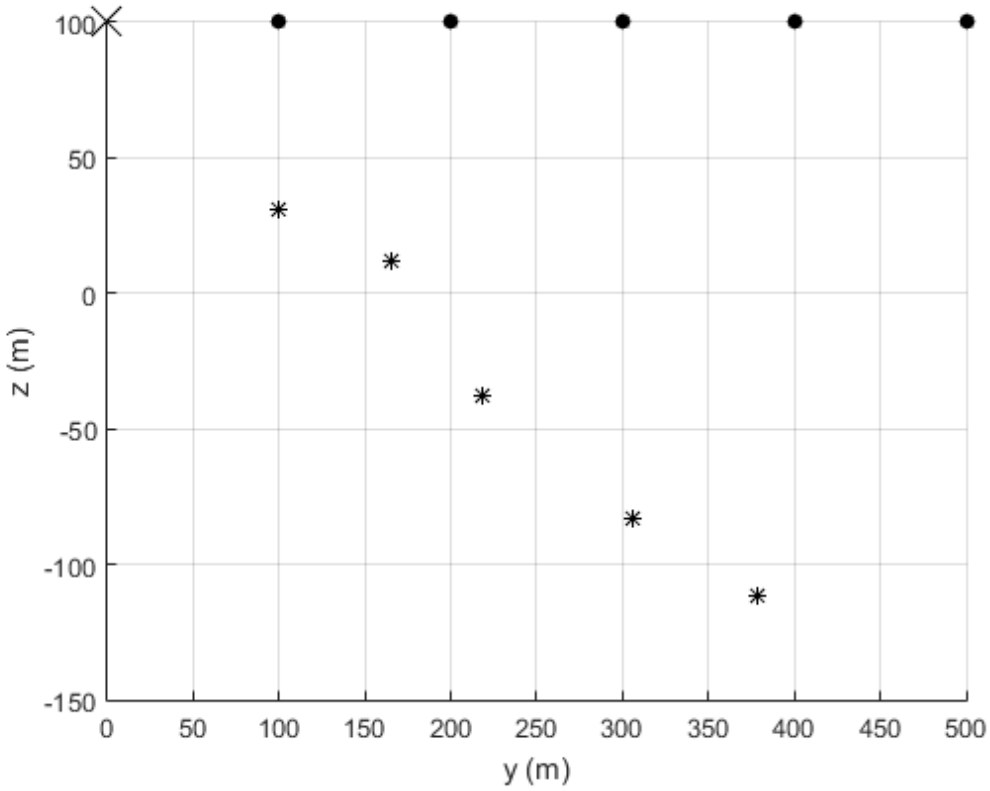
Σχήμα 4.18 Μετατόπιση σε σχέση με τον αριθμό των σημάτων που επηρεάζονται με μηδενική καθυστέρηση.

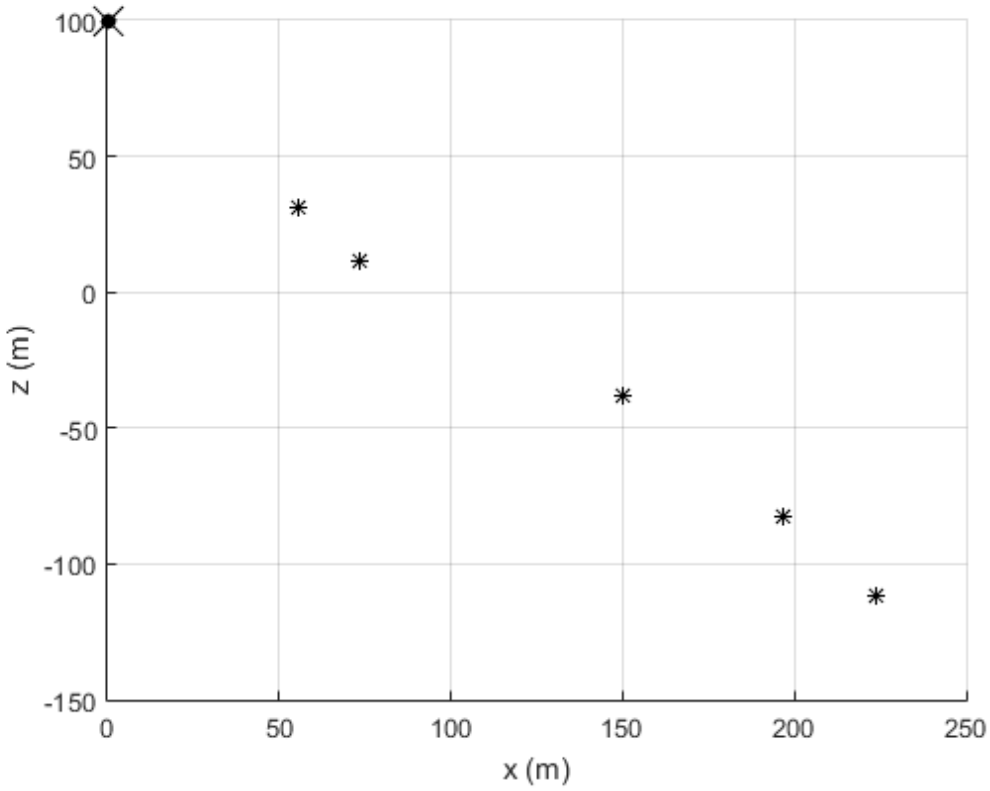


Σχήμα 4.19 Μετατόπιση σε σχέση με τον αριθμό των σημάτων που επηρεάζονται με καθυστέρηση 333ns.

Τέλος εξάγονται τα αποτελέσματα του πειράματος όταν εισάγεται η ίδια καθυστέρηση στην ομάδα των δορυφόρων 1, 2, 8, 9.άγει καθυστέρηση ίση με 333ns προκύπτουν τα παρακάτω διαγράμματα σχήμα 4.20. Η μέγιστη μετατόπιση που προκύπτει είναι τα 330m έναντι των 420m του απλού αλγορίθμου.







Σχήμα 4.20 (α), (β), (γ) Σχεδιάγραμμα όπου φαίνονται οι φυσικές (κύκλοι) και εσφαλμένες (αστερίσκοι) θέσεις των δεκτών-θυμάτων, με άξονες (χ, y), (y, z) και (x, z) αντίστοιχα.

5. Επίλογος – Συμπεράσματα

Τα αποτελέσματα που προέκυψαν από τη μοντελοποίηση του συστήματος δείχνουν ότι η διάταξη εκπληρώνει τους στόχους που τέθηκαν, δηλαδή προκαλεί σημαντική μετατόπιση στη θέση που υπολογίζει ένας δέκτης. Η ανάλυση βέβαια έγινε για την πιο απλή περίπτωση, όπου ο δέκτης υπολογίζει τη θέση του χωρίς να διαθέτει κάποιον αλγόριθμο ως αντίμετρο. Επιπλέον, όπως αναφέρθηκε προηγουμένως η προσομοίωση περιορίστηκε στην λύση των εξισώσεων θέσης, δοθέντων των ψευδοαποστάσεων. Επομένως τα συμπεράσματα που εξάγονται μπορούν να αξιολογηθούν μόνο υπό το πρίσμα των περιορισμών που τέθηκαν.

Ένα σημαντικό μειονέκτημα που προκύπτει είναι ότι ο χρήστης δεν μπορεί να ορίσει την μετατόπιση που θα προκαλέσει στον δέκτη. Αυτό έχει ως συνέπεια να χάνει σε ευελιξία αλλά και να έχει περιορισμένη πιθανότητα να προκαλέσει μια επιτυχημένη επίθεση. Η πιο απλή εξήγηση αυτού είναι ότι αν ο δέκτης έχει προλάβει να κλειδώσει τη θέση του, η λειτουργία της διάταξης θα προκαλούσε μια ακαριαία μετατόπιση στην υπολογισθείσα θέση του. Μια τέτοια συμπεριφορά είναι εύκολο να ανιχνευθεί.

Σε κάθε περίπτωση η πραγματοποίηση πειραμάτων σε πραγματικές συνθήκες κρίνεται απαραίτητη προκυμμένου να εξαχθούν ασφαλή συμπεράσματα.

Βιβλιογραφία

[1] Elliott D. Kaplan, Christopher J. Hegarty “Undestanding GPS Principles and Applications”

[2] Αριστείδης Ι. Φωτίου, Χρήστος Κ. Πικριδάς “GPS και ΓΕΩΔΑΙΤΙΚΕΣ ΕΦΑΡΜΟΓΕΣ”, ΖΗΤΗ 2012

[3] Gilbert Strang, Kai Borre “Linear Algebra, Geodesy, and GPS” WELLESLEY – CAMBRIDGE PRESS

[4] http://www.gps.gov/

[5] N. O.Tippenhauer C. Popper K. B. Rasmussen S. Capkun “On the Requirements for Successful GPS Spoofing Attacks”

Παράρτημα

```
%%% Initial orbit positions
RAAN =
[272.847;272.847;272.847;272.847;332.847;332.847;332.847;332.847;32.8
47;32.847;32.847;32.847;92.847;92.847;92.847;92.847;152.847;152.847;1
52.847;152.847;212.847;212.847;212.847;212.847];
Arg_of_lat =
[268.126;161.786;11.676;41.806;80.956;173.336;309.976;204.376;111.876
;11.796;339.666;241.556;135.226;265.446;35.136;167.356;197.046;302.59
6;66.066;333.686;238.886;345.226;105.206;135.346];
Inclination = 55*ones(24,1);
Radius = 22000; % km


function [ fi, theta ] = sv_orbits2spherical_coordinates( Arg_of_lat,
Inclination, RAAN )
%   Η συνάρτηση αυτή μετατρέπει τις δοσμένες τροχιές των δορυφόρων σε
%   σφαιρικές συντεταγμένες 0<fi<360 και -90<theta<90
theta = 2*pi/360*asind(sind(Arg_of_lat).*sind(Inclination));
%fi = RAAN + acosd(cos(theta));
for i = [1:length(RAAN)]
if Arg_of_lat(i)>=0 & Arg_of_lat(i)<=90
    fi(i,1) = 2*pi/360*(RAAN(i) +
atand(tand(Arg_of_lat(i)).*cosd(Inclination(i))));
elseif Arg_of_lat(i)>90 & Arg_of_lat(i)<180
    fi(i,1) = 2*pi/360*(RAAN(i) + 180 +
atand(tand(Arg_of_lat(i)).*cosd(Inclination(i))));
elseif Arg_of_lat(i)>=180 & Arg_of_lat(i)<270
    fi(i,1) = 2*pi/360*(180+ RAAN(i) +
atand(tand(Arg_of_lat(i)).*cosd(Inclination(i))));
else
    fi(i,1) = 2*pi/360*(360+ RAAN(i) +
atand(tand(Arg_of_lat(i)).*cosd(Inclination(i))));
end
end
end

function [X, Y, Z ] = sv_in_los_calculator( r_x, r_y, r_z, x, y, z )
%       Η συνάρτηση αυτή υπολογίζει τους δορυφόρους που βρίσκονται σε
οπτική
%   επαφή με τον δέκτη. Τα ορίσματα εισόδου είναι οι συντεταγμένες
του
%   δέκτη r_x, r_y, r_z και οι συντεταγμένες των δορυφόρων x, y, z
    dumb1 = size(x); dumb2 = 1;
    unit_vec = [r_x r_y r_z]/(earthRadius/1000); % υπολογισμός του
    %   μοναδιαίου διανύσματος του δέκτη
    for i = 1:dumb1(1,1)
        if [x(i) y(i) z(i)] * unit_vec' > norm([r_x r_y r_z]);
```

```
            X(dumb2) = x(i); Y(dumb2) = y(i); Z(dumb2) = z(i);
            dumb2 = dumb2+1;
        end
    end
end


function [ p ] = pseudorange_calc( r_x, r_y, r_z, X, Y, Z,
time_offset )
%   Η συνάρτηση αυτή υπολογίζει τις ψευδοαποστάσεις μεταξύ δορυφόρων
και
%   δέκτη δοθέντος του time_offset. Με X, Y, Z παριστάνονται οι
%   συντεταγμένες των δορυφόρων και με
%   r_x, r_y, r_z οι συντεταγμένες του δέκτη.
p=dist([X' Y' Z'],[r_x, r_y,
r_z]')+physconst('LightSpeed')/1000*time_offset;
end

function [ H ] = H_matrix_construction(aprox_r_x, aprox_r_y,
aprox_r_z, X, Y, Z  )
%       Κατασκευή του πίνακα H
    aprox_sv2rec_dist = dist([X' Y' Z'],[aprox_r_x, aprox_r_y,
aprox_r_z]');
    aprox_sv2rec_dist1 = aprox_sv2rec_dist; aprox_sv2rec_dist1(:,2) =
aprox_sv2rec_dist; aprox_sv2rec_dist1(:,3) = aprox_sv2rec_dist;
    aprox_sv2rec_dist = aprox_sv2rec_dist1;
    dumb = size(X);
    aprox_r_x(2:dumb(1,2)) = aprox_r_x; aprox_r_y(2:dumb(1,2)) =
aprox_r_y; aprox_r_z(2:dumb(1,2)) = aprox_r_z;
    H = [X'-aprox_r_x' Y'-aprox_r_y' Z'-
aprox_r_z']./aprox_sv2rec_dist;
    dumb1 = size(H);
    H(:, dumb1(1,2)+1) = ones(dumb1(1,1),1);
end

function [d_r_x_final, d_r_y_final, d_r_z_final, d_r_t_final  ] =
diff_calculation( aprox_r_x, aprox_r_y, aprox_r_z, aprox_time_offset,
X, Y, Z, p, number_of_iterations)
%   Η συνάρτηση αυτή υπολογίζει την συνολική μετατόπιση % %  από την
αρχική  εκτιμώμενη θέση. Σαν ορίσματα παίρνει την εκτιμώμενη θέση και
%   προσεγγιστικό time_offset και τον αριθμό των επαναλήψεων
%   Ο αλγόριθμος που χρησιμοποιείται είναι η μέθοδος των ελαχίστων
%   τετραγώνων.
for i=[1:number_of_iterations]
    [ H ] = H_matrix_construction(aprox_r_x(i), aprox_r_y(i),
aprox_r_z(i), X, Y, Z  );
    [ aprox_p ] = pseudorange_calc( aprox_r_x(i), aprox_r_y(i),
aprox_r_z(i), X, Y, Z, aprox_time_offset(i) );
    [d_r] = (H'* H)^(-1)*H'*(aprox_p-p);
```

```
    d_r_x(i) = d_r(1,1); d_r_y(i) = d_r(2,1); d_r_z(i) = d_r(3,1);
d_r_time_offset(i) = -d_r(4,1)*1000/physconst('LightSpeed');
    aprox_r_x(i+1) = aprox_r_x(i) + d_r_x(i); aprox_r_y(i+1) =
aprox_r_y(i) + d_r_y(i); aprox_r_z(i+1) = aprox_r_z(i) + d_r_z(i);
    aprox_time_offset(i+1) = aprox_time_offset(i) +
d_r_time_offset(i);
end
    d_r_x_final = sum(d_r_x); d_r_y_final = sum(d_r_y); d_r_z_final =
sum(d_r_z); d_r_t_final = sum(d_r_time_offset);
end

function [d_r_x_final, d_r_y_final, d_r_z_final, d_r_t_final  ] =
diff_calculation_modified( aprox_r_x, aprox_r_y, aprox_r_z,
aprox_time_offset, X, Y, Z, p, number_of_iterations)
%   Η συνάρτηση αυτή υπολογίζει την συνολική μετατόπιση από την
αρχική
%   εκτιμώμενη θέση. Σαν ορίσματα παίρνει την εκτιμώμενη θέση και
%   προσεγγιστικό time_offset και τον αριθμό των επαναλήψεων
%   Ο αλγόριθμος που χρησιμοποιείται είναι η μέθοδος των ελαχίστων
%   τετραγώνων με βάρη.
for i=[1:number_of_iterations]
%    aprox_r_x(i) = r_x(i); aprox_r_y(i) = r_y(i); aprox_r_z(i) =
r_z(i); aprox_time_offset(i) = time_offset(i);
    [ H ] = H_matrix_construction(aprox_r_x(i), aprox_r_y(i),
aprox_r_z(i), X, Y, Z  );
    [ aprox_p ] = pseudorange_calc( aprox_r_x(i), aprox_r_y(i),
aprox_r_z(i), X, Y, Z, aprox_time_offset(i) );

    [d_r] = (H'* H)^(-1)*H'*(aprox_p-p);

     for j=[1:length(p)]
         S(j,j) = (H(j,:)*d_r)^2;
     end
     C = S^-1;

     [d_r] = (H'*C* H)^(-1)*H'*C*(aprox_p-p);

    d_r_x(i) = d_r(1,1); d_r_y(i) = d_r(2,1); d_r_z(i) = d_r(3,1);
d_r_time_offset(i) = -d_r(4,1)*1000/physconst('LightSpeed');
    aprox_r_x(i+1) = aprox_r_x(i) + d_r_x(i); aprox_r_y(i+1) =
aprox_r_y(i) + d_r_y(i); aprox_r_z(i+1) = aprox_r_z(i) + d_r_z(i);
    aprox_time_offset(i+1) = aprox_time_offset(i) +
d_r_time_offset(i);
end
    d_r_x_final = sum(d_r_x); d_r_y_final = sum(d_r_y); d_r_z_final =
sum(d_r_z); d_r_t_final = sum(d_r_time_offset);
end

%% Σχηματισμός και απεικόνιση του αστερισμού των δορυφόρων
```

```
% Φόρτωση των τροχιών των δορυφόρων
close all
Initial_orbit_positions
% Καθορισμός της θέσης του δέκτη
r_fi = 0; r_theta = 0; r_Radius = earthRadius/1000; time_offset=0;
[ fi, theta ] = sv_orbits2spherical_coordinates( Arg_of_lat,
Inclination, RAAN );
[x, y, z] = sph2cart(fi, theta, Radius);
[r_x, r_y, r_z]=sph2cart(r_fi, r_theta, r_Radius);
[X, Y, Z] = sv_in_los_calculator( r_x, r_y, r_z, x, y, z );
%[ p ] = pseudorange_calc( r_x, r_y, r_z, X, Y, Z, time_offset );
%% Απεικόνιση των τροχιών των δορυφόρων
[ fi_orbit, theta_orbit ] = sv_orbits2spherical_coordinates(
[0:1:359]', 55*ones(360,1), 272.847*ones(360,1) );
[x_orbit1, y_orbit1, z_orbit1] = sph2cart(fi_orbit, theta_orbit,
Radius);
[ fi_orbit, theta_orbit ] = sv_orbits2spherical_coordinates(
[0:1:359]', 55*ones(360,1), 332.847*ones(360,1) );
[x_orbit2, y_orbit2, z_orbit2] = sph2cart(fi_orbit, theta_orbit,
Radius);
[ fi_orbit, theta_orbit ] = sv_orbits2spherical_coordinates(
[0:1:359]', 55*ones(360,1), 32.847*ones(360,1) );
[x_orbit3, y_orbit3, z_orbit3] = sph2cart(fi_orbit, theta_orbit,
Radius);
[ fi_orbit, theta_orbit ] = sv_orbits2spherical_coordinates(
[0:1:359]', 55*ones(360,1), 92.847*ones(360,1) );
[x_orbit4, y_orbit4, z_orbit4] = sph2cart(fi_orbit, theta_orbit,
Radius);
[ fi_orbit, theta_orbit ] = sv_orbits2spherical_coordinates(
[0:1:359]', 55*ones(360,1), 152.847*ones(360,1) );
[x_orbit5, y_orbit5, z_orbit5] = sph2cart(fi_orbit, theta_orbit,
Radius);
[ fi_orbit, theta_orbit ] = sv_orbits2spherical_coordinates(
[0:1:359]', 55*ones(360,1), 212.847*ones(360,1) );
[x_orbit6, y_orbit6, z_orbit6] = sph2cart(fi_orbit, theta_orbit,
Radius);
figure
earth_sphere('km')
hold on
plot3(x_orbit1, y_orbit1, z_orbit1,'k:')
plot3(x_orbit2, y_orbit2, z_orbit2,'k:')
plot3(x_orbit3, y_orbit3, z_orbit3,'k:')
plot3(x_orbit4, y_orbit4, z_orbit4,'k:')
plot3(x_orbit5, y_orbit5, z_orbit5,'k:')
plot3(x_orbit6, y_orbit6, z_orbit6,'k:')
scatter3(x, y, z, 'black')
%% Απεικόνιση τροχιών και δορυφόρων που βρίσκονται σε οπτική επαφή με
τον δέκτη
figure
```

```
plot3(x_orbit1, y_orbit1, z_orbit1,'k:')
plot3(x_orbit2, y_orbit2, z_orbit2,'k:')
plot3(x_orbit3, y_orbit3, z_orbit3,'k:')
plot3(x_orbit4, y_orbit4, z_orbit4,'k:')
plot3(x_orbit5, y_orbit5, z_orbit5,'k:')
plot3(x_orbit6, y_orbit6, z_orbit6,'k:')
earth_sphere('km')
scatter3(x, y, z, 'black')
scatter3(X, Y, Z, 'black', 'filled')
dumb =size(X);
for i=[1:dumb(1,2)]
    text(X(i)+1000, Y(i)+1000, Z(i)+1000, int2str(i))
end
scatter3(r_x, r_y, r_z, 100, 'black', 'filled')
%% Υπολογισμός μετατόπισης των θέσεων και απεικόνιση
%%%%% attacker
a_x = r_x; a_y = r_y; a_z = r_z + 0.1;
[ p_a ] = pseudorange_calc( a_x, a_y, a_z, X, Y, Z, time_offset );
%offset = 100 % σε m
%%% δημιουργία πλέγματος δεκτών θυμάτων
number_of_iterations=4;
for k=[1:5]
    for j=[1:1]
            v_x(k, j) = r_x;
            v_y(k, j) = r_y + 0.1*k;
            v_z(k, j) = r_z + 0.1*j;
            [ p ] = pseudorange_calc( v_x(k,j), v_y(k,j), v_z(k,j),
X, Y, Z, time_offset );
        offset(k,j) = dist([a_x a_y a_z],[v_x(k,j) v_y(k,j)
v_z(k,j)]');
        % χρησιμοποιούμε την καινούρια μεταβλητή ps ώστε να μην
αλλάζει η p
        % σε κάθε επανάληψη
        ps = p;
        ps(1, 1) = p_a(1, 1) + offset(k,j)+0.1;
        ps(2, 1) = p_a(2, 1) + offset(k,j)+0.1;
       % ps(3, 1) = p_a(3, 1) + offset(k,j)+0.1;
        %ps(4, 1) = p_a(4, 1) + offset(k,j)+0.1;
        %ps(5, 1) = p_a(5, 1) + offset(k,j)+0.1;
        %ps(6, 1) = p_a(6, 1) + offset(k,j)+0.1;
        %ps(7, 1) = p_a(7, 1) + offset(k,j)+0.1;
        ps(8, 1) = p_a(8, 1) + offset(k,j)+0.1;
        ps(9, 1) = p_a(9, 1) + offset(k,j)+0.1;

[d_r_x_final, d_r_y_final, d_r_z_final, d_r_t_final  ] =
diff_calculation_modified( v_x(k,j), v_y(k,j), v_z(k,j), time_offset,
X, Y, Z, ps, number_of_iterations );
```

```
v_x_modified(k,j) = v_x(k,j) + d_r_x_final-6371; v_y_modified(k,j) =
v_y(k,j) + d_r_y_final; v_z_modified(k,j) = v_z(k,j) + d_r_z_final;
    end
end
figure
for n=[1:5]
scatter3(v_x(n,:)-6371, v_y(n,:), v_z(n,:),'filled','black')
hold on
scatter3(v_x_modified(n,:),
v_y_modified(n,:),v_z_modified(n,:),'black','*')
hold on
end
scatter3(a_x-6371, a_y, a_z,200,'black', 'x')
%%
figure
for n=[1:5]
scatter(1000*(v_x(n,:)-6371), 1000*v_y(n,:),'filled','black')
xlabel('x (m)')
ylabel('y (m)')
grid on
hold on
scatter(1000*v_x_modified(n,:),1000* v_y_modified(n,:),'black','*')
hold on
end
scatter(1000*(a_x-6371), 1000*a_y,200,'black', 'x')
%%
figure
for n=[1:5]
scatter(1000* v_y(n,:), 1000*v_z(n,:),'filled','black')
xlabel('y (m)')
ylabel('z (m)')
grid on
hold on
scatter( 1000*v_y_modified(n,:),1000*v_z_modified(n,:),'black','*')
hold on
end
scatter( 1000*a_y, 1000*a_z,200,'black', 'x')
%%
figure
for n=[1:5]
scatter(1000*( v_x(n,:)-6371), 1000*v_z(n,:),'filled','black')
xlabel('x (m)')
ylabel('z (m)')
grid on
hold on
scatter( 1000*v_x_modified(n,:),1000*v_z_modified(n,:),'black','*')
hold on
end
scatter( 1000*(a_x-6371), 1000*a_z,200,'black', 'x')
```