ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ανάπτυξη και Υλοποίηση Πρωτοκόλλου Απόδειξης Τοποθεσίας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Δημητρίου Κουνά

Επιβλέπουσα: Θεοδώρα Βαρβαρίγου
Καθηγήτρια Ε.Μ.Π

Αθήνα, Μάρτιος 2019

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ανάπτυξη και Υλοποίηση Πρωτοκόλλου Απόδειξης Τοποθεσίας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Δημητρίου Κουνά

Επιβλέπουσα: Θεοδώρα Βαρβαρίγου
Καθηγήτρια Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 1η Απριλίου 2019.

(Υπογραφή)	(Υπογραφή)	(Υπογραφή)
……	……	……
Θεοδώρα Βαρβαρίγου	Εμμανουήλ Βαρβαρίγος	Συμεών Παπαβασιλείου
Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π

Αθήνα, Μάρτιος 2019

……...

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

Περίληψη

Οι υπηρεσίες που βασίζονται στην τοποθεσία του χρήστη εμφανίζουν μεγάλη αύξηση τα τελευταία χρόνια, εξαιτίας της διείσδυσης των έξυπνων κινητών συσκευών στην καθημερινότητα. Οι υπηρεσίες αυτές εξαρτώνται από την ειλικρίνεια του χρήστη, προκειμένου να αποκτήσουν γνώση της τοποθεσίας του. Σε περιπτώσεις όπου υπάρχει όφελος από την παρουσία σε μία συγκεκριμένη τοποθεσία, ο χρήστης έχει κίνητρο να τροποποιήσει τη συσκευή του ώστε να αναφέρει ψευδή τοποθεσία στις υπηρεσίες. Από την άλλη, ορισμένες υπηρεσίες δεν μπορούν να βασίζονται στην ειλικρίνεια του χρήστη καθώς έχουν υψηλότερες απαιτήσεις ασφαλείας όσον αφορά την τοποθεσία του.

Για την αντιμετώπιση των ζητημάτων αυτών, έχουν προταθεί αρκετά πρωτόκολλα με σκοπό την απόδειξη της τοποθεσίας του χρήστη. Σε αυτά, η συσκευή του χρήστη ανακαλύπτει γειτονικές συσκευές, οι οποίες στέλνουν τεμάχια που πιστοποιούν την τοποθεσία του. Ο χρήστης με βάση τα τεμάχια αυτά κατασκευάζει την απόδειξη τοποθεσίας, ένα ψηφιακό πιστοποιητικό της παρουσίας του σε ένα συγκεκριμένο σημείο του χωροχρόνου. Είναι σημαντικό η διαδικασία αυτή να είναι ασφαλής και να μην παραβιάζει την ιδιωτικότητα των χρηστών που συμμετέχουν.

Στην εργασία αυτή αναπτύσσεται ένα καινοτόμο πρωτόκολλο απόδειξης τοποθεσίας με σκοπό να επιλύσει τα προβλήματα των υπαρχόντων και βασίζεται στους υπερήχους για την επικοινωνία μεταξύ των κόμβων. Με την καταγραφή βίντεο που απεικονίζει το χρήστη και με την ενσωμάτωση σε αυτό της συνεδρίας υπερήχων, πιστοποιείται όχι μόνο η τοποθεσία της συσκευής, αλλά και του ιδιοκτήτη της.

Το πρωτόκολλο που προτείνεται είναι ευέλικτο, καθώς μπορεί να χρησιμοποιηθεί ανεξαρτήτως αρχής πιστοποίησης και υπηρεσίας τοποθεσίας. Επίσης, είναι επεκτάσιμο, καθώς μπορεί να συνδυαστεί με σχήμα εμπιστοσύνης/φήμης και αξιολόγησης της συμπεριφοράς των χρηστών. Για τη δοκιμή του προτεινόμενου πρωτοκόλλου υλοποιείται η εφαρμογή QuietPlace για συσκευές με λειτουργικό σύστημα Android.

Λέξεις Κλειδιά: απόδειξη τοποθεσίας, ιδιωτικότητα, υπηρεσίες τοποθεσίας, επικοινωνία μέσω υπερήχων, έξυπνες κινητές συσκευές

Abstract

Location-based services have significantly increased over the past few years, due to the penetration of smart mobile devices into everyday life. These services rely on the honesty of the user in order to acquire his/her location. In cases where there is benefit from being present in a particular location, the user has the incentive to modify his device to report a false location to these services. On the other hand, some services cannot rely on the user's honesty because they have higher security requirements with regard to the user's location.

To address these issues, several protocols have been proposed with the purpose of proving the user's location. In these, the user's device discovers neighboring devices, which send segments of information that certify the his/her location. The user constructs a proof of location based on these segments. The proof of location is a digital certificate of the user's presence at a specific point of space-time. It is important that this process is safe and does not violate the privacy of the users involved.

In this thesis, an innovative proof of location protocol is proposed and developed with the purpose of solving the problems of the existing ones. The protocol is based on ultrasound for the communication between the nodes. By capturing a video that depicts the user himself and by integrating the ultrasound session in it, not only the device's but also the owner's location is certified.

The proposed protocol is flexible, as it can be used independently of the certification authority and the location-based service being used. It is also expandable, as it can be combined with a trust/reputation-based schema and evaluation of user behavior. To test the proposed protocol, an Android application called QuietPlace is implemented.

Keywords: proof of location, privacy, location-based services, ultrasound communication, smart mobile devices

Η διπλωματική εργασία αυτή αποτελεί το τελευταίο στάδιο της φοίτησής μου στο τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσοβίου Πολυτεχνείου και αποτελεί για εμένα το πρώτο έργο ακαδημαϊκής έρευνας.

Ευχαριστώ ιδιαίτερα την καθηγήτρια Θεοδώρα Βαρβαρίγου για την ευκαιρία που μου έδωσε να εμβαθύνω σε ζητήματα πρωτοκόλλων επικοινωνίας, κρυπτογραφίας και ανάπτυξης εφαρμογών.

Επίσης, ευχαριστώ τον υποψήφιο διδάκτορα Ορφέα Βουτυρά για την βοήθεια και την καθοδήγησή του καθ' όλη τη διάρκεια της εκπόνησης της εργασίας.

Τέλος, ευχαριστώ όλους όσους ήταν δίπλα μου κατά τα δημιουργικά αυτά χρόνια.

Πίνακας περιεχομένων

Πίνακας σχημάτων

Πίνακας πινάκων

1 Εισαγωγή

1.1 Επιστημονικό πεδίο

Ο άνθρωπος πάντα είχε την ανάγκη γνώσης της τοποθεσίας του. Δίχως αυτήν δε θα μπορούσε να αναπτύξει πλήθος δραστηριοτήτων, όπως την αστρονομία, την τοπογραφία, τη ναυτιλία και την αεροπορία. Από τα αρχαία χρόνια είχε την ανάγκη να προσδιορίσει την τοποθεσία του και κατασκεύαζε μηχανισμούς για να το επιτύχει. Κατάφερε έτσι να κατακτήσει τις θάλασσες και τον ουρανό και να γνωρίσει όλο τον κόσμο.

Τα σύγχρονα τεχνολογικά επιτεύγματα έδωσαν τη δυνατότητα για ακριβή εντοπισμό της τοποθεσίας. Ο εντοπισμός της τοποθεσίας δεν είναι πλέον προνόμιο επιστημόνων και στρατιωτικών, αλλά μία υπηρεσία διαθέσιμη σε όλους. Παράλληλα, οι «έξυπνες» κινητές συσκευές (smartphones, tablets κ.τ.λ.) συνδυάζουν ένα τρίπτυχο ιδανικό για την εξάπλωση των υπηρεσιών βασιζόμενων σε τοποθεσία (location-based services). Πρώτον, οι συσκευές αυτές διαθέτουν τη δυνατότητα γεωεντοπισμού μέσω GPS, WiFi και δικτύου κινητής τηλεφωνίας. Δεύτερον, έχουν την ικανότητα να εκτελέσουν πληθώρα εφαρμογών, οι οποίες μπορούν να εκμεταλλευτούν τη θέση της συσκευής. Τρίτον, οι κινητές συσκευές μπορούν να έχουν αδιάλειπτη πρόσβαση στο διαδίκτυο και συνεπώς να μεταδίδουν την τοποθεσία τους στις εφαρμογές, σχεδόν σε όποιο σημείο και αν βρίσκονται.

Τα χαρακτηριστικά αυτά καλλιέργησαν ένα γόνιμο έδαφος ώστε να υπάρξει μεγάλη αύξηση στις υπηρεσίες τοποθεσίας τα τελευταία χρόνια [1]. Πλέον, οι εφαρμογές πέραν του εξατομικευμένου περιεχομένου που παρέχουν ανάλογα με τις προτιμήσεις και το ιστορικό του χρήστη, λαμβάνουν υπόψη και την τοποθεσία του, προκειμένου να αποκτήσουν νέες δυνατότητες. Από την εμφάνιση προτάσεων με βάση την τοποθεσία μέχρι και την πρόσβαση σε απόρρητα έγγραφα μόνο όταν κάποιος βρίσκεται σε εξουσιοδοτημένη περιοχή, η τοποθεσία λαμβάνει πρωταγωνιστικό ρόλο στην αλληλεπίδραση του ανθρώπου με τις συσκευές.

Ωστόσο, οι υπηρεσίες αυτές βασίζονται στην ειλικρίνεια του χρήστη προκειμένου να αποκτήσουν γνώση της τοποθεσίας του. Η συσκευή του χρήστη δίνει ναι μεν τη δυνατότητα εντοπισμού τοποθεσίας, αλλά δεν είναι υπεύθυνη για την μεταβίβαση της πληροφορίας αυτής στις εφαρμογές. Ειδικότερα όταν ο χρήστης έχει κάποιο όφελος από την παρουσία του σε κάποια τοποθεσία, έχει και κίνητρο να δηλώσει ψεύτικη τοποθεσία στην αντίστοιχη εφαρμογή.

Η ανάγκη για ακριβή εντοπισμό της τοποθεσίας του χρήστη καθώς και για επιβεβαίωση αυτής είναι πιο καίρια από ποτέ. Για το λόγο αυτό, έχει αναπτυχθεί πληθώρα πρωτοκόλλων απόδειξης τοποθεσίας (proof of location protocols) που επιτρέπουν στις εφαρμογές να επιβεβαιώσουν την τοποθεσία του χρήστη, ωστέ αυτός να μην μπορεί (ή να είναι για αυτόν δύσκολο) να δηλώσει μία ψεύτικη τοποθεσία.

1.2 Σκοπός της εργασίας

Η εργασία αυτή έχει ως αρχικό σκοπό να αναλύσει τις διαθέσιμες μεθόδους εντοπισμού τοποθεσίας και να αναδείξει την ανάγκη για ασφαλή απόδειξή της. Στη συνέχεια στοχεύει στο να ερευνήσει τα χαρακτηριστικά των υπαρχόντων πρωτοκόλλων απόδειξης τοποθεσίας, να εντοπίσει αδυναμίες σε αυτά και να προτείνει λύσεις.

Αφού καθορίστηκαν οι χρήστες, τα χαρακτηριστικά και οι προδιαγραφές των πρωτοκόλλων απόδειξης τοποθεσίας, μελετήθηκαν αρκετά από αυτά και συγκρίθηκαν σε πίνακες. Εντοπίστηκαν στη συνέχεια ελλείψεις στην αντιμετώπιση ορισμένων επιθέσεων και κακόβου-

λων ενεργειών και προτάθηκαν λύσεις. Αναπτύχθηκε στη συνέχεια ένα πρωτότυπο πρωτόκολλο απόδειξης τοποθεσίας. Οι υπέρηχοι αποτέλεσαν βάση για την επικοινωνία μεταξύ των κόμβων. Η συνεδρία μεταξύ των κόμβων καταγράφεται από τον χρήστη σε βίντεο που τον περιλαμβάνει, ώστε να αποδεικνύεται όχι μόνο η τοποθεσία της συσκευής του, αλλά και του ίδιου. Τέλος, το προτεινόμενο πρωτόκολλο υλοποιήθηκε ως εφαρμογή για συσκευές με λειτουργικό σύστημα Android.

1.3 Δομή περιεχομένου

Η εργασία αποτελείται από επτά κεφάλαια. Στο παρόν και πρώτο κεφάλαιο γίνεται η εισαγωγή στο αντικείμενο και τον σκοπό της εργασίας. Στο δεύτερο κεφάλαιο γίνεται λόγος για τα σύγχρονα συστήματα εντοπισμού τοποθεσίας. Στο τρίτο κεφάλαιο γίνεται αναφορά στα πρωτόκολλα απόδειξης τοποθεσίας, όπου παρουσιάζονται οι χρήσεις, τα χαρακτηριστικά, οι προδιαγραφές και οι αδυναμίες τους. Επίσης συγκρίνονται σε πίνακες ορισμένα πρωτόκολλα της βιβλιογραφίας. Στο τέταρτο κεφάλαιο παρουσιάζεται ένα πρωτότυπο πρωτόκολλο απόδειξης τοποθεσίας, το οποίο επιδιώκει να επιλύσει ορισμένα υπάρχοντα προβλήματα. Στο πέμπτο κεφάλαιο περιγράφεται η υλοποίηση των λειτουργιών του πρωτοκόλλου που προτείνεται. Στο έκτο κεφάλαιο γίνονται κάποιες πειραματικές μετρήσεις και σχόλια σχετικά με την απόδοση του φυσικού στρώματος που χρησιμοποιήθηκε καθώς και της υλοποίησης του πρωτοκόλλου. Στο έβδομο κεφάλαιο δίνονται κατευθύνσεις για μελλοντική εργασία και βελτιώσεις πάνω στο πρωτόκολλο που προτείνεται, καθώς και ερευνητικές επεκτάσεις που προκύπτουν.

2 Συστήματα γεωεντοπισμού (Geolocation or localization systems)

2.1 Ορισμοί

Ως **γεωεντοπισμός** εννοείται ο προσδιορισμός ή η εκτίμηση της γεωγραφικής θέσης (γεωγραφικές συντεταγμένες) μίας ηλεκτρονικής συσκευής [2].

Προκειμένου να επιτευχθεί ο γεωεντοπισμός, απαιτείται ένα **σύστημα εντοπισμού τοποθεσίας ή σύστημα γεωεντοπισμού**, δηλαδή ένας μηχανισμός για τον υπολογισμό της θέσης ενός αντικειμένου στο χώρο.

2.2 Απαραίτητα στοιχεία και συμμετέχοντες

Ένα σύστημα εντοπισμού τοποθεσίας (geolocation system) **αποτελείται από τρία (3) στοιχεία** [3]:

1. Αισθητήρες τοποθεσίας, οι οποίοι λαμβάνουν ηλεκτρομαγνητικά σήματα από άλλες συσκευές και επιτρέπουν τον υπολογισμό της σχετικής θέσης της συσκευής.
2. Αλγόριθμος υπολογισμού θέσης, ο οποίος χρησιμοποιεί τα δεδομένα (μετρικές) που λαμβάνονται από τους αισθητήρες, για να εκτιμήσει την τοποθεσία της συσκευής.
3. Σύστημα προβολής, το οποίο είναι υπεύθυνο για την εμφάνιση της τοποθεσίας της συσκευής.

Για παράδειγμα, το σύστημα γεωεντοπισμού ενός κινητού τηλεφώνου με δέκτη GPS αποτελείται από τα εξής στοιχεία:

1. Αισθητήρας GPS, ο οποίος λαμβάνει σήματα από τους δορυφόρους.
2. Το πρόγραμμα το οποίο εκτελεί η κινητή συσκευή προκειμένου να ερμηνεύσει τα σήματα που δέχεται και να υπολογίσει την τοποθεσία της συσκευής.
3. Η οθόνη της συσκευής και το πρόγραμμα γραφικής αναπαράστασης της τοποθεσίας, ώστε να εμφανίζεται η τοποθεσία της συσκευής πάνω σε χάρτη.

Οι **συμμετέχοντες** σε ένα σύστημα εντοπισμού τοποθεσίας είναι:

- Ο **χρήστης (target)**, ο οποίος επιθυμεί να προσδιορίσει τη θέση του.
- Τα **σημεία αναφοράς - φάροι (beacons, anchors ή landmarks)**, τα οποία είναι κόμβοι ενός δικτύου και υπολογίζουν την τοποθεσία του χρήστη ή τον βοηθούν να υπολογίσει ο ίδιος την τοποθεσία του. Οι θέσεις των σημείων αναφοράς θεωρούνται γνωστές.
- Πιθανώς να χρησιμοποιείται κάποιος κεντρικός **διακομιστής** που συντονίζει τη διαδικασία.

2.3 Κατηγορίες των συστημάτων γεωεντοπισμού

Τα συστήματα γεωεντοπισμού μπορούν να κατηγοριοποιηθούν με βάση πολλούς άξονες. Η κατηγοριοποίηση αυτή δεν είναι απόλυτη, δηλαδή ένα σύστημα μπορεί να ανήκει και στις δύο κατηγορίες κάποιου άξονα. Βασιζόμενοι στο [4] και κάνοντας ορισμένες αλλαγές και προσθήκες, παρουσιάζουμε ορισμένες από αυτές.

1. Ως προς την **περιοχή εφαρμογής (area of deployment)**, τα συστήματα εντοπισμού τοποθεσίας διακρίνονται σε εσωτερικού (indoor) και εξωτερικού (outdoor) χώρου.

2. Ως προς την **υπολογιζόμενη τοποθεσία** διακρίνονται σε απόλυτα (absolute) και σχετικά (relative). Τα απόλυτα συστήματα υπολογίζουν τις γεωγραφικές συντεταγμένες του στόχου (ακριβής γεωγραφική τοποθεσία), ενώ τα σχετικά συστήματα υπολογίζουν τη σχετική θέση του στόχου ως προς τα σημεία αναφοράς.
3. Ως προς την **αρχιτεκτονική** διακρίνονται σε στενά συνδεδεμένα (tightly coupled) και χαλαρά συνδεδεμένα (loosely coupled). Στην πρώτη κατηγορία οι κόμβοι που συμμετέχουν στο σύστημα (στόχος και σημεία αναφοράς) βρίσκονται σε διαρκή επικοινωνία με κάποιον κεντρικό διακομιστή, ο οποίος αναλαμβάνει να εκτελέσει τον αλγόριθμο υπολογισμού θέσης. Στη δεύτερη κατηγορία δεν υφίσταται κεντρικός διακομιστής και ο στόχος υπολογίζει τη θέση του εκτελώντας τον αλγόριθμο.
4. Ως προς την **ασφάλεια – κρυπτογράφηση**, τα συστήματα εντοπισμού τοποθεσίας διακρίνονται σε ασφαλή (secure) και ανοιχτά (open). Στα ασφαλή συστήματα η επικοινωνία μεταξύ των κόμβων γίνεται με κρυπτογράφηση, ενώ στα ανοιχτά χωρίς. Για παράδειγμα, το GPS διαθέτει τόσο ανοιχτές συχνότητες για τους πολίτες, όσο και ασφαλείς-κρυπτογραφημένες για στρατιωτικές χρήσεις [5].
5. Ως προς τον **εξοπλισμό** που χρησιμοποιείται, τα συστήματα εντοπισμού τοποθεσίας διακρίνονται σε αυτά που χρησιμοποιούν ετικέτες αναγνωριστικού με ραδιοσυχνότητες (RFID tags), αυτά που οι κόμβοι διαθέτουν ασύρματους αισθητήρες (wireless sensors) και αυτά που λειτουργούν με βάση τις «έξυπνες» κινητές συσκευές (smart phones, tablets). Βέβαια, υπάρχουν και τα υβριδικά (hybrid) συστήματα, τα οποία συνδυάζουν τις παραπάνω τεχνολογίες.
6. Ως προς το **κέντρο υπολογισμού**, τα συστήματα εντοπισμού τοποθεσίας χωρίζονται σε βασιζόμενα στο δίκτυο (network-based) και βασιζόμενα στην κινητή συσκευή (mobile-based). Στην πρώτη κατηγορία, η συσκευή του χρήστη στέλνει σήματα στους σταθμούς αναφοράς του δικτύου, οι οποίοι υπολογίζουν τη θέση του χρήστη. Στη δεύτερη κατηγορία, η συσκευή του χρήστη λαμβάνει σήματα από τους σταθμούς αναφοράς και υπολογίζει η ίδια την θέση της.
7. Ως προς την **τοποθεσία των σημείων αναφοράς**, διακρίνονται σε δορυφορικά (satellite) και επίγεια (terrestrial). Τα δορυφορικά συστήματα είναι ιδανικά για χρήση σε εξωτερικούς χώρους, ενώ τα επίγεια χρησιμοποιούνται κυρίως σε εσωτερικούς χώρους.
8. Ως προς τον **υπολογισμό απόστασης**, διακρίνονται σε ελεύθερα απόστασης, όπου αρκεί η ύπαρξη σημάτων από τους φάρους (beacons) και δεν υπολογίζεται απόσταση από αυτούς και σε βασιζόμενα στην απόσταση, όπου με βάση τριγωνισμού η τριπλευρισμού έχουμε εύρεση τοποθεσίας με μεγαλύτερη ακρίβεια.
9. Ως προς την **γνώση της τοποθεσίας των σημείων αναφοράς**, τα συστήματα γεωεντοπισμού διακρίνονται σε βασιζόμενα σε άγκυρες (anchor-based) και σε μη βασιζόμενα σε άγκυρες. Στην πρώτη περίπτωση, δεν γνωρίζουν όλα τα σημεία αναφοράς τη γεωγραφική τους θέση, αλλά μόνο ορισμένα από αυτά (άγκυρες). Τα υπόλοιπα υπολογίζουν τη θέση τους με βάση τις άγκυρες. Στη δεύτερη περίπτωση, όλα τα σημεία αναφοράς γνωρίζουν τη γεωγραφική τους θέση.

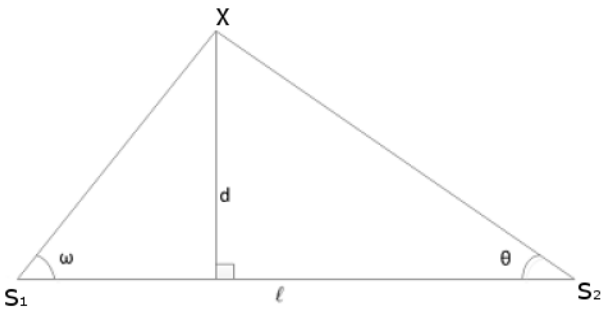
2.4 Αρχές λειτουργίας

Οι βασικές αρχές λειτουργίας των συστημάτων εντοπισμού τοποθεσίας είναι ο τριγωνισμός (triangulation) και ο τριπλευρισμός (trilateration) [3]. Ο τριγωνισμός είναι γνωστός από τους αρχαίους Έλληνες και Αιγύπτιους, οι οποίοι χρησιμοποιούσαν πρώιμους θεοδόλιχους, όπως περιγράφει ο Ήρων ο Αλεξανδρεύς [6]. Ο τριπλευρισμός χρησιμοποιούνταν λιγότερο σε σχέση με τον τριγωνισμό, ωστόσο με την ανάπτυξη των ηλεκτρονικών συσκευών μέτρησης αποστάσεων έγινε προτιμώμενη αρχή λειτουργίας [7].

2.4.1 Τριγωνισμός

Ο τριγωνισμός [4] υπολογίζει τη θέση του στόχου, χρησιμοποιώντας τις γωνίες παρατήρησης από σημεία αναφοράς με γνωστή μεταξύ τους απόσταση.

Θεωρούμε δύο σημεία αναφοράς $S_1(x_1, y_1, z_1)$, $S_2(x_2, y_2, z_2)$ που βρίσκονται σε **απόσταση l** μεταξύ τους. Θεωρούμε επιπλέον στόχο X(x, y, z). Το S_1 βλέπει το στόχο με **γωνία ω** ως προς S_2, ενώ το S_2 βλέπει το στόχο με **γωνία θ** ως προς S_1, όπως φαίνεται στην παρακάτω εικόνα.



Σχήμα 2.1: Τριγωνισμός [4]

Η απόσταση d μεταξύ του X και του ευθυγράμμου τμήματος S_1S_2 προκύπτει από την τριγωνομετρία ως εξής:

$$l = \frac{d}{\tan(\omega)} + \frac{d}{\tan(\theta)} = d\left(\frac{\cos(\omega)}{sin(\omega)} + \frac{\cos(\theta)}{sin(\theta)}\right) = d\frac{\sin(\omega+\theta)}{\sin(\omega)\sin(\theta)}$$

και τελικά

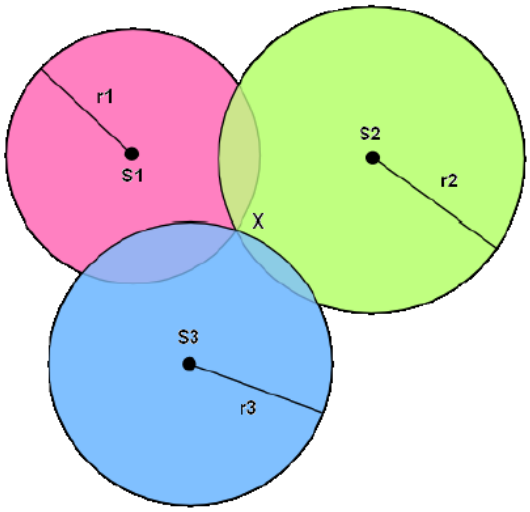
$$d = l\frac{\sin(\omega)\sin(\theta)}{\sin(\omega+\theta)}$$

Γνωρίζοντας την απόσταση d, ο X έχει πλήρη γνώση των στοιχείων του τριγώνου και συνεπώς μπορεί να υπολογίσει την απόλυτη θέση του.

2.4.2 Τριπλευρισμός

Ο τριπλευρισμός υπολογίζει την θέση του στόχου, χρησιμοποιώντας την απόστασή του από τρία σημεία αναφοράς [4].

Θεωρούμε ότι έχουμε τρία σημεία αναφοράς στο χώρο, τα $S_1(x_1, y_1, z_1)$, $S_2(x_2, y_2, z_2)$ και $S_3(x_3, y_3, z_3)$. Επιπλέον, θεωρούμε στόχο X(x, y, z), ο οποίος απέχει απόσταση r_1, r_2, r_3 από τα σημεία αναφοράς S_1, S_2, S_3 αντίστοιχα.



Σχήμα 2.2: Τριπλευρισμός [4]

Από τον τύπο της Ευκλείδειας απόστασης έχουμε τις εξής σχέσεις:

$$r_1^2 = (x - x_1)^2 + (y - y_1)^2 + (z - z_1)^2$$

$$r_2^2 = (x - x_2)^2 + (y - y_2)^2 + (z - z_2)^2$$

$$r_3^2 = (x - x_3)^2 + (y - y_3)^2 + (z - z_3)^2$$

Η ακριβής θέση του στόχου X, δηλαδή οι συντεταγμένες (x, y, z), μπορούν να υπολογιστούν επιλύοντας το παραπάνω σύστημα.

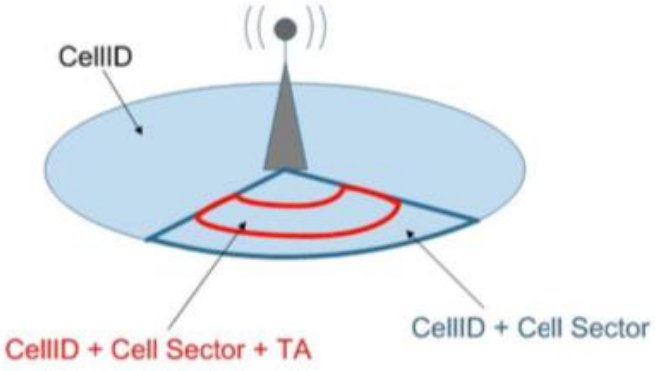
Ένας τρόπος επίλυσης είναι η εφαρμογή της μεθόδου των ελαχίστων τετραγώνων.

2.5 Μέθοδοι εντοπισμού τοποθεσίας

Οι μέθοδοι εντοπισμού τοποθεσίας βασίζονται στις αρχές που αναφέρθηκαν παραπάνω. Προκειμένου να αποκτήσουν γνώση των αποστάσεων ή των γωνιών, χρησιμοποιούν ορισμένες πληροφορίες, όπως η Γωνία Άφιξης (Angle of Arrival – AOA), η Λαμβανόμενη Ισχύς Σήματος (Received Signal Strength – RSS), ο Χρόνος Άφιξης (Time of Arrival – TOA), η Διαφορά Χρόνου Άφιξης (Time Difference of Arrival –TDOA) κ.α.

2.5.1 Ταυτότητα κυψέλης (Cell ID)

Η μέθοδος αυτή χρησιμοποιείται σε δίκτυα κινητής τηλεφωνίας. Το δίκτυο γνωρίζει σε ποια κυψέλη (cell) είναι συνδεδεμένη η συσκευή του χρήστη (στόχος) καθώς και την τοποθεσία και την εμβέλεια της κυψέλης. Έτσι, προκύπτει το συμπέρασμα πως ο στόχος βρίσκεται μέσα στην ακτίνα εμβέλειας της κυψέλης. Η μέθοδος Cell ID έχει μικρή ακρίβεια, καθώς η εμβέλεια της κυψέλης στα δίκτυα GSM κυμαίνεται από 2 έως 20 km. Συνεπώς, η μέθοδος αυτή παρέχει περισσότερο μία εκτίμηση (σχετική θέση ως προς την κυψέλη) παρά εντοπισμό τοποθεσίας.



Σχήμα 2.3: Η μέθοδος Cell ID [3]

Βελτιώσεις πάνω σε αυτή τη μέθοδο μπορούν να επιτευχθούν με τη χρήση τομέων (sectors) και της τεχνικής timing advance. Χρησιμοποιώντας διαφορετικές κεραίες αντί μίας πολυκατευθυντικής κεραίας για κάθε κυψέλη, είναι δυνατόν να προσδιοριστεί ο τομέας του κύκλου στον οποίο ανήκει ο στόχος. Επίσης, η τεχνική timing advance επιτρέπει την εκτίμηση της απόστασης του στόχου από την κεραία. Υλοποιώντας αυτές τις τεχνικές, μπορεί να επιτευχθεί ακριβέστερος εντοπισμός του στόχου [3].

2.5.2 Λαμβανόμενη Ισχύς Σήματος (Received Signal Strength – RSS)

Όταν ένα σήμα διαδίδεται στο χώρο, χάνει την ισχύ του καθώς απομακρύνεται από τον πομπό. Το γεγονός αυτό επιτρέπει να εκτιμήσουμε την απόσταση μεταξύ πομπού και δέκτη, μετρώντας την ισχύ που λαμβάνει ο δέκτης και έχοντας ως γνωστά κάποια άλλα στοιχεία.

Χρησιμοποιώντας την απλοποιημένη μέθοδο που περιγράφεται στο [4], θεωρούμε ότι ο δέκτης λαμβάνει ισχύ

$$P_r = \frac{P_1}{d^2}$$

όπου P_r η ισχύς που λαμβάνει ο δέκτης, P_1 η λαμβανόμενη ισχύς σε απόσταση 1 m από τον πομπό, d η απόσταση μεταξύ πομπού και δέκτη, α η σταθερά διάδοσης.

Στον ελεύθερο χώρο η σταθερά διάδοσης είναι α=2. Σε αστικό χώρο και για σήματα WiFi η σταθερά διάδοσης είναι α=4. Στους εσωτερικούς χώρους όμως η τιμή της εξαρτάται από πολλούς παράγοντες. Κατά συνέπεια, η μέθοδος RSS χρειάζεται μελέτη του χώρου και λήψη μετρήσεων βαθμονόμησης, προκειμένου να κατασκευαστεί το μοντέλο απωλειών που θα χρησιμοποιηθεί. Επιπλέον, πρέπει να ληφθούν υπόψη τα χαρακτηριστικά καναλιού (channel characteristics), τα οποία επηρεάζουν τις μετρήσεις RSS.

Αν χρησιμοποιούνται τουλάχιστον τρεις πομποί, η μέθοδος αυτή συνδυάζεται με τον τριπλευρισμό για τον εντοπισμό της τοποθεσίας του δέκτη-στόχου [8] [9].

2.5.3 Γωνία Άφιξης (Angle of Arrival – AOA)

Η μέθοδος AOA βασίζεται στον τριγωνισμό, όπου η θέση του χρήστη-στόχου προσδιορίζεται γνωρίζοντας τις γωνίες παρατήρησής του από δύο σημεία αναφοράς με γνωστή τοποθεσία.

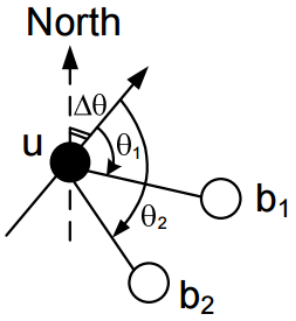
Τα σημεία αναφοράς είναι σταθμοί βάσης (base stations) και απαιτείται να έχουν πολλές κεραίες, ώστε να μπορούν να προσδιορίσουν τη γωνία άφιξης του σήματος από τον στόχο.

Για την εύρεση τοποθεσίας σε δισδιάστατο επίπεδο απαιτείται η συνεισφορά δύο τουλάχιστον σταθμών βάσης.

Η τεχνική αυτή έχει δύο αρνητικά. Αφενός, τα σήματα που φτάνουν στους σταθμούς από διαφορετικά μονοπάτια (multipath signals) λόγω π.χ. ανακλάσεων μπορούν να τους «μπερδέψουν» και να συμπεράνουν διαφορετική τοποθεσία. Αφετέρου, η εγκατάσταση διατάξεων κεραιών έχει κόστος και είναι ευαίσθητη διαδικασία.

Μία εναλλακτική υλοποίηση μετράει τις γωνίες με τις οποίες ο στόχος βλέπει τους σταθμούς βάσης. Στην περίπτωση αυτή δε χρειάζεται οι σταθμοί να διαθέτουν συστοιχία κεραιών (αρκεί και η πολυκατευθυντική κεραία).

Έστω ότι ο στόχος Χ έχει έναν γνωστό προσανατολισμό Δθ ως προς το Βορρά. Δύο σημεία αναφοράς b_1 και b_2 εκπέμπουν σήμα προς αυτόν. Το σήμα από τον b_1 φτάνει με σχετική γωνία άφιξης θ_1, ενώ από τον b_2 με γωνία θ_2.



Σχήμα 2.4: Η μέθοδος AOA [4]

Συνεπώς, οι απόλυτες AOA είναι $AOA_1=\Delta\theta+\theta_1$ και $AOA_2=\Delta\theta+\theta_2$.

Κάθε απόλυτη AOA προσδιορίζει το στόχο πάνω σε μία ευθεία που διέρχεται από το σημείο αναφοράς και τον ίδιο το στόχο. Έχοντας δύο σημεία αναφοράς προκύπτουν δύο ευθείες. Θεωρώντας γνωστές τις θέσεις των δύο σημείων αναφοράς, ο στόχος μπορεί να προσδιορίσει την τοποθεσία του στο σημείο τομής των δύο ευθειών [4].

2.5.4 Χρόνος Άφιξης (Time of Arrival – TOA)

Η μέθοδος αυτή [3] [4] βασίζεται στο χρόνο που χρειάζεται ένα σήμα για να ταξιδέψει από έναν κόμβο σε έναν άλλο. Γνωρίζοντας το χρόνο διάδοσης (propagation time) του σήματος, η απόσταση μεταξύ των δύο κόμβων μπορεί να προσδιοριστεί θεωρώντας πως η ταχύτητα των ηλεκτρομαγνητικών σημάτων είναι περίπου ίση με την ταχύτητα του φωτός, $c = 3 \cdot 10^8 \ {}^{m}/_{s}$.

Συνεπώς, υπολογίζεται η απόσταση $d = c \cdot t$, όπου t ο χρόνος διάδοσης του σήματος.

Η TOA μπορεί να υπολογιστεί είτε μετρώντας τη φάση του ληφθέντος φέροντος σήματος στενής ζώνης είτε με απευθείας μέτρηση του χρόνου άφιξης ενός στενού παλμού ευρείας ζώνης. Η πρώτη περίπτωση δεν έχει καλά αποτελέσματα σε περιβάλλοντα πολλαπλών ανακλάσεων.

Για να υπολογιστεί η TOA, ο πομπός στέλνει ένα σήμα στο οποίο συμπεριλαμβάνει το χρόνο που αυτό εστάλη (timestamp). Ο δέκτης λαμβάνει το σήμα και υπολογίζει πόσο χρόνο αυτό έκανε για να διαδοθεί. Προϋπόθεση είναι ο πομπός και ο δέκτης να έχουν συγχρονισμένα ρολόγια.

Η τεχνική αυτή παρέχει μεγαλύτερη ακρίβεια από την Cell ID [3].

2.5.5 Διαφορά Χρόνου Άφιξης (Time Difference of Arrival – TDOA)

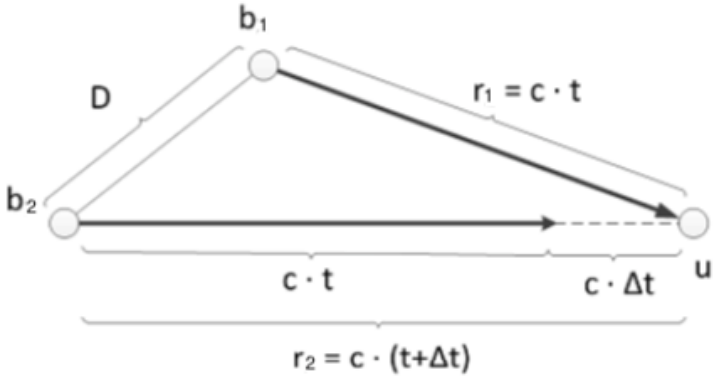
Η μέθοδος αυτή [4] μπορεί να χρησιμοποιηθεί όταν δεν υπάρχει συγχρονισμός των ρολογιών μεταξύ στόχου και σημείων αναφοράς, αλλά υπάρχει μεταξύ των σημείων αναφοράς.

Τα σημεία αναφοράς εκπέμπουν την ίδια χρονική στιγμή, αλλά ο χρόνος εκπομπής δεν είναι γνωστός. Γνωστή είναι μόνο η διαφορά χρόνου με την οποία φτάνουν στο δέκτη – στόχο τα σήματα.

Θεωρούμε ότι έχουμε δύο σημεία αναφοράς b1 και b2 καθώς και ένα δέκτη – στόχο u, τη θέση του οποίου θέλουμε να προσδιορίσουμε.

Το σήμα από τον b1 φτάνει σε χρόνο t, ενώ το σήμα από τον b2 φτάνει σε χρόνο t + Δt. Η απόσταση D μεταξύ των σημείων αναφοράς θεωρείται γνωστή.

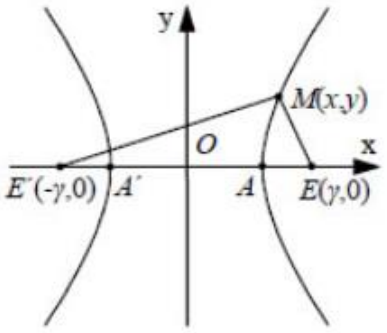
Άρα, ο b1 απέχει $r_1 = c \cdot t$ και ο b2 απέχει $r_2 = c \cdot (t + \Delta t)$, όπου c η ταχύτητα του φωτός.



Σχήμα 2.5: Η μέθοδος TDOA [4]

Από τα παραπάνω ισχύει $|r_2 - r_1| = c \cdot \Delta t$.

Η σχέση αυτή ταυτίζεται με τον τύπο της υπερβολής, αν θεωρήσουμε άγνωστο σημείο Μ το στόχο u και εστίες Ε, Ε' τα σημεία αναφοράς, όπως φαίνεται στο παρακάτω σχήμα.



Σχήμα 2.6: Γραφική παράσταση υπερβολής [4]

Ο τύπος της υπερβολής είναι $|ME' - ME| = 2\alpha$, που σε καρτεσιανές συντεταγμένες ανάγεται στον:

$$\frac{x^2}{a^2} - \frac{y^2}{\beta^2} = 1, \text{ όπου } \beta = \sqrt{\gamma^2 - a^2} \text{ και } E'E = 2\gamma$$

Από τις παραπάνω έχουμε $2a = c \cdot \Delta t$ και $2\gamma = D$.

Οπότε καταλήγουμε πως ο στόχος u ανήκει στην υπερβολή με τύπο:

$$\frac{4x^2}{(c \cdot \Delta t)^2} - \frac{4y^2}{D^2 - (c \cdot \Delta t)^2} = 1$$

Από την εκπομπή δύο σημείων αναφοράς μπορούμε να συμπεράνουμε την υπερβολή πάνω στην οποία βρίσκεται ο στόχος. Έχοντας περισσότερα σημεία αναφοράς, μπορούμε να υπολογίσουμε τη θέση του στόχου από τις τομές των υπερβολών.

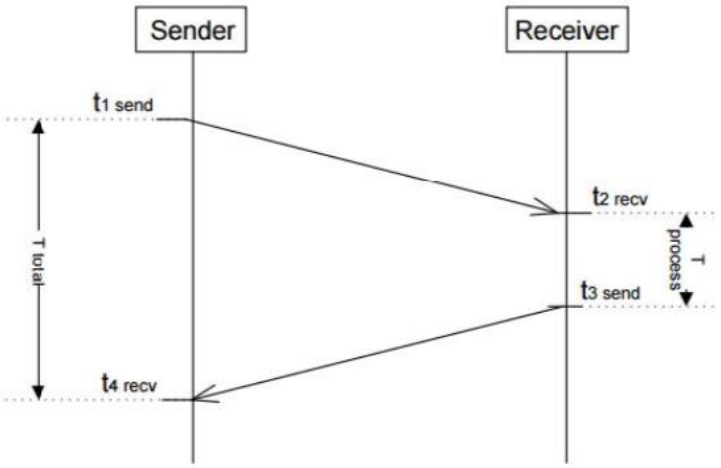
Παραλλαγές της μεθόδου αυτής αποτελούν οι Observed Time Difference of Arrival (OTDOA), Uplink Time Difference of Arrival (U-TDOA) και Enhanced – Observed Time Difference (E-OTD) [3].

2.5.6 Χρόνος διάδοσης μετ' επιστροφής (Round Trip Time – RTT)

Η μέθοδος RTT βασίζεται στη μέτρηση του χρόνου διάδοσης ενός σήματος από τον κόμβο A στον κόμβο B και ξανά πίσω στον A [4].

Τα ρολόγια των κόμβων δεν χρειάζεται να είναι συγχρονισμένα. Μόνο ο A χρησιμοποιεί απόλυτες χρονικές στιγμές, ενώ ο B καταγράφει μόνο χρονική διάρκεια, ως εξής:

Έστω ότι ο κόμβος A επιθυμεί να μάθει την απόστασή του από τον κόμβο B. Ο A αποστέλλει στον B ένα πακέτο στο οποίο ενσωματώνει τη χρονική στιγμή αποστολής t_1. Το πακέτο αυτό φτάνει στον κόμβο B τη χρονική στιγμή t_2. Ο κόμβος B χρειάζεται χρονικό διάστημα επεξεργασίας Δt_p μέχρι να επαναπροωθήσει το πακέτο στον A. Ενσωματώνει το Δt_p στο πακέτο και το στέλνει πίσω στον A τη χρονική στιγμή t_3. Το πακέτο φτάνει στον A τη χρονική στιγμή t_4.



Σχήμα 2.7: Η μέθοδος RTT [4]

Ο κόμβος A γνωρίζει μόνο τις χρονικές στιγμές t_1 και t_4, καθώς και το χρονικό διάστημα επεξεργασίας Δt_p.

Υπολογίζει το χρόνο διάδοσης μετ' επιστροφής

$$RTT = t_4 - t_1 - \Delta t_p$$

Συνεπώς, η απόσταση d μεταξύ A και B είναι

$$d = \frac{RTT}{2} \cdot c = \frac{(t_4 - t_1 - \Delta t_p) \cdot c}{2}$$

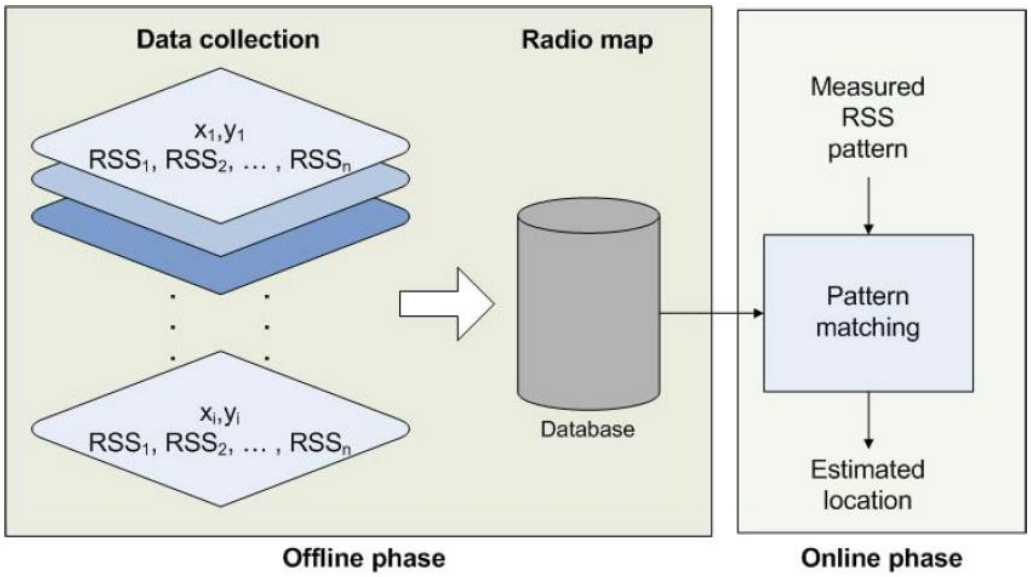
2.5.7 Ηλεκτρομαγνητικό αποτύπωμα (fingerprinting ή radio map)

Η μέθοδος αυτή [3] χρησιμοποιείται σε συστήματα που κάνουν χρήση της λαμβανόμενης ισχύος σήματος (Received Signal Strength – RSS).

Στόχος είναι η κατασκευή ενός χάρτη που περιέχει την ισχύ των λαμβανόμενων σημάτων σε κάθε σημείο ενός (συνήθως εσωτερικού) χώρου. Η θέση του στόχου εκτιμάται συγκρίνοντας την ισχύ σημάτων που αυτός λαμβάνει με αυτή που είναι αποθηκευμένη στο σύστημα.

Η αρχή του fingerprinting αποτελείται από δύο φάσεις:

- Στην **offline φάση (φάση εκπαίδευσης)** κατασκευάζεται ο χάρτης σημάτων. Ο χώρος που ενδιαφέρει χωρίζεται σε πλέγμα και σε κάθε περιοχή αυτού μετρούνται τα RSS που λαμβάνονται από τα διάφορα access points ή σημεία αναφοράς που βρίσκονται στο χώρο. Για κάθε περιοχή (x_i, y_i, z_i) του πλέγματος, όλα τα λαμβανόμενα RSS τοποθετούνται σε διάνυσμα $V_{(xi,yi,zi)}=[RSS_{1(xi,yi,zi)}, RSS_{2(xi,yi,zi)}, \dots, RSS_{n(xi,yi,zi)}]$ το οποίο αποτελεί το **αποτύπωμα (fingerprint)** αυτής της περιοχής του πλέγματος. Τα αποτυπώματα του πλέγματος αποθηκεύονται στη βάση δεδομένων του συστήματος.
- Στην **online φάση** γίνεται ο εντοπισμός του στόχου. Συγκεκριμένα, ένας στόχος ο οποίος βρίσκεται στον χώρο ενδιαφέροντος, συλλέγει τις τιμές RSS που λαμβάνει στο σημείο στο οποίο βρίσκεται. Κατασκευάζει το διάνυσμα-αποτύπωμα και το αποστέλλει στο διακομιστή (server) του συστήματος εντοπισμού θέσης. Ο server χρησιμοποιεί το αποτύπωμα του στόχου και τα αποθηκευμένα δεδομένα και με βάση κάποιον αλγόριθμο υπολογίζει τη θέση του στόχου μέσα στο πλέγμα.



Σχήμα 2.8: Η διαδικασία του fingerprinting [3]

Ο αλγόριθμος που χρησιμοποιεί το σύστημα εντοπισμού τοποθεσίας μπορεί να είναι ντετερμινιστικός (deterministic), πιθανολογικός (probabilistic), ή να βασίζεται σε μηχανική μάθηση (machine learning).

- Οι **ντετερμινιστικοί αλγόριθμοι** υπολογίζουν τη θέση του στόχου λαμβάνοντας υπόψη μόνο την τιμή των μετρούμενων RSS. Συσχετίζουν το αποτύπωμα που λαμβάνει ο στόχος με τα αποτυπώματα που είναι αποθηκευμένα στη βάση δεδομένων.
- Οι **πιθανολογικοί αλγόριθμοι** υπολογίζουν τη θέση του στόχου θεωρώντας τις μετρήσεις ως τυχαίες διαδικασίες (κατανομές), κατά κύριο λόγο κανονικές κατανομές (Gaussian distributions). Κατά την offline φάση, για κάθε σημείο αναφοράς, μετριέται η μέση τιμή (mean value) και η διακύμανση (variance) για την κατανομή RSS. Έπειτα

υπολογίζονται οι κατανομές για κάθε σημείο του χώρου. Η πιο πιθανή τοποθεσία εκτιμάται ως η τοποθεσία του στόχου.
- Οι **αλγόριθμοι που βασίζονται σε μηχανική μάθηση** εξελίχθηκαν εξαιτίας του υπολογιστικού κόστους των παραπάνω αλγορίθμων. Χρησιμοποιούν κατά κύριο λόγο Νευρωνικά Δίκτυα (Neural Networks), Ασαφή Λογική (Fuzzy Logic) κ.α. Το πλεονέκτημά τους είναι η δυνατότητα για εντοπισμό του στόχου σε πραγματικό χρόνο.

Αντί να μετράει ο στόχος τις RSS που λαμβάνει από τα σημεία αναφοράς, είναι δυνατόν να μετρούν τα σημεία αναφοράς την RSS που λαμβάνουν από τον στόχο, προσπαθώντας να εκτιμήσουν την απόσταση που απέχουν από αυτόν.

Όπως αναφέρθηκε, η θέση του στόχου εκτιμάται με βάση το πλέγμα που έχει κατασκευαστεί κατά την πρώτη φάση. Συνεπώς, η ακρίβεια των συστημάτων που βασίζονται στο fingerprinting είναι το πολύ όση και η απόσταση μεταξύ των γραμμών του πλέγματος.

Επιπλέον, η λαμβανόμενη RSS σε κάθε σημείο του χώρου εξαρτάται από πολλούς παράγοντες, όπως από την ποιότητα του δέκτη του στόχου, την ύπαρξη κινητών εμποδίων κ.α. Ο αλγόριθμος που χρησιμοποιείται είναι υπεύθυνος να δώσει σωστό αποτέλεσμα με βάση το αποτύπωμα που λαμβάνει ο στόχος.

Συνεπώς, εκτός του πλέγματος, καθοριστικός για την ακρίβεια του συστήματος είναι ο αλγόριθμος που χρησιμοποιείται.

2.6 Δορυφορικά συστήματα εντοπισμού τοποθεσίας (Global Navigation Satellite Systems – GNSS)

Τα δορυφορικά συστήματα γεωεντοπισμού χρησιμοποιούν δορυφόρους που παρέχουν σε μία συσκευή-δέκτη τη δυνατότητα να προσδιορίσει τη θέση της στο χώρο (γεωγραφικό μήκος, πλάτος, ύψος) καθώς και την τοπική ώρα με μεγάλη ακρίβεια. Μπορεί να έχουν παγκόσμια (π.χ. GPS) ή τοπική (π.χ. Beidou) κάλυψη και λειτουργούν ανεξάρτητα από την ύπαρξη άλλης τηλεπικοινωνιακής υποδομής.

Υλοποιήσεις αποτελούν [10]:

- **GPS (Global Positioning System)** [11]**:** Ανήκει στην Κυβέρνηση των Ηνωμένων Πολιτειών Αμερικής και διαχειρίζεται από την Αμερικανική Πολεμική Αεροπορία (United States Air Force). Αποτελεί το πρώτο σύστημα δορυφορικού εντοπισμού που αναπτύχθηκε και τέθηκε σε λειτουργία.
- **GLONASS (Global Navigation Satellite System)** [12]**:** Παγκόσμιο σύστημα, η ανάπτυξή του οποίου ξεκίνησε στη Σοβιετική Ένωση. Ανήκει στη Ρωσική Ομοσπονδία.
- **Galileo** [13]**:** Παγκόσμιο σύστημα που αναπτύσσεται από την Ευρωπαϊκή Ένωση μέσω του Ευρωπαϊκού Οργανισμού Διαστήματος (European Space Agency).
- **BeiDou** [14]**:** Τοπικό σύστημα που ανήκει στην Λαϊκή Δημοκρατία της Κίνας και διαχειρίζεται από την Κινέζικη Εθνική Διαχείριση Διαστήματος (China National Space Administration).
- **IRNSS/NavIC (Indian Regional Navigation Satellite System/Navigation Indian Constellation)** [15]**:** Τοπικό σύστημα που ανήκει και διαχειρίζεται από την Κυβέρνηση της Ινδίας. Αποτελεί αυτόνομο σύστημα σχεδιασμένο να καλύπτει την περιοχή της Ινδίας και 1500 km γύρω από την Ινδική ηπειρωτική χώρα.
- **QZSS (Quasi-Zenith Satellite System)** [16]**:** Τοπικό σύστημα που ανήκει στην Κυβέρνηση της Ιαπωνίας και λειτουργεί από την QZS System Service Inc. Προς το παρόν

έχει συμπληρωματικό ρόλο, βελτιώνοντας την κάλυψη του GPS στην Ανατολική Ασία και την Ωκεανία, με σκοπό να γίνει αυτόνομο σύστημα στο μέλλον.

2.6.1 Λειτουργία των GNSS

Τα δορυφορικά συστήματα βασίζονται στη γνωστή θέση των δορυφόρων, οι οποίοι αποτελούν σημεία αναφοράς. Ο υπολογισμός της θέσης γίνεται αφού πρώτα υπολογιστεί η απόσταση του στόχου από τον κάθε δορυφόρο. Η απόσταση υπολογίζεται με βάση την τεχνική Time of Arrival – TOA [4].

Στο απλοποιημένο μοντέλο θεωρείται ότι τα σήματα που στέλνουν οι δορυφόροι διαδίδονται σφαιρικά. Αυτό σημαίνει πως αν ένας στόχος προσδιορίσει την απόστασή του, έστω r, από έναν δορυφόρο, εκτιμά τη θέση του πάνω σε μία σφαίρα ακτίνας r με κέντρο το δορυφόρο.

Σύμφωνα με τη μέθοδο TOA, η απόσταση του δέκτη από δορυφόρο i υπολογίζεται ίση με

$$r_i = c \cdot (t_{ri} - t_{si})$$

όπου
t_{ri} η χρονική στιγμή λήψης του σήματος από τον δορυφόρο i,
t_{si} η χρονική στιγμή αποστολής του σήματος από τον δορυφόρο i,
$c = 3 \cdot 10^8\ {}^{m}/_{s}$ η ταχύτητα του φωτός

Με την γνώση που αποκτά ο δέκτης από έναν δορυφόρο, προσδιορίζει τη θέση του πάνω στη σφαίρα

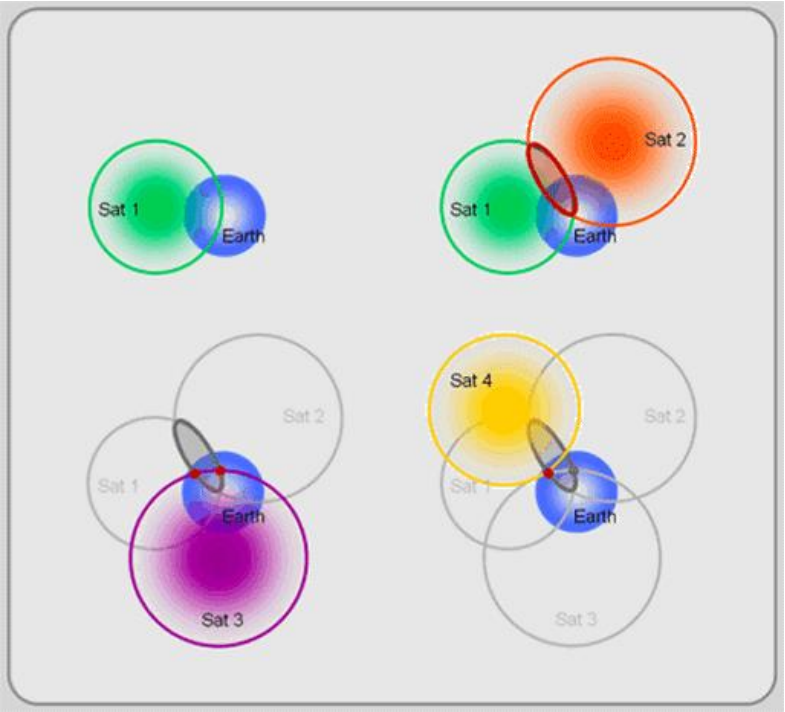
$$r_i = \sqrt{(X_i - X)^2 + (Y_i - Y)^2 + (Z_i - Z)^2}$$

όπου (X,Y,Z) η θέση του δέκτη και (X_i, Y_i, Z_i) η θέση του δορυφόρου i.

Αν θεωρήσουμε ότι η Γη δεν έχει υψομετρικές διαφορές, ή με άλλα λόγια δε μας ενδιαφέρει το υψόμετρο του δέκτη, τότε αρκούν 3 δορυφόροι για τον προσδιορισμό της θέσης του (μόνο γεωγραφικό πλάτος και μήκος). Η σφαίρα του δεύτερου δορυφόρου τέμνεται με του πρώτου και προσδιορίζει κύκλο. Η σφαίρα του τρίτου δορυφόρου τέμνεται με τον κύκλο και προσδιορίζει δύο σημεία πάνω σε αυτόν. Το δεδομένο υψόμετρο δημιουργεί την τέταρτη σφαίρα με κέντρο το κέντρο της Γης και τελικά προσδιορίζει σημείο.

Αν θεωρήσουμε ότι η Γη έχει υψομετρικές διαφορές, τότε το ρόλο της σφαίρας που δημιουργήθηκε λόγω δεδομένου υψόμετρου παίρνει ένας τέταρτος δορυφόρος.

Συνεπώς, για τον προσδιορισμό της θέσης με βάση το GPS χρειάζονται τέσσερις δορυφόροι.



Σχήμα 2.9: Προσδιορισμός θέσης με χρήση δορυφορικού συστήματος.
Πηγή: http://giscommons.org/chapter-2-input/

Ο τέταρτος δορυφόρος λύνει ένα επιπλέον σημαντικό πρόβλημα. Όπως αναφέρθηκε στην παράγραφο για την τεχνική TOA, απαιτείται συγχρονισμός μεταξύ πομπού και δέκτη. Οι πομποί-δορυφόροι, διαθέτουν ατομικά ρολόγια με ακρίβεια που φτάνει μέχρι και 3 ns και είναι συγχρονισμένοι μεταξύ τους. Ο δέκτης αφενός δε διαθέτει ρολόι τόσο μεγάλης ακρίβειας, αφετέρου πρέπει να συγχρονιστεί με το δίκτυο των δορυφόρων.

Έστω ότι το ρολόι του δέκτη διαφέρει κατά δt από το ρολόι του δικτύου των δορυφόρων.

Τότε, ο δέκτης καταστρώνει την εξίσωση

$$r_i = c \cdot (t_{ri} - t_{si} + \delta_t) = \sqrt{(X_i - X)^2 + (Y_i - Y)^2 + (Z_i - Z)^2}$$

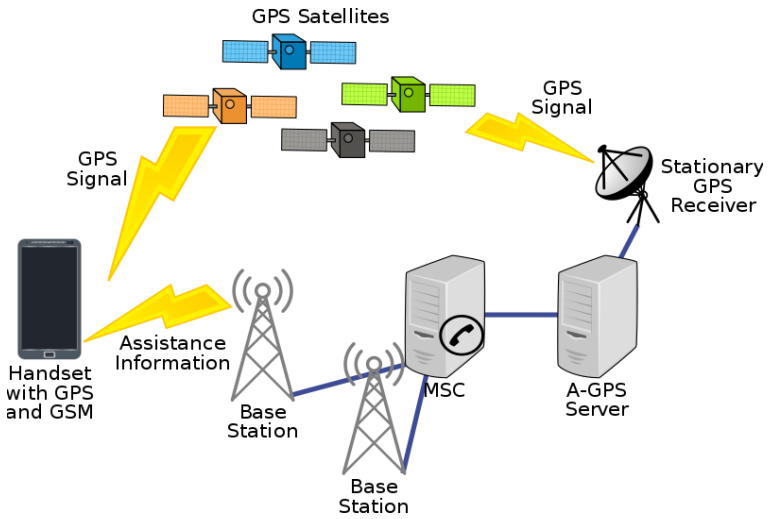
για κάθε δορυφόρο i από τον οποίο λαμβάνει σήμα.

Οι τέσσερις άγνωστοι είναι οι X, Y, Z, δt. Συνεπώς, χρειάζονται 4 δορυφόροι για τον προσδιορισμό τόσο της θέσης όσο και το συγχρονισμό του ρολογιού του δέκτη.

Το GPS έχει καθυστέρηση που μπορεί να ξεπεράσει το 1 λεπτό για τον αρχικό προσδιορισμό της θέσης του δέκτη (Time To First Fix – TTFF). Για το λόγο αυτό έχουν αναπτυχθεί βελτιώσεις, όπως το Υποβοηθούμενο GPS (Assisted GPS – A-GPS).

2.6.2 Assisted GPS (A-GPS)

Το A-GPS λύνει το πρόβλημα της καθυστέρησης στην αρχική εύρεση της τοποθεσίας του χρήστη, από το οποίο υποφέρει το GPS. Το δίκτυο κινητής τηλεφωνίας παρέχει στη συσκευή του χρήστη επιπλέον πληροφορίες, με αποτέλεσμα να έχουμε εύρεση τοποθεσίας μόλις σε λίγα δευτερόλεπτα.



Σχήμα 2.10: Το σύστημα A-GPS
Πηγή: https://commons.wikimedia.org/wiki/File:A-GPS.svg

Το σύστημα αυτό βοηθά ιδιαίτερα σε περιπτώσεις όπου τα σήματα των δορυφόρων είναι ασθενή λόγω μετεωρολογικών φαινομένων ή ανακλώνται από εμπόδια.

Το A-GPS λειτουργεί σε δίκτυα GSM, GPRS και UMTS και παρέχει ακρίβεια καλύτερη από τις μεθόδους Cell ID, E-OTD και OTDOA [3].

2.6.3 Χρήσεις των δορυφορικών συστημάτων γεωεντοπισμού (GNSS)

Εκτός από την παροχή πληροφοριών για την τοποθεσία, η ώρα που παρέχει το GPS και γενικότερα τα δορυφορικά συστήματα πλοήγησης χρησιμοποιείται σε πληθώρα εφαρμογών. Πέραν της απλής γνώσης της ακριβούς τρέχουσας ώρας από ένα τερματικό, τα συστήματα πλοήγησης δίνουν τη δυνατότητα για συγχρονισμό των ρολογιών των διαφόρων μερών κάθε συστήματος με μεγάλη ακρίβεια. Η ανάγκη αυτή είναι έκδηλη σε πολλές εφαρμογές, όπου απαιτείται συμφωνία μεταξύ απομακρυσμένων συσκευών για την τρέχουσα ώρα (π.χ. εκτέλεση τραπεζικών συναλλαγών).

Οι χρήσεις των GNSS [17] περιλαμβάνουν τα εξής:

- Εύρεση τοποθεσίας και πλοήγηση.
- Δρομολόγηση κλήσεων από δίκτυο κινητής τηλεφωνίας.
- Χρονολόγηση τραπεζικών συναλλαγών.
- Δίκτυα ηλεκτρικής ενέργειας για βέλτιστη παροχή ενέργειας και πρόληψη διακοπών.
- Υπολογιστικά κέντρα (data centers).
- Χρηματιστήρια για συγχρονισμό επενδυτικών κινήσεων.
- Καθοδήγηση αεροπλάνων από τον πύργο ελέγχου.

2.6.4 Αδυναμίες των δορυφορικών συστημάτων γεωεντοπισμού (GNSS)

Ο γεωεντοπισμός με χρήση δορυφόρων είναι περισσότερο διαδεδομένος από κάθε άλλο τρόπο γεωεντοπισμού. Ωστόσο, οι αδυναμίες που υπάρχουν θα μπορούσαν από το να μπερδέψουν έναν οδηγό αυτοκινήτου μέχρι και να οδηγήσουν σε πανικό τις χρηματιστηριακές αγορές [18] ή να θέσουν εκτός πορείας ένα αεροσκάφος.

Τα σήματα που εκπέμπουν οι δορυφόροι είναι αρκετά χαμηλής ενέργειας σε σχέση με την κοσμική ακτινοβολία. Συνεπώς, είναι εύκολο για κάποιον να τα παρεμβάλλει, εμποδίζοντας

την άφιξη του σήματος στο χρήστη. Επιπλέον, λόγω της έλλειψης κρυπτογράφησης, μπορεί κανείς να εκπέμψει με σχετικά μικρό κόστος και ισχύ ψευδή σήματα, μπερδεύοντας έτσι το χρήστη πως βρίσκεται σε λανθασμένη τοποθεσία.

Το Υπουργείο Εσωτερικής Ασφαλείας των Η.Π.Α. χαρακτήρισε το GPS ως «ένα μοναδικό σημείο αποτυχίας για κρίσιμες εφαρμογές» ("a single point of failure for critical applications") [19].

Οι αδυναμίες των GNSS [20] συνοψίζονται στα εξής:

1. **Παρεμβολή (jamming):** Τα σήματα των δορυφόρων GPS είναι πολύ ασθενή. Ένας κακόβουλος χρήστης μπορεί να χρησιμοποιεί συσκευή που δεν επιτρέπει στα σήματα των δορυφόρων να φτάσουν στους δέκτες των χρηστών.
2. **Απάτη (spoofing):** Παρόμοια με την παρεμβολή, είναι δυνατή η παραγωγή ψευδών σημάτων που ως στόχο έχουν να «μπερδέψουν» τον δέκτη και να συμπεράνει πως βρίσκεται σε άλλη τοποθεσία από αυτή που πραγματικά βρίσκεται.
3. **Φυσικά φαινόμενα:** Τα σήματα των δορυφόρων είναι δυνατόν να επηρεαστούν σημαντικά από φυσικά φαινόμενα, όπως για παράδειγμα από έντονη ηλιακή δραστηριότητα.
4. **Έλλειψη προτύπων (standards) και χαμηλή απόδοση δεκτών:** Οι δέκτες που πωλούνται στο εμπόριο δεν έχουν πάντα αναμενόμενη ποιότητα, με αποτέλεσμα να δυσλειτουργούν. Παράδειγμα αποτελούν οι οικονομικοί δέκτες που ενσωματώνονται σε κινητά τηλέφωνα (smartphones).
5. **Κακή απόδοση λόγω εμποδίων:** Δέντρα, ψηλά κτήρια και άλλα πιθανά εμπόδια προκαλούν δυσλειτουργία του συστήματος γεωεντοπισμού.
6. **Αδυναμία λειτουργίας σε εσωτερικούς χώρους:** Τα σήματα των δορυφόρων καθιστούν αδύνατο το γεωεντοπισμό σε εσωτερικούς και υπόγειους χώρους.
7. **Μεγάλη κατανάλωση ενέργειας:** Οι δέκτες GPS καταναλώνουν μεγάλη ποσότητα ενέργειας, γεγονός που εμποδίζει τη χρήση τους σε συσκευές με περιορισμένους πόρους (π.χ. αισθητήρες IoT).
8. **Απροστάτευτοι δορυφόροι στο διάστημα:** Οι δορυφόροι μπορεί να καταστραφούν είτε από κάποιο αντικείμενο είτε από κάποιο αντίπαλο κράτος.

2.6.5 Μέτρα προστασίας των GNSS

Τα δορυφορικά συστήματα γεωεντοπισμού, παρά τις αδυναμίες τους και τα τρωτά τους σημεία, αποτελούν την ευρέως χρησιμοποιούμενη τεχνολογία στον κόσμο.

Το Ίδρυμα Ανθεκτικής Πλοήγησης και Χρονομέτρησης (Resilient Navigation and Timing Foundation) αναφέρεται στο τρίπτυχο «Προστασία, Ανθεκτικότητα, Αύξηση» -- "Protect, Toughen and Augment" (PTA), το οποίο αναλύεται στα εξής [19]:

- Προστασία των δορυφόρων και των σημάτων που εκπέμπουν, τόσο με ανίχνευση και αντιμετώπιση επιθέσεων όσο και με κανονισμούς για παρεμβολές γειτονικών συχνοτήτων.
- Ανθεκτικότητα των χρηστών και του εξοπλισμού, με χρήση πολλαπλών δεκτών που είναι ανεκτικοί σε παρεμβολές και απάτες.
- Αύξηση των πηγών PNT (Position, Navigation and Timing – Τοποθεσία, Πλοήγηση και Ώρα) με δημιουργία ενός συμπληρωματικού συστήματος, όπως το eLoran.

2.7 LORAN (LOng RAnge Navigation)

Το LORAN [20], [21] είναι ένα επίγειο σύστημα εντοπισμού τοποθεσίας που αναπτύχθηκε από τις Η.Π.Α. κατά τη διάρκεια του 2ου Παγκοσμίου Πολέμου. Αρχικά χρησιμοποιήθηκε σε πλοία και έπειτα σε αεροπλάνα. Βασίζεται στην τεχνική Time Difference Of Arrival (TDOA).

Στην αρχική του έκδοση (Loran-A) είχε εμβέλεια 2.400 χιλιομέτρων και ακρίβεια της τάξης των δεκάδων μιλίων (περίπου 16 χλμ.). Η έκδοση Loran-B είχε ακρίβεια ορισμένων δεκάδων ποδιών (περίπου 3 μέτρων) αλλά δεν τέθηκε σε λειτουργία λόγω τεχνικών προβλημάτων. Η τρίτη έκδοση, Loran-C, είχε μεγαλύτερη εμβέλεια από την πρώτη και ακρίβεια εκατοντάδων ποδιών (περίπου 30 μέτρων). Τα σήματα που λάμβανε ένας δέκτης LORAN χρειάζονταν περαιτέρω ερμηνεία προκειμένου να εκτιμηθεί η τοποθεσία. Η ακρίβεια ήταν περισσότερο θέμα ποιότητας σήματος και εμπειρίας του χειριστή, παρά περιορισμοί του εξοπλισμού και των σημάτων.

Οι αδυναμίες του GPS και γενικότερα των GNSS επανέφεραν στο προσκήνιο το LORAN. Η τελευταία έκδοση, eLoran (Enhanced Loran) άρχισε να αναπτύσσεται από τις Η.Π.Α. στα μέσα της δεκαετίας του 1990. Το eLoran αποτελεί αναβάθμιση του Loran-C, αλλά μπορεί να χρησιμοποιήσει τους ίδιους σταθμούς εκπομπής. Λειτουργεί με μεγαλύτερη ισχύ από ότι τα GNSS και συνεπώς είναι δύσκολο να υποστεί παρεμβολές. Επιπλέον, χρησιμοποιεί χαμηλές συχνότητες (90-110 kHz) και απαιτεί μεγάλες κεραίες για την εκπομπή, κάτι που κάνει την παρεμβολή ιδιαίτερα απαιτητική [22]. Το eLoran παρέχει ακρίβεια 8 μέτρων για την τοποθεσία και 100 nanosecond για το χρόνο που λαμβάνει ο δέκτης [23]. Επίσης, λειτουργεί και σε εσωτερικούς χώρους, σε αντίθεση με τα GNSS. Συνεπώς, είναι ένα αυτόνομο σύστημα και ικανό να λειτουργήσει ως συμπληρωματικό των GNSS.

Ωστόσο, λόγω της κυριαρχίας του GPS και του απαιτούμενου κόστους το eLoran δεν χρησιμοποιείται. Η Ακτοφυλακή (Coast Guard) των Η.Π.Α., υπεύθυνη για τα συστήματα LORAN, σταμάτησε την εκπομπή LORAN-C το Φεβρουάριο του 2010.

2.8 Σύγκριση GPS-Loran

Με βάση το [20] κατασκευάζουμε τον παρακάτω συγκριτικό πίνακα:

	GPS	**LORAN**
Ισχύς σημάτων	Αδύναμα	Ισχυρά
Ανοχή σε φυσικά φαινόμενα	Όχι	Ναι
Ανοχή σε παρεμβολές	Όχι	Ναι
Προστασία εξοπλισμού	Όχι	Ναι
Ακρίβεια	8 μέτρα	15 μέτρα μέχρι 10 εκατοστά [24]
Λειτουργία σε εσωτερικό χώρο	Όχι	Ναι

2.9 Συστήματα γεωεντοπισμού εσωτερικού χώρου (Indoor Positioning Systems - IPS)

Όπως αναφέρθηκε, τα GNSS δεν μπορούν να χρησιμοποιηθούν σε εσωτερικούς χώρους. Τα συστήματα IPS βασίζονται σε διαφορετική υποδομή, προκειμένου να ανταπεξέλθουν στις απαιτήσεις ενός εσωτερικού χώρου.

Οι εσωτερικοί χώροι παρουσιάζουν πολλαπλές ανακλάσεις λόγω διάταξης και δομικών υλικών. Επιπλέον, εμποδίζουν τα σήματα των δορυφόρων, τα οποία είτε δεν φτάνουν καθόλου είτε φτάνουν εξασθενημένα. Ακόμα, στους εσωτερικούς χώρους λειτουργούν πολλές ηλεκτρικές και ηλεκτρονικές συσκευές.

Ορισμένες από τις ασύρματες τεχνολογίες που χρησιμοποιούνται στα IPS είναι τα ασύρματα δίκτυα WiFi, το Bluetooth, οι υπέρυθρες ακτίνες (IR), οι υπέρηχοι, καθώς και τα RFID tags [4].

2.10 Χαρτογράφηση δικτύων Wi-Fi

Ένας συνήθης τρόπος γεωεντοπισμού, ο οποίος δεν απαιτεί επιπλέον υποδομή και πρωτόκολλα, είναι η χαρτογράφηση των δικτύων Wi-Fi [25], [26]. Με άλλα λόγια, η διατήρηση μίας βάσης δεδομένων που αντιστοιχεί κάθε ασύρματο σημείο πρόσβασης (Wi-Fi Access Point) με ένα σημείο στο χάρτη. Κάθε ασύρματο δίκτυο έχει τη δική του ταυτότητα, η οποία αποτελείται από το όνομα (SSID) και τη διεύθυνση MAC.

Ορισμένοι πάροχοι υπηρεσιών τοποθεσίας (π.χ. Google) χρησιμοποιούν τα δεδομένα από συσκευές που διαθέτουν Wi-Fi και GPS (π.χ. smartphones), ώστε να προσδιορίσουν την τοποθεσία των δικτύων. Οι συσκευές γνωρίζουν την τοποθεσία τους με βάση το GPS, το Cell ID και το Wi-Fi. Παράλληλα, αποθηκεύουν τις ταυτότητες των ασύρματων δικτύων που «βλέπουν» σε κάθε τοποθεσία και στέλνουν τα δεδομένα στον πάροχο υπηρεσιών τοποθεσίας.

Με τον τρόπο αυτό μπορούμε να έχουμε εκτίμηση της τοποθεσίας ενός προσωπικού υπολογιστή ο οποίος δεν διαθέτει GPS, αλλά είναι συνδεδεμένος σε ένα δίκτυο Wi-Fi. Επιπλέον, μπορούμε να έχουμε ταχύτερο εντοπισμό σε περιοχές που δεν έχουν ισχυρό σήμα GPS.

2.11 Κωδικοποίηση τοποθεσίας (Location encoding ή geocoding)

Η έννοια της κωδικοποίησης τοποθεσίας (geocoding) έχει διπλή σημασία:

Αφενός, αναφέρεται στην υπολογιστική διαδικασία που μετατρέπει γεωγραφικά ονόματα (π.χ. διευθύνσεις) σε γεωγραφικές συντεταγμένες [27].

Αφετέρου, αναφέρεται σε ένα σύστημα το οποίο αντιστοιχεί αριθμούς (π.χ. συντεταγμένες), ονόματα (π.χ. διεύθυνση) ή άλλου είδους αναγνωριστικά (π.χ. αλληλουχία χαρακτήρων και αριθμών) σε τοποθεσίες [28], [29].

Στο σημείο αυτό θα ασχοληθούμε με την δεύτερη σημασία του όρου.

Υπάρχουν πολλά συστήματα κωδικοποίησης τοποθεσίας, η ακρίβεια των οποίων ποικίλει. Επιπλέον, άλλα είναι ευκολότερο να χρησιμοποιηθούν από ανθρώπους, ενώ άλλα είναι σχεδιασμένα για χρήση από μηχανές. Στην ενότητα αυτή, θα αναφέρουμε ορισμένα από αυτά, στην προσπάθειά μας να επιλέξουμε το καταλληλότερο για χρήση σε ένα περιβάλλον αποδείξεων τοποθεσίας.

2.11.1 Διευθύνσεις και αριθμοί

Το πιο γνώριμο σύστημα κωδικοποίησης τοποθεσίας είναι η διευθυνσιοδότηση οδών και αριθμοδότηση κτιρίων. Αυτό το σύστημα υπάρχει τουλάχιστον από το 1512, όπου αναπτύχθηκε σε μία περιοχή του Παρισιού [30]. Με το τρίπτυχο [οδός, αριθμός, πόλη] μπορεί κανείς συνήθως να αναφερθεί σε ένα κτίριο σε μία χώρα. Αν υπάρχει αμφιβολία, χρειάζεται να προστεθούν περισσότερες πληροφορίες. Για παράδειγμα, υπάρχει περιοχή Αμπελόκηποι τόσο στην περιοχή της Αθήνας όσο και σε αυτή της Θεσσαλονίκης. Σε αυτή την περίπτωση, πρέπει

να προστεθεί και η περιοχή, ούτως ώστε η τοποθεσία να είναι σαφώς ορισμένη. Επιπλέον, η διευθυνσιοδότηση διαφέρει από χώρα σε χώρα και δεν είναι καθολικά τυποποιημένη.

Συνεπώς, η χρήση διευθύνσεων είναι βολική για την καθημερινή μας συνεννόηση, όμως δεν ενδείκνυται όταν απαιτείται ακρίβεια ή χρήση από υπολογιστές.

2.11.2 Γεωγραφικό πλάτος και μήκος (συντεταγμένες)

Με την ενσωμάτωση των δυνατοτήτων γεωεντοπισμού και πλοήγησης στα κινητά τηλέφωνα (smartphones), η αναφορά σε μία τοποθεσία με χρήση συντεταγμένων γίνεται όλο και πιο γνώριμη.

Το γεωγραφικό πλάτος και μήκος είναι συνήθως δεκαδικοί αριθμοί που εκφράζουν μοίρες και αναφέρονται σε ένα σημείο πάνω στη Γη, με ακρίβεια που εξαρτάται από τον αριθμό τον δεκαδικών ψηφίων που παρέχονται. Μπορεί επίσης να εκφράζονται με μοίρες, λεπτά και δευτερόλεπτα.

Παρόλο που οι συντεταγμένες είναι το σύνηθες σύστημα που χρησιμοποιείται όταν εισάγουμε πληροφορίες τοποθεσίας σε υπολογιστές, έχουν δύο σημαντικά μειονεκτήματα. Αφενός, είναι πολύ δύσκολο να απομνημονευτούν. Αφετέρου, επειδή αναφέρονται σε σημεία, χρειάζονται τουλάχιστον τρία προκειμένου να ορίσουν μία περιοχή.

2.11.3 What3words [31]

Το what3words χωρίζει την επιφάνεια της Γης σε τετράγωνα 3 επί 3 μέτρα, δίνοντας σε κάθε ένα από αυτά μία ονομασία που αποτελείται από 3 λέξεις. Για παράδειγμα, η διεύθυνση ///graduated.sleepy.laptops, αναφέρεται σε ένα κομμάτι του κτιρίου της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Ε.Μ.Π.

Οι διευθύνσεις του what3words είναι σύντομες και εύκολα απομνημονεύσιμες. Είναι βολικές σε περίπτωση που χρειάζεται άμεση ενημέρωση (π.χ. τηλεφωνική) για μία τοποθεσία, ή για κάποιον που δεν έχει συνηθίσει το σχήμα διευθυνσιοδότησης μίας χώρας.

Τα μειονεκτήματα του συστήματος αυτού καθιστούν περιορισμένες τις δυνατότητές του. Αρχικά, οι διευθύνσεις παρέχονται σε πολλές γλώσσες, αλλά δεν έχουν καμία σχέση μεταξύ τους. Για παράδειγμα, η διεύθυνση που αναφέρθηκε παραπάνω στα Ελληνικά είναι ///κλειδώνω.περιμένει.κράνη. Συνεπώς, μία διεύθυνση έχει τόσες παραλλαγές όσες και οι γλώσσες που υποστηρίζει το σύστημα. Επιπλέον, παρόμοιες λέξεις μπορεί να αναφέρονται σε εντελώς διαφορετικές τοποθεσίες. Για παράδειγμα, η διεύθυνση ///graduate.sleepy.laptops αναφέρεται σε μία τοποθεσία στην Κίνα. Το γεγονός αυτό θα μπορούσε να προκαλέσει πρόβλημα σε περίπτωση τυπογραφικού λάθους ή παρανόησης. Ωστόσο, αυτό γίνεται σκόπιμα ώστε το λάθος να είναι προφανές [32]. Επίσης, οι γειτονικές διευθύνσεις δεν έχουν καμία σχέση μεταξύ τους, δυσκολεύοντας κάποιον να καταλάβει αν δύο τετράγωνα βρίσκονται κοντά. Τέλος, το σύστημα είναι κλειστού κώδικα και ελέγχεται από μία επιχείρηση, δυσκολεύοντας την ευρεία χρήση του.

2.11.4 Geohash [33], [34]

Το Geohash κωδικοποιεί μία τοποθεσία σε μία αλληλουχία γραμμάτων και αριθμών. Χρησιμοποιεί 32 χαρακτήρες, συγκεκριμένα τους αριθμούς 0-9 και τα γράμματα A-Z εκτός των A, I, L, O.

Τα geohashes αναπαριστούν περιοχές. «Κόβοντας» χαρακτήρες από τα δεξιά μειώνεται η ακρίβεια, αυξάνεται δηλαδή την περιοχή που περιγράφεται. Τα γειτονικά σημεία έχουν συχνά (όχι πάντα) ίδια προθέματα.

Υπάρχουν 5 ασυνέχειες, δηλαδή περιοχές όπου γειτονικά σημεία δεν έχουν παρόμοια προθέματα. Αυτά είναι στα γεωγραφικά μήκη 180 και 0, στον Ισημερινό, καθώς και στο Βόρειο και Νότιο πόλο.

2.11.5 Geohash-36 [35]

Το Geohash-36 είναι παρόμοιο με το Geohash, αλλά χρησιμοποιεί διαφορετικό αλγόριθμο και περιλαμβάνει 36 χαρακτήρες.

Είναι σχεδιασμένο περισσότερο για χρήση σε URLs, ηλεκτρονική αποθήκευση και επικοινωνία, παρά για ανθρώπινη χρήση. Περιλαμβάνει όμοιους χαρακτήρες σε κεφαλαία και μικρά, τους οποίους θεωρεί διαφορετικούς (case-sensitive). Αυτό αποτελεί σημαντική δυσκολία για τη χρήση σε ανθρώπινη συνεννόηση. Όπως και το Geohash, παρέχει μεταβαλλόμενη ακρίβεια, η οποία μειώνεται όσο λιγότερους χαρακτήρες έχει το hash.

Η αναφορά σε τοποθεσίες γίνεται με βάση το παρακάτω πλέγμα. Κάθε ένα από τα 36 τετράγωνα αποτελεί ένα επιπλέον εμφωλευμένο πλέγμα, κ.ο.κ.

2	3	4	5	6	7
8	9	b	B	C	d
D	F	g	G	h	H
j	J	K	l	L	M
n	N	P	q	Q	r
R	t	T	V	W	X

Σχήμα 2.11: Το πλέγμα του Geohash-36 [28]

Οι περιοχές μέσα σε κάθε τετράγωνο έχουν το ίδιο πρόθεμα. Ωστόσο, μεταξύ διαφορετικών τετραγώνων δημιουργούνται ασυνέχειες. Για παράδειγμα, η περιοχή g2 βρίσκεται πιο κοντά στην 9X, παρά στην g7. Αυτό δεν αντικατοπτρίζεται στα hashes των περιοχών. Πέραν αυτού, ο τρόπος με τον οποίο είναι διαμορφωμένο το πλέγμα, καθώς και η χρήση μικρών και κεφαλαίων γραμμάτων, δυσκολεύουν το χρήστη να συμπεράνει τη γειτνίαση και την απόσταση των περιοχών.

2.11.6 Mapcode [36]

Η κωδικοποίηση Mapcode αναφέρεται σε σημεία και όχι περιοχές. Ένα σημείο έχει τον παγκόσμιο μοναδικό κωδικό του, καθώς και έναν ή περισσότερους τοπικούς κωδικούς (με πρόθεμα χώρας). Επιπλέον, υποστηρίζει πολλά αλφάβητα, όπως Ελληνικό, Ινδικό, Κυριλλικό κ.α. Το γεγονός αυτό μπορεί να προκαλέσει πρόβλημα σε περιπτώσεις που χρησιμοποιούνται χαρακτήρες που είναι κοινοί σε πολλά αλφάβητα.

Το MapCode λαμβάνει υπόψη τις πυκνοκατοικημένες περιοχές, δίνοντας σε αυτές συντομότερους εναλλακτικούς κωδικούς. Για παράδειγμα, στη διεύθυνση «Ηρώων Πολυτεχνείου 9, Ζωγράφου» αντιστοιχεί ο παγκόσμιος κωδικός SKK3T.MMYF, καθώς και οι τοπικοί κωδικοί GRC MR.KMJ, GRC ΜΨ.43ΜΠ, GRC MLB3.TX, GRC FJBV.LDP.

Το σύστημα είναι δωρεάν και ανοιχτού κώδικα.

2.11.7 Open Post Code [37]

Οι κωδικοί Open Post Code αναφέρονται σε περιοχές. Παρόμοια με τα geohash, «κόβοντας» χαρακτήρες από τα δεξιά αυξάνεται το μέγεθος της αναφερόμενης περιοχής. Το OPC χρησιμοποιεί 25 χαρακτήρες που απαρτίζουν το παρακάτω πλέγμα 5x5.

2	3	4	5	6
7	8	9	C	D
F	G	H	J	K
L	M	N	P	Q
R	T	V	W	X

Σχήμα 2.12: Το αρχικό πλέγμα του Open Post Code [28]

Όπως και στα geohashes, παρουσιάζονται ασυνέχειες στα σύνορα των τετραγώνων. Για παράδειγμα, η περιοχή H2 βρίσκεται πιο κοντά στην 8X, παρά στην H6. Κάθε τοποθεσία έχει έναν μοναδικό παγκόσμιο κωδικό. Σε ορισμένες χώρες (π.χ. Ιρλανδία) οι τοποθεσίες διαθέτουν επιπλέον τοπικό κωδικό.

Το 2015 το πλέγμα επανασχεδιάστηκε, όπως φαίνεται στο παρακάτω σχήμα.

6	7	8	9	B
5	N	P	Q	C
4	M	X	R	D
3	L	W	T	F
2	K	J	H	G

Σχήμα 2.13: Το νέο πλέγμα του Open Post Code [37]

Το σύστημα είναι δωρεάν και ανοιχτού κώδικα.

2.11.8 Natural Area Code (NAC) [38]

Οι κωδικοί NAC αποτελούνται από 3 αλληλουχίες χαρακτήρων που χωρίζονται με κενό. Η πρώτη υποδεικνύει το γεωγραφικό πλάτος, η δεύτερη το γεωγραφικό μήκος και η τρίτη είναι προαιρετική και αναφέρεται σε υψόμετρο.

Χρησιμοποιούνται 30 χαρακτήρες, οι οποίοι απαρτίζουν ένα τρισδιάστατο πλέγμα 30x30x30. Ένας κωδικός NAC μπορεί να αναφέρεται σε ένα σημείο, σε μία γραμμή, σε μία περιοχή ή ακόμα και σε ένα τρισδιάστατο χώρο [39]. Παρόλο που μικρότεροι κωδικοί αναφέρονται σε μεγαλύτερες περιοχές, δεν έχουν απαραίτητα κοινό πρόθεμα με τις περιοχές που περιέχουν. Το σύστημα παρουσιάζει ασυνέχεια στο γεωγραφικό μήκος 180 και στους πόλους.

Απαιτείται άδεια για τη χρήση του και είναι κλειστού κώδικα.

2.11.9 Maidenhead Locator System [40]

Ο κώδικας αυτός αναπτύχθηκε από την κοινότητα των ραδιοερασιτεχνών. Οι συντεταγμένες συμπιέζονται σε μία σύντομη αλληλουχία χαρακτήρων, στην οποία εναλλάσσονται ζεύγη γραμμάτων και αριθμών. Σε κάθε ζεύγος, ο πρώτος χαρακτήρας αναφέρεται στο γεωγραφικό μήκος και ο δεύτερος στο γεωγραφικό πλάτος. Το πρώτο ζεύγος προσδιορίζει μία από τις 324 περιοχές στην οποία χωρίζεται η υδρόγειος.

Κάθε ζευγάρι προσδιορίζει μία υποπεριοχή μέσα σε αυτή που καθορίζει το προηγούμενο ζευγάρι. Συνεπώς, όσο περισσότερα ζευγάρια προστίθενται, τόσο μικρότερη γίνεται η αναφερόμενη περιοχή (αυξάνεται η ακρίβεια).

Ένα παράδειγμα αποτελεί ο κώδικας **BL11bh16.**

Παρόμοια συστήματα, τα οποία διαιρούν την επιφάνεια της Γης σε πλέγμα είναι τα World Geographic Reference System (GEOREF) [41], Global Area Reference System (GARS) [42], Universal Transverse Mercator (UTM) [43] και World Meteorological Organization (WMO) squares [44].

2.11.10 Open Location Code (Plus codes) [45]

Το σύστημα αυτό αναπτύχθηκε από την Google και τέθηκε σε λειτουργία τον Οκτώβριο του 2014. Χρησιμοποιεί κωδικούς που στην πλήρη μορφή τους έχουν μήκος 10 ή 11 χαρακτήρες. Οι κωδικοί στην πλήρη μορφή τους είναι παγκόσμια μοναδικοί και αναφέρονται σε περιοχές, όχι σημεία.

Στη συντομότερη μορφή τους, οι Plus codes έχουν μήκος 4-7 χαρακτήρες (τοπικοί κωδικοί). Μπορούν να χρησιμοποιηθούν αυτούσιοι όταν γίνεται αναζήτηση σε απόσταση 50 km από την ζητούμενη τοποθεσία. Παγκόσμια, μπορούν να χρησιμοποιηθούν δίνοντας μαζί την πόλη στην οποία ανήκει η ζητούμενη τοποθεσία.

Το αρχικό πλέγμα έχει 9 γραμμές και 18 στήλες, χωρίζοντας έτσι την υδρόγειο σε περιοχές (blocks) των 20 x 20 μοιρών. Κάθε block διαιρείται σε 20 x 20 υποπεριοχές έως και 4 φορές, φτάνοντας σε περιοχές μεγέθους 14x14 m. Στο σημείο αυτό ο πλήρης κωδικός έχει μήκος 10 χαρακτήρων. Από το επίπεδο αυτό, γίνεται μια τελευταία διαίρεση σε πλέγμα 5x4 υποπεριοχών, όπου πλέον κάθε περιοχή έχει μέγεθος περίπου 3x3 m. Για το επίπεδο αυτό απαιτούνται συνολικά 11 χαρακτήρες.

Για παράδειγμα, θεωρούμε τον κωδικό 8GC2CMXR+X6.

Ο κωδικός είναι πλήρης και παγκόσμιος (global code). Οι πρώτοι τέσσερις χαρακτήρες (8GC2) είναι ο κωδικός περιοχής (area code), ο οποίος περιγράφει μία περιοχή περίπου

100x100 km. Οι τελευταίοι έξι χαρακτήρες (CMXR+X6) είναι ο τοπικός κωδικός (local code) και περιγράφει μία περιοχή 14x14 m. Ο τοπικός κωδικός θα λειτουργήσει αν τον αναζητήσουμε έχοντας εστιάσει στην περιοχή που μας ενδιαφέρει. Ωστόσο, έχοντας τον παγκόσμιο χάρτη χρειάζεται να δώσουμε και την περιοχή στην οποία ανήκει. Στην περίπτωσή μας, αναζητώντας «CMXR+X6 Ιθάκη», παίρνουμε τη ζητούμενη περιοχή.

Όσο μικρότερος είναι ο κωδικός, τόσο μεγαλύτερη η περιοχή στην οποία αναφέρεται.

Γειτονικές περιοχές έχουν παρόμοιους κωδικούς. Όμως, οι χαρακτήρες που χρησιμοποιούνται δεν είναι συνεχείς, διότι έχουν αφαιρεθεί ορισμένοι χαρακτήρες του αλφαβήτου. Αυτό καθιστά δύσκολο για το χρήστη να συμπεράνει με χειροκίνητο τρόπο την απόσταση μεταξύ των περιοχών.

Οι κωδικοί παρουσιάζουν τρεις ασυνέχειες, στο γεωγραφικό μήκος 180 και στους πόλους. Ωστόσο, οι περιοχές αυτές έχουν πολύ μικρό πληθυσμό.

Οι plus codes μπορούν να κωδικοποιηθούν και να αποκωδικοποιηθούν χωρίς σύνδεση στο διαδίκτυο. Επιπλέον, είναι ανοιχτού κώδικα και ενσωματωμένοι στους χάρτες Google.

2.12 Επιλέγοντας το κατάλληλο σύστημα κωδικοποίησης τοποθεσίας

Τα διάφορα χαρακτηριστικά των συστημάτων κωδικοποίησης τοποθεσίας τα καθιστούν λιγότερο ή περισσότερο κατάλληλα για χρήση σε ένα περιβάλλον αποδείξεων τοποθεσίας.

Τα επιθυμητά χαρακτηριστικά ενός συστήματος κωδικοποίησης τοποθεσίας για χρήση σε πρωτόκολλα απόδειξης τοποθεσίας είναι:

1. Ένας κωδικός να αντιστοιχεί σε μοναδική περιοχή και κάθε περιοχή να έχει μοναδικό κωδικό.
2. Να χρησιμοποιεί πλέγμα περιοχών και όχι σημεία, υποστηρίζοντας έτσι την ευκολότερη επιβεβαίωση της γειτνίασης των κόμβων μέσα στην ίδια περιοχή, χωρίς να απαιτείται υπολογισμός απόστασης.
3. Γειτονικές περιοχές να έχουν παρόμοιους κωδικούς και κοινά προθέματα, διευκολύνοντας τον υπολογισμό της απόστασης των κόμβων. Δοθέντων δύο κωδικών, θα πρέπει να είναι εύκολος ο υπολογισμός της απόστασης, της σχετικής τους θέσης και του μεγέθους των περιοχών που αναπαριστούν.
4. Να υποστηρίζει διαβάθμιση του μεγέθους των περιοχών, με χρήση κωδικών αντίστοιχου μεγέθους (μικραίνοντας ένα κωδικό να αναφέρεται σε μεγαλύτερη περιοχή, η οποία περιλαμβάνει την αρχική). Το χαρακτηριστικό αυτό συμβάλλει στην μεταβαλλόμενη ακρίβεια τοποθεσίας και την προστασία της ιδιωτικότητας.
5. Να μπορεί να λειτουργήσει χωρίς σύνδεση στο διαδίκτυο, καθώς κατά τη δημιουργία της απόδειξης τοποθεσίας ενδέχεται να μην υπάρχει κάλυψη δικτύου.
6. Να είναι δωρεάν, ανοιχτού κώδικα και να διαθέτει υποστήριξη από ευρέως διαδεδομένες πλατφόρμες.

Με βάση τα συστήματα κωδικοποίησης τοποθεσίας που περιγράψαμε, καθώς και τα επιθυμητά χαρακτηριστικά, μία καλή λύση φαίνεται να είναι το Plus codes (Open Location Code)

3 Πρωτόκολλα Απόδειξης Τοποθεσίας (Proof of Location Protocols)

3.1 Ορισμοί

Ένα **πρωτόκολλο Απόδειξης Τοποθεσίας (Proof of Location protocol)** είναι ένα σύστημα-μηχανισμός με τον οποίο οι χρήστες μπορούν με τη βοήθεια άλλων οντοτήτων-χρηστών να αποκτούν απόδειξη της τοποθεσίας τους. Με την απόδειξη αυτή, οι εφαρμογές μπορούν να επιβεβαιώσουν την τοποθεσία του χρήστη για κάποια χρονική στιγμή.

Τα πρωτόκολλα Απόδειξης Τοποθεσίας παρουσιάζουν μεγάλη ποικιλία σχεδιασμού, αρχιτεκτονικής, υποδομής, ορολογίας που χρησιμοποιούν και στόχου που επιδιώκουν να πετύχουν. Στην ενότητα αυτή γίνεται προσπάθεια να οριστούν τα στοιχεία που χρησιμοποιούν τα περισσότερα πρωτόκολλα υπό ένα γενικότερο πρίσμα. Ορισμένα στοιχεία μπορεί να έχουν διαφορετική ονομασία σε κάθε πρωτόκολλο.

Απόδειξη Τοποθεσίας – AT (Location Proof - LP) [46], [47], [48]: Ένα ψηφιακό πιστοποιητικό το οποίο επικυρώνει την τοποθεσία ενός χρήστη σε μια συγκεκριμένη χρονική στιγμή. Μία απόδειξη τοποθεσίας μπορεί να αποτελείται από ένα ή περισσότερα Τεμάχια Απόδειξης Τοποθεσίας, ανάλογα με το πρωτόκολλο που χρησιμοποιείται.

Τεμάχιο Απόδειξης Τοποθεσίας – TAT (Location Proof Share-Segment) [47] **:** Ένα κομμάτι πληροφορίας που παράγει ένας χρήστης για να επικυρώσει την τοποθεσία ενός άλλου χρήστη σε μία συγκεκριμένη χρονική στιγμή.

Οι **χρήστες ενός πρωτοκόλλου AT** είναι οι οντότητες που χρησιμοποιούν το σύστημα απόδειξης τοποθεσίας. Ένας χρήστης μπορεί να αναλάβει διάφορους ρόλους κατά τη διάρκεια ζωής του στο σύστημα. Σε ένα πρωτόκολλο AT συμμετέχουν συνήθως οι παρακάτω χρήστες:

- **Αποδεικνύων (Prover):** Ο χρήστης ο οποίος καλείται να αποδείξει σε έναν άλλο χρήστη ότι βρισκόταν σε μία συγκεκριμένη τοποθεσία μία συγκεκριμένη χρονική στιγμή. Παρουσιάζει σε αυτόν την απόδειξη τοποθεσίας, η οποία έχει επικυρωθεί από τους Μάρτυρες.
- **Μάρτυρας (Witness):** Ο χρήστης ο οποίος βρίσκεται κοντά στον prover και ελέγχει αν αυτός αναφέρει αληθή τοποθεσία. Κάθε μάρτυρας κατασκευάζει το δικό του τεμάχιο απόδειξης τοποθεσίας, το οποίο και αποστέλλει στον prover.
- **Επιβεβαιωτής (Verifier):** Ο χρήστης ο οποίος θέλει να επιβεβαιώσει αν μία συγκεκριμένη χρονική στιγμή ο prover βρισκόταν πράγματι στην τοποθεσία που αναφέρει. Για να το πετύχει αυτό ελέγχει την εγκυρότητα της απόδειξης τοποθεσίας που του αποστέλλει ο prover. Ο επιβεβαιωτής είναι συνήθως η εφαρμογή που βασίζεται στην τοποθεσία του χρήστη (location-based service), αλλά μπορεί ακόμα και να είναι ένας φίλος ή συνεργάτης του αποδεικνύοντος [49], ακόμα και ένας δικαστής [50], ο οποίος καλείται να επιβεβαιώσει το άλλοθι ενός κατηγορούμενου.

Σε ένα τυπικό σύστημα Απόδειξης Τοποθεσίας, ένας αποδεικνύων P θέλει να αποδείξει σε έναν επιβεβαιωτή V ότι μία ορισμένη χρονική στιγμή βρισκόταν σε μία ορισμένη τοποθεσία. Για να το πετύχει αυτό, ανακαλύπτει γειτονικούς μάρτυρες W_i, οι οποίοι επιβεβαιώνουν αν ο P αναφέρει αληθή τοποθεσία και στέλνουν σε αυτόν τεμάχια απόδειξης τοποθεσίας. Με βάση αυτά, ο P κατασκευάζει την απόδειξη τοποθεσίας την οποία διατηρεί αποθηκευμένη και την

παρουσιάζει στον V όταν του ζητηθεί. Διακρίνονται έτσι δύο φάσεις, η φάση της δημιουργίας της AT και η φάση της επιβεβαίωσής της.

Αξίζει να αναφερθεί ότι ο ρόλος του μάρτυρα και του επιβεβαιωτή μπορεί να συμπίπτουν, όπως συμβαίνει στο [51], όπου ο επιβεβαιωτής βρίσκεται κοντά στον αποδεικνύοντα και αρκεί να επιβεβαιώσει την εγγύτητά τους. Σε αυτή την περίπτωση δεν υφίστανται τεμάχια απόδειξης τοποθεσίας. Επίσης, η δημιουργία και επιβεβαίωση της AT αποτελούν ένα στάδιο.

Σε ένα σύστημα απόδειξης τοποθεσίας μπορεί να συμμετέχουν επιπλέον οντότητες που φροντίζουν για τη σωστή λειτουργία του. Αυτές είναι:

- **Αρχή Πιστοποίησης/Τρίτη Έμπιστη Οντότητα (Certificate Authority/Third Trusted Party):** Διατηρεί τον κατάλογο των χρηστών που είναι εγγεγραμμένοι στο σύστημα και είναι υπεύθυνη για την έκδοση των κρυπτογραφικών κλειδιών των νέων χρηστών. Εκτελεί επιπλέον έλεγχο της ταυτότητας και των ψηφιακών υπογραφών των χρηστών.
- **Διακομιστής Αποδείξεων Τοποθεσίας (Proof of Location Server)** [49]**:** Σε ορισμένα πρωτόκολλα χρησιμοποιείται ένας διακομιστής ο οποίος συλλέγει τις αποδείξεις τοποθεσίας από τους αποδεικνύοντες (provers). Είναι υπεύθυνος για τη μεταβίβασή τους στον επιβεβαιωτή.

3.2 Εντοπισμός τοποθεσίας και απόδειξη τοποθεσίας

Στο σημείο αυτό θα εξηγήσουμε τη διαφορά μεταξύ του εντοπισμού και της απόδειξης τοποθεσίας και θα διερευνήσουμε περιπτώσεις στις οποίες το πρώτο μπορεί να περιλαμβάνει το δεύτερο.

Ο εντοπισμός τοποθεσίας είναι ο προσδιορισμός της γεωγραφικής θέσης ενός αντικειμένου, στην περίπτωσή μας μίας συσκευής.

Από την άλλη, η απόδειξη τοποθεσίας είναι η επιβεβαίωση της τοποθεσίας στην οποία η συσκευή ισχυρίζεται ότι βρίσκεται.

Φυσικά, για να μπορεί να ισχυριστεί μια συσκευή ότι βρίσκεται σε κάποια τοποθεσία, σημαίνει ότι έχει προσδιορίσει προηγουμένως την τοποθεσία αυτή. Τι γίνεται όμως στην περίπτωση που ο εντοπισμός της τοποθεσίας δεν γίνεται από την ίδια τη συσκευή;

Όπως είδαμε παραπάνω, είναι δυνατόν το δίκτυο (network-based) να υπολογίζει τη θέση της συσκευής με μεθόδους όπως η Cell ID. Τότε, θεωρώντας το δίκτυο ως verifier, μπορούμε να πούμε πως ταυτόχρονα με τον εντοπισμό, λαμβάνει και την απόδειξη της τοποθεσίας της συσκευής. Οι μέθοδοι όμως που βασίζονται στο δίκτυο υπονομεύουν την ιδιωτικότητα του χρήστη και απαιτούν τη συμβολή υπολογιστικών πόρων του δικτύου. Εκτός αυτού, μπορεί το δίκτυο να αποδέχεται την τοποθεσία της συσκευής ως έγκυρη, όχι όμως και οποιοσδήποτε verifier. Ο verifier είναι συνήθως μία εφαρμογή αποκομμένη από το δίκτυο του χρήστη [52].

Από την άλλη, στην καθημερινότητα χρησιμοποιούνται μέθοδοι που βασίζονται στην ίδια τη συσκευή (mobile-based) για να προσδιοριστεί η θέση της (π.χ. GPS, Loran). Από τη στιγμή που ο χρήστης έχει πρόσβαση στη συσκευή, μπορεί να παρουσιάζει ψευδείς τοποθεσίες στις υπηρεσίες που τον ενδιαφέρουν. Αυτές οι μέθοδοι δεν συμπεριλαμβάνουν απόδειξη τοποθεσίας, ωστόσο σέβονται την ιδιωτικότητα του χρήστη, καθώς ο υπολογισμός γίνεται τοπικά στη συσκευή.

Στη βιβλιογραφία [1], [46] γίνεται αναφορά σε υπολογιστικό υλικό ανεκτικό στην αλλοίωση (tamper-resistant hardware), όπως το Trusted Platform Module [53], [54]. Με τη χρήση του καθίσταται αδύνατη η αλλοίωση της τοποθεσίας που υπολογίζει ο δέκτης GPS στη συσκευή του χρήστη. Ωστόσο, η υποδομή αυτή δε διατίθεται σε κάθε συσκευή και έχει επιπλέον

κόστος. Εκτός αυτού, δεν έχει αποτέλεσμα αν φτάνουν στο δέκτη αλλοιωμένα σήματα GPS με σκοπό να τον «μπερδέψουν».

Συνεπώς, υπάρχει ανάγκη για ένα σύστημα που θα επιβεβαιώνει την τοποθεσία που υπολόγισε η ίδια η συσκευή του χρήστη, παρέχοντας απόδειξη τοποθεσίας προς οποιονδήποτε verifier ο χρήστης επιλέξει.

3.3 Χρήσεις των πρωτοκόλλων απόδειξης τοποθεσίας

Τα πρωτόκολλα απόδειξης τοποθεσίας μπορούν να βρουν χρησιμότητα σε πέντε γενικές κατηγορίες. Ωστόσο, εν δυνάμει μπορούν να χρησιμοποιηθούν σε όσες εφαρμογές βασίζονται στην τοποθεσία του χρήστη.

3.3.1 Έλεγχος πρόσβασης με βάση την τοποθεσία (Location-based access control)

Η πρόσβαση σε φυσικούς πόρους με βάση την τοποθεσία είναι κάτι πολύ οικείο για τον άνθρωπο. Για παράδειγμα, η πρόσβαση στους φυσικούς φακέλους των ασθενών είναι δυνατή μόνο με τη φυσική παρουσία στο χώρο που αποθηκεύονται. Όμως, με την εξάπλωση του διαδικτύου και του υπολογιστικού νέφους, τα αρχεία ψηφιοποιούνται και αποθηκεύονται ηλεκτρονικά. Ωστόσο, επιθυμούμε η πρόσβαση να είναι δυνατή μόνο με τη φυσική παρουσία των γιατρών στο χώρο του νοσοκομείου κατά τις ώρες εργασίας τους. Η τοποθεσία αυτού που θέλει να αποκτήσει πρόσβαση σε περιορισμένους πόρους θα πρέπει να αποδεικνύεται [48].

Ένα άλλο παράδειγμα αποτελεί η παροχή υπηρεσιών και περιεχομένου με βάση την τοποθεσία. Για παράδειγμα, ορισμένες ταινίες δεν είναι διαθέσιμες σε κάποιες χώρες λόγω πνευματικών δικαιωμάτων. Οι χρήστες μπορούν να χρησιμοποιήσουν εικονικά δίκτυα (VPNs) και σήραγγες (tunnels) ώστε να εμφανίζονται με διεύθυνση IP άλλης χώρας. Αν ο πάροχος των ταινιών ζητάει από τους χρήστες απόδειξη τοποθεσίας, τότε μία τέτοια παράκαμψη θα είναι αδύνατη.

3.3.2 Επιβράβευση τακτικών επισκεπτών και πελατών

Πολλές επιχειρήσεις και εφαρμογές θέλουν να επιβραβεύουν τους τακτικούς πελάτες ή επισκέπτες τους. Ωστόσο, η δυνατότητα των χρηστών να δηλώνουν ψευδείς επισκέψεις εμποδίζει την υλοποίηση τέτοιων στρατηγικών. Για παράδειγμα, στο Foursquare, όποιος δηλώνει την παρουσία του σε μία τοποθεσία τις περισσότερες φορές από κάθε άλλον μέσα σε διάστημα 30 ημερών γίνεται Δήμαρχος (Mayor) της τοποθεσίας [55]. Η επιχείρηση που πιθανόν σχετίζεται με την τοποθεσία μπορεί να επιβραβεύει το Δήμαρχο, προσφέροντας για παράδειγμα δωρεάν προϊόντα. Συνεπώς, δημιουργείται το κίνητρο της εξαπάτησης [1].

3.3.3 Επιβεβαίωση ιστορικού τοποθεσίας

Οι Αποδείξεις Τοποθεσίας που αφορούν παρελθοντικές χρονικές στιγμές θα ήταν ιδιαίτερα χρήσιμες σε περιπτώσεις όπου αμφισβητείται η εμπλοκή ή όχι ενός ατόμου σε ένα συμβάν. Για παράδειγμα, θα μπορούσε κανείς να αποδείξει το άλλοθι του κατά τη διάρκεια ενός εγκλήματος ή τη μη εμπλοκή του σε ένα ατύχημα, προκειμένου να μην υποστεί τις συνέπειες. Ειδικά στην περίπτωση του άλλοθι, η χρήση ψηφιακών ΑΤ υπερισχύει έναντι παραδοσιακών πειστηρίων, όπως περιγράφεται στο [50]. Συγκεκριμένα, είναι δυσκολότερο να παραποιη-

θούν (unforgeability), συσχετίζουν άμεσα και αναμφισβήτητα τις ταυτότητες των υποκειμένων (κατηγορούμενος και μάρτυρας) με το άλλοθι και αποτρέπουν την απώλεια των άλλοθι από τη μνήμη των υποκειμένων με το πέρασμα του χρόνου.

3.3.4 Υπηρεσίες κοινωνικής δικτύωσης

Η τοποθεσία έχει πλέον μεγάλη σημασία στα μέσα κοινωνικής δικτύωσης, καθώς προστίθενται συνεχώς υπηρεσίες που την απαιτούν. Συχνά οι χρήστες δηλώνουν την παρουσία τους σε κάποια τοποθεσία ή ανταλλάσσουν το στίγμα τους μεταξύ τους, προκειμένου ο ένας να συναντήσει τον άλλον. Αν και σε αυτές τις περιπτώσεις δεν τίθεται σημαντικό θέμα ασφαλείας, η εφαρμογή Αποδείξεων Τοποθεσίας θα μπορούσε να συντελέσει στην ειλικρίνεια μεταξύ των χρηστών. Άλλωστε, τα μέσα κοινωνικής δικτύωσης χρησιμοποιούνται εκτός των άλλων για συναλλαγές και για εύρεση εργασίας [48].

3.3.5 Παρακολούθηση προσώπων και αντικειμένων

Σημαντική είναι η ανάγκη που έχουν οι επιχειρήσεις να επιβεβαιώνουν την τοποθεσία των εργαζομένων και των προϊόντων τους. Για τους εργαζόμενους ενδιαφέρει η ώρα άφιξης και αναχώρησης. Επιπλέον, μπορεί να δίνεται ανταμοιβή σε εργαζόμενους που χρησιμοποιούν φιλικό προς το περιβάλλον τρόπο μετακίνησης από και προς το χώρο εργασίας τους [56]. Από την άλλη, οι επιχειρήσεις έχουν την ανάγκη να παρακολουθούν την πορεία που ακολουθούν τα φορτία τους αλλά και οι οδηγοί τους, ώστε να πληρώνονται για τις πραγματικές διαδρομές που εκτελούν.

3.4 Κακόβουλοι χρήστες

Σε ένα σύστημα Απόδειξης Τοποθεσίας μπορεί να υπάρξουν οι παρακάτω κακόβουλοι χρήστες [47], [48], [57]:

1. **Υποκλοπέας:** Κρυφακούει την επικοινωνία νόμιμων (legitimate) χρηστών του συστήματος με σκοπό να αποκτήσει γνώση της ταυτότητας ή της θέσης τους.

2. **Κακόβουλος prover:** Επιδιώκει να εκδώσει μία ΑΤ για μία τοποθεσία στην οποία δεν βρέθηκε ή για μια τοποθεσία στην οποία βρέθηκε αλλά κάποια διαφορετική χρονική στιγμή. Μπορεί να εξαπατά έναν η περισσότερους witnesses ότι βρίσκεται πράγματι κοντά τους ή να επεμβαίνει στο περιεχόμενο των ΤΑΤ που λαμβάνει από αυτούς. Επιπλέον, επιδιώκει να δημιουργήσει μόνος του ΑΤ ή να «κλέψει» ΑΤ άλλων χρηστών και να τις παρουσιάσει ως δικιές του. Μπορεί ακόμα να θέλει να αποκτήσει πληροφορίες για την ταυτότητα των witnesses που βρίσκονται κοντά του. Μπορεί να επιδιώκει τη δημιουργία πολλών ταυτοτήτων-χρηστών οι οποίοι λειτουργούν ως witnesses και παράγουν ΑΤ για λογαριασμό του (Sybil attack [58]).

3. **Κακόβουλος verifier:** Επιδιώκει να εκθέσει την τοποθεσία του prover ή να υποκλέψει την τοποθεσία του χωρίς την έγκρισή του. Μπορεί επιπλέον να λειτουργεί ως ενδιάμεσος, χρησιμοποιώντας τις αποδείξεις τοποθεσίας που αυτός του στέλνει ως δικές του.

4. **Κακόβουλος witness:** Επιδιώκει σκόπιμα ένα η περισσότερα από τα παρακάτω:
   - να μη συνεργαστεί με τον prover (Denial Of Service)

- να εκδώσει ΤΑΤ το οποίο αναφέρεται σε τοποθεσία μακριά από αυτή που αναφέρει ο prover, καθιστώντας την ΑΤ άκυρη
- να εκδώσει ΤΑΤ το οποίο πιστοποιεί μία ψευδή τοποθεσία στην οποία ο prover δεν έχει φυσική παρουσία (συνεργασία με prover).
- να εκδώσει περισσότερα από ένα ΤΑΤ για την ίδια ΑΤ, ίσως χρησιμοποιώντας διαφορετικές ταυτότητες, με σκόπο να ενισχύσει την εγκυρότητά της
- να ανακαλύψει πληροφορίες για την ταυτότητα του prover

5. **Κακόβουλη CA (Certificate Authority):** Ψεύδεται σχετικά με τους ελέγχους που πραγματοποιεί στις ταυτότητες των χρηστών, μεροληπτεί ευνοώντας κάποιους χρήστες και αδικώντας άλλους ή ακόμα και εκθέτει την ταυτότητα των χρηστών.

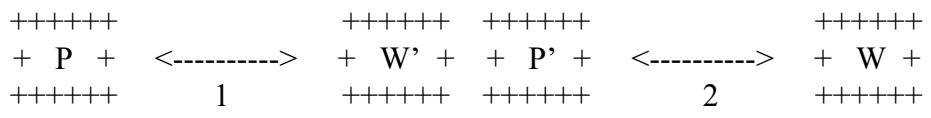
6. **Κακόβουλος server:** Διαρρέει πληροφορίες που αφορούν τους χρήστες, δεν παραδίδει τις αποδείξεις τοποθεσίας στον verifier. Μπορεί ακόμα να συνεργάζεται με την CA για την αποκάλυψη τόσο της ταυτότητας όσο και της τοποθεσίας των χρηστών [49].

3.5 Είδη επιθέσεων

Οι επιθέσεις περιγράφονται αναλυτικά στα [1], [47], [48], [56]. Μπορεί να υποκινούνται από έναν κακόβουλο χρήστη ή να προκύπτουν από συνεργασία κακόβουλων χρηστών.

1. **Απάτη απόστασης (Distance fraud):** Ένας κακόβουλος prover προσπαθεί να πείσει ένα ειλικρινή witness ότι βρίσκεται πιο κοντά του από ότι στην πραγματικότητα. Συνεπώς, εκδίδει ΑΤ με ψευδή τοποθεσία.

2. **Επίθεση ενδιάμεσου (Mafia fraud-Man in the middle):** Ο στόχος του επιτιθέμενου είναι να αναπαράγει μια συνεδρία που περιλαμβάνει έναν prover P και ένα witness W, με σκοπό να εξαπατήσει τον W ότι ο P βρίσκεται πράγματι κοντά του.



Ο επιτιθέμενος δημιουργεί δύο κακόβουλους κόμβους, ένα witness W' και έναν prover P'. Αυτοί οι 2 κόμβοι χρησιμοποιούνται ως πύλη (gateway) προκειμένου να ταυτοποιηθεί ο χρήστης P στον χρήστη W.

Στην πρώτη συνεδρία, το πρωτόκολλο εκτελείται μεταξύ του κακόβουλου witness W' και του prover P, με σκοπό να αποκτήσει ο W' το αίτημα του P για έκδοση ΑΤ, μαζί με πιθανά κρυπτογραφικά στοιχεία, τα οποία εξαρτώνται από το κάθε πρωτόκολλο.

Στη δεύτερη συνεδρία, ο κακόβουλος prover P' προσποιείται στον W ότι είναι ο P, με σκοπό να αποσπάσει τελικά μία έγκυρη ΑΤ που έχει εκδοθεί για τον P.

Η επίθεση αυτή μπορεί να εκτελείται από κάποιον τρίτο ο οποίος θέλει να αποκτήσει μία ΑΤ στο όνομα του χρήστη P, αλλά και εν γνώση του P, ώστε να εμφανίζεται ότι βρίσκεται κοντά στον W και να αποκτήσει μία ΑΤ χωρίς να βρίσκεται πράγματι σε αυτή την τοποθεσία.

3. **Υποκλοπή απόστασης (Distance hijacking):** Ένας κακόβουλος χρήστης M προσπαθεί να υποκλέψει μία συνεδρία ενός ειλικρινούς prover P. Ο M περιμένει από τον P να

επιβεβαιώσει ότι γειτνιάζει με τα witnesses W_i, και έπειτα προσπαθεί να υποκλέψει από αυτόν τα ΤΑΤ που συλλέγει.

4. **Συνεργασία prover-prover (Terrorist fraud):** Σε αυτή την περίπτωση ένας prover P_1 που βρίσκεται στην τοποθεσία X, συνεργάζεται με έναν prover P_2, που βρίσκεται στην τοποθεσία Y, ώστε ο P_2 να συλλέξει ΤΑΤ από γειτονικούς του witnesses για λογαριασμό του P_1, ώστε τελικά να δημιουργήσει μία ΑΤ που παρουσιάζει τον P_1 στη θέση Y.

5. **Συνεργασία witness-witness:** Οι μάρτυρες συνεργάζονται μεταξύ τους ώστε είτε να επιβεβαιώσουν μία ψευδή τοποθεσία για τον prover P, είτε να μην συμμετάσχουν σκόπιμα στην εκτέλεση του πρωτοκόλλου.

6. **Συνεργασία prover-witness:** Ένας prover P ζητά από έναν witness W να επιβεβαιώσει πως βρίσκεται σε μία ψευδή τοποθεσία. Ο W αποστέλλει ένα ή περισσότερα ΤΑΤ που πιστοποιούν τον ψευδή ισχυρισμό του P.

3.6 Έγκυρες και αληθείς αποδείξεις τοποθεσίας

Στο σημείο αυτό είναι σημαντικό να γίνει κατανοητή η διαφορά μεταξύ έγκυρης και αληθούς απόδειξης τοποθεσίας και κατ' αντιστοιχία μεταξύ άκυρης και ψευδούς απόδειξης τοποθεσίας.

Αληθής είναι η απόδειξη τοποθεσίας που αναφέρεται σε μία τοποθεσία στην οποία ο prover πράγματι υπήρξε την αναφερόμενη χρονική στιγμή.
Ψευδής είναι η απόδειξη τοποθεσίας που αναφέρεται σε μία τοποθεσία στην οποία ο prover δεν βρισκόταν την αναφερόμενη χρονική στιγμή.

Έγκυρη είναι η απόδειξη τοποθεσίας που ικανοποιεί τις απαιτήσεις του πρωτοκόλλου και γίνεται δεκτή από την CA και τον verifier.
Άκυρη είναι η απόδειξη τοποθεσίας η οποία έχει παραβιάσει τους κανόνες του πρωτοκόλλου και δεν γίνεται αποδεκτή από την CA και τον verifier.

Ονομάζουμε **ορθή** την έγκυρη και αληθή απόδειξη τοποθεσίας.
Στόχος των πρωτοκόλλων απόδειξης τοποθεσίας είναι κάθε έγκυρη ΑΤ να είναι και αληθής, με άλλα λόγια να εντοπίζονται ψευδείς ισχυρισμοί και να ακυρώνονται.

3.7 Χαρακτηριστικά των πρωτοκόλλων Α.Τ.

Υπάρχουν αρκετά πρωτόκολλα απόδειξης τοποθεσίας, κάθε ένα από τα οποία παρουσιάζει διαφορετικά χαρακτηριστικά. Οι επιλογές εξαρτώνται από τους στόχους και τη σχεδίαση του κάθε πρωτοκόλλου. Η ύπαρξη πολλών χαρακτηριστικών δεν οδηγεί απαραίτητα σε ένα αποδοτικό και ασφαλές πρωτόκολλο.
Μετά από εκτενή μελέτη της βιβλιογραφίας διακρίθηκαν τα βασικά χαρακτηριστικά των πρωτοκόλλων απόδειξης τοποθεσίας.

1. **Αρχιτεκτονική σταδίου Α - Δημιουργία ΑΤ:** Για τη δημιουργία της ΑΤ ο prover επικοινωνεί με γειτονικούς του κόμβους-witnesses. Αυτοί οι κόμβοι μπορεί να είναι άλλοι χρήστες, οπότε έχουμε μία αρχιτεκτονική **κόμβο-προς-κόμβο (peer-to-peer)**, ή

μπορεί να είναι κόμβοι που ελέγχονται από μία κεντρική αρχή (ή τον verifier), οπότε έχουμε μία **κεντρικοποιημένη (centralized)** αρχιτεκτονική. Στη δεύτερη κατηγορία εμπίπτει και η περίπτωση που χρησιμοποιείται server κατά τη διαδικασία. Ενδέχεται στη διαδικασία να συνδυάζονται κόμβοι και κεντρική αρχή, οπότε έχουμε μια **υβριδική (hybrid)** αρχιτεκτονική.

2. **Αρχιτεκτονική σταδίου Β - Επιβεβαίωση ΑΤ:** Η επιβεβαίωση της ΑΤ του prover μπορεί να γίνεται απευθείας από τον verifier με **άμεση (direct)** επιβεβαίωση, ή μπορεί να εμπλέκει server/CA/άλλους κόμβους, οπότε πρόκειται για **έμμεση (indirect)** επιβεβαίωση.

3. **Χρήση Τρίτης Έμπιστης Οντότητας/Αρχής Πιστοποίησης (TTP/CA):** Ορισμένα πρωτόκολλα θεωρούν την ύπαρξη αρχής πιστοποίησης, η οποία είναι υπεύθυνη για τη δημιουργία νέων χρηστών του συστήματος καθώς και για τη διατήρηση της ταυτότητάς τους. Αν και η αρχή πιστοποίησης αποτελεί έναν εύκολο τρόπο να επαληθευτεί η ταυτότητα ενός prover που παραδίδει ΑΤ σε έναν verifier, η δυσλειτουργία της μπορεί να οδηγήσει σε κατάρρευση ολόκληρου του συστήματος (single point of failure).

4. **Φυσικό στρώμα:** Για τον εντοπισμό των witnesses από τον prover και την πιστοποίησή του από αυτούς, χρησιμοποιείται συνήθως ένα φυσικό στρώμα μικρής εμβέλειας. Αρκετές υλοποιήσεις χρησιμοποιούν Bluetooth, WiFi ή ZigBee. Άλλες χρησιμοποιούν δίκτυα ευρείας περιοχής και χαμηλής ενέργειας (LPWAN - low-power wide-area network), όπως το LoRa.

5. **Κωδικοποίηση τοποθεσίας (geocoding):** Η τοποθεσία ενός κόμβου μπορεί να περιγραφεί με διάφορους τρόπους, όπως περιγράψαμε σε προηγούμενη ενότητα. Κάποια πρωτόκολλα χρησιμοποιούν συγκεκριμένο σύστημα geocoding, άλλα το θεωρούν αδιάφορο, ενώ άλλα αναφέρονται αυθαίρετα σε τοποθεσίες (π.χ. χώρα, πόλη, κ.τ.λ.).

6. **Εύρεση τοποθεσίας:** Ένα πρωτόκολλο ΑΤ μπορεί να διαθέτει το δικό του σύστημα εύρεσης τοποθεσίας του prover, ή να επαληθεύει την τοποθεσία που δίνεται από το GPS και από άλλες πηγές. Υπάρχουν επίσης υβριδικές υλοποιήσεις, που συνδυάζουν τις δύο παραπάνω τεχνικές γεωεντοπισμού.

7. **Έλεγχος εγγύτητας-γειτνίασης:** Αποτελεί μία διαδικασία κατά την οποία οι witnesses επιβεβαιώνουν ότι ο prover βρίσκεται πράγματι κοντά τους. Δύο γνωστές μέθοδοι είναι η ταχεία ανταλλαγή δυαδικών αριθμών (distance bounding, fast-bit exchange) [56] και η σύγκριση ηλεκτρομαγνητικών σημάτων-δικτύων της περιοχής [57].

8. **Κίνητρο συμμετοχής:** Στα περισσότερα πρωτόκολλα υπάρχουν χρήστες που πιστοποιούν την τοποθεσία του prover, ή ακόμα και την προσδιορίζουν. Για το λόγο αυτό μπορεί να είναι επιθυμητή η παροχή κινήτρου σε αυτούς, όπως για παράδειγμα η ανταμοιβή σε κάποιο κρυπτονόμισμα. Με τον τρόπο αυτό θα συνεχίσουν να συμμετέχουν στο σύστημα παρέχοντας απαραίτητους πόρους για τη λειτουργία του.

9. **Μεταβαλλόμενη ακρίβεια τοποθεσίας:** Δίνει τη δυνατότητα στον prover να επιλέγει την ακρίβεια με την οποία θα δώσει την τοποθεσία του στον verifier. Για παράδειγμα, η τοποθεσία του μπορεί να δίνεται με ακρίβεια ορισμένων μέτρων, ή με το όνομα της

πόλης στην οποία βρίσκεται, σε περίπτωση που χρησιμοποιείται μία αυθαίρετη κωδικοποίηση τοποθεσίας.

10. **Ανεξαρτησία από verifier (verifier-agnostic):** Η απόδειξη τοποθεσίας που παράγεται δεν αφορά έναν συγκεκριμένο verifier, αλλά μπορεί να χρησιμοποιηθεί από πολλούς. Το χαρακτηριστικό αυτό είναι προϋπόθεση για την πλήρη υποστήριξη ΑΤ που εκδίδει ο prover χωρίς να του ζητηθούν και χωρίς να αφορούν έναν συγκεκριμένο verifier. Για παράδειγμα, κατά τη δημιουργία μίας ΑΤ που αποτελεί άλλοθι, ο χρήστης δεν γνωρίζει σε ποιον verifier θα πρέπει να αναφέρεται. Σε επόμενη ενότητα γίνεται αναφορά στο ζήτημα αυτό.

11. **Αλυσίδες Αποδείξεων Τοποθεσίας:** Ο prover μπορεί να κατασκευάσει αλυσίδες από ΑΤ για τοποθεσίες που επισκέφθηκε, τις οποίες δεν μπορεί να αλλοιώσει (tamper-proof) ή μπορεί να αλλοιώσει αλλά αυτό θα είναι εμφανές (tamper-evident). Με τον τρόπο αυτό ο verifier μπορεί να παρακολουθήσει το ιστορικό τοποθεσιών του prover. Για την προστασία της ιδιωτικότητας του prover, δίνεται η δυνατότητα να επιλέγει κάποιο κομμάτι της αλυσίδας που θέλει να παρουσιάσει, καθώς και να αποκρύψει τα στοιχεία ορισμένων ΑΤ της αλυσίδας, αλλά όχι την ύπαρξή τους σε αυτήν. Στη βιβλιογραφία αναφέρονται ως provenance chains. Ο αναγνώστης παραπέμπεται στο [59] για περισσότερες πληροφορίες.

3.8 Προδιαγραφές των πρωτοκόλλων Α.Τ.

Τα πρωτόκολλα απόδειξης τοποθεσίας θα πρέπει να ικανοποιούν ορισμένες προδιαγραφές, ώστε να εξασφαλίζεται η ασφαλής λειτουργία τους και η ατρωσία σε επιθέσεις, καθώς και να προστατεύεται η ιδιωτικότητα των χρηστών που μετέχουν σε αυτό.

Η ανάλυση των προδιαγραφών βασίζεται στο [47], με προσθήκες που προέκυψαν από την έρευνα και κατανόηση των αναγκών για ασφαλή και ιδιωτικά πρωτόκολλα.

3.8.1 Προδιαγραφές ασφαλείας

1. **Ακεραιότητα δεδομένων (data integrity-unforgeability):** Θα πρέπει να είναι αδύνατον για έναν prover να τροποποιήσει τα ΤΑΤ που δέχεται από τους witnesses. Επίσης, θα πρέπει να είναι αδύνατον για έναν τρίτο να επέμβει στα ΤΑΤ και την ΑΤ που τελικά δημιουργείται και αποστέλλεται στον verifier, χωρίς αυτό να είναι εμφανές.

2. **Αδυναμία Απόκρυψης/Προσθήκης ΤΑΤ:** Θα πρέπει να είναι αδύνατο για τον prover να επιλέξει ποια ΤΑΤ που δέχθηκε θα συμπεριλάβει στην ΑΤ που κατασκευάζει. Αυτό σημαίνει πως δεν μπορεί να προσθέτει ή να αφαιρεί ΤΑΤ κατά βούληση. Ακόμα και να το κάνει, θα πρέπει αυτό να είναι εμφανές και η ΑΤ να θεωρείται άκυρη.

3. **Μη μεταβιβάσιμη πληροφορία (non-transferability):** Η ΑΤ που παράγει ο prover θα πρέπει να είναι δεμένη με την ταυτότητά του (proof of ownership) και να μην μπορεί να χρησιμοποιηθεί από κάποιον άλλο χρήστη για να επιβεβαιώσει την τοποθεσία του στον verifier.

4. **Αντοχή στην απάτη απόστασης (distance fraud):** Το πρωτόκολλο θα πρέπει να φροντίζει ώστε να γίνεται έλεγχος εγγύτητας μεταξύ των witnesses και του prover, ώστε

να μην μπορεί αυτός να τους εξαπατήσει ότι βρίσκεται πιο κοντά τους από ότι στην πραγματικότητα.

5. **Αντοχή στην επίθεση ενδιάμεσου (mafia fraud):** Η συνεδρία μεταξύ prover P και witness W_i θα πρέπει να είναι μοναδική για κάθε ΑΤ και να μην είναι δυνατόν να αναπαραχθεί από κάποιον κακόβουλο ενδιάμεσο χρήστη (man in the middle).

6. **Αντοχή στην υποκλοπή απόστασης (distance hijacking):** Τα ΤΑΤ που παράγουν οι witnesses θα πρέπει να αφορούν αποκλειστικά τη συγκεκριμένη ΑΤ που ζητάει ο prover, για τον οποίο εκτελείται η διαδικασία ελέγχου εγγύτητας. Για οποιονδήποτε άλλο χρήστη τα ΤΑΤ αυτά θα πρέπει να είναι άχρηστα.

7. **Αντοχή στη συνεργασία P-P:** Θα πρέπει να είναι αδύνατον για έναν prover να συλλέξει ΤΑΤ για λογαριασμό ενός άλλου prover. Η προδιαγραφή αυτή ικανοποιείται από τον συνδυασμό της μη μεταβιβασιμότητας, της αντοχής στην απάτη απόστασης και της αντοχής στην υποκλοπή απόστασης.

8. **Αντοχή στη συνεργασία P-W:** Ένας prover θα πρέπει να μην είναι σε θέση να γνωρίζει ποιο witness του έστειλε κάθε ΤΑΤ, καθώς και αν σε αυτό το ΤΑΤ που του απέστειλε εγκρίνει ή απορρίπτει τον ισχυρισμό του. Αν ο ισχυρισμός του prover απορρίπτεται, είναι επιθυμητό αντί να μην στέλνεται ΤΑΤ, να στέλνεται απορριπτικό ΤΑΤ. Έτσι, ο prover δεν μπορεί να συμπεράνει την απόφαση του witness.

9. **Αντοχή στη συνεργασία W-W:** Τα witnesses δε θα πρέπει να γνωρίζουν αν το καθένα έχει εγκρίνει η απορρίψει τον ισχυρισμό του prover. Το πρωτόκολλο πρέπει να αποκρύπτει πιθανά στοιχεία που θα επιτρέψουν στα witnesses να επικοινωνήσουν μεταξύ τους.

10. **Μοναδικότητα ΤΑΤ:** Θα πρέπει να υπάρχει έλεγχος ότι κάθε witness παράγει ακριβώς ένα ΤΑΤ για τη συγκεκριμένη ΑΤ. Η προδιαγραφή αυτή ικανοποιείται και στην περίπτωση που ένα ΤΑΤ αποτελεί ΑΤ.

11. **Όχι μοναδικό σημείο αποτυχίας (single point of failure):** Η εξάρτηση σε φορείς που μπορεί να θέσουν το σύστημα εκτός λειτουργίας αν αποτύχουν (π.χ. αν πέσουν θύματα επίθεσης) θα πρέπει να αποφεύγεται.

3.8.2 Προδιαγραφές ιδιωτικότητας

1. **Ανωνυμία και αδυναμία συσχετισμού:** Συσχετισμός σημαίνει ότι κάποιος μπορεί να συμπεράνει ότι δύο μηνύματα προέρχονται από τον ίδιο χρήστη. Η αδυναμία συσχετισμού ισοδυναμεί με την ανωνυμία ενός χρήστη ως προς κάποια οντότητα. Αναφερόμαστε σε αυτή την προδιαγραφή ως ΑΑΣ (Ανωνυμία και Αδυναμία Συσχετισμού). Διακρίνουμε τις παρακάτω περιπτώσεις και υποπεριπτώσεις.

   α. Ανωνυμία κατά το στάδιο Α - Δημιουργία ΑΤ: Κατά την ανταλλαγή μηνυμάτων μεταξύ ενός prover P και ενός witness Wx, θα πρέπει να μην μαθαίνει ο ένας την ταυτότητα του άλλου. Επίσης, πρέπει να είναι αδύνατον για κάποιον τρίτο, καθώς και για τους άλλους witnesses να αποκτήσουν γνώση της ταυτότητας των P και Wx. Συγκεκριμένα:

i. Αδυναμία συσχετισμού prover (στάδιο Α): Ένας witness δε θα πρέπει να μπορεί να συμπεράνει αν δύο αιτήσεις για ΑΤ προέρχονται από τον ίδιο prover.

ii. Αδυναμία συσχετισμού witness (στάδιο Α): Ένας prover δε θα πρέπει να μπορεί να συμπεράνει αν δύο ΤΑΤ (στην ίδια ή διαφορετική συνεδρία) που λαμβάνει προέρχονται από τον ίδιο witness.

β. Ανωνυμία κατά το στάδιο Β - Επιβεβαίωση ΑΤ: Ο verifier θα πρέπει να μαθαίνει μόνο την ταυτότητα του prover που του έστειλε την ΑΤ. Δε θα πρέπει να αναγνωρίζει την ταυτότητα των witnesses που συμμετείχαν στη δημιουργία της ΑΤ, εκτός αν είναι επιστρατευμένα από αυτόν και τα θεωρεί έμπιστα (trusted). Κανένας άλλος εκτός του verifier και την CA που πιθανώς χρησιμοποιείται δε θα πρέπει να μπορεί να δει την ταυτότητα του prover και των witnesses που περιλαμβάνονται στην ΑΤ. Συγκεκριμένα:

i. Αδυναμία συσχετισμού prover (στάδιο Β): Κανένας άλλος εκτός από τον verifier και την CA δε θα πρέπει να μπορεί να συμπεράνει αν δύο ΑΤ ανήκουν στον ίδιο prover.

ii. Αδυναμία συσχετισμού witness (στάδιο Β): Κανένας δε θα πρέπει να είναι σε θέση να αναγνωρίσει αν δύο ΤΑΤ προέρχονται από το ίδιο witness, εκτός αν αυτό απαιτείται για την διατήρηση στοιχείων φήμης (reputation) σε σχήματα εμπιστοσύνης (trust schemas).

Ο συσχετισμός είναι αδύνατος αν η ταυτότητα του χρήστη εμφανίζεται με ψευδώνυμα [49] ή κρυπτογραφημένη [47] μέσα στα μηνύματα. Επίσης, οι υπογραφές των χρηστών θα πρέπει με κάποιο τρόπο να προστατεύονται, ώστε να μην είναι εύκολο για κάποιον κακόβουλο να προσπαθήσει να μάθει σε ποιον ανήκουν.

2. **Ιδιωτικότητα τοποθεσίας witness:** Η τοποθεσία των witnesses δε θα πρέπει να αποκαλύπτεται μέσα στα ΤΑΤ ή την ΑΤ. Αντ' αυτού, είναι δυνατόν να εκφράζεται η απόσταση από τον prover, αφού αρκεί να πιστοποιηθεί ότι ο witness βρίσκεται κοντά στον prover.

3. **Ιδιωτικότητα τοποθεσίας prover:** Η τοποθεσία του prover θα πρέπει να γίνεται γνωστή μόνο στους witnesses που καλούνται να την πιστοποιήσουν, καθώς και στον verifier. Είναι επιθυμητό να επιλέγει ο prover την ακρίβεια με την οποία αυτή θα γίνεται γνωστή στον verifier.

4. **Ιδιοκτησία ΑΤ:** Ο prover είναι ιδιοκτήτης της ΑΤ που παράγει μετά από την πιστοποίηση (τα ΤΑΤ) που λαμβάνει από τους witnesses. Διατηρεί την ΑΤ αποθηκευμένη στη μνήμη του και την παρουσιάζει μόνο στον verifier με τη θέλησή του όταν του ζητηθεί. Επιπλέον, δεν είναι υποχρεωμένος να αποκαλύπτει στοιχεία που μπορεί να εκθέσουν την ταυτότητα και την τοποθεσία του πριν και μετά τη δημιουργία της ΑΤ.

3.9 Ενδιαφέροντα θέματα στα πρωτόκολλα Απόδειξης Τοποθεσίας

Στα πρωτόκολλα Απόδειξης Τοποθεσίας εντοπίζονται ορισμένα θέματα στα οποία δεν έχει δοθεί ικανοποιητική λύση. Στο σημείο αυτό, περιγράφουμε τις βασικές δυσκολίες που προκύπτουν και προτείνουμε τρόπους για την αντιμετώπισή τους.

3.9.1 Το πρόβλημα των Ισχυρών Ταυτοτήτων (Strong Identities)

Σε ένα περιβάλλον αποδείξεων τοποθεσίας, είτε ενδιαφέρει η επιβεβαίωση της τοποθεσίας μιας συσκευής είτε ενός φυσικού προσώπου.

Στην πρώτη περίπτωση, αρκεί η εκτέλεση του πρωτοκόλλου από τη συσκευή, όπως έχουμε δει μέχρι στιγμής. Για παράδειγμα, αν μία εταιρεία επιθυμεί να επιβεβαιώσει τη διαδρομή που ακολούθησε ένα φορτηγό της, δεν έχει παρά να ενσωματώσει σε αυτό μία συσκευή που θα αποκτά ΑΤ κατά τη διάρκεια του δρομολογίου. Η εταιρεία επιθυμεί να παρακολουθεί το φορτίο της ανεξάρτητα από τον εργαζόμενο που οδηγεί κάθε στιγμή. Μία τέτοια προσέγγιση θα αρκούσε και σε εφαρμογές που δεν θέτουν σημαντικές απαιτήσεις ασφαλείας, όπως για παράδειγμα σε μία εφαρμογή που ανταμείβει τους τακτικούς πελάτες ενός καταστήματος.

Στη δεύτερη περίπτωση, επιδιώκουμε την επιβεβαίωση της παρουσίας ενός φυσικού προσώπου σε μία τοποθεσία, μία συγκεκριμένη χρονική στιγμή. Η συσκευή λειτουργεί ως ενδιάμεσος, αναλαμβάνοντας να εκτελέσει το πρωτόκολλο για λογαριασμό του χρήστη. Η συσκευή δεν βρίσκεται πάντοτε στα χέρια του ιδιοκτήτη της, είτε σκόπιμα (π.χ. για να προσποιηθεί ότι βρίσκεται σε άλλη τοποθεσία), είτε άσκοπα (π.χ. σε περίπτωση απώλειας ή κλοπής). Σε μία εφαρμογή όπου κρίνεται ένοχος ή αθώος ο χρήστης, όπως και σε μία εφαρμογή που επιβεβαιώνει ότι ένα συγκεκριμένο πρόσωπο οδηγούσε κατά τη διάρκεια ενός ατυχήματος, θα πρέπει να είναι αδύνατον για ένα χρήστη να παρουσιάζεται σε διαφορετική τοποθεσία. Σε αυτές τις περιπτώσεις απαιτείται η χρήση ισχυρών ταυτοτήτων.

Η **Ισχυρή Ταυτότητα (Strong Identity)** είναι ένα κομμάτι πληροφορίας που ταυτοποιεί το χρήστη, είναι δύσκολο να αλλοιωθεί και ενσωματώνεται στην ΑΤ. Με τον τρόπο αυτό μπορούμε να συνδέσουμε τον ίδιο το χρήστη με την συγκεκριμένη ΑΤ, και όχι απλά τη συσκευή του.

Τα περισσότερα πρωτόκολλα της βιβλιογραφίας δεν ασχολούνται με τις ισχυρές ταυτότητες. Αρκεί για αυτά να επιβεβαιωθεί η τοποθεσία της συσκευής του χρήστη και αδιαφορούν για το αν αυτός βρίσκεται μαζί της.

Ιδιαίτερη αναφορά στις Ισχυρές Ταυτότητες γίνεται στο [46]. Οι συγγραφείς προτείνουν την εφαρμογή διαδικασίας πρόκλησης-απάντησης (challenge-response) ανάμεσα στον prover και το witness. Στην απάντηση πρέπει ο prover να συμπεριλάβει κάποιο στοιχείο από την πρόκληση καθώς και κάποιο αναγνωριστικό στοιχείο, όπως για παράδειγμα φωτογραφία του ή ηχογράφησή του. Με τον τρόπο αυτό πιστοποιείται πως ο συγκεκριμένος χρήστης βρισκόταν μαζί με τη συσκευή, στην τοποθεσία που αναφέρει η ΑΤ.

Οι ισχυρές ταυτότητες μελετώνται σε βάθος στο επόμενο κεφάλαιο.

3.9.2 Πολλές συσκευές – μία ταυτότητα

Κανένα πρωτόκολλο απόδειξης τοποθεσίας δεν μπορεί να είναι απόλυτα ασφαλές, αν δεν εμποδίζει δύο ή περισσότερες συσκευές από το να εμφανίζονται με την ίδια ταυτότητα.

Ένας χρήστης μπορεί να συνεργαστεί με κάποιον άλλον, δίνοντάς του π.χ. το ιδιωτικό του κλειδί ή τον κωδικό του, ακόμα και τη συσκευή του. Για παράδειγμα, έστω ότι δύο φοιτητές Α και Β επιθυμούν να αποκτήσουν ένα πιστοποιητικό παρακολούθησης ενός σεμιναρίου. Ο

Α δεν συμμετείχε ποτέ στο σεμινάριο, αλλά ο Β, ο οποίος το παρακολούθησε, είχε μαζί του συσκευή με την ταυτότητα του χρήστη Α. Έτσι, μπόρεσε να συλλέξει απόδειξη τοποθεσίας για λογαριασμό του Α.

Συνεπώς, πρέπει αφενός να αποτρέπεται ο διαμοιρασμός της ταυτότητας (κωδικός ή κλειδιά) του χρήστη και αφετέρου να επιβεβαιώνεται η μοναδικότητα της συσκευής. Θα πρέπει επιπλέον να λαμβάνεται υπόψη η κλοπή ή απώλεια της συσκευής.

Φυσικά, τίποτα από αυτά δεν είναι αναγκαίο αν χρησιμοποιούνται ισχυρές ταυτότητες αδύνατες να παραποιηθούν.

Αποτροπή διαμοιρασμού κλειδιών

Οι συγγραφείς του [1] υποστηρίζουν πως ο χρήστης μπορεί να αποτραπεί από το να μοιράσει το ιδιωτικό του κλειδί, αν μαζί με αυτό αναγκάζεται να μοιράσει ιδιωτικές πληροφορίες.

Ένας άλλος τρόπος είναι να ελέγξουμε αν είναι δυνατόν ο χρήστης να έχει μετακινηθεί όσο υποστηρίζει μεταξύ διαδοχικών AT που παράγει. Μία εκδοχή της μεθόδου αυτής παρουσιάζεται στο [56]. Ωστόσο, τίθεται ζήτημα ιδιωτικότητας, καθώς ο verifier θα πρέπει να γνωρίζει και την προηγούμενη θέση του χρήστη, ή θα πρέπει να υπάρχει άλλος φορέας που θα διενεργεί τον έλεγχο αυτό. Σε κάθε περίπτωση, διαρρέουν προσωπικά στοιχεία του χρήστη, το οποίο και καλούμαστε να αποφύγουμε.

Μία πιθανή λύση είναι η αποθήκευση των ιδιωτικών κλειδιών σε ασφαλείς συσκευές, όπως είναι οι έξυπνες κάρτες (Smart Cards) ή τα USB Tokens. Οι συσκευές αυτές καθιστούν πολύ δύσκολη την απόκτηση των κλειδιών από κάποιον τρίτο [60] και σε συνδυασμό με κωδικό (π.χ. PIN) προσφέρουν πιστοποίηση πολλών παραγόντων (multi-factor authentication – MFA) [61] . Ωστόσο, απαιτείται επιπλέον συσκευή ανάγνωσης, κάτι που δυσκολεύει την υλοποίηση σε ένα περιβάλλον όπου χρησιμοποιούνται κινητές συσκευές. Επίσης, χρειάζεται κάποια διαχειριστική αρχή που θα είναι υπεύθυνη για την έκδοση των καρτών.

Ο χρήστης εξακολουθεί να έχει τη δυνατότητα να συνεργαστεί με κάποιον, δίνοντάς του την κάρτα και τον κωδικό του. Οι Smart Cards λύνουν το πρόβλημα των πολλαπλών συσκευών, όχι όμως και των ισχυρών ταυτοτήτων.

Έλεγχος μοναδικότητας συσκευής

Αναγνώριση της συσκευής είναι δυνατόν να πραγματοποιηθεί χρησιμοποιώντας μοναδικά αναγνωριστικά (Unique IDs). Αυτά είναι δυνατόν να παρέχονται από το υλικό (hardware), όπως για παράδειγμα η διεύθυνση MAC ή ο αριθμός IMEI ή το λογισμικό (software), όπως για παράδειγμα χαρακτηριστικά του λειτουργικού συστήματος, ρυθμίσεις κ.α. Άλλα UIDs αναγνωρίζουν μία συσκευή (π.χ. Android ID), ενώ άλλα αναγνωρίζουν μία συγκεκριμένη εγκατάσταση μιας εφαρμογής (π.χ. UUID στην πλατφόρμα Android) [62], [63]. Τα αναγνωριστικά αυτά, ωστόσο, μπορούν να αλλοιωθούν από προχωρημένους χρήστες [64].

Μία άλλη πρόταση γίνεται στο [65]. Οι συγγραφείς αναπτύσσουν ένα σύστημα που χρησιμοποιεί τις κατασκευαστικές ατέλειες της κάθε κάρτας δικτύου WiFi (NIC – Network Interface Card) για να εντοπίσει από ποια συσκευή προέρχεται ένα μήνυμα. Οι ατέλειες κάθε NIC έχουν ως αποτέλεσμα εκπομπές που διαφέρουν από τις θεωρητικά αναμενόμενες και ταυτοποιούν μοναδικά τη NIC. Έτσι, μπορεί να εντοπιστεί μία συσκευή που χρησιμοποιεί το ίδιο ιδιωτικό κλειδί με μία άλλη.

Το σύστημα είναι παθητικό, δηλαδή δεν απαιτείται ενέργεια από τη συσκευή του χρήστη. Είναι διαφανές (ο χρήστης δεν αντιλαμβάνεται την παρουσία του) και επιπλέον δεν είναι δυνατόν να αποφευχθεί, εκτός και αν η συσκευή δεν εκπέμπει καθόλου. Οι συγγραφείς υπόσχονται ακρίβεια 99% στον εντοπισμό μιας διαφορετικής κάρτας δικτύου.

Αξίζει να σημειωθεί, πως η εφαρμογή ισχυρής ταυτότητας λύνει το πρόβλημα των πολλών συσκευών, καθώς ανεξάρτητα από τη συσκευή ταυτοποιείται το άτομο που την κατέχει. Το αντίθετο όμως δεν ισχύει.

3.9.3 Αδυναμία απόκρυψης-προσθήκης TAT

Είναι πολύ σημαντικό να συμπεριλαμβάνονται στην τελική AT όλες οι απαντήσεις (TAT) που λαμβάνει ο prover από τα witnesses, είτε θετικές (εγκρίνουν τον ισχυρισμό του) είτε αρνητικές (απορρίπτουν τον ισχυρισμό του). Θα πρέπει να είναι αδύνατον για τον prover να αφαιρέσει ή να προσθέσει TAT από την AT που παραδίδει στον verifier, καθώς με αυτόν τον τρόπο είτε μπορεί να συμπεριλάβει μόνο τα θετικά μηνύματα, είτε να συνεργαστεί με επιπλέον witnesses για την παραγωγή επιπλέον θετικών μηνυμάτων.

Ορισμένα πρωτόκολλα θεωρούν πως αρκεί μόνο ένα witness για να εγκριθεί ο ισχυρισμός του prover. Αυτό αφενός μπορεί να ευνοήσει μία συνεργασία με ένα γνωστό witness, αφετέρου δεν δίνει την ευκαιρία σε άλλα witnesses να εκφράσουν τη γνώμη τους και να δείξουν πως ακολουθούν πιστά το πρωτόκολλο, σε περίπτωση που εφαρμόζεται κάποιο σχήμα εμπιστοσύνης. Άλλα πρωτόκολλα υποστηρίζουν περισσότερα witnesses, ωστόσο θεωρούν πως είναι στην ευχέρεια του prover να επιλέξει ποια TAT θα παρουσιάσει στον verifier, οδηγώντας στα κενά ασφαλείας που αναφέρθηκαν παραπάνω.

Ένα βήμα προς την σωστή κατεύθυνση γίνεται στο [66]. Οι κόμβοι (στην περίπτωση του πρωτοκόλλου είναι provers) συμπεριλαμβάνουν στα μηνύματά τους όλους τους υπόλοιπους κόμβους που «βλέπουν». Έτσι, ο server μπορεί να κατασκευάσει έναν γράφο με κορυφές τους κόμβους και ακμές την αναφορά ότι ο ένας εντόπισε τον άλλον. Απαιτώντας από τα witnesses να εκπέμπουν (broadcast) ένα μήνυμα παρουσίας μετά το αίτημα του prover και να κατασκευάζουν πίνακα με γειτονικά witnesses, μπορούμε να κατασκευάσουμε έναν αντίστοιχο γράφο από witnesses. Με βάση το γράφο αυτό ο server ή ο verifier μπορεί να εντοπίσει witnesses που αποκρύπτουν την παρουσία τους, ενώ παράλληλα έχει πλήρη γνώση του αριθμού και της προέλευσης των TAT που αναμένει να λάβει από τον prover.

3.9.4 Προληπτικές αποδείξεις τοποθεσίας ανεξαρτήτως verifier

Ο verifier συνήθως είναι μία εφαρμογή που ζητάει από έναν χρήστη (prover) την απόδειξη της τοποθεσίας του. Ο verifier σε αυτή την περίπτωση καθορίζει τις προδιαγραφές της απόδειξης τοποθεσίας, όπως για παράδειγμα την ακρίβεια με την οποία δίνεται η τοποθεσία του χρήστη.

Είναι όμως πιθανό ο χρήστης να επιθυμεί την έκδοση απόδειξης τοποθεσίας χωρίς να έχει ζητηθεί από κάποιον, με σκοπό να τη χρησιμοποιήσει στο μέλλον. Σε αυτή την περίπτωση, μπορεί να γνωρίζει στα πλαίσια ποιας εφαρμογής (verifier) θα δημιουργήσει την AT, αλλά μπορεί να μην γνωρίζει προς ποιον verifier θα απευθύνεται η AT ή να θέλει να κατασκευάσει AT που απευθύνεται σε πολλούς verifiers [1], [48].

Γίνεται κατανοητό πως η μορφή και το περιεχόμενο των αποδείξεων τοποθεσίας εξαρτάται από τις συνθήκες υπό τις οποίες παράγονται και από τον verifier στον οποίο απευθύνονται.

Ως προς τις **συνθήκες υπό τις οποίες παράγονται**, οι αποδείξεις τοποθεσίας μπορούν να χωριστούν σε ενεργές (προληπτικές) και παθητικές (αντιδραστικές).

- Οι **ενεργές** αποδείξεις τοποθεσίας παράγονται από τον prover χωρίς να έχει ζητηθεί από κάποιον verifier. Πιθανώς να χρησιμοποιηθούν στο μέλλον. Είναι πιθανό ο prover

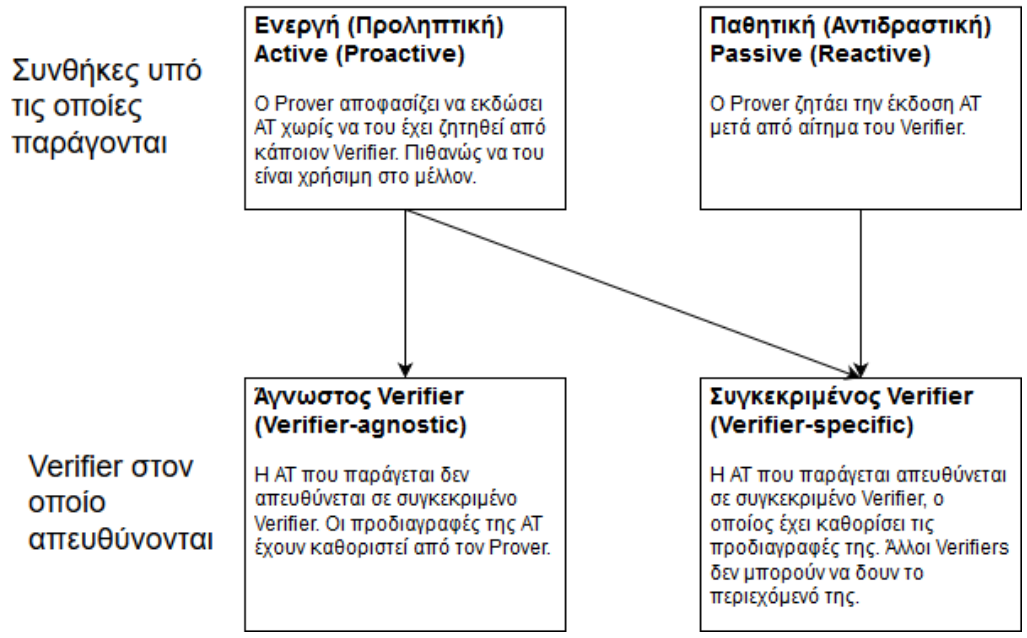
να μην γνωρίζει σε ποιον verifier θα απευθύνεται μία ενεργή απόδειξη τοποθεσίας. Αυτού του είδους οι αποδείξεις τοποθεσίας είναι ιδιαίτερα χρήσιμες σε περιπτώσεις όπου ο prover καλείται να παρουσιάσει κάποιο άλλοθι, γιατί δεν μπορεί να γνωρίζει εκ των προτέρων ότι κάτι τέτοιο θα του ζητηθεί.

- Οι **παθητικές** αποδείξεις τοποθεσίας δημιουργούνται από τον prover ως αντίδραση σε αίτημα ενός verifier. Ο prover γνωρίζει σε ποιον verifier απευθύνεται η ΑΤ που θα παράγει.

Ως προς τον **verifier στον οποίο απευθύνονται**, οι αποδείξεις τοποθεσίας μπορούν να χωριστούν σε αγνώστου verifier και συγκεκριμένου verifier.

- Οι αποδείξεις τοποθεσίας **αγνώστου verifier** έχουν γενική μορφή και μπορούν να απευθυνθούν σε οποιονδήποτε verifier συμμετέχει στο πρωτόκολλο που ακολουθείται.
- Οι αποδείξεις τοποθεσίας **συγκεκριμένου verifier** έχουν συγκεκριμένο παραλήπτη και δεν μπορούν να διαβαστούν από άλλους verifiers.

Οι παθητικές Α.Τ. οδηγούν απαραίτητα σε συγκεκριμένο verifier, ενώ οι ενεργές μπορεί να αναφέρονται τόσο σε συγκεκριμένο όσο και σε άγνωστο verifier, όπως φαίνεται στο παρακάτω σχήμα.



Σχήμα 3.1: Κατηγοριοποίηση Α.Τ. ως προς συνθήκες παραγωγής και verifier.

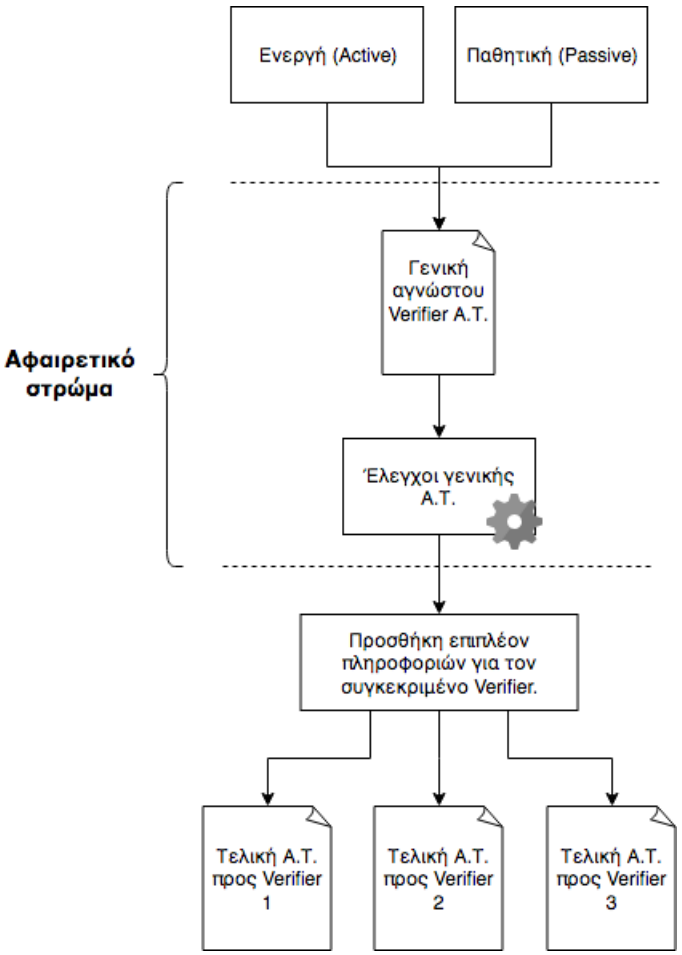
Η υποστήριξη αποδείξεων τοποθεσίας αγνώστου verifier είναι προϋπόθεση για την υποστήριξη ενεργών αποδείξεων τοποθεσίας.

Ωστόσο, σε κάθε περίπτωση ο τελικός παραλήπτης της ΑΤ είναι ένας verifier στον οποίο ο prover εμπιστεύεται την σχετική με την τοποθεσία του πληροφορία. Σε κάθε verifier ο prover επιθυμεί να αποκαλύψει διαφορετικό επίπεδο ακρίβειας τοποθεσίας και φροντίζει ώστε η ΑΤ που αποστέλλει να μπορεί να διαβαστεί μόνο από τον συγκεκριμένο verifier (κρυπτογράφηση με το δημόσιο κλειδί του verifier).

Έτσι, μπορούμε να θεωρήσουμε ένα ευέλικτο σχήμα κατασκευής αποδείξεων τοποθεσίας, όπου όλες οι ΑΤ είναι αγνώστου verifier μέχρι να χρειαστεί να σταλούν σε κάποιον verifier.

Δημιουργείται ένα αφαιρετικό στρώμα, μία προσωρινή απόδειξη τοποθεσίας η οποία περιέχει γενικές πληροφορίες. Η προσωρινή, αγνώστου verifier απόδειξη τοποθεσίας βρίσκεται αποθηκευμένη στη συσκευή του χρήστη. Όταν χρειαστεί να αποσταλεί σε κάποιον verifier, με την προσθήκη των απαραίτητων πληροφοριών μπορεί να μετατραπεί σε απόδειξη τοποθεσίας συγκεκριμένου verifier, έτοιμη να επιβεβαιωθεί από αυτόν [48].

Σχηματικά, η διαδικασία αυτή φαίνεται στο παρακάτω σχήμα, όπου μία γενική (generic) AT με την προσθήκη των κατάλληλων πληροφοριών μπορεί να μετατραπεί σε τρεις διαφορετικές ειδικές (specific) AT συγκεκριμένου verifier.



Σχήμα 3.2: Μετατροπή γενικής απόδειξης τοποθεσίας σε ειδικές αποδείξεις τοποθεσίας.

Σε γενικές γραμμές, τα στοιχεία που διαφοροποιούν την ειδική-τελική από την γενική-προσωρινή AT είναι πως στην ειδική AT ορίζεται η προτιμώμενη ακρίβεια τοποθεσίας που αποκαλύπτεται στον verifier, καθώς και κρυπτογραφείται το μήνυμα ώστε να μπορεί να διαβαστεί μόνο από τον συγκεκριμένο verifier [47], [48].

3.10 Δομικά στοιχεία πρωτοκόλλων A.T.

Προκειμένου να ικανοποιηθούν οι προδιαγραφές που αναφέρθηκαν παραπάνω, τα πρωτόκολλα απόδειξης τοποθεσίας χρησιμοποιούν διάφορες τεχνολογίες. Στην ενότητα αυτή παρουσιάζονται τα βασικά δομικά στοιχεία (building blocks) που συναντώνται στα πρωτόκολλα της βιβλιογραφίας.

3.10.1 Ταυτοποίηση των χρηστών

Η ταυτοποίηση των χρηστών περιλαμβάνει τη διαχείριση και τον έλεγχο των ταυτοτήτων και των κρυπτογραφικών τους κλειδιών. Μπορεί να πραγματοποιηθεί με τους εξής τρόπους:

- **Αρχή Πιστοποίησης (Certificate Authority):** Διαχειρίζεται τους χρήστες που συμμετέχουν στο σύστημα και επιβεβαιώνει τις υπογραφές τους [47], [49].
- **Blockchain:** Η εγκυρότητα των πληροφοριών που υποβάλλουν οι χρήστες καθώς και των ταυτοτήτων τους ελέγχεται από αποκεντρωμένους κόμβους, οι οποίοι φτάνουν σε συμφωνία (consensus) μεταξύ τους [67], [68].
- **Self-Signed:** Κάθε κόμβος υπογράφει τα μηνύματα που παράγει χωρίς να γνωρίζει το δημόσιο κλειδί του κάποια αρχή πιστοποίησης και συνεπώς χωρίς να γίνεται επιβεβαίωση της ταυτότητάς του. Οι κόμβοι με τους οποίους επικοινωνεί αποφασίζουν αν θα τον εμπιστευτούν [69].

3.10.2 Ιδιωτικότητα ταυτότητας και υπογραφής

Τόσο η ταυτότητα όσο και η υπογραφή που χρησιμοποιούν οι χρήστες μπορούν να εκθέσουν την ιδιωτικότητά τους. Για το λόγο αυτό, είναι επιθυμητό να μην εμφανίζονται αυτούσιες μέσα στα μηνύματα.

Με τους παρακάτω τρόπους είναι δυνατή η απόκρυψη της ταυτότητας και της υπογραφής των χρηστών:

- **Ψευδώνυμα:** Κάθε χρήστης του συστήματος διαθέτει ορισμένα ψευδώνυμα που μπορεί να χρησιμοποιεί ως ταυτότητες στα μηνύματα που στέλνει. Η CA είναι υπεύθυνη για την αντιστοίχιση των ψευδωνύμων με την πραγματική τους ταυτότητα [49], [70].
- **Κατακερματισμοί (hashes) και κρυπτογραφία:** Τόσο η ταυτότητα όσο και η υπογραφή μπορεί να εμφανίζεται κατακερματισμένη ή κρυπτογραφημένη μέσα στα μηνύματα, με σκοπό να αποκαλυφθεί αργότερα [48].
- **Κρυπτογραφικές δεσμεύσεις (commitments)** [71]**,** [72]**:** Χρησιμοποιώντας κρυπτογραφικές μεθόδους οι χρήστες αποκρύπτουν προσωρινά την ταυτότητα ή την υπογραφή τους, την οποία αποκαλύπτουν αργότερα όταν χρειαστεί [47], [73].
- **Ομαδικές υπογραφές** [74]**:** Χρησιμοποιούνται συνήθως από την πλευρά των witnesses. Δίνουν τη δυνατότητα κάθε χρήστης να υπογράφει ένα μήνυμα με ξεχωριστό ιδιωτικό κλειδί, αλλά η υπογραφή να επιβεβαιώνεται με ένα ομαδικό δημόσιο κλειδί. Προστατεύεται έτσι η ταυτότητα του υπογράφοντα, αλλά προκύπτει το συμπέρασμα πως αυτός ανήκει σε μία ορισμένη ομάδα [47], [73].

3.10.3 Έλεγχος γειτνίασης

Ο έλεγχος γειτνίασης αποτελεί βασικό στοιχείο των πρωτοκόλλων απόδειξης τοποθεσίας. Στη βιβλιογραφία χρησιμοποιούνται οι παρακάτω τρόποι:

- **Όριο απόστασης (distance bounding)** [75]**,** [76]**:** Αποτελούν την πλέον αξιόπιστη τεχνική για τον έλεγχο γειτνίασης. Μεταξύ prover και witness γίνεται μία ταχεία ανταλλαγή bit (fast bit exchange). Τα bit αυτά συνδέονται με κρυπτογραφικά δεδομένα, ώστε να επιβεβαιώνεται τόσο η γειτνίαση όσο και η ταυτότητα του prover. Ωστόσο, για την εφαρμογή των τεχνικών αυτών απαιτείται μεγάλη ακρίβεια στη μέτρηση του χρόνου, η οποία είναι συνήθως αδύνατη χωρίς ειδικό εξοπλισμό [77], [48].

- **Φάροι (Beaconing):** Ο prover καταγράφει γνωστά σήματα που εκπέμπουν ορισμένα σημεία αναφοράς-φάροι. Παρουσιάζοντας τα σήματα αυτά μπορεί να αποδείξει τη γειτνίασή του με το σημείο αναφοράς [69].
- **Πλαίσιο αναφοράς (context-based):** Χρησιμοποιούνται χαρακτηριστικά σημάτων του περιβάλλοντος για να προσεγγιστεί η θέση του prover και κατά συνέπεια η γειτνίαση του prover με τα witnesses [57], [66].
- **Εκπνοή χρόνου (timeout-based):** Μετράται ο χρόνος που χρειάζεται για την αποστολή ενός μηνύματος από το witness στον prover και αντίστροφα, με σκοπό να προσεγγιστεί η μεταξύ τους απόσταση [51]. Αν ο prover απαντήσει μέσα σε ορισμένο χρονικό διάστημα, τότε θεωρείται πως γειτνιάζει με το witness. Θα μπορούσε κανείς να πει πως αποτελεί μία απλοποιημένη εκδοχή των μεθόδων distance bounding.

3.10.4 Κωδικοποίηση τοποθεσίας

Ένα πρωτόκολλο απόδειξης τοποθεσίας μπορεί να μην χρησιμοποιεί κάποια κωδικοποίηση τοποθεσίας, δηλαδή να αναφέρεται σε τοποθεσίες με γεωγραφικές συντεταγμένες.

Μπορεί όμως να αναφέρεται στην τοποθεσία με κάποιον από τους παρακάτω τρόπους:

- **Συντεταγμένες πλέγματος:** Κατασκευάζεται ένα πλέγμα με το οποίο περιγράφεται η θέση των κόμβων [57], [66].
- **Σύστημα geocoding:** Χρησιμοποιείται κάποιο σύστημα κωδικοποίησης τοποθεσίας, όπως για παράδειγμα το [68], το οποίο χρησιμοποιεί geohash.
- **Αυθαίρετο:** Η τοποθεσία εκφράζεται με διάφορες μορφές, ανάλογα με το επίπεδο ακρίβειας με το οποίο δίνεται. Για παράδειγμα, η τοποθεσία αναφέρεται ως χώρα, πόλη, ταχυδρομικός κώδικας, συντεταγμένες κ.τ.λ. [56], [78].

3.10.5 Επίπεδα ακρίβειας τοποθεσίας

Τα πρωτόκολλα που υποστηρίζουν μεταβαλλόμενη ακρίβεια τοποθεσίας, την τοποθετούν στις αποδείξεις τοποθεσίας με έναν από τους παρακάτω τρόπους:

- **Ακρίβεια πλέγματος:** Σε περίπτωση που το πρωτόκολλο εκφράζει την τοποθεσία με βάση κάποιο πλέγμα, όπως αναφέρθηκε παραπάνω, τότε η ακρίβεια εκφράζεται με υποδιαιρέσεις του πλέγματος αυτού [57], [66].
- **Πολλαπλή κρυπτογράφηση (multiple encryption):** Έστω ότι η τοποθεσία εκφράζεται με i επίπεδα ακριβείας. Κάθε επίπεδο ακρίβειας τοποθεσίας L_i κρυπτογραφείται με ένα διαφορετικό συμμετρικό κλειδί s_i. Η AT περιέχει όλα τα κρυπτογραφημένα $s(L_i)$ και ο prover δίνει στον verifier το αντίστοιχο κλειδί, ανάλογα με την ακρίβεια που επιθυμεί να αποκαλύψει [48].

  Παρόμοια, αντί για κρυπτογράφηση μπορεί να χρησιμοποιηθεί δέσμευση για κάθε επίπεδο ακρίβειας τοποθεσίας, ώστε να αναπαρίσταται ως $C(L_i, r_i)$, όπου r_i τυχαίος αριθμός.

  Οι μέθοδοι αυτές έχουν ως αποτέλεσμα να παράγονται μεγάλες σε μέγεθος AT, αφού πρέπει να ενσωματώνονται σε αυτές όλα τα κρυπτογραφημένα επίπεδα ακρίβειας. Επίσης, απαιτείται από τα witness να ελέγχουν ξεχωριστά το κάθε επίπεδο τοποθεσίας L_i για το αν αποτελεί μία λιγότερο αναλυτική περιγραφή του L_{i-1}.
- **Αλυσίδες κατακερματισμού (hash chains):** Παράγονται με τη διαδοχική εφαρμογή συναρτήσεων κατακερματισμού (hash functions) επί της τοποθεσίας εκφρασμένης με τη μεγαλύτερη δυνατή ακρίβεια και ενός τυχαίου αριθμού (seed). Είναι πιο ευέλικτες

από την προηγούμενη μέθοδο, καθώς στην απόδειξη τοποθεσίας απαιτείται να συμπεριληφθεί μόνο το τελικό αποτέλεσμα του κατακερματισμού (κεφαλή της αλυσίδας). Δοθείσης της επιθυμητής ακρίβειας τοποθεσίας και του αντίστοιχου κομματιού της αλυσίδας, ο verifier μπορεί να επαναλάβει τη διαδικασία μέχρι να φτάσει στην κεφαλή της αλυσίδας, επιβεβαιώνοντας έτσι πως ο prover δήλωσε σε αυτόν σωστά το επίπεδο ακρίβειας της τοποθεσίας του. [47], [78]. Οι αλυσίδες κατακερματισμού μελετώνται σε βάθος στο επόμενο κεφάλαιο.

Είναι δυνατόν να χρησιμοποιούνται συνδυαστικά σχήματα που κάνουν χρήση κρυπτογραφίας και αλυσίδων κατακερματισμού [1], [56].

3.11 Επισκόπηση πρωτοκόλλων Α.Τ.

Στην παρούσα ενότητα παρουσιάζουμε συγκριτικούς πίνακες για διάφορα πρωτόκολλα Α.Τ. που είναι διαθέσιμα στη βιβλιογραφία. Η σύγκριση γίνεται με βάση τα χαρακτηριστικά και τις προδιαγραφές που αναφέρθηκαν παραπάνω.

Στην τελευταία στήλη κάθε πίνακα γίνεται αναφορά στο προτεινόμενο πρωτόκολλο της παρούσας εργασίας, το QuietPlace, το οποίο παρουσιάζεται στο επόμενο κεφάλαιο.

Σημειώνεται πως για το FOAM [67], [78] δεν υπάρχουν επαρκείς πληροφορίες σχετικά με τις προδιαγραφές και συνεπώς δεν περιλαμβάνεται στους αντίστοιχους πίνακες.

3.11.1 Χαρακτηριστικά

	FOAM [68], [79]	**VProof** [69]	**APPLAUS** [49]	**PROPS** [47]	**STAMP** [56]	**Blockchain PoL** [67]	**Alice** [57]	**Location Based Handshake** [66]
Αρχιτεκτονική δημιουργίας ΑΤ	P2P	Centralized	P2P	P2P	Hybrid	P2P	Centralized	Centralized
Αρχιτεκτονική επαλήθευσης ΑΤ	Ανεπαρκή στοιχεία	Indirect	Indirect	Direct	Indirect	Indirect	Indirect	Indirect
TTP/CA	Όχι	Όχι	Ναι	Ναι. Μόνο για δημιουργία χρηστών.	Ναι	Όχι	Ναι	Όχι. Χρειάζεται μόνον αν οι provers θέλουν τα μόνιμα κλειδιά του verifier.
Φυσικό στρώμα	LoRa	2.4 GHz	Bluetooth	Αδιάφορο	Bluetooth & WiFi	Bluetooth, Bluetooth SMART, Zigbee	WiFi	WiFi, LTE, Bluetooth
Κωδικοποίηση τοποθεσίας	Geohash	Συντεταγμένες	Αδιάφορο	Συντεταγμένες	Αυθαίρετο[1]	Συντεταγμένες	Πλέγμα	Πλέγμα
Εύρεση τοποθεσίας	Ναι	Συνδυάζει το GPS με σταθμούς εκπομπής	Όχι	Όχι	Όχι	Όχι	Ναι	Όχι
Έλεγχος γειτνίασης	Ναι	Όχι, ο χρήστης απλά λαμβάνει πακέτα	Όχι	Ναι, distance-bounding	Ναι, distance-bounding	Όχι, απλός έλεγχος αν η τοποθεσία που αναφέρει ο prover βρίσκεται στο εύρος της ζεύξης.	Ναι	Ναι, location tags
Κίνητρο συμμετοχής	Ναι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι
Μεταβαλλόμενη ακρίβεια τοποθεσίας	Ναι	Όχι	Όχι	Ναι	Ναι	Όχι	Ναι	Ναι, δύσκολα διαχειρίσιμη. Εξαρτάται από το είδος των σημάτων που χρησιμοποιούνται.
Ανεξαρτησία από verifier	Ανεπαρκή στοιχεία	Όχι	Ναι	Ναι	Ναι	Ναι	Ναι	Όχι
Υποστήριξη αλυσίδων ΑΤ	Όχι	Ναι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι

Πίνακας 1: Χαρακτηριστικά πρωτοκόλλων Α.Τ. (μέρος Α)

[1] π.χ. χώρα, πόλη, συντεταγμένες, ανάλογα με την ακρίβεια που δίνεται

	CLIP [78]	**Enabling New Mobile Applications…** [46]	**Proving Your Location …** [48]	**LINK** [52]	**Veriplace** [1]	**Where have you been?** [73]	**WORAL** [70]	**Alibi Systems** [50]	**QuietPlace**
Αρχιτεκτονική δημιουργίας AT	Hybrid	Centralized	Centralized	P2P	Centralized	Hybrid	Hybrid	Hybrid	Hybrid
Αρχιτεκτονική επαλήθευσης AT	Indirect	Direct ή Indirect	Direct	Indirect	Indirect	Direct	Direct	Direct ή Indirect[2]	Indirect
TTP/CA	Ναι	Προαιρετικά ως Sign-On provider.	Ναι	Ναι	Ναι	Δεν αναφέρεται	Ναι, ως Service Provider.	Ναι	Ναι
Φυσικό στρώμα	WiFi, Bluetooth	WiFi, κεραίες κινητής	WiFi, κεραίες κινητής	Bluetooth, δυνατότητα για WiFi	WiFi	WiFi, Bluetooth	WiFi	Αδιάφορο	Υπέρηχοι
Κωδικοποίηση τοποθεσίας	Αυθαίρετο[1]	Συντεταγμένες	Αυθαίρετο[1]	Αδιάφορο	Αδιάφορο	Αδιάφορο	Αδιάφορο	Αδιάφορο	Plus Codes
Εύρεση τοποθεσίας	Ναι[3]	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι
Έλεγχος γειτνίασης	Όχι (αναφέρεται αλλά δεν υλοποιείται)	Όχι	Όχι	Όχι	Όχι	Ναι	Όχι	Όχι	Ναι, timeout-based
Κίνητρο συμμετοχής	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Ναι	Όχι	Ναι
Μεταβαλλόμενη ακρίβεια τοποθεσίας	Ναι	Όχι	Ναι	Όχι	Ναι	Ναι	Ναι	Όχι	Ναι
Ανεξαρτησία από verifier	Ναι	Ναι	Ναι	Όχι	Ναι	Ναι	Ναι	Ναι	Ναι
Υποστήριξη αλυσίδων AT	Ναι	Όχι	Όχι	Όχι	Όχι	Ναι	Ναι	Όχι	Όχι

Πίνακας 2: Χαρακτηριστικά πρωτοκόλλων A.T. (μέρος B)

[2] Στην περίπτωση που το witness δεν αποκρύπτει την ταυτότητά του (centralized-trusted witness) γίνεται απευθείας επιβεβαίωση από τον verifier. Στην περίπτωση που το witness αποκρύπτει την ταυτότητά του (P2P), πριν την επιβεβαίωση από τον verifier γίνεται συννενόηση μεταξύ prover-witness.

[3] Υπολογισμός σχετικής τοποθεσίας με αισθητήρα επιτάχυνσης

3.11.2 Προδιαγραφές ασφαλείας

	VProof [69]	**APPLAUS** [49]	**PROPS** [47]	**STAMP** [56]	**Blockchain PoL** [67]	**Alice** [57]	**Location Based Hand-shake** [66]	**CLIP** [78]	**Enabling New Mobile Applica-tions…** [46]	**Proving Your Loca-tion…** [48]	**LINK** [52]	**Veriplace** [1]	**Where have you been?** [73]	**WORAL** [70]	**Alibi Systems** [50]	**QuietPlace**
Ακεραιότητα δεδομένων	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι
Αδυναμία Απόκρυ-ψης/Προσθήκης ΤΑΤ	-[7]	Όχι	Όχι	Όχι	Όχι	Ναι[4]	Ναι	Όχι	Όχι	Όχι	Ναι	Ναι	Ναι	Ναι[5]	Όχι	Ναι
Μη μεταβιβάσιμη πλη-ροφορία	Όχι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι
Αντοχή στην απάτη από-στασης	Όχι	Όχι	Ναι	Ναι	Όχι	Ναι	Ναι	Όχι[6]	Ναι	Όχι	Όχι	Όχι	Ναι	Όχι	Όχι	Ναι
Αντοχή στην επίθεση εν-διάμεσου (relay)	Όχι	Όχι	Ναι	Ναι	Όχι	Ναι	Όχι	Όχι[6]	Ναι	Όχι	Όχι	Ναι	Ναι	Ναι	Όχι	Ναι
Αντοχή στην υποκλοπή απόστασης	Όχι	Όχι	Ναι	Ναι	Όχι	Όχι	Όχι	Όχι[6]	Όχι	Όχι	Όχι	Όχι	Ναι	Όχι	Όχι	Ναι
Αντοχή στη συνεργασία P-P	Όχι	Όχι	Ναι	Ναι	Όχι	Όχι	Όχι	Όχι[6]	Όχι	Όχι	Όχι	Όχι	Ναι	Όχι	Όχι	Ναι
Αντοχή στη συνεργασία P-W	-[7]	Ναι	Όχι	Ναι	Όχι	Ναι[8]	-[7]	Ναι	Όχι	Ναι	Ναι	Όχι	Ναι	Ναι	Όχι	Ναι
Αντοχή στη συνεργασία W-W	-[7]	Ναι	Ναι	Ναι	Όχι	Ναι[8]	-[7]	Ναι	Όχι	Ναι	Ναι	Ναι[9]	Ναι[9]	Ναι	Ναι[9]	Ναι
Μοναδικότητα ΤΑΤ	-[7]	Όχι	Ναι	Ναι	Ναι	Ναι[4]	-[7]	Ναι	Ναι	Όχι	Ναι	Ναι	Ναι	Ναι[5]	Ναι	Ναι
Όχι μοναδικό σημείο α-ποτυχίας	Όχι	Όχι	Ναι	Όχι	Ναι	Όχι	Ναι	Όχι	Ναι	Ναι	Όχι	Όχι	Όχι	Ναι	Ναι	Όχι

Πίνακας 3: Προδιαγραφές ασφαλείας πρωτοκόλλων Α.Τ.

[4] Γιατί τα APs ενημερώνουν το server για τις ΑΤ

[5] Ωστόσο, επιλέγεται ένα witness από την Location Authority. Μπορεί έτσι να αποφευχθεί η επιλογή ενός witness που έχει διαφορετική άποψη.

[6] Γίνεται αναφορά σε distance bounding πρωτόκολλα, τα οποία αν υλοποιηθούν θα ικανοποιούνται αυτές οι προδιαγραφές.

[7] Δεν υφίσταται η έννοια του witness.

[8] Γιατί τα APs θεωρούνται trusted από τους παρόχους υπηρεσιών τοποθεσίας

[9] Αρκεί 1 ΤΑΤ, το οποίο όμως εμποδίζει άλλαwitnesses να εκφέρουν άποψη.

3.11.3 Προδιαγραφές ιδιωτικότητας

	VProof [69]	**APPLAUS** [49]	**PROPS** [47]	**STAMP** [56]	**Blockchain PoL** [67]	**Alice** [57]	**Location Based Handshake** [66]	**CLIP** [78]	**Enabling New Mobile Applications…** [46]	**Proving Your Location…** [49]	**LINK** [52]	**Veriplace** [1]	**Where have you been?** [73]	**WORAL** [70]	**Alibi Systems** [50]	**QuietPlace**
ΑΑΣ prover στο Στάδιο Α	Ναι	Ναι	Ναι	Ναι	Ναι[10]	Όχι	Ναι	Ναι	Προαιρετικά, με ψευδώνυμα	Ναι	Όχι	Όχι	Όχι	Ναι	Ναι	Ναι
ΑΑΣ prover στο Στάδιο Β	Ναι	Όχι	Ναι	Ναι	Ναι[10]	Όχι	Ναι	Όχι	Ναι, εκτός αν Sign-on provider	Ναι	Όχι	Όχι	Ναι	Όχι	Όχι	Ναι
ΑΑΣ witness στο Στάδιο Α	-[7]	Ναι	Ναι	Ναι	Ναι[10]	Όχι	-[7]	Ναι	Όχι	Ναι	Όχι	Όχι	Προαιρετική[11]	Ναι	Ναι	Ναι
ΑΑΣ witness στο Στάδιο Β	-[7]	Ναι	Ναι	Ναι	Ναι[10]	Όχι	-[7]	Όχι	Όχι	Ναι	Όχι	Όχι	Προαιρετική[11]	Όχι	Όχι	Ναι
Ιδιωτικότητα τοποθεσίας prover	Όχι[12]	Ναι	Ναι	Ναι	Όχι	Μερική[13]	Ναι	Ναι	Ναι	Ναι	Όχι	Ναι	Όχι	Όχι	Ναι	Ναι
Ιδιωτικότητα τοποθεσίας witness	-[7]	Ναι	Ναι	Ναι	Όχι	Είναι γνωστή	-[7]	Όχι	Όχι	Όχι	Όχι	Γνωστή τοποθεσία	Ναι	Όχι	Ναι	Ναι
Ιδιοκτησία ΑΤ	Όχι[12]	Όχι	Ναι	Ναι	Όχι	Μερική[13]	Όχι	Ναι	Ναι[14]	Ναι	Όχι	Μερική[15]	Ναι	Όχι	Ναι	Ναι

Πίνακας 4: Προδιαγραφές ιδιωτικότητας πρωτοκόλλων Α.Τ.

[10] εξαρτάται από τη χρήση πολλαπλών ταυτοτήτων-ψευδωνύμων

[11] Το witness μπορεί να υπογράψει με το ιδιωτικό του κλειδί ή με ομαδική υπογραφή.

[12] γιατί απαιτεί να στέλνονται όλα τα προηγούμενα Proofs

[13] απαιτείται να στέλνει το witness ένα κομμάτι πληροφορίας στο Server

[14] εξαρτάται από τη συμπεριφορά των APs

[15] απαιτείται η αποστολή ορισμένων πληροφοριών που μπορεί να οδηγήσουν σε πλήρη αποκάλυψη της ταυτότητας και θέσης του χρήστη

3.12 Διαγράμματα ροής των πρωτοκόλλων Α.Τ.

Τα πρωτόκολλα απόδειξης τοποθεσίας παρουσιάζουν μεγάλες διαφορές στη διαδικασία που ακολουθούν προκειμένου να επιβεβαιωθεί η τοποθεσία του prover.

Η εκτέλεσή τους γενικά μπορεί να χωριστεί σε τρία στάδια:

1. **Προετοιμασία:** Γίνονται οι απαραίτητες ενέργειες και ρυθμίσεις προκειμένου να μπορεί να λειτουργήσει το πρωτόκολλο. Τίθεται σε λειτουργία ο απαραίτητος εξοπλισμός (π.χ. server [49], access points [78]), οι χρήστες αποκτούν κρυπτογραφικά κλειδιά, γίνονται οι απαραίτητες βαθμονομήσεις [69] κ.α.

2. **Δημιουργία ΑΤ:** Στο στάδιο αυτό ο prover επικοινωνεί με τα witnesses, ανταλλάσσει στοιχεία με αυτά και τα «πείθει» πως βρίσκεται πράγματι στην τοποθεσία που υποστηρίζει ότι είναι. Θεμελιώδες στοιχείο του σταδίου αυτού είναι η εκτέλεση ελέγχου γειτνίασης. Στο τέλος του σταδίου ο prover έχει αποκτήσει τα διαπιστευτήρια ΤΑΤ από τα witnesses και μπορεί να κατασκευάσει την απόδειξη τοποθεσίας.

   Το στάδιο αυτό χωρίζεται στα τρία παρακάτω μέρη:

   i) Δημιουργία ομάδας επικοινωνίας: Γίνεται η πρώτη επικοινωνία των κόμβων που θα συμμετάσχουν στη δημιουργία της ΑΤ για τον prover. Εκτός του prover και των witnesses, είναι δυνατόν να συμμετέχουν τρίτες οντότητες (π.χ. CA [52]), ή τοπικές αρχές (π.χ. Location Authority [73]).

   ii) Δήλωση και επικύρωση τοποθεσίας: Στη συνέχεια γίνεται αναφορά στην τοποθεσία και ελέγχεται από το witness αν ο prover βρίσκεται πράγματι στην τοποθεσία που ισχυρίζεται.

   iii) Ενέργειες witness και prover: Στο τελευταίο μέρος το witness αποστέλλει το τεμάχιο απόδειξης τοποθεσίας στον prover και πιθανώς και άλλες πληροφορίες σε κάποια τρίτη οντότητα [57], [73], [70]. Ο prover με τη σειρά του μπορεί να επικοινωνεί και αυτός με κάποιον τρίτο [1], [50], [70].

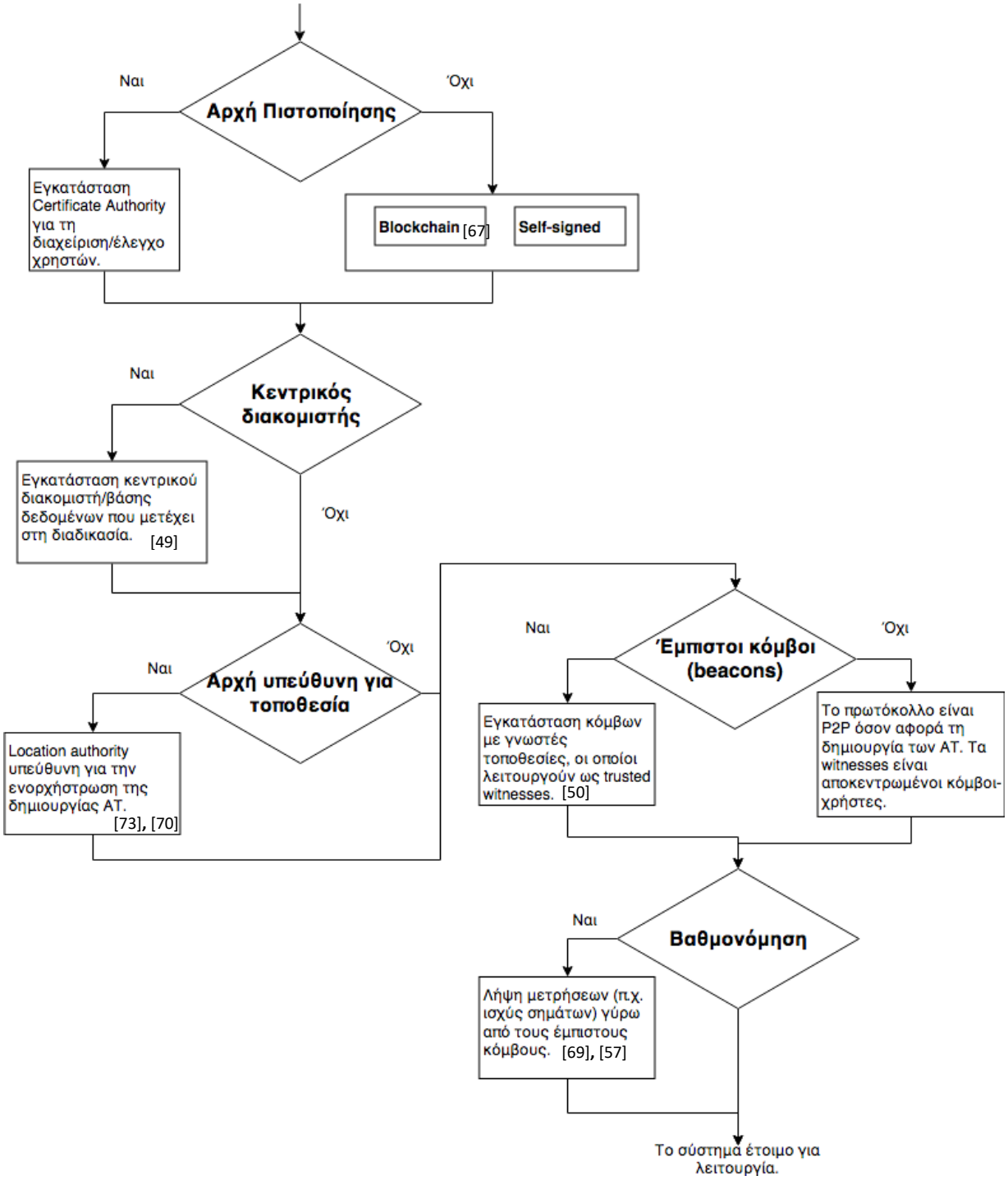
3. **Επιβεβαίωση ΑΤ:** Στο στάδιο αυτό ο prover επικοινωνεί με τον verifier (άμεσα ή έμμεσα), και παρουσιάζει σε αυτόν την απόδειξη τοποθεσίας, η οποία περιλαμβάνει τα διαπιστευτήρια ΤΑΤ που έλαβε από τα witnesses. Ο verifier ελέγχει την εγκυρότητα των στοιχείων που υπέβαλλε ο prover προκειμένου να «πειστεί» για τον ισχυρισμό του.

   Το στάδιο αυτό χωρίζεται στα δύο παρακάτω μέρη:

   i) Απόκτηση της ΑΤ από τον verifier: Αρχικά ο verifier πρέπει να αποκτήσει την ΑΤ του prover, προκειμένου να ελέγξει την εγκυρότητά της.

   ii) Ενέργειες verifier: Έπειτα, ο verifier, έχοντας λάβει την ΑΤ του prover, εκτελεί ελέγχους και συμπεραίνει αν θα δεχτεί ή όχι τον ισχυρισμό του prover. Μπορεί επίσης να επικοινωνεί με άλλες οντότητες πριν [69], [57] και μετά [47] τους ελέγχους που πραγματοποιεί.

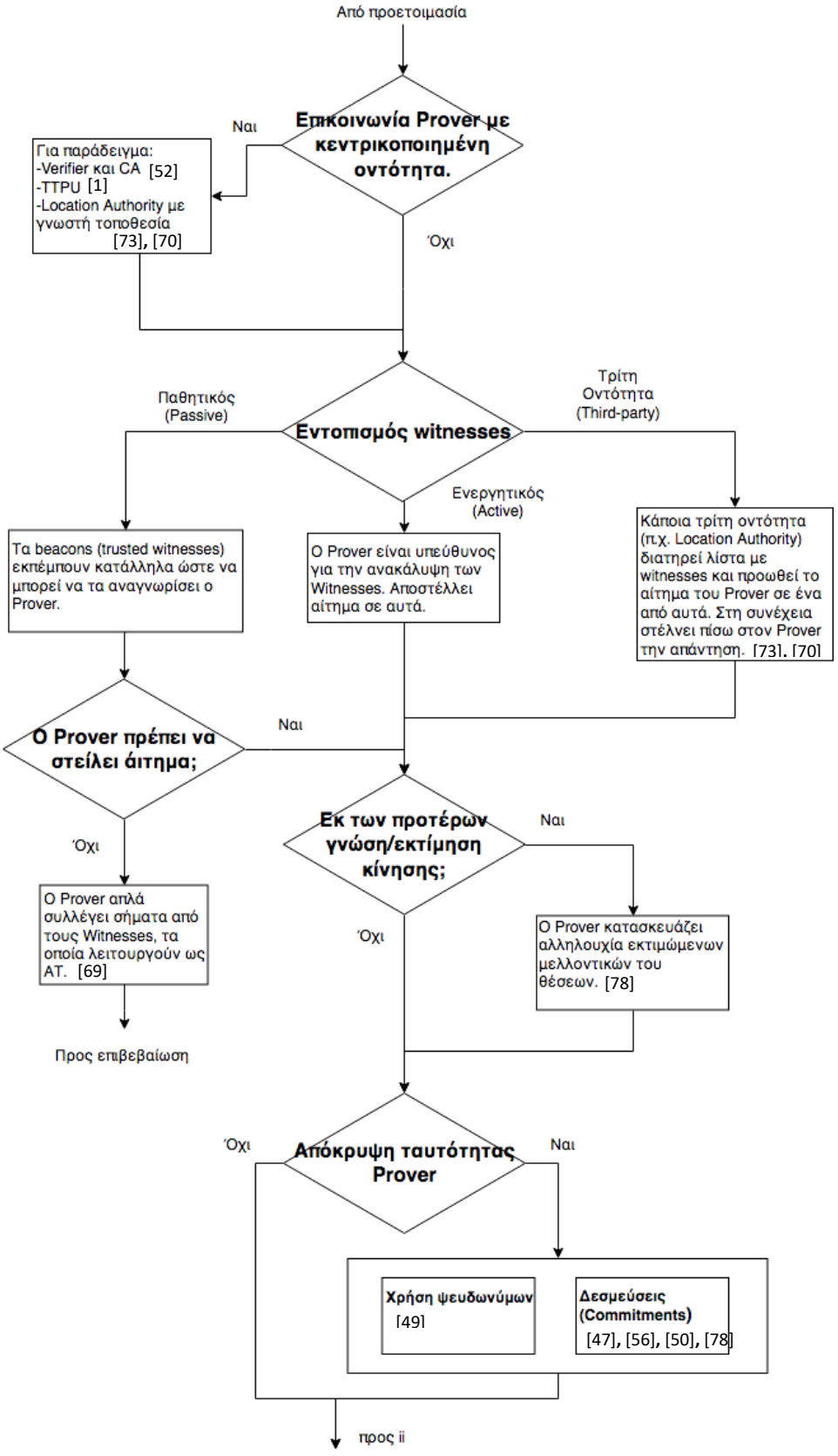
3.12.1 Προετοιμασία Α.Τ.



Σχήμα 3.3: Προετοιμασία συστήματος απόδειξης τοποθεσίας.

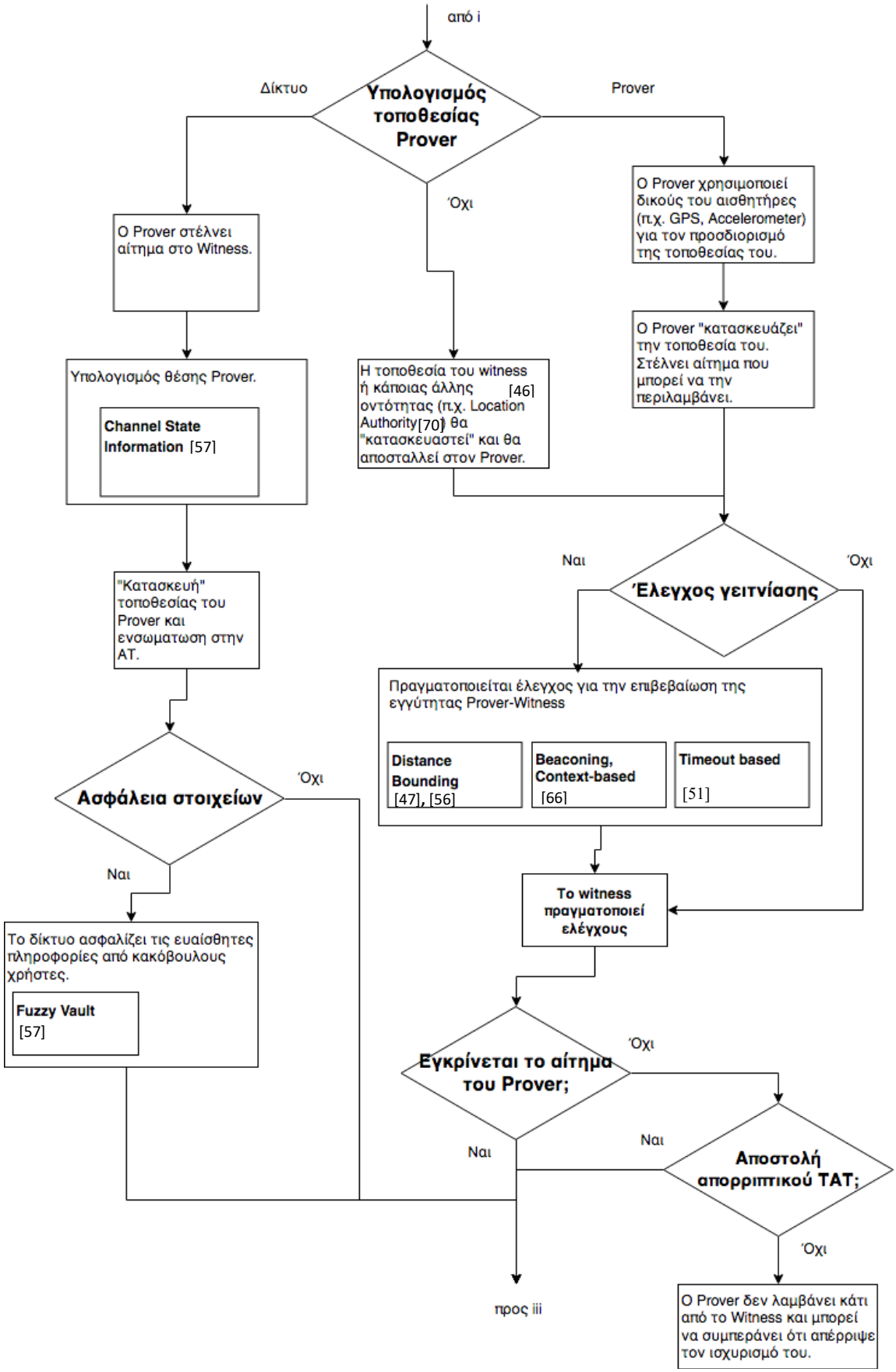
3.12.2 Δημιουργία Α.Τ.

i) Δημιουργία ομάδας επικοινωνίας



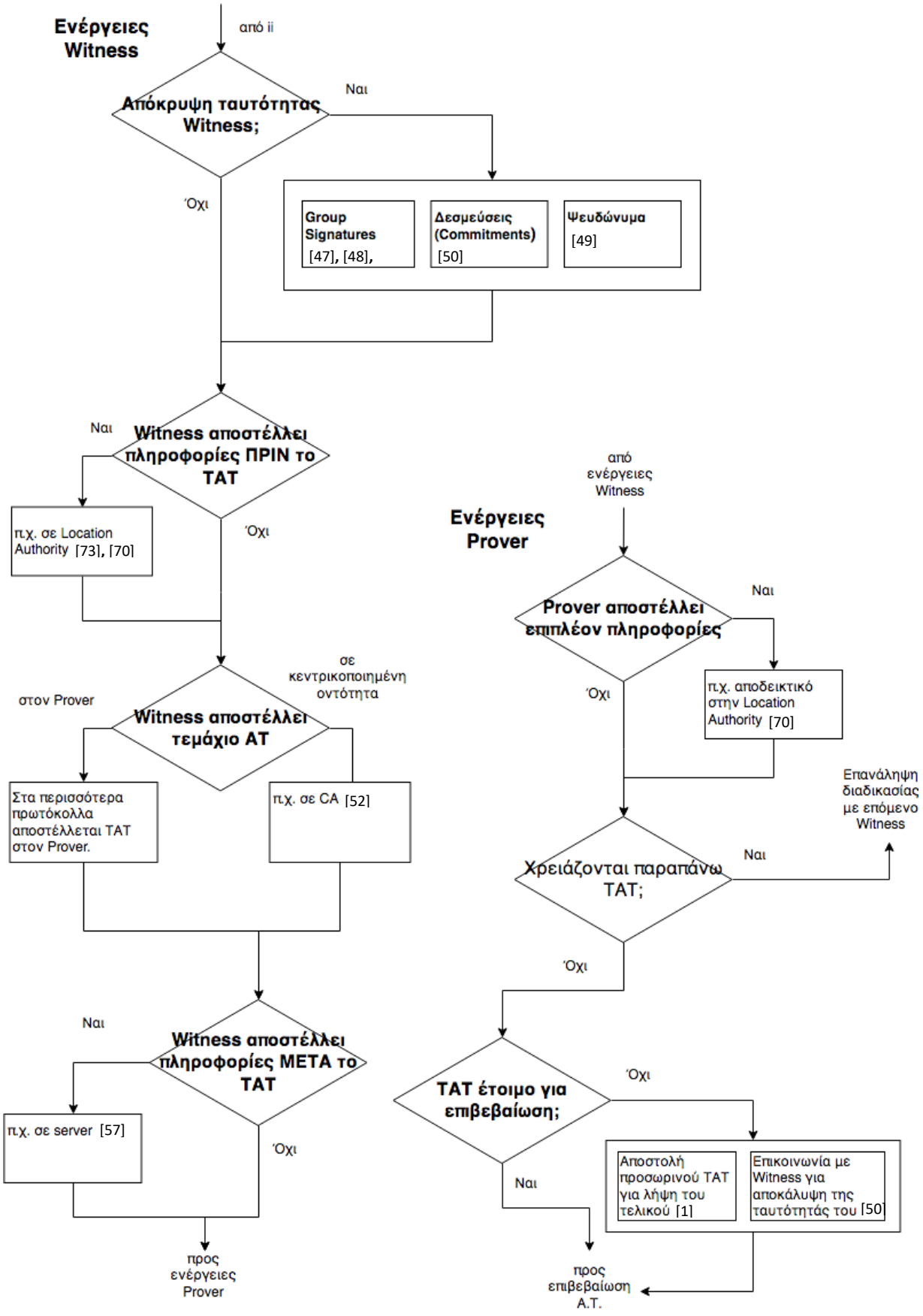
Σχήμα 3.4: Δημιουργία Α.Τ. - Δημιουργία ομάδας επικοινωνίας.

ii) Δήλωση και επικύρωση τοποθεσίας



Σχήμα 3.5: Δημιουργία Α.Τ. - Δήλωση και επικύρωση τοποθεσίας.

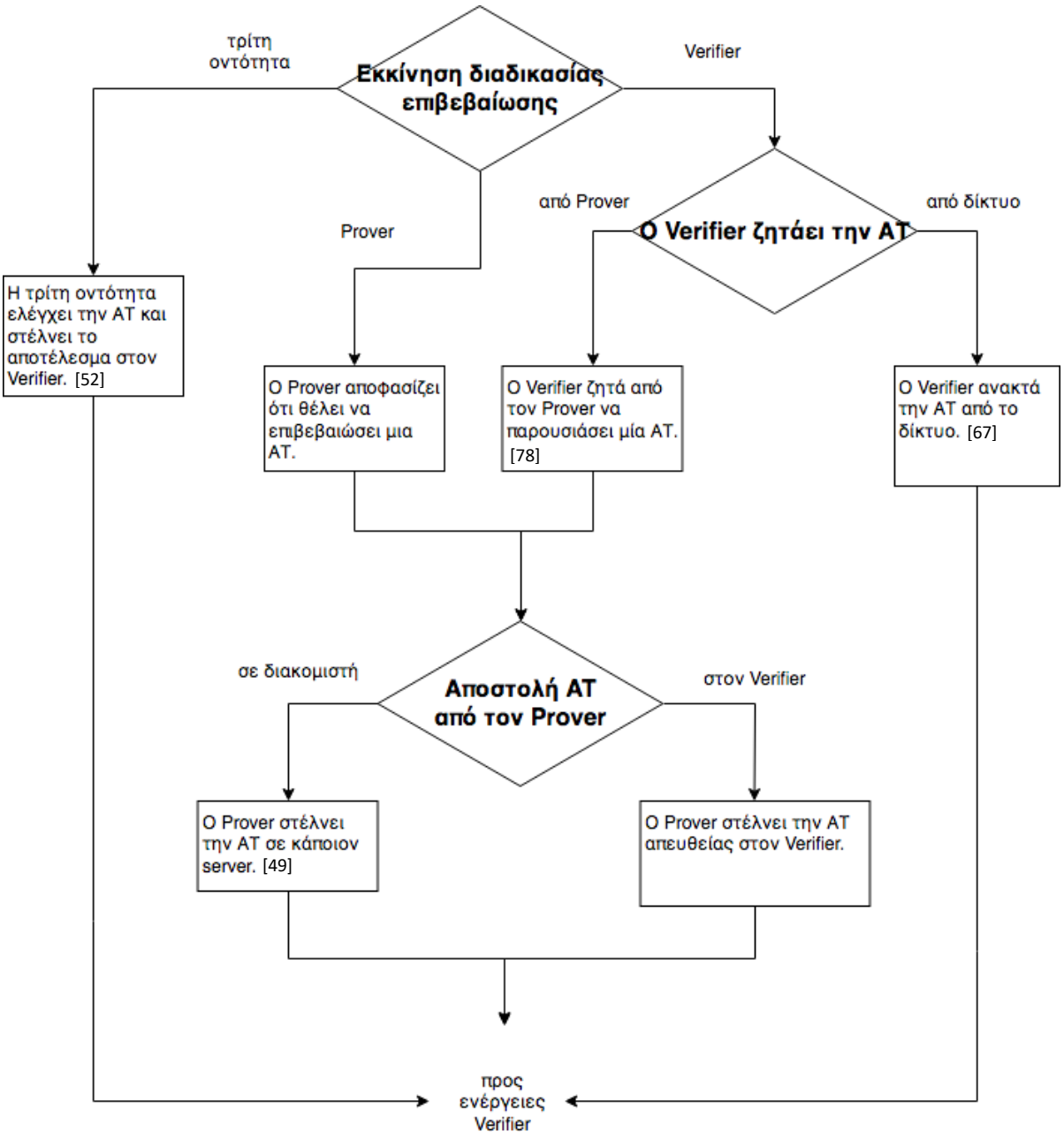
iii) Ενέργειες witness και prover



Σχήμα 3.6: Δημιουργία Α.Τ. - Ενέργειες witness και prover.

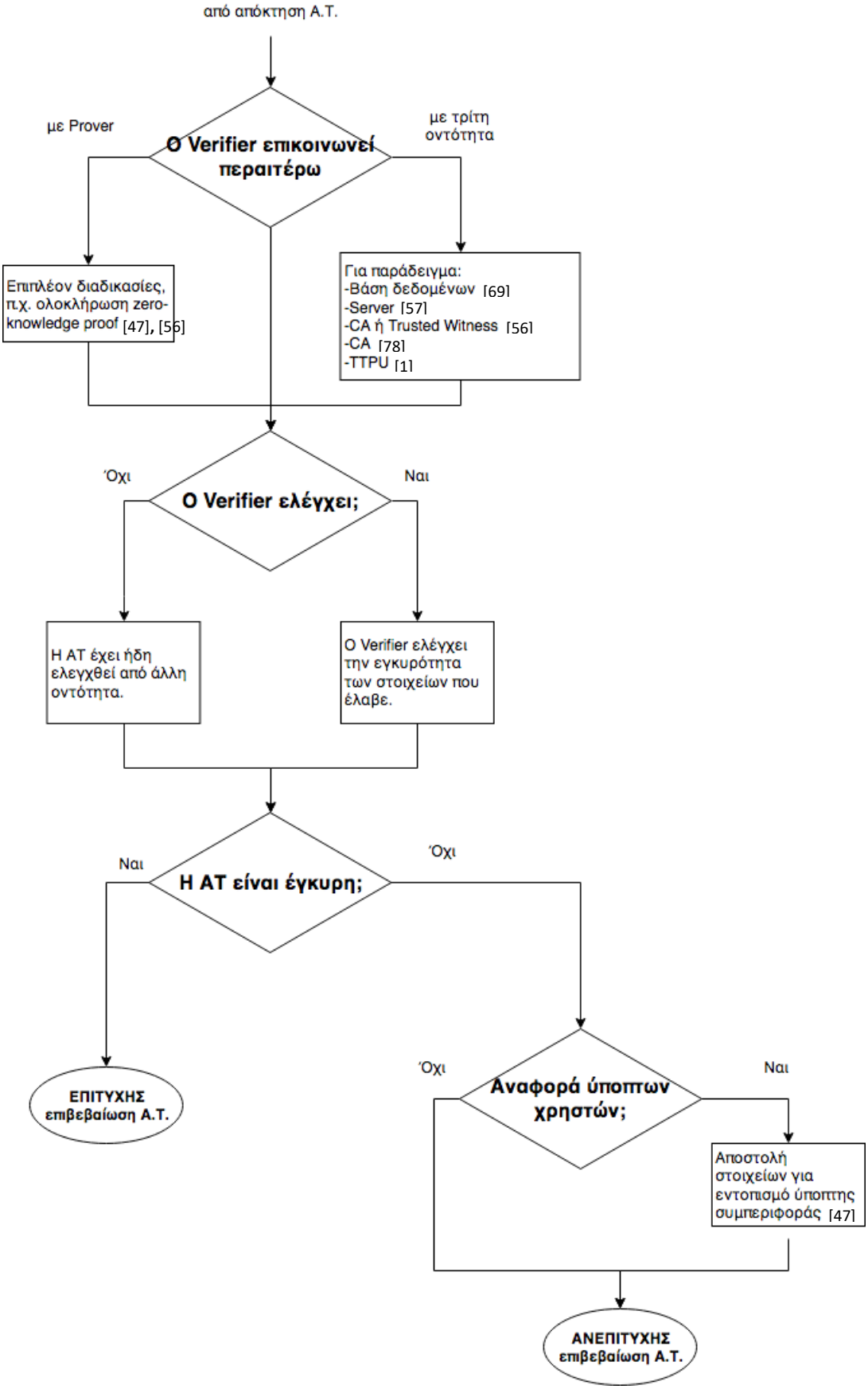
3.12.3 Επιβεβαίωση Α.Τ.

i) Απόκτηση της ΑΤ από τον verifier



Σχήμα 3.7: Επιβεβαίωση Α.Τ. - Απόκτηση της Α.Τ. από τον verifier.

ii) Ενέργειες verifier

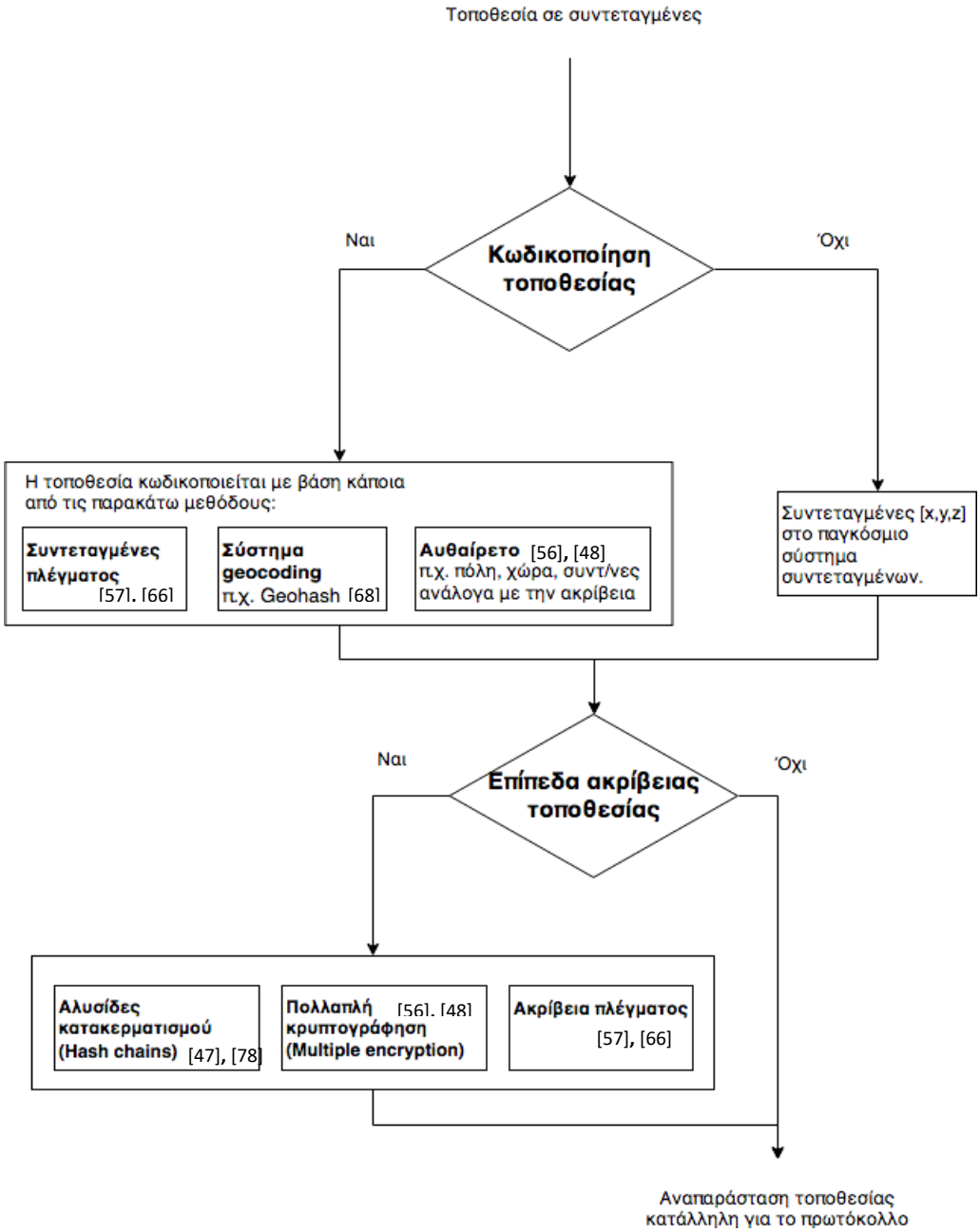


Σχήμα 3.8: Επιβεβαίωση Α.Τ. - Ενέργειες verifier.

3.12.4 Αναπαράσταση τοποθεσίας

Κατά το στάδιο της δημιουργίας απόδειξης τοποθεσίας κατασκευάζεται η αναπαράσταση της τοποθεσίας από τον prover ή τα γειτονικά witnesses, όπως φαίνεται στο διάγραμμα ροής του σταδίου Bii.

Ο κόμβος που αναλαμβάνει να εκτελέσει τη διαδικασία αυτή έχει στη διάθεσή του την τοποθεσία του σε συντεταγμένες. Αν το πρωτόκολλο χρησιμοποιεί κωδικοποίηση τοποθεσίας, τότε ο κόμβος πρέπει να μετατρέψει την τοποθεσία στην αντίστοιχη κωδικοποίηση. Επιπλέον, αν το πρωτόκολλο υποστηρίζει μεταβαλλόμενη ακρίβεια τοποθεσίας, τότε πρέπει να παράγει τα διαφορετικά επίπεδα ακρίβειας. Η διαδικασία της αναπαράστασης τοποθεσίας παρουσιάζεται στο παρακάτω διάγραμμα και έχει ως είσοδο την τοποθεσία σε συντεταγμένες και ως έξοδο τη μορφή που απαιτεί το εκάστοτε πρωτόκολλο.



Σχήμα 3.9: Διαδικασία αναπαράστασης τοποθεσίας.

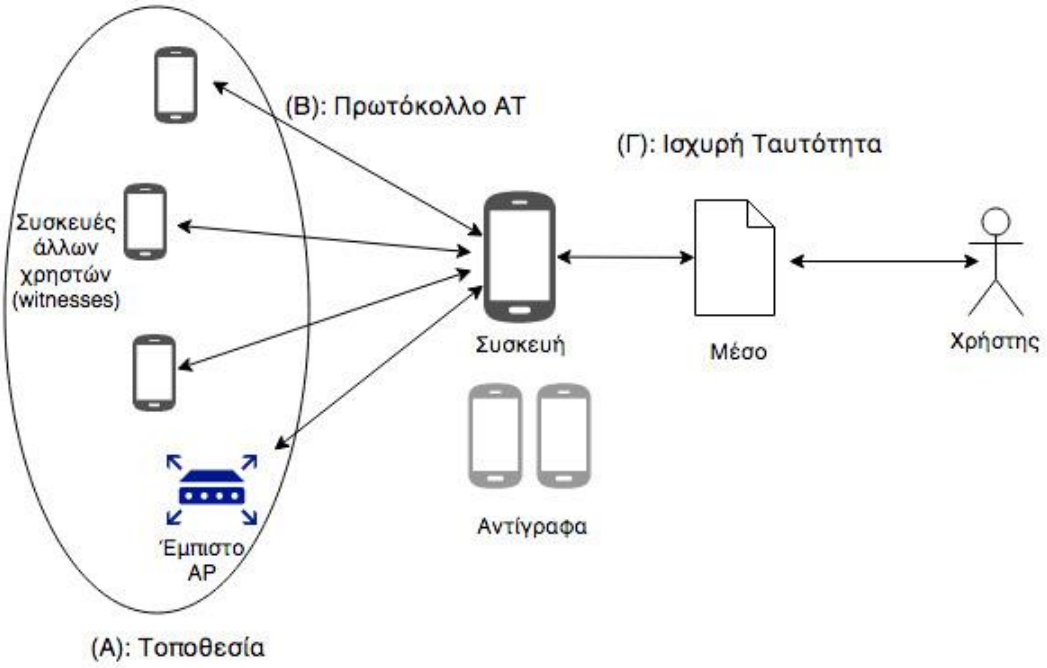
4 QuietPlace: Ένα πρωτόκολλο ισχυρών ταυτοτήτων

4.1 Εμβάθυνση στις ισχυρές ταυτότητες

Στην πιο αυστηρή μορφή τους, τα πρωτόκολλα απόδειξης τοποθεσίας αποσκοπούν στην επιβεβαίωση της παρουσίας ενός ατόμου σε μία τοποθεσία μία ορισμένη χρονική στιγμή.

Η διαδικασία αυτή είναι γνωστή κυρίως σε δικαστικά θέματα, όπου συχνά ένας μάρτυρας (witness) καλείται να επιβεβαιώσει την παρουσία (άλλοθι) του κατηγορουμένου (prover) σε μία τοποθεσία. Στις φυσικές αποδείξεις τοποθεσίας, ένας μάρτυρας αρκεί να συνδέσει τον κατηγορούμενο με μία τοποθεσία, δίχως να εμπλέκεται η κινητή συσκευή κανενός εκ των δύο.

Τα πρωτόκολλα απόδειξης τοποθεσίας έρχονται να διευκολύνουν τη διαδικασία αυτή, εισάγοντας έναν ενδιάμεσο, τη συσκευή του χρήστη, η οποία με τη βοήθεια άλλων συσκευών αναλαμβάνει να διεκπεραιώσει τη διαδικασία. Οι σχέσεις μεταξύ των οντοτήτων φαίνονται στο παρακάτω σχήμα.



Σχήμα 4.1: Οντότητες πρωτοκόλλου απόδειξης τοποθεσίας με ισχυρές ταυτότητες.

Η σχέση (A) ικανοποιείται είτε από συσκευές με γνωστή τοποθεσία, οι οποίες λειτουργούν ως έμπιστοι μάρτυρες (trusted witnesses) και μπορεί να είναι π.χ. access points γνωστά στον verifier, είτε από συσκευές άλλων χρηστών.

Η σχέση (B) αφορά το πρωτόκολλο με το οποίο επιβεβαιώνεται η γειτνίαση των συσκευών με αυτή του χρήστη. Στο σημείο αυτό επικεντρώνονται τα περισσότερα πρωτόκολλα απόδειξης τοποθεσίας που έχουν αναπτυχθεί. Επιβεβαιώνουν δηλαδή την τοποθεσία μίας συσκευής που φέρει τα διαπιστευτήρια (credentials) του χρήστη.

Ωστόσο, δεν λαμβάνουν υπόψη την περίπτωση ο χρήστης να έχει δώσει τη συσκευή του σε κάποιον άλλον, ή να έχει μοιράσει τα διαπιστευτήριά του σε συσκευές-αντίγραφα, που παρουσιάζονται σαν τη δική του.

Η σχέση (Γ) αφορά το αντικείμενο της παρούσας εργασίας, δηλαδή την ανάπτυξη μίας μεθόδου ισχυρών ταυτοτήτων, η οποία θα συνδέει τη συσκευή που εκτελεί ένα πρωτόκολλο απόδειξης τοποθεσίας με το άτομο που την κρατάει. Όπως αναφέραμε παραπάνω, η υλοποίηση ενός πρωτοκόλλου ισχυρών ταυτοτήτων επιλύει το πρόβλημα των πολλών συσκευών με την ίδια ταυτότητα, καθώς συσχετίζει τον ίδιο το χρήστη με τη συσκευή που μετέχει σε μία συγκεκριμένη συνεδρία (session) του πρωτοκόλλου απόδειξης τοποθεσίας (συσχέτιση των διαδικασιών (Β)-(Γ)).

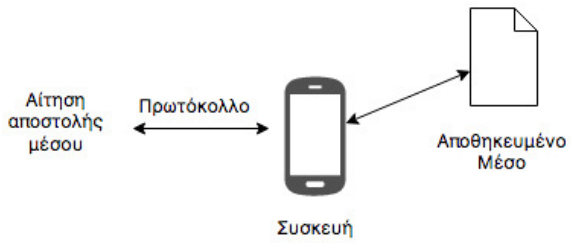
Για την συσχέτιση του χρήστη με τη συσκευή του, απαιτείται ένα μέσο το οποίο παράγεται από τη συσκευή και περιέχει πληροφορίες που ταυτοποιούν το χρήστη. Αυτό το μέσο πρέπει να είναι δύσκολο έως αδύνατο να αλλοιωθεί ή να αναπαραχθεί σε μία άλλη συνεδρία.

4.1.1 Υπάρχουσες προτάσεις

Στο ζήτημα των ισχυρών ταυτοτήτων αναφέρεται κυρίως το [46]. Σε αυτό προτείνονται διαδικασίες πρόκλησης και απάντησης (challenge-response) ανάμεσα στο witness και τον prover.

4.1.1.1 Αποστολή φωτογραφίας χρήστη

Στην απλή περίπτωση, το witness ζητά από τον prover (συσκευή χρήστη) να συμπεριλάβει μία φωτογραφία του χρήστη στο αίτημα για έκδοση AT. Ωστόσο, ένας κακόβουλος χρήστης μπορεί να έχει δώσει σε κάποιον άλλον τη συσκευή του μαζί με μία αποθηκευμένη φωτογραφία του. Ο συνεργαζόμενος χρήστης που συμμετέχει στο πρωτόκολλο αποστέλλει αυτή τη φωτογραφία όταν του ζητείται, προσποιούμενος πως είναι ο ιδιοκτήτης της συσκευής. Συνεπώς, η απλή αποστολή φωτογραφίας στο witness δεν παρέχει επαρκή ασφάλεια.

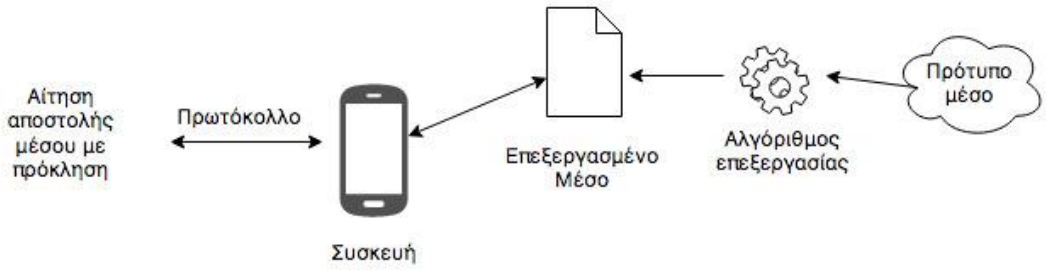


Σχήμα 4.2: Απάτη ισχυρής ταυτότητας με αποθηκευμένο μέσο.

4.1.1.2 Αποστολή φωτογραφίας χρήστη με τυχαίο αριθμό (nonce)

Βελτιώνοντας την παραπάνω πρόταση, οι συγγραφείς προτείνουν τη συμμετοχή ενός τυχαίου αριθμού στη διαδικασία. Συγκεκριμένα, το witness στέλνει στον prover έναν τυχαίο αριθμό (nonce). Τότε, ο prover πρέπει να συμπεριλάβει στην απάντησή του μία φωτογραφία στην οποία να φαίνεται ο ιδιοκτήτης της συσκευής μαζί με ένα χαρτί, στο οποίο έχει γράψει τον αριθμό αυτό. Η πρόταση αυτή εμποδίζει τη χρήση μίας παλαιότερης φωτογραφίας, ωστόσο υπάρχει το ενδεχόμενο να χρησιμοποιείται μία παλαιότερη φωτογραφία η οποία επεξεργάζεται ψηφιακά. Για παράδειγμα, η συσκευή διαθέτει μία αποθηκευμένη φωτογραφία που απεικονίζει τον ιδιοκτήτη να κρατάει ένα λευκό χαρτί (πρότυπο μέσο). Αφού η συσκευή

λάβει τον τυχαίο αριθμό, χρησιμοποιεί αλγόριθμο ψηφιακής επεξεργασίας εικόνας και ενσωματώνει στο λευκό χαρτί τον αριθμό αυτό. Αποστέλλει την παραποιημένη φωτογραφία (επεξεργασμένο μέσο) στο witness εξαπατώντας το.



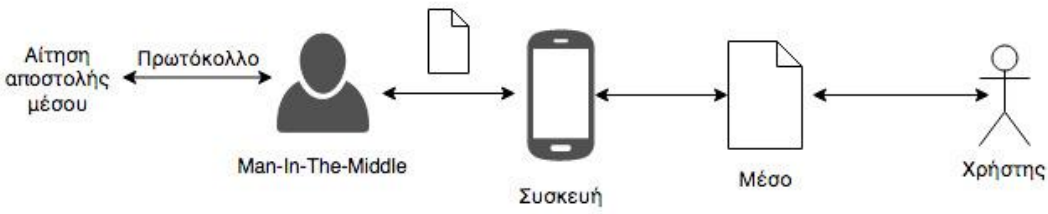
Σχήμα 4.3: Απάτη ισχυρής ταυτότητας με επεξεργασία πρότυπου μέσου.

4.1.1.3 Αποστολή ηχογραφημένης πρότασης

Για την αντιμετώπιση της δυνατότητας επεξεργασίας της εικόνας, οι συγγραφείς προτείνουν την ηχογράφηση μίας πρότασης από την πλευρά του χρήστη. Το witness στέλνει μία πρόταση ως πρόκληση στον prover. Ο χρήστης πρέπει να ηχογραφήσει τον εαυτό του να διαβάζει την πρόταση αυτή. Και σε αυτή την περίπτωση μπορεί να εφαρμοστεί επεξεργασία φωνής ώστε ένας τρίτος να παρουσιάζει τη φωνή του ως αυτή του ιδιοκτήτη της συσκευής. Επίσης, είναι δυνατόν να έχουν προηχογραφηθεί οι λέξεις, όμως στη συνένωσή τους το αποτέλεσμα θα ήταν φανερά αφύσικο. Η μέθοδος αυτή είναι η ασφαλέστερη από τις τρεις που προτείνονται.

4.1.2 Επιθέσεις ενδιάμεσου (relay attacks)

Στις παραπάνω περιπτώσεις πρέπει να λαμβάνεται υπόψη η περίπτωση που ένας τρίτος, ο οποίος έχει στα χέρια του μία συσκευή-αναμεταδότη ή μία συσκευή με τα ψηφιακά κλειδιά του νόμιμου χρήστη, μεταβιβάζει σε αυτόν τις προκλήσεις του AP και λαμβάνει τις απαντήσεις, λειτουργώντας ως ενδιάμεσος (man-in-the-middle). Για την αντιμετώπιση της απάτης αυτής, είναι δυνατόν να χρησιμοποιηθούν οι μέθοδοι ελέγχου γειτνίασης που αναφέρονται στο προηγούμενο κεφάλαιο. Οι συγγραφείς του [46] προτείνουν να τίθενται χρονικοί περιορισμοί μεταξύ της πρόκλησης και της απάντησης (timeout-based).



Σχήμα 4.4: Επίθεση ενδιάμεσου σε περιβάλλον ισχυρών ταυτοτήτων.

4.1.3 Η σημασία του μέσου

Από τα παραπάνω γίνεται κατανοητό πως αναζητούμε ένα μέσο που θα «δένει» την ταυτότητα του χρήστη με τη συσκευή που το παράγει καθώς και με τη συγκεκριμένη συνεδρία απόδειξης τοποθεσίας που εκτελείται.

Το μέσο αυτό θα πρέπει να είναι όσο το δυνατόν δυσκολότερο να αλλοιωθεί και θα πρέπει να περιλαμβάνει όσο το δυνατόν περισσότερα στοιχεία της συνεδρίας απόδειξης τοποθεσίας που εκτελείται.

Στις προαναφερθείσες μεθόδους, οι συγγραφείς βασίζονται είτε στη φωτογραφία είτε στον ήχο. Η μεν φωτογραφία είναι εύκολο να παραποιηθεί ως προς τα στοιχεία συνεδρίας που περιλαμβάνει (τυχαίος αριθμός). Η δε ήχος είναι εύκολο να παραποιηθεί ως προς την ταυτότητα του χρήστη (π.χ. δύο άνθρωποι με παρόμοιες φωνές προσποιούνται ο ένας τον άλλον).

Αν λάβουμε τα θετικά από τις δύο παραπάνω περιπτώσεις, προκύπτει πως πρέπει να χρησιμοποιήσουμε βίντεο ως το μέσο που θα ταυτοποιεί την παρουσία του χρήστη.

Πώς όμως θα ενσωματώσουμε τη συνεδρία μέσα στο αρχείο βίντεο; Ένας τρόπος θα ήταν ο χρήστης να πρέπει να καταγράψει σε βίντεο τον εαυτό του να σημειώνει σε ένα χαρτί έναν τυχαίο αριθμό που στάλθηκε από το witness, όπως γίνεται με την φωτογραφία παραπάνω. Ένας άλλος τρόπος θα ήταν να πρέπει ο χρήστης να διαβάσει μια πρόταση που στέλνει το witness, καταγράφοντας τη σε βίντεο. Και οι δυο λύσεις απαιτούν την ενεργό συμμετοχή του χρήστη, κάτι που δεν είναι επιθυμητό. Ιδανική θα ήταν η ενσωμάτωση της ίδιας της συνεδρίας απόδειξης τοποθεσίας μέσα στο βίντεο του χρήστη, σε συνδυασμό με την εμφάνιση του προσώπου του μέσα σε αυτό. Τα ηλεκτρομαγνητικά κύματα κατά την εκτέλεση ενός πρωτοκόλλου απόδειξης τοποθεσίας δεν μπορούν να ενσωματωθούν σε βίντεο, οι υπέρηχοι όμως μπορούν.

Στο [51] αναπτύσσεται ένα πρωτόκολλο, ονόματι Echo, το οποίο επιβεβαιώνει τη γειτνίαση μεταξύ ενός prover και ενός verifier, οι οποίοι βρίσκονται κοντά ο ένας με τον άλλον. Ο verifier στέλνει μήνυμα προς τον prover μέσω ηλεκτρομαγνητικών κυμάτων, το οποίο περιέχει έναν τυχαίο αριθμό. Ο prover πρέπει μέσα σε περιορισμένο χρονικό διάστημα να απαντήσει στον verifier μέσω υπερήχων, αποστέλλοντας τον αριθμό αυτό.

Με βάση την κεντρική ιδέα του Echo, θα κατασκευάσουμε ένα πρωτόκολλο, το QuietPlace, στο οποίο τα μηνύματα μεταξύ prover και witness θα έχουν τη μορφή υπερήχων. Η όλη συνεδρία καταγράφεται από τον prover σε βίντεο, περιέχοντας όλα τα μηνύματα που ανταλλάχθηκαν μέσω υπερήχων. Μετά τη λήξη της διαδικασίας, ο verifier θα είναι σε θέση να επαληθεύσει ότι το βίντεο λήφθηκε κοντά στα συγκεκριμένα witnesses και περιλαμβάνει τον χρήστη. Για το πρώτο σκέλος, αρκεί η ανάλυση των υπερήχων που υπάρχουν στο βίντεο. Για το δεύτερο σκέλος απαιτούνται αλγόριθμοι αναγνώρισης προσώπου (face recognition), το οποίο είναι εκτός του αντικειμένου της παρούσας εργασίας.

4.2 Υπέρηχοι: Θετικά και Αρνητικά

Το QuietPlace χρησιμοποιεί υπερήχους για την επικοινωνία μεταξύ prover και witness. Οι υπέρηχοι και γενικά ο ήχος ως μέσο διάδοσης έχει θετικά και αρνητικά.

Οι υπέρηχοι λειτουργούν ανεξαρτήτως πλατφόρμας, σε οποιαδήποτε συσκευή διαθέτει ηχείο και μικρόφωνο. Επιπλέον, δεν απαιτείται ζεύξη των συσκευών, όπως συμβαίνει με το Bluetooth ή το WiFi. Συνεπώς, μειώνεται ο χρόνος που απαιτείται για την εγκατάσταση της σύνδεσης [80]. Οι υπέρηχοι επιπλέον δυσκολεύουν τις επιθέσεις ενδιάμεσου (man in the middle). Αυτό, επειδή έχουν τοπική ισχύ και δεν μπορούν να μεταδοθούν σε μεγάλες αποστάσεις χωρίς να μετατραπούν σε ηλεκτρομαγνητικά κύματα. Συνεπώς, εισάγεται επιπλέον χρόνος επεξεργασίας για τον ενδιάμεσο, κάτι που θα οδηγήσει στον ευκολότερο εντοπισμό του [51].

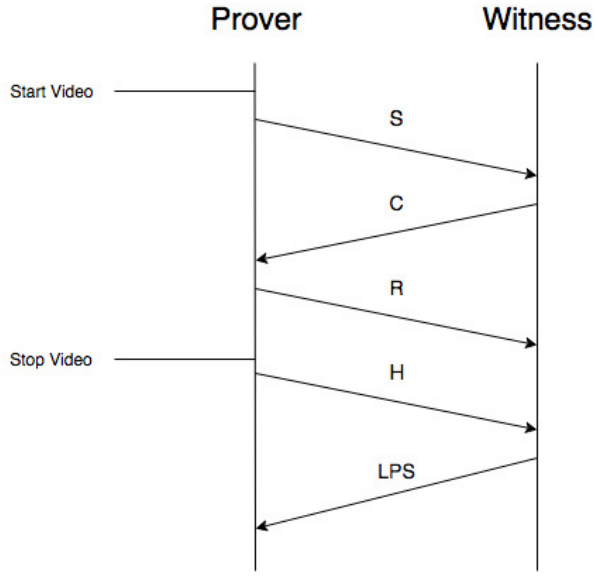
Τέλος, οι υπέρηχοι είναι ιδανικοί για χρήση σε περιβάλλοντα ευαίσθητα σε ηλεκτρομαγνητικές παρεμβολές, όπως για παράδειγμα στο αεροπλάνο κατά τη διάρκεια μιας πτήσης.

Από την άλλη πλευρά, προκειμένου να εκκινηθεί η διαδικασία έκδοσης απόδειξης τοποθεσίας, πρέπει τα witnesses να ελέγξουν για την ύπαρξη μηνυμάτων στο χώρο. Αυτό σημαίνει πως πρέπει να ενεργοποιούν περιοδικά το μικρόφωνό τους για να λάβουν το αίτημα του prover. Η απαίτηση αυτή θέτει προβληματισμούς για την κατανάλωση ενέργειας αλλά και για την ιδιωτικότητα των χρηστών. Μία λύση σε αυτό θα μπορούσε να είναι η αρχική ειδοποίηση για την εκκίνηση του πρωτοκόλλου να γίνεται μέσα από άλλο μέσο, όπως για παράδειγμα μέσω WiFi, το οποίο είναι συνήθως ενεργοποιημένο στις κινητές συσκευές και αναζητεί από προεπιλογή γειτονικά δίκτυα. Αυτό δε θα μας απασχολήσει στην εργασία αυτή. Επιπλέον, η μετάδοση μέσω υπερήχων είναι ευαίσθητη στο θόρυβο και συνεπώς μπορεί να μη λειτουργεί καλά σε θορυβώδη περιβάλλοντα.

4.3 Μία πρώτη προσέγγιση

Αρχικά θα προσεγγίσουμε το προτεινόμενο πρωτόκολλο χωρίς να δώσουμε σημασία στο ακριβές περιεχόμενο των μηνυμάτων που ανταλλάσσονται καθώς και σε τεχνικές απόκρυψης ταυτότητας ή μεταβαλλόμενης ακρίβειας τοποθεσίας. Θα θεωρήσουμε δύο συσκευές, τον prover (P) και το witness (W). Ο prover επιθυμεί να επιβεβαιώσει την παρουσία του κοντά στον witness.

Τα μηνύματα που ανταλλάσσονται φαίνονται στο παρακάτω σχήμα.



Σχήμα 4.5: Μηνύματα που ανταλλάσσονται μεταξύ prover και witness.

Συγκεκριμένα:

1. Ο prover αρχίζει την εγγραφή του βίντεο, στο οποίο φαίνεται ο χρήστης που κρατάει τη συσκευή.
2. Ο prover αποστέλλει μέσω υπερήχων μήνυμα S (start), στο οποίο εμπεριέχει την ταυτότητά του, τη χρονική στιγμή και την τοποθεσία στην οποία υποστηρίζει ότι βρίσκεται. Μέσα στο μήνυμα S περιλαμβάνει και ένα hash του πρώτου frame του βίντεο που καταγράφει. Αυτό το hash λειτουργεί ως δέσμευση (commitment) πως έχει ξεκινήσει την καταγραφή και δε θα αλλοιώσει το βίντεο στη συνέχεια.

3. Το witness αποστέλλει μία πρόκληση C (challenge), η οποία περιέχει την ταυτότητα του witness, την τρέχουσα χρονική στιγμή καθώς και έναν τυχαίο αριθμό (nonce). Ο αριθμός αυτός έχει ως σκοπό να καταστήσει μοναδική και μη αναπαράξιμη τη συνεδρία.
4. Ο prover καλείται να απαντήσει όσο το δυνατόν γρηγορότερα, αποστέλλοντας πίσω στο witness απάντηση R (response) με τον τυχαίο αριθμό που έλαβε.
5. Το witness μετρά το χρονικό διάστημα ανάμεσα στην πρόκληση C και την απάντηση R, για να εκτιμήσει αν ο prover βρίσκεται πράγματι κοντά του.
6. Ο prover ολοκληρώνει την εγγραφή του βίντεο και παράγει το hash H του αρχείου βίντεο. Το αποστέλλει στο witness.
7. Το witness τοποθετεί την απόφασή του (θετική ή αρνητική) μαζί με το hash H και τα μηνύματα C, R σε ένα μήνυμα LPS (Location Proof Segment) και το αποστέλλει στον prover.

Στη συνέχεια, ο verifier θα κληθεί να επιβεβαιώσει τον ισχυρισμό του prover.

Ο verifier θα πρέπει να ελέγξει:
1. Την απόφαση που έλαβε το witness.
2. Αν το hash του βίντεο ταιριάζει με αυτό που περικλείει το witness στο LPS.
3. Αν το hash του πρώτου frame του βίντεο συμπίπτει με αυτό που περικλείει το witness στο LPS.
4. Αν στον ήχο του βίντεο υπάρχει η συνεδρία μεταξύ prover και witness.
5. Αν στο βίντεο απεικονίζεται ο νόμιμος χρήστης (legitimate owner) της συσκευής.

4.3.1 Ανοχή σε προαποθηκευμένο μέσο

Στο παραπάνω παράδειγμα είναι εύκολο ένας κακόβουλος χρήστης να συνδυάσει ένα προμαγνητοσκοπημένο βίντεο στο οποίο φαίνεται ο ιδιοκτήτης της συσκευής με τον πραγματικό ήχο κατά τη συνεδρία. Θα προκύψει έτσι ένα αρχείο το οποίο θα περιέχει και τον ιδιοκτήτη και τη συνεδρία, χωρίς πράγματι αυτός να βρίσκεται εκεί.

Για να αποφύγουμε αυτή την επίθεση, χρειαζόμαστε έναν τρόπο να «δέσουμε» τη ροή βίντεο με τη ροή ήχου. Απαιτούμε από το witness στην πρόκληση C να περιλαμβάνει και έναν δεύτερο τυχαίο αριθμό (nonce 2). Κατά τη λήψη της C, ο χρήστης της συσκευής θα πρέπει να διαβάσει τον αριθμό αυτό, ώστε να ακούγεται στο βίντεο.

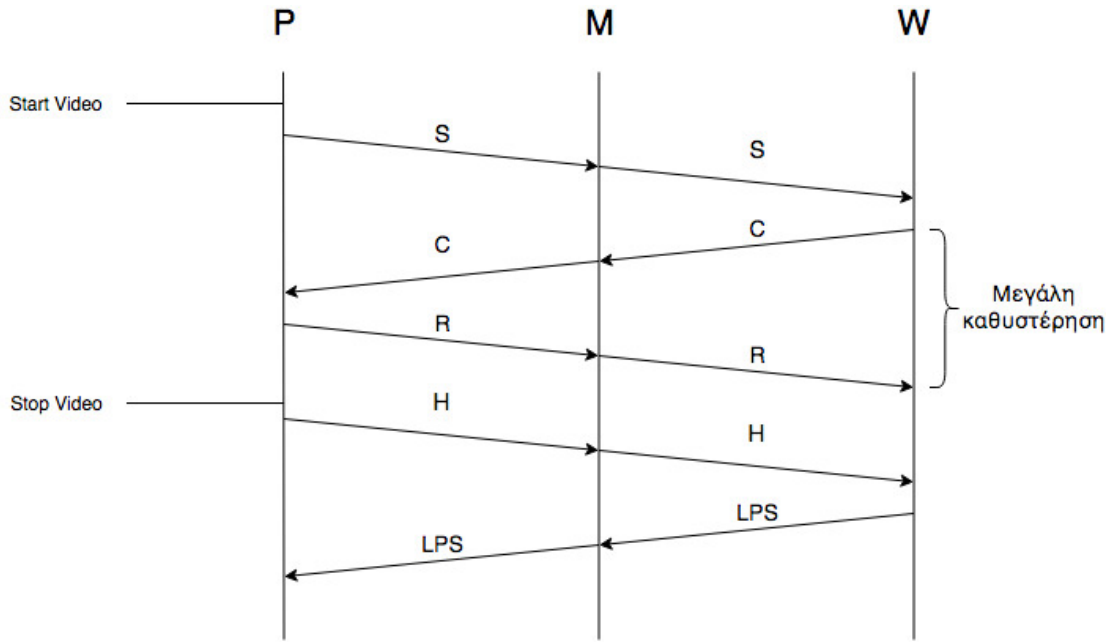
4.3.2 Ανοχή στις επιθέσεις ενδιάμεσου (Man In The Middle attacks)

Στην παράγραφο αυτή θα διερευνήσουμε το κατά πόσον το προτεινόμενο πρωτόκολλο είναι σε θέση να ανιχνεύσει την ύπαρξη ενδιάμεσου. Ο ενδιάμεσος M βρίσκεται κοντά στο witness ενώ ο prover μαζί με τον χρήστη βρίσκονται μακριά από το witness.

Διακρίνουμε δύο περιπτώσεις, στη μία ο ενδιάμεσος M απλά αναπαράγει τα μηνύματα του prover P, ενώ στην άλλη διαθέτει τα κλειδιά του.

4.3.2.1 Ο ενδιάμεσος M απλά αναπαράγει τα μηνύματα (relay attack)

Στην πρώτη περίπτωση ο M είναι ένας απλός αναμεταδότης των μηνυμάτων του prover, όπως περιγράφεται στο [46]. Ο M βρίσκεται κοντά στον W ενώ ο P (και ο φυσικός χρήστης που μας ενδιαφέρει) είναι απομακρυσμένος.



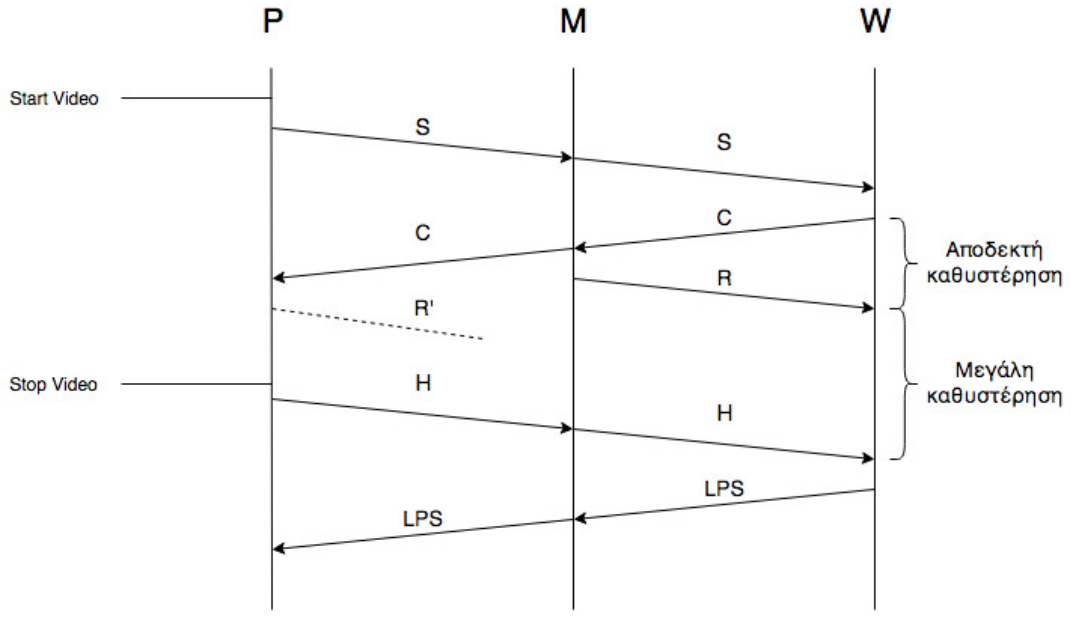
Σχήμα 4.6: Αναπαραγωγή μηνυμάτων από ενδιάμεσο.

Η καθυστέρηση που παρατηρεί το witness ανάμεσα στα μηνύματα C και R είναι μεγάλη, οπότε η απάτη εντοπίζεται και αποστέλλεται ακυρωτικό LPS.

4.3.2.2 Ο ενδιάμεσος M διαθέτει τα κλειδιά του prover

Σε αυτή την περίπτωση ο P και ο M εμφανίζονται ως συσκευές του ίδιου χρήστη. Ο M απαντά απευθείας, αφού μπορεί να χρησιμοποιήσει την υπογραφή του P. Ο P παράγει ψευδή ηχητικά σήματα που καταγράφονται στο βίντεο, τα οποία παρουσιάζονται με διακεκομμένη γραμμή, προκειμένου να φαίνεται πως απαντά κατευθείαν στα μηνύματα του W.

Η απαίτηση για ισχυρές ταυτότητες με χρήση βίντεο αποκαλύπτει πως ο χρήστης βρίσκεται μακριά.

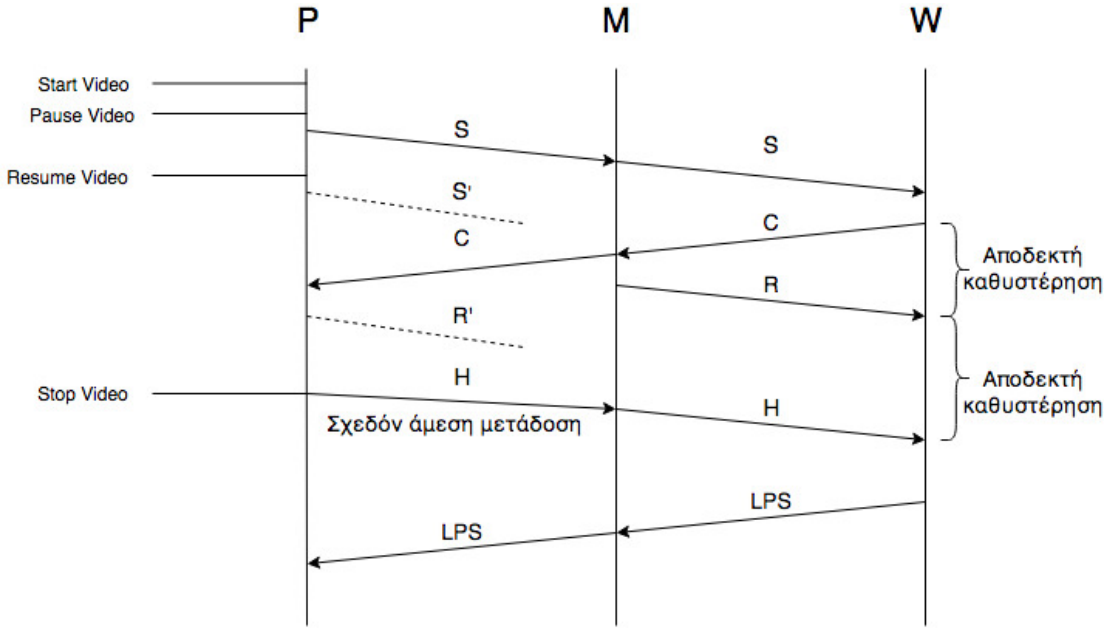


Σχήμα 4.7: Χρήση κλειδιών του prover από τον ενδιάμεσο.

Ενώ η καθυστέρηση που βλέπει ο W μεταξύ των μηνυμάτων C και R είναι αποδεκτή, παρουσιάζεται μεγάλη καθυστέρηση μεταξύ R και H.

Ακόμα και αν ο P έχει κάποιον τρόπο να μεταβιβάσει γρήγορα το H στον M ώστε ο W να δει αποδεκτή καθυστέρηση, ο verifier μπορεί να ελέγξει τις διαφορές χρόνου μεταξύ S και R' στο βίντεο του P και μεταξύ S και R στα μηνύματα που λαμβάνει ο W.

Ο P μπορεί επιπλέον να μειώσει τη διαφορά χρόνου μεταξύ S και R'. Για να το πετύχει αυτό, ξεκινά την καταγραφή, λαμβάνει το hash του πρώτου frame και διακόπτει προσωρινά την καταγραφή (pause). Μεταβιβάζει το S στον M, και μετά από λίγο συνεχίζει (resume) την καταγραφή και εκπέμπει ένα ψευδές ηχητικό σήμα S', όπως φαίνεται στο παρακάτω σχήμα.



Σχήμα 4.8: Παύση καταγραφής βίντεο και επαναποστολή μηνύματος S από τον prover.

Και αυτή η απάτη μπορεί να εντοπιστεί από τον verifier, ο οποίος βλέπει πως το βίντεο που δημιούργησε ο prover είναι αρκετά μικρότερο από τον χρόνο εκτέλεσης του πρωτοκόλλου (χρονικό διάστημα μεταξύ S και H). Εκτός αυτού, αν το βίντεο ελέγχεται από άνθρωπο, κάτι λογικό σε περιβάλλον ισχυρών ταυτοτήτων, η διακοπή του βίντεο θα είναι αισθητή σε αυτόν.

4.4 Μοντέλο του συστήματος

Οι provers, τα witnesses και οι verifiers είναι εγγεγραμμένοι ως χρήστες σε μία Αρχή Πιστοποίησης (CA). Αυτή διατηρεί λίστα με τους χρήστες και παρέχει σε αυτούς κλειδιά. Παράλληλα, εφαρμόζει ένα σχήμα εμπιστοσύνης και αξιολογεί τους κόμβους για τη συμπεριφορά τους. Είναι σημαντικό η CA να παρέχει και άλλες υπηρεσίες με τα ίδια κλειδιά (π.χ. e-mail), κάτι που λειτουργεί ανασταλτικά στην προσπάθεια των κακόβουλων χρηστών να μοιραστούν τα κλειδιά τους. Η πρακτική αυτή είναι ιδιαίτερα διαδεδομένη σε εφαρμογές ταυτοποίησης που βασίζονται σε έναν πάροχο ταυτότητας (Single Sign On).

Το σύστημά μας βασίζεται στο διαχωρισμό της γνώσης. Η CA μαθαίνει μόνο τις ταυτότητες των χρηστών που συμμετείχαν σε μια συνεδρία και αξιολογεί τη συμπεριφορά τους. Ο verifier μαθαίνει μόνο την τοποθεσία του prover, καθώς και πόσο αξιόπιστη είναι η πληροφορία αυτή σύμφωνα με την CA. Παράλληλα, λαμβάνει το βίντεο από τον prover ώστε να εφαρμόσει έλεγχο ισχυρών ταυτοτήτων.

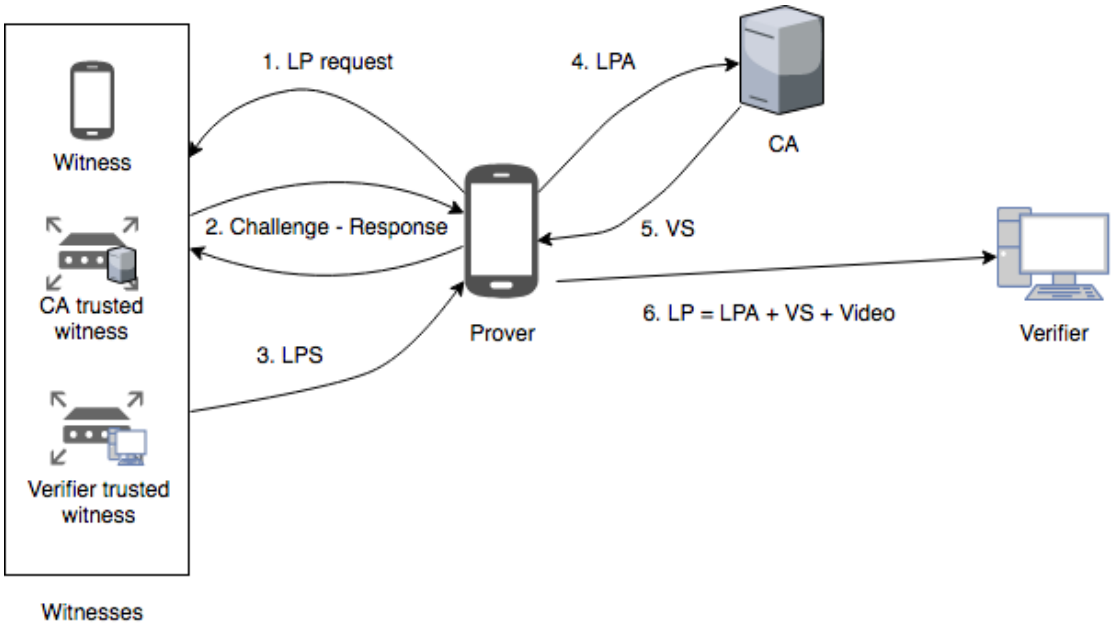
Τόσο η CA όσο και ο verifier μπορούν να έχουν έμπιστα witnesses. Οι έμπιστοι κόμβοι για την CA σημαίνουν μεγάλη εμπιστοσύνη. Οι έμπιστοι κόμβοι για τον verifier σημαίνουν άμεση αποδοχή της AT, ανεξάρτητα από την απάντηση των άλλων witnesses. Ο verifier μαθαίνει την ταυτότητα μόνο των έμπιστων για αυτόν witnesses.

Η ύπαρξη CA και verifier ως ξεχωριστές οντότητες δίνει αφενός τη δυνατότητα εφαρμογής σχήματος εμπιστοσύνης χωρίς να εκθέτει την ταυτότητα των χρηστών στον verifier. Εκτός αυτού, δίνει οικονομικό κίνητρο στην CA, η οποία παρέχει την έκδοση AT ως υπηρεσία στους verifiers. Το οικονομικό όφελος που έχει συμβάλλει στην επέκταση ενός δικτύου έμπιστων witnesses που η CA μπορεί να εγκαθιστά.

Στην παρούσα εργασία δεν θα ασχοληθούμε με το σχήμα εμπιστοσύνης που εφαρμόζει η CA, αλλά μόνο με τα μηνύματα που ανταλλάσσονται μεταξύ των οντοτήτων.

Σημειώνεται ότι ο ρόλος της CA και του verifier μπορεί να ταυτίζεται σε ειδικές εφαρμογές. Για παράδειγμα, ένα νοσοκομείο θέλει να επιβεβαιώσει πως ένας συγκεκριμένος γιατρός βρίσκεται στο γραφείο του, προκειμένου να παρέχει σε αυτόν πρόσβαση στα αρχεία των ασθενών. Σε αυτή την περίπτωση, το νοσοκομείο παρέχει τις ταυτότητες στους χρήστες του και διαθέτει trusted witnesses τοποθετημένα στις αίθουσες, λειτουργώντας ως CA. Παράλληλα ελέγχει την τοποθεσία του γιατρού, λειτουργώντας ως verifier.

Το μοντέλο που θεωρούμε φαίνεται στο παρακάτω σχήμα.



Σχήμα 4.9: Μοντέλο του συστήματος.

Ο prover, αφού συλλέξει τα LPS από όλα τα witnesses, τα τοποθετεί σε ένα μήνυμα LPA (Location Proof Assertion – Ισχυρισμός Απόδειξης Τοποθεσίας), το οποίο αποστέλλει στην CA για έλεγχο. Η CA, αφού πραγματοποιήσει ελέγχους απαντά με το μήνυμα VS (Verifier Segment – Τεμάχιο Verifier). Ο prover αποθηκεύει τα στοιχεία αυτά και όποτε θέλει να επιβεβαιώσει την απόδειξη τοποθεσίας κατασκευάζει το μήνυμα LP (Location Proof – Απόδειξη Τοποθεσίας) και το αποστέλλει στον verifier.

Η διαδικασία και το περιεχόμενο των μηνυμάτων περιγράφονται αναλυτικά σε επόμενη ενότητα.

4.5 Απαραίτητα υποσυστήματα

Στην ενότητα αυτή αναλύουμε τους θεμέλιους λίθους (primitives) που θα χρησιμοποιήσουμε για την ικανοποίηση των προδιαγραφών ασφαλείας και ιδιωτικότητας.

4.5.1 Κωδικοποίηση τοποθεσίας (geocoding)

Για την κωδικοποίηση της τοποθεσίας θα χρησιμοποιήσουμε τα plus codes [45]. Το σύστημα αυτό είναι δωρεάν, ανοιχτού κώδικα και παρέχει τη δυνατότητα για μεταβαλλόμενη ακρίβεια τοποθεσίας.

Τα plus codes αναφέρονται σε περιοχές και όχι σημεία. Η ακρίβεια που παρέχουν είναι μέχρι περιοχές περίπου 3x3 μέτρων. Θα χρησιμοποιηθούν όμως οι πλήρεις κωδικοί στη βασική τους μορφή, αποτελούμενοι από 10 χαρακτήρες και περιγράφοντας μία περιοχή περίπου 14x14 μέτρα. Αυτή η επιλογή γίνεται γιατί τυπικά η ακρίβεια του GPS στα smartphones δεν μπορεί να φτάσει τα 3 μέτρα [81].

Χρειαζόμαστε τις παρακάτω λειτουργίες:

- Encode (latitude, longitude): Μετατρέπει συντεταγμένες της μορφής (latitude, longitude) σε plus code δέκα χαρακτήρων.
- Decode (pluscode): Μετατρέπει το pluscode σε ζεύγος συντεταγμένων (latitude, longitude).
- Reduce accuracy (pluscode, level): Μειώνει το επίπεδο της ακρίβειας του πλήρους pluscode στο επίπεδο level.

Δε χρειάζεται να γίνει υπολογισμός απόστασης μεταξύ της περιοχής που δηλώνει ο prover και το witness. Αρκεί witness και prover να βρίσκονται στην ίδια περιοχή που ορίζει το plus code, προκειμένου να προχωρήσει το πρωτόκολλο στον έλεγχο γειτνίασης. Άλλωστε, σε δοκιμές που πραγματοποιήθηκαν οι υπέρηχοι έχουν μικρή εμβέλεια και συνεπώς οι συσκευές πρέπει να βρίσκονται στην ίδια περιοχή 14x14 μέτρων που ορίζει το πλήρες plus code προκειμένου να μπορούν να επικοινωνήσουν μεταξύ τους.

4.5.2 Κρυπτογραφικές δεσμεύσεις (commitments)

Για να αποκρύψουμε την ταυτότητα των χρηστών καθώς και άλλα ευαίσθητα στοιχεία θα χρησιμοποιήσουμε κρυπτογραφικές δεσμεύσεις.

Ένα σχήμα δέσμευσης αποτελεί έναν ηλεκτρονικό τρόπο για την προσωρινή απόκρυψη ενός μηνύματος το οποίο δεν μπορεί να αλλοιωθεί. Σκοπός είναι αυτό το μήνυμα να αποκαλυφθεί αργότερα.

Η διαδικασία αποτελείται από δύο στάδια:

- Στο πρώτο στάδιο (δέσμευση – commitment), ο αποστολέας «κλειδώνει» μία τιμή και την αποστέλλει στο δέκτη.
- Στο δεύτερο στάδιο (αποδέσμευση – decommitment), ο αποστολέας στέλνει στο δέκτη το κλειδί, δίνοντάς του έτσι πρόσβαση στο μήνυμα.

Ένα απλό σχήμα δέσμευσης

Έστω h() μία συνάρτηση κατακερματισμού (hashing function).

Στο στάδιο της δέσμευσης, ένας αποστολέας που θέλει να δεσμευτεί για ένα μήνυμα m, παράγει έναν τυχαίο αριθμό r και υπολογίζει τη δέσμευση C=h(m|r). Στέλνει το C στον δέκτη.

Στο στάδιο της αποδέσμευσης, ο αποστολέας στέλνει το m|r στον δέκτη. Αυτός επιβεβαιώνει πως η δέσμευση που έλαβε αρχικά αφορούσε τις συγκεκριμένες τιμές [73].

Το σχήμα αυτό μπορεί να είναι ανεπαρκές για εφαρμογές που απαιτείται υψηλό επίπεδο ασφάλειας, και αυτό γιατί ο δέκτης μπορεί με διαδοχικές προσπάθειες κατακερματισμού (brute-force) να βρει το ζεύγος m|r που περιέχει η δέσμευση C. Εκτός αυτού, μπορεί να έχει υπολογίσει προηγουμένως όλα τα $h(m_i|r_i)$ για κάθε πιθανό m_i, r_i, κατασκευάζοντας έναν πίνακα αντιστροφής hash (rainbow table [82], [83]). Τότε, αρκεί να αναζητήσει στον πίνακα τη δέσμευση που έλαβε και θα αποκτήσει άμεσα γνώση του μηνύματος m.

Υπάρχουν διάφορα ασφαλέστερα σχήματα δεσμεύσεων, όπως τα [71], [72]. Το σχήμα δέσμευσης που θα χρησιμοποιηθεί πρέπει να λειτουργεί με το μοντέλο της απεριόριστης υπολογιστικής ισχύος του δέκτη (computationally unbounded), προκειμένου να παρέχει τη μέγιστη ασφάλεια. Το πρωτόκολλο που προτείνεται λειτουργεί ανεξάρτητα από το σχήμα που θα επιλεχθεί.

4.5.3 Επίπεδα ακρίβειας τοποθεσίας και αλυσίδες κατακερματισμού (hash chains)

Για την υποστήριξη μεταβαλλόμενης ακρίβειας τοποθεσίας θα χρησιμοποιήσουμε αλυσίδες κατακερματισμού.

Μία αλυσίδα κατακερματισμού είναι η συνεχόμενη εφαρμογή μίας συνάρτησης κατακερματισμού σε ένα κομμάτι δεδομένων [84]. Ωστόσο, ο όρος μπορεί να χρησιμοποιηθεί και για άλλους συνδυασμούς, όπου ορισμένα δεδομένα συνδέονται με συναρτήσεις κατακερματισμού, όπως για παράδειγμα περιγράφεται στο [59].

Αν γνωρίζουμε εκ των προτέρων την ακρίβεια τοποθεσίας που απαιτείται από τον verifier, τότε αρκεί να τη συμπεριλάβουμε στην απόδειξη τοποθεσίας. Όμως, το ζητούμενο είναι να παράγουμε AT ανεξάρτητα από τον verifier. Σε αυτή την περίπτωση πρέπει να βρούμε έναν τρόπο να συμπεριλάβουμε μέσα στην AT όλες τις δυνατές ακρίβειες τοποθεσίας, με τρόπο ώστε να αποκαλύπτεται στον verifier η ακρίβεια που ο prover επιθυμεί.

Οι αλυσίδες κατακερματισμού παρέχουν έναν πιο ευέλικτο τρόπο χειρισμού των επιπέδων ακρίβειας τοποθεσίας και διευκολύνουν τον έλεγχο της εγκυρότητάς τους, όπως αναφέρθηκε στο προηγούμενο κεφάλαιο.

4.5.3.1 Απλές αλυσίδες κατακερματισμού

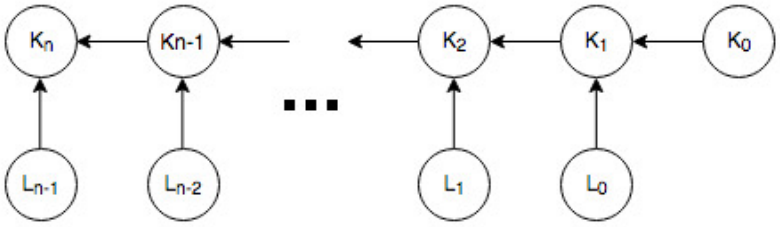
Στο [85] γίνεται λόγος για ένα σχήμα απόκρυψης της τοποθεσίας με hash chain. Θα εξηγήσουμε τη λειτουργία του προσαρμόζοντάς το στη χρήση plus codes για την περιγραφή της τοποθεσίας.

Συγκεκριμένα, θεωρούμε n επίπεδα ακρίβειας τοποθεσίας. Συνεπώς, η τοποθεσία μπορεί να περιγραφεί ως L_i, $0 \leq i < n$, όπου με L_0 η τοποθεσία με μέγιστη ακρίβεια και L_{n-1} η τοποθεσία με ελάχιστη ακρίβεια.

Ο prover υπολογίζει έναν τυχαίο αριθμό K_0. Επιπλέον h() είναι μία συνάρτηση κατακερματισμού.

Τότε ο prover παράγει την αλυσίδα:

$K = K_n|K_{n-1} \ldots K_2|K_1|K_0$, όπου $K_{i+1} = h(L_i|K_i)$, για $0 \leq i < n$, η οποία αναπαρίσταται στο παρακάτω σχήμα. Ονομάζουμε το K_n ως κεφαλή της αλυσίδας.



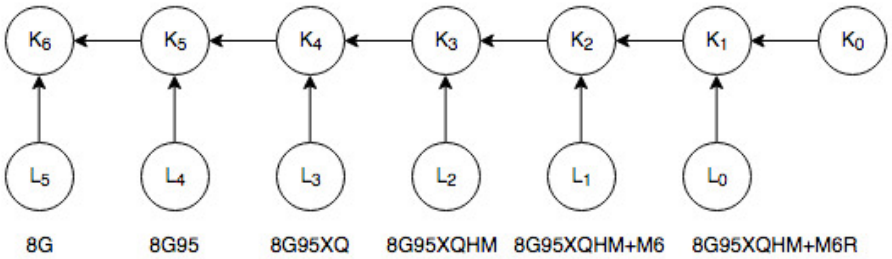
Σχήμα 4.10: Απλή αλυσίδα κατακερματισμού

Για παράδειγμα, έστω η τοποθεσία L_0=8G95XQHM+M6R. Τότε L_1=8G95XQHM+M6, L_2=8G95XQHM, L_3=8G95XQ, L_4=8G95 και τέλος L_5=8G. Τα plus codes δίνουν 6 επίπεδα ακρίβειας τοποθεσίας, στη μεγαλύτερη δυνατή μορφή τους με 11 χαρακτήρες.

Ο prover παράγει την αλυσίδα:

$K = K_6|K_5|K_4|K_3|K_2|K_1|K_0|$, όπου $K_{i+1} = h(L_i|K_i)$, για $0 \leq i < 6$

Οπτικά η αλυσίδα φαίνεται στο παρακάτω σχήμα:



Σχήμα 4.11: Απλή αλυσίδα κατακερματισμού εφαρμοσμένη σε Plus Code.

Ο prover γνωρίζει φυσικά το L_0, την ακριβή του τοποθεσία. Το witness μπορεί να ελέγξει την εγκυρότητα της αλυσίδας αν διαθέτει τα K_6, L_0, K_0.

Στην AT που ο prover στέλνει στον verifier, υπάρχει μόνο το K_6. Για να επιβεβαιωθεί η τοποθεσία του prover με ακρίβεια L_i, ο prover δεν έχει παρά να στείλει στον verifier τα L_i, K_i. Τότε ο verifier μπορεί να ελέγξει το κομμάτι της αλυσίδας μέχρι να φτάσει στο K_6.

Το σχήμα αυτό απαιτεί την αποστολή λιγότερων πληροφοριών προς το witness, αφού δε χρειάζεται να αποσταλεί το κλειδί για κάθε ακρίβεια τοποθεσίας. Επιπλέον, στην AT αρκεί να υπάρχει μόνο το K_6, το οποίο ονομάζουμε κεφαλή της αλυσίδας κατακερματισμού.

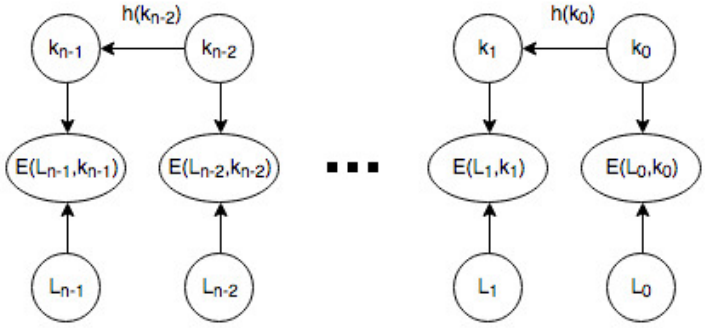
Σημείωση: Η συνάρτηση κατακερματισμού h() πρέπει να ικανοποιεί τα εξής, τα οποία περιγράφονται στο [86]*:*

- *Preimage resistance: Η τιμή της συνάρτησης h(x) για οποιαδήποτε είσοδό της x υπολογίζεται εύκολα. Το αντίστροφο όμως δεν ισχύει: για οποιοδήποτε y, δεν μπορεί να βρεθεί x ώστε h(x)=y.*
- *Second preimage resistance: Για οποιοδήποτε δοθέν m, είναι υπολογιστικά δύσκολη η εύρεση m' με την ιδιότητα h(m) = h(m').*
- *Collision resistance: Δεν μπορούν να υπολογιστούν δύο διαφορετικές είσοδοι m, m' που να δίνουν την ίδια έξοδο, δηλαδή h(m)=h(m').*

4.5.3.2 Αλυσίδες κατακερματισμού με κρυπτογραφία

Μία παραλλαγή των παραπάνω αλυσίδων συναντάμε στο [1]. Χρησιμοποιούνται κλειδιά για να κρυπτογραφήσουν κάθε ακρίβεια τοποθεσίας, παρόμοια με την προηγούμενη παράγραφο, όμως τώρα τα κλειδιά αυτά συνδέονται μεταξύ τους σε μια αλυσίδα κατακερματισμού.

Ο prover παράγει ένα τυχαίο κλειδί k_0. Κάθε επίπεδο τοποθεσίας αναπαρίσταται στην κρυπτογραφημένη μορφή $E(L_i, k_i)$, για $0 \leq i < n$, δηλαδή με την κρυπτογράφηση της τοποθεσίας L_i με κλειδί k_i. Κάθε κλειδί προκύπτει κατακερματίζοντας το προηγούμενο, δηλαδή $k_i = h(k_{i-1})$, για $0 < i < n$.

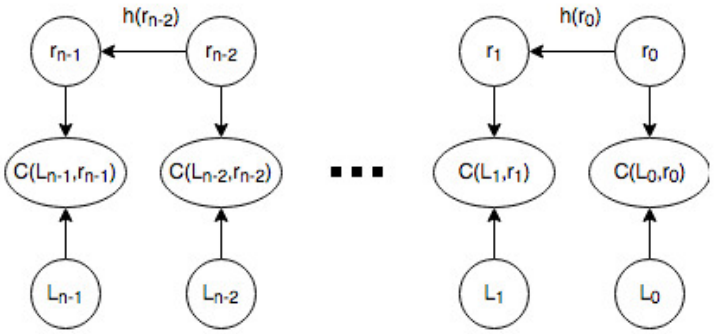


Σχήμα 4.12: Αλυσίδα κατακερματισμού με κρυπτογραφία.

Η εγκυρότητα της αλυσίδας μπορεί να ελεγχθεί από το witness αν έχει στη διάθεσή του τα $E(L_{n-1}, k_{n-1})$ καθώς και τα L_0, k_0. Η AT μπορεί να περιέχει μόνο το $E(L_{n-1}, k_{n-1})$, ενώ αρκεί να αποσταλεί το αντίστοιχο L_i, k_i στον verifier, για να επιβεβαιώσει την ορθότητα της αλυσίδας μέχρι να φτάσει στο $E(L_{n-1}, k_{n-1})$. Διαφορετικά, η AT μπορεί να περιέχει όλα τα $E(L_i, k_i)$ και ο prover να στέλνει το αντίστοιχο κλειδί στον verifier.

Μία άλλη παραλλαγή αντί για κλειδιά χρησιμοποιεί δεσμεύσεις και κατακερματισμό και χρησιμοποιείται στο [56].

Ο prover υπολογίζει έναν τυχαίο αριθμό r_0. Κάθε επίπεδο τοποθεσίας αναπαρίσταται με τη δέσμευση $C(L_i, r_i)$, για $0 \leq i < n$ και κάθε $r_i = h(r_{i-1})$, για $0 < i < n$.



Σχήμα 4.13: Αλυσίδα κατακερματισμού με κρυπτογραφικές δεσμεύσεις.

4.6 Περισσότερα του ενός witnesses

Όπως είναι αναμενόμενο, συχνά απαιτούνται περισσότερα από ένα witness, τα οποία καλούνται να επικυρώσουν την τοποθεσία του prover.

Αμέσως μετά το αίτημα του prover για έκδοση AT, κάθε witness δηλώνει την παρουσία του. Αυτό μπορεί να γίνει για παράδειγμα συμπεριλαμβάνοντας σε ένα μήνυμα WP (Witness Presence – Παρουσία Μάρτυρα) την ταυτότητά του σε μία δέσμευση. Αφού όλα τα witnesses δηλώσουν την παρουσία τους, κάθε ένα από αυτά κατασκευάζει ένα πίνακα στον οποίο περιλαμβάνονται όλα τα υπόλοιπα που εξέπεμψαν μήνυμα παρουσίας. Ο πίνακας του κάθε witness μπορεί να ελεγχθεί από την CA, ώστε να εντοπιστούν συνεργασίες (π.χ. κάποιο witness που δεν είδε κανείς αλλά έστειλε TAT). Με τον τρόπο αυτό αποφεύγεται η δυνατότητα απόκρυψης/προσθήκης TAT.

Μετά την αποστολή των μηνυμάτων παρουσίας από τα witness, ξεκινά η διαδικασία ελέγχου γειτνίασης του prover με κάθε ένα από αυτά, ώσπου να πραγματοποιηθεί για όλα τα witnesses και τελικά ο prover να λάβει ένα TAT από κάθε ένα από αυτά. Κάθε witness μπορεί να κατασκευάσει ένα δεύτερο πίνακα, που να περιέχει όλα τα witnesses που έστειλαν TAT. Με τον τρόπο αυτό η CA θα μπορεί να επιβεβαιώσει πως ο prover εχει συμπεριλάβει όλα τα TAT που στάλθηκαν σε αυτόν, λειτουργώντας ως επιπλέον προστασία στην απόκρυψη/προσθήκη TAT.

Κατά την επικοινωνία του prover με κάθε witness είναι σημαντικό να μεριμνηθεί ώστε να μην υπάρχουν συγκρούσεις στο μέσο επικοινωνίας. Αυτό σημαίνει ότι το πολύ ένα witness μπορεί να εκπέμπει μηνύματα κάθε χρονική στιγμή.

4.7 Περιγραφή του πρωτοκόλλου

Στο σημείο αυτό θα περιγράψουμε την πλήρη λειτουργία του πρωτοκόλλου. Αρχικά όμως θα περιγράψουμε τα σύμβολα που αντιστοιχούν σε κάθε διαδικασία.

Σύμβολο	**Εξήγηση**
$m_1 \| m_2$	Συνένωση (concatenation) των μηνυμάτων m1 και m2.
$C(m, r)$	Δέσμευση του μηνύματος m με τυχαίο αριθμό r.
$h(m)$	Κατακερματισμός του μηνύματος m με συνάρτηση h.
$E_{key}(m)$	Κρυπτογράφηση του μηνύματος m με κλειδί key.
$S_{key}(m)$	Υπογραφή (signature) του μηνύματος m με κλειδί key.
K_u	Δημόσιο κλειδί του χρήστη u.
k_u	Ιδιωτικό κλειδί του χρήστη u.
$hS_{key}(m)$	$h(S_{key}(m))$: Κατακερματισμός της υπογραφής του μηνύματος m με κλειδί key.

Πίνακας 5: Σύμβολα που χρησιμοποιούνται.

4.7.1 Δημιουργία Απόδειξης Τοποθεσίας

Θεωρούμε πως υπάρχουν n witnesses στη γειτονιά του prover.
Οι ταυτότητες των οντοτήτων αναπαρίστανται με τα παρακάτω σύμβολα:

P: Prover
W_i: i-οστό Witness, όπου $1 \leq i \leq n$
CA: Certificate Authority
V: Verifier

Αρχικά ο prover στέλνει μήνυμα Prover Request – PR προς τους γειτονικούς του κόμβους (broadcast):

$$PR = C(P, r_p)|L_0|K_0|t_1|CA$$

όπου
P: η ταυτότητα του prover (π.χ. διεύθυνση email)
r_p: τυχαίος αριθμός που παράγει ο prover για τη δέσμευση $C(P, r_p)$
L_0: η τοποθεσία του prover με τη μέγιστη δυνατή ακρίβεια
K_0: ο τυχαίος αριθμός (seed) για την κατασκευή της αλυσίδας κατακερματισμού
t_1: η τρέχουσα χρονική στιγμή
CA: ταυτότητα της CA (π.χ. hostname)

Κάθε witness ελέγχει πως η L_0 βρίσκεται κοντά του, καθώς και πως η χρονική στιγμή t_1 είναι έγκυρη, δηλαδή εντός ενός διαστήματος από τη στιγμή που έλαβε το μήνυμα. Με βάση την δεδομένη ταυτότητα της CA, το witness επιλέγει ποια ταυτότητά του θα χρησιμοποιήσει. Με την ταυτότητα αυτή θα πρέπει να είναι εγγεγραμμένο στην αντίστοιχη CA.

Κάθε witness δηλώνει την παρουσία του και συνεπώς την πρόθεσή του να συμμετάσχει στην παροχή απόδειξης τοποθεσίας προς τον prover.

Έτσι, κάθε witness W_i στέλνει το μήνυμα Witness Presence – WP_i:

$$WP_i = C(W_i, r_{w_i})|n_\iota$$

όπου
W_i: η ταυτότητα του witness i
r_{wi}: τυχαίος αριθμός που παράγει το witness για τη δέσμευση $C(W_i, r_{wi})$
n_i: τυχαίος αριθμός

Η διαδικασία αυτή δίνει τη δυνατότητα σε κάθε witness να παρατηρεί ποιοι άλλοι κόμβοι συμμετέχουν στη συνεδρία. Αυτό θα χρησιμοποιηθεί από την CA για τον εντοπισμό κακόβουλων witnesses, όπως θα δούμε στη συνέχεια.

Ο prover ξεκινάει την καταγραφή του βίντεο και κατασκευάζει το μήνυμα Start:

$$Start = C(P, r_p)|K_n|t|h(f1)$$

όπου
K_n: το τελευταίο στοιχείο – κεφαλή της αλυσίδας κατακερματισμού τοποθεσίας

t: η τρέχουσα χρονική στιγμή
$h(f_1)$: ο κατακερματισμός του πρώτου frame του βίντεο

Στέλνει στα witnesses το μήνυμα

$$hsStart = Start|hS_{k_p}(Start)$$

Το μήνυμα Start αποτελεί τη δήλωση που καλούνται να επιβεβαιώσουν τα witnesses και διαδραματίζει μείζονα ρόλο.

Κάθε witness ελέγχει κατά πόσον η αναπαράσταση του K_n είναι έγκυρη για το συγκεκριμένο K_0 και L_0 που έλαβε στο μήνυμα PR. Επίσης, αν η χρονική στιγμή t είναι έγκυρη, δηλαδή εντός ενός συγκεκριμένου διαστήματος από τη στιγμή που έλαβε το μήνυμα.

Αν ικανοποιούνται τα παραπάνω, τότε συνεχίζει η εκτέλεση του πρωτοκόλλου.

Το witness αποθηκεύει επίσης τη χρονική στιγμή λήψης του μηνύματος Start, t_{Srec}.

Ακολουθεί ο έλεγχος γειτνίασης ανάμεσα στον prover και σε κάθε witness. Η σειρά με την οποία τα witnesses στέλνουν την πρόκληση (Challenge – C_i) είναι ίδια με τη σειρά που έστειλαν το μήνυμα παρουσίας WP_i.

Κάθε witness i κατασκευάζει το μήνυμα

$$C_i = C\left(W_i, r_{w_i}\right)|n_{1i}|n_{2i}$$

όπου
n_1: τυχαίος αριθμός πρόκλησης με τον οποίο πρέπει να απαντήσει ο prover
n_2: τυχαίος αριθμός τον οποίο θα πρέπει να διαβάσει ο χρήστης

Το witness στέλνει στον prover το μήνυμα

$$hsC_i = C_i|hS_{k_{wi}}(C_i)$$

Ο prover λαμβάνει το μήνυμα και ετοιμάζει την απάντησή του Response – R_i:

$$R_i = C\left(P, r_p\right)|n_{1i}|n_{2i}$$

Στέλνει στο witness i το μήνυμα

$$hsR_i = R_i|hS_{k_p}(R_i)$$

Κάθε witness μετράει τον χρόνο μετ' επιστροφής (Round Trip Time – RTT) μεταξύ C_i και R_i και λαμβάνει μία απόφαση "answer", η οποία αναπαρίσταται με 1 bit (π.χ. 0=accept, 1=decline), ανάλογα με το αν εγκρίνει ή αν απορρίπτει το αίτημα του prover.
Το witness αποθηκεύει επίσης τη χρονική στιγμή λήψης του μηνύματος R, t_{Rrec}.

Όταν ολοκληρωθεί ο έλεγχος εγγύτητας με όλα τα witnesses, ο prover σταματάει την καταγραφή του βίντεο και παράγει τον κατακερματισμό του αρχείου βίντεο, h(V). Κατασκευάζει το μήνυμα Video Hash – VH:

$$VH = C\left(P, r_p\right)|h(V)$$

Στέλνει στα witnesses το μήνυμα

$$hsVH = VH|hS_{k_p}(VH)$$

Το witness αποθηκεύει τη χρονική στιγμή λήψης του μηνύματος VH, t_{VHrec}.

Μετά τη λήψη του μηνύματος αυτού, κάθε witness κατασκευάζει το τεμάχιο απόδειξης τοποθεσίας TAT (Location Proof Segment – LPS):

$$LPS_i = W_i|h(Start)|hsC_i|hsR_i|S_{k_{wi}}(C_i)|r_{w_i}|answer|hsVH|t_{Srec}|t_{Rrec}|t_{VHrec}$$

Και στέλνει στον prover το μήνυμα

$$eLPS_i = C(W_i, r_{w_i})|E_{K_{CA}}(LPS_i)$$

Σε αυτό περιλαμβάνει μεταξύ άλλων την πρόκληση και την απάντηση, τον τυχαίο αριθμό για τη δέσμευση (r_{w_i}) και την υπογραφή του για την πρόκληση $S_{k_{wi}}(C_i)$.

Το μήνυμα αυτό είναι κρυπτογραφημένο με το δημόσιο κλειδί της CA και συνεπώς ο prover δεν μπορεί να το αλλοιώσει. Το witness δεν χρειάζεται να υπογράψει το μήνυμα, καθώς η ταυτότητά του επαληθεύεται από την υπογραφή $S_{k_{wi}}(C_i)$.

Όταν ολοκληρωθεί η αποστολή των LPS από όλα τα witnesses, κάθε ένα από αυτά κατασκευάζει μία λίστα με όλα τα witnesses που έστειλαν μήνυμα παρουσίας WP_i καθώς και LPS, συμπεριλαμβανομένου και του εαυτού του.

Έστω το witness i. Για κάθε witness που έστειλε μήνυμα παρουσίας, το i προσθέτει το αντίστοιχο WP στη λίστα του. Για κάθε witness που έστειλε LPS, το i προσθέτει το αντίστοιχο n_1 στη λίστα του. Σε περίπτωση που κάποιο witness j έστειλε μήνυμα παρουσίας αλλά δεν έστειλε LPS, τότε αποστέλλεται αντίστοιχο n_{1j}=0.

Με αυτή τη διαδικασία η CA θα εντοπίσει witnesses που συνεργάζονται με τον prover για την παραγωγή LPS ή την απόπειρα του prover να αποκρύψει κάποιο LPS που δεν εγκρίνει το αίτημά του. Επίσης, μπορεί να εντοπίσει αν πράγματι κάποιο witness δεν απέστειλε LPS στον prover, σε περίπτωση που υπάρχει μήνυμα παρουσίας αλλά όχι ο αντίστοιχος τυχαίος αριθμός n_{1i}.

Η λίστα που παράγει το witness i είναι η εξής:

$$LIST_i = WP_1|n_{11}|WP_2|n_{12}|\ldots|WP_n|n_{1n}$$

Κάθε witness αποστέλλει στον prover το μήνυμα

$$eLIST_i = C(W_i, r_{w_i})|E_{K_{CA}}(LIST_i|S_{k_{wi}}(LIST_i))$$

Αφού ο prover συλλέξει τα τεμάχια από όλα τα witnesses, θα πρέπει να προσθέσει τα στοιχεία που επιβεβαιώνουν την ταυτότητά του και συγκεκριμένα την υπογραφή του για το μήνυμα S, $S_{k_p}(Start)$, την υπογραφή του για το μήνυμα VH, $S_{k_p}(VH)$, τον τυχαίο αριθμό για τη δέσμευση, r_p, και την υπογραφή του για κάθε απάντηση προς τα witnesses, $S_{k_p}(R_i)$.

Κατασκευάζει το μήνυμα Ισχυρισμού Απόδειξης Τοποθεσίας (Location Proof Assertion – LPA):

$$LPA = P|r_p|Start|S_{k_p}(Start)|S_{k_p}(VH)|eLPS_1|eLIST_1|S_{k_p}(R_1)|\ldots|eLPS_n|eLIST_n|S_{k_p}(R_n)$$

Ο prover αποθηκεύει το μήνυμα αυτό στη μνήμη του και μπορεί να το χρησιμοποιήσει όποτε επιθυμεί ή όποτε του ζητηθεί από τον verifier. Ικανοποιείται δηλαδή η προδιαγραφή της ιδιοκτησίας AT.

4.7.2 Επιβεβαίωση Απόδειξης Τοποθεσίας

Όταν έρθει η στιγμή της επιβεβαίωσης, ο prover στέλνει στην CA το μήνυμα

$$eLPA = C(P, r_p)|E_{K_{CA}}(LPA|S_{k_P}(LPA))$$

Η CA αφού αποκρυπτογραφήσει το μήνυμα πρέπει να πραγματοποιήσει τους παρακάτω ελέγχους:

1. Αποδεσμεύει τη δέσμευση $C(P, r_p)$ όπου αυτή εμφανίζεται με τη χρήση του r_p για να ελέγξει την ταυτότητα του prover.
2. Ελέγχει αν η υπογραφές $S_{k_P}(LPA)$, $S_{k_p}(Start)$, $S_{k_p}(VH)$ αντιστοιχούν στον prover.

Για κάθε LPS:

3. Ελέγχει αν το $h(Start)$ αντιστοιχεί στο μήνυμα Start.
4. Ελέγχει την ταυτότητά του witness αποδεσμεύοντας τη δέσμευση $C(W_i, r_{w_i})$ με τη χρήση του r_{w_i}.
5. Ελέγχει αν η υπογραφή του witness $S_{k_{wi}}(C_i)$ είναι έγκυρη.
6. Ελέγχει αν η υπογραφή του prover $S_{k_p}(R_i)$ είναι έγκυρη.
7. Ελέγχει αν η υπογραφή του prover $S_{k_p}(VH)$ είναι έγκυρη.
8. Ελέγχει αν οι αριθμοί $n_{1i}|n_{2i}$ είναι ίδιοι σε πρόκληση και απάντηση.

Στη συνέχεια, συνολικά:

9. Ελέγχει αν όλες οι λίστες (LIST) έχουν το ίδιο περιεχόμενο και με βάση αυτές κατασκευάζει γράφο που απεικονίζει ποια witness είδαν ποια.
10. Ελέγχει αν οι κατακερματισμένες υπογραφές του prover και witness αντιστοιχούν στις υπογραφές τους.

Αν η υπογραφή του witness ή του prover είναι λάθος, τότε το LPS θεωρείται άκυρο.
Το ίδιο ισχύει αν το h(S) μέσα στο LPS δεν αντιστοιχεί στο S.
Αν οι αριθμοί $n_{1i}|n_{2i}$ δεν είναι ίδιοι σε πρόκληση και απάντηση αλλά το witness έχει απαντήσει θετικά, τότε σημαίνει πως δεν έχει εκτελέσει σωστά το πρωτόκολλο ή είναι κακόβουλο.

Ανεξάρτητα από το αν είναι έγκυρα τα LPS, η CA κατασκευάζει το Αποτύπωμα Συνεδρίας (Session Fingerprint – SF). Αυτό πρόκειται για τον κατακερματισμό της συνένωσης όλων των μηνυμάτων που θα πρέπει να περιλαμβάνονται στο βίντεο, και συγκεκριμένα

$$SF = h(S|C_1|R_1| \dots |C_n|R_n)$$

Με αυτό το μήνυμα η CA συνοψίζει τη συνεδρία την οποία έλεγξε.
Επίσης, η CA υπολογίζει τις μέσες χρονικές στιγμές των μηνυμάτων Start, R και VH, σύμφωνα με τις μετρήσεις που έχουν συμπεριλάβει στα LPS τα witnesses.

Στη συνέχεια η CA εφαρμόζει το σχήμα εμπιστοσύνης της στα έγκυρα LPS. Κατασκευάζει το Τεμάχιο Επιβεβαιωτή (Verifier Segment – VS):

$$VS = (CA|Start|P|h(V)|SF|score_1|ans_1| \dots |score_m|ans_m|t_{Smean}|t_{Rmean}|t_{VHmean})$$

όπου
m: τα συνολικά έγκυρα LPS, με m≤n
$score_i$: η βαθμολογία του LPS i με βάση το σχήμα εμπιστοσύνης
ans_i: η αντίστοιχη απάντηση (π.χ. 0=accept, 1=decline)
t_{Smean}, t_{Rmean}, t_{VHmean}: οι μέσες χρονικές στιγμές

Κρυπτογραφεί και υπογράφει το μήνυμα αυτό με το ιδιωτικό του κλειδί, στέλνοντας στον prover το

$$eVS = CA|E_{k_{CA}}(VS)|S_{k_{CA}}(VS)$$

Ο prover αποθηκεύει το μήνυμα αυτό και μπορεί κατά βούληση να συνεχίσει την επιβεβαίωση με τον verifier. Επίσης, είναι απαραίτητο να αποθηκεύσει την αλυσίδα κατακερματισμού τοποθεσίας, την τοποθεσία με τη μεγαλύτερη δυνατή ακρίβεια, καθώς και τη δέσμευση που χρησιμοποίησε. Αυτά τα στοιχεία είναι απαραίτητα προκειμένου να κατασκευάσει την απόδειξη τοποθεσίας (Location Proof – LP).

Κατασκευάζει το μήνυμα

$$LP = P|Start|eVS|K_i|L_i|V$$

Σε αυτό περιλαμβάνεται το eVS που παρέλαβε από την CA και επιπλέον το μήνυμα Start, το βίντεο V καθώς και τα στοιχεία που απαιτούνται για την επιβεβαίωση της τοποθεσίας, δηλαδή το επιλεγμένο επίπεδο ακρίβειας τοποθεσίας L_i καθώς και τον αντίστοιχο αριθμό K_i.

Αποστέλλει στον verifier το μήνυμα

$$eLP = E_{K_V}\big(LP|S_{k_P}(LP)\big)$$

Ως προς τα λαμβανόμενα μηνύματα, ο verifier εκτελεί τους παρακάτω ελέγχους:

1. Ελέγχει την υπογραφή $S_{k_P}(LP)$.
2. Ελέγχει την υπογραφή $S_{k_{CA}}(VS)$.
3. Ελέγχει πως το hash του πρώτου frame του βίντεο που έλαβε ταυτίζεται με το h(f1) που περιέχεται στο μήνυμα Start. Επίσης πως το h(V) αντιστοιχεί πράγματι στο βίντεο V που έστειλε ο prover.
4. Το Start και η ταυτοτητα P που περιέχεται στο μήνυμα VS είναι ίδια με αυτά που περιλαμβάνει ο prover στο LP.
5. Με διαδοχικούς κατακερματισμούς μπορεί από τα K_i, L_i να φτάσει στο K_n που περιέχεται στο μήνυμα S.

Ως προς την ανάλυση του βίντεο ο verifier πρέπει να ελέγξει τα παρακάτω:

1. Αναγνώριση του προσώπου του χρήστη στο βίντεο.
2. Έλεγχος πως ο χρήστης διαβάζει την αλληλουχία αριθμών n_{2i}.

3. Έλεγχος πως η συνεδρία που περιέχεται στο βίντεο είναι αυτή που έλεγξε η CA.

Τα δύο πρώτα στάδια αφορούν την αναγνώριση προσώπου και φωνής, ζητήματα που δεν μας απασχολούν στην παρούσα εργασία.

Για το τρίτο στάδιο, ο verifier έχει τη δυνατότητα να ελέγξει τη συνεδρία που πραγματοποίησε ο prover. Αφού διαθέτει τα σήματα από το βίντεο, μπορεί να εκτελέσει ό,τι έλεγχο επιθυμεί, χωρίς να εκτίθεται η ταυτότητα των witnesses. Μπορεί για παράδειγμα να επιβεβαιώσει πως οι τιμές των n_{1i}, n_{2i} είναι σωστές, ή πως τα διαστήματα μεταξύ προκλήσεων και απαντήσεων είναι αποδεκτά. Επίσης, μπορεί να υπολογίσει τα μέσα χρονικά διαστήματα μεταξύ των μηνυμάτων Start, R, VH, σύμφωνα με τις μετρήσεις των witnesses και να τις συγκρίνει με αυτές που μετράει στο βίντεο.

Ωστόσο, ένας απλός έλεγχος είναι να υπολογίσει το αποτύπωμα συνεδρίας από το βίντεο, SF_{vid} και να το συγκρίνει με το SF που έλαβε από την CA.

Το πρωτόκολλο σε αυτό το σημείο ολοκληρώνεται. Ο verifier με βάση τις απόψεις και την αξιοπιστία των witnesses που περιλαμβάνονται στο VS, επιλέγει αν θα δεχτεί ή όχι τον ισχυρισμό του prover.

Σημειώνεται πως το πρωτόκολλο μπορεί να λειτουργήσει και χωρίς ισχυρές ταυτότητες. Σε αυτή την περίπτωση, ο prover δεν καταγράφει βίντεο και δεν υπάρχουν τα σχετικά με το βίντεο μηνύματα.

Επίσης, ο verifier έχει τη δυνατότητα να ενημερώνει την CA σχετικά με τα witnesses τα οποία θεωρεί έμπιστα. Αν η CA βρει LPS που προέρχεται από έμπιστο witness ως προς τον verifier στο μήνυμα LPA που λαμβάνει από τον prover, μπορεί να συμπεριλάβει την ταυτότητά του στο μήνυμα VS.

4.8 Ανάλυση χαρακτηριστικών και προδιαγραφών

Στο σημείο αυτό θα περιγράψουμε τα χαρακτηριστικά του προτεινόμενου πρωτοκόλλου, καθώς και το κατά πόσον ανταποκρίνεται στις προδιαγραφές που έχουμε θέσει.

4.8.1 Χαρακτηριστικά

1. Αρχιτεκτονική σταδίου A - Δημιουργία AT
Υβριδική: Οι μάρτυρες (witnesses) μπορεί να είναι άλλοι χρήστες ή έμπιστοι κόμβοι από την CA και/ή τον verifier.

2. Αρχιτεκτονική σταδίου B - Επαλήθευση AT
Έμμεση: Στη διαδικασία επαλήθευσης εμπλέκεται η CA, προκειμένου να επιβεβαιώσει τις ταυτότητες και τις υπογραφές των χρηστών.

3. Χρήση Τρίτης Έμπιστης Οντότητας/Αρχής Πιστοποίησης (TTP/CA)
Ναι: Χρησιμοποιείται Αρχή Πιστοποίησης, η οποία είναι υπεύθυνη για τη διαχείριση των χρηστών, τον έλεγχο της ταυτότητας και της υπογραφής τους, καθώς και για τον εντοπισμό συνεργαζόμενων χρηστών. Η CA εφαρμόζει ένα σχήμα εμπιστοσύνης με βάση το οποίο αξιολογεί τους χρήστες που συμμετέχουν στο σύστημα.

4. Φυσικό στρώμα
Υπέρηχοι: Η συνεδρία μεταξύ prover και witnesses πραγματοποιείται μέσω υπερήχων.

5. Κωδικοποίηση τοποθεσίας (geocoding)
Plus codes: Το προτεινόμενο πρωτόκολλο χρησιμοποιεί το σύστημα κωδικοποίησης τοποθεσίας plus codes (πρώην open location code).

6. Εύρεση τοποθεσίας
Όχι: Η τοποθεσία παρέχεται στις συσκευές των χρηστών από το λειτουργικό σύστημα. Το πρωτόκολλο επιβεβαιώνει την τοποθεσία με βάση τους γειτονικούς κόμβους.

7. Έλεγχος εγγύτητας-γειτνίασης
Ναι (timeout-based): Το πρωτόκολλο βασίζεται στην μέτρηση του χρόνου μετ' επιστροφής (Round Trip Time – RTT) μεταξύ μίας πρόκλησης και μίας απάντησης. Τα μηνύματα αυτά στέλνονται μέσω υπερήχων.

8. Κίνητρο συμμετοχής
Ναι: Θεωρούμε πως οι διάφορες CAs μπορούν να παρέχουν τις υπηρεσίες τους στους verifiers με κάποιο κόστος. Αυτό τους δίνει κίνητρο να εκτελούν τις διαδικασίες ελέγχου (υπογραφών, ταυτοτήτων, σχήμα εμπιστοσύνης) αλλά και να διευρύνουν το δίκτυο έμπιστων κόμβων που διαθέτουν.

9. Μεταβαλλόμενη ακρίβεια τοποθεσίας
Ναι: Με τη χρήση hash chains παρέχεται η δυνατότητα στον prover να ορίσει εκείνος την ακρίβεια με την οποία θα γνωστοποιήσει την τοποθεσία του στον verifier.

10. Ανεξαρτησία από verifier (verifier-agnostic)
Ναι: Η AT που παράγεται κατά τη διάρκεια μία συνεδρίας μπορεί να χρησιμοποιηθεί από οποιονδήποτε verifier επιλέξει ο χρήστης.

11. Αλυσίδες Αποδείξεων Τοποθεσίας
Όχι: Το πρωτόκολλο που προτείνεται δεν υποστηρίζει αλυσίδες ΑΤ (provenance chains). Κάθε ΑΤ που εκδίδεται είναι αυτόνομη και δεν συσχετίζεται με άλλες.

4.8.2 Προδιαγραφές ασφαλείας

1. Ακεραιότητα δεδομένων (data integrity-unforgeability)
Ναι: Τα μηνύματα προστατεύονται με υπογραφές ή/και κρυπτογραφία. Συνεπώς, είναι αδύνατον να τροποποιηθούν χωρίς αυτό να είναι εμφανές.

2. Αδυναμία Απόκρυψης/Προσθήκης ΤΑΤ
Ναι: Η CA μπορεί να επιβεβαιώσει πόσοι witnesses ήταν παρόντες κατά τη διάρκεια της συνεδρίας, καθώς και πόσοι από αυτούς απέστειλαν ΤΑΤ (LPS) στον prover. Συνεπώς, αν ο prover προσθέσει ή αφαιρέσει ΤΑΤ από το LPA που στέλνει στην CA, αυτή θα το εντοπίσει.

3. Μη μεταβιβάσιμη πληροφορία (non-transferability)
Ναι: Κατά τη διάρκεια της δημιουργίας ΑΤ αλλά και κατά την επιβεβαίωση, ο prover υπογράφει τα μηνύματα που στέλνει στους υπόλοιπους κόμβους. Η ΑΤ που στέλνεται προς επιβεβαίωση στον verifier περιέχει την ταυτότητα του χρήστη, η οποία έχει ελεγχθεί από την CA. Συνεπώς, δεν μπορεί κάποιος άλλος χρήστης να παρουσιάσει μία ΑΤ ως δική του, χωρίς να έχει συμμετάσχει ο ίδιος στη διαδικασία απόκτησης και επιβεβαίωσής της.

4. Αντοχή στην απάτη απόστασης (distance fraud)
Ναι: Το πρωτόκολλο ελέγχει τη γειτνίαση witness-prover με μηνύματα πρόκλησης-απάντησης μέσω υπερήχων. Κάθε witness μετρά τον χρόνο μετ' επιστροφής μεταξύ της πρόκλησης και της απάντησης, και βγάζει ανάλογο συμπέρασμα. Η χρήση υπερήχων ενισχύει την αντοχή στην απάτη απόστασης, καθώς προκειμένου να μεταδοθεί το μήνυμα σε μεγάλες αποστάσεις απαιτείται η μετατροπή του σε άλλο είδος σήματος (π.χ. ηλεκτρομαγνητικό). Το γεγονός αυτό εισάγει επιπλέον καθυστέρηση, με αποτέλεσμα οι κακόβουλοι χρήστες να εντοπίζονται εύκολα από τα witnesses.

5. Αντοχή στην επίθεση ενδιάμεσου (mafia fraud)
Ναι: Η χρήση τυχαίων αριθμών στις προκλήσεις των witnesses εξασφαλίζει τη μοναδικότητα της συνεδρίας. Όπως είδαμε στην αντίστοιχη ενότητα, είναι αδύνατον για έναν ενδιάμεσο να αναπαράγει τη συνεδρία και να αποκτήσει έγκυρα ΤΑΤ από τα witnesses, είτε διαθέτει τα κλειδιά του prover είτε όχι (απλή αναμετάδοση μηνυμάτων).

6. Αντοχή στην υποκλοπή απόστασης (distance hijacking)
Ναι: Τα ΤΑΤ που παράγονται από τα witnesses και αποστέλλονται στον prover είναι συσχετισμένα με με μία ανταλλαγή μηνυμάτων πρόκλησης-απάντησης. Το γεγονός αυτό σε συνδυασμό με τον έλεγχο ταυτοτήτων και υπογραφών που εκτελεί η CA έχει ως αποτέλεσμα να μην μπορεί ένας χρήστης να χρησιμοποιήσει κάποιο ΤΑΤ, χωρίς να το έχει «κερδίσει» ο ίδιος, εκτελώντας τον έλεγχο εγγύτητας.

7. Αντοχή στη συνεργασία P-P
Ναι: Με την ικανοποίηση των παραπάνω προδιαγραφών προκύπτει πως το προτεινόμενο πρωτόκολλο εμποδίζει δύο χρήστες να συνεργαστούν ώστε ο ένας να παράγει AT για λογαριασμό του άλλου. Ακόμα και αν ο χρήστης P' διαθέτει τα κλειδιά του χρήστη P, η απαίτηση για ισχυρές ταυτότητες αποκαλύπτει τη συνεργασία.

8. Αντοχή στη συνεργασία P-W
Ναι: Ο prover δεν γνωρίζει την πραγματική ταυτότητα του κάθε witness με το οποίο επικοινωνεί, καθώς αυτή εμφανίζεται με τη μορφή δέσμευσης. Επίσης, οι υπογραφές των witnesses είναι κατακερματισμένες. Επιπλέον, κάθε witness στέλνει TAT, ανεξάρτητα από το αν εγκρίνει ή απορρίπτει τον ισχυρισμό του prover, ο οποίος δεν έχει τη δυνατότητα να δει την απάντηση του witness, καθώς το μήνυμα είναι κρυπτογραφημένο.

9. Αντοχή στη συνεργασία W-W
Ναι: Παρόμοια, τα witnesses δεν μαθαίνουν το ένα την ταυτότητα του άλλου ούτε είναι σε θέση να γνωρίζουν την απάντηση που έδωσε το κάθε ένα από αυτά.

10. Μοναδικότητα TAT
Ναι: Η CA ελέγχει πως ο Ισχυρισμός Απόδειξης Τοποθεσίας (LPA) που λαμβάνει από τον prover περιέχει μόνο και μόνο ένα TAT από κάθε witness.

11. Όχι μοναδικό σημείο αποτυχίας (single point of failure)
Όχι: Η CA μπορεί να αποτελέσει μοναδικό σημείο αποτυχίας, σε περίπτωση που δυσλειτουργεί. Ωστόσο, όλοι οι χρήστες του συστήματος (provers, witnesses, verifiers) μπορεί να είναι εγγεγραμμένοι σε περισσότερες από μία CAs. Εκτός αυτού, ο prover μπορεί να κρατήσει το μήνυμα LPA μέχρι η CA να λειτουργήσει ξανά.

4.8.3 Προδιαγραφές Ιδιωτικότητας

1. Προστασία ταυτότητας κατά το στάδιο A: Δημιουργία AT
Ναι: Οι ταυτότητες των χρηστών που συμμετέχουν σε μία συνεδρία δημιουργίας AT είναι κρυμμένες με δεσμεύσεις, ενώ οι υπογραφές τους είναι κατακερματισμένες. Συνεπώς, κανείς δεν μπορεί να συμπεράνει την ταυτότητα τους.

2. Προστασία ταυτότητας κατά το στάδιο B: Επιβεβαίωση AT
Ναι: Ο verifier μαθαίνει την ταυτότητα του prover στον οποίο αναφέρεται η εν λόγω AT. Δεν μαθαίνει την ταυτότητα των witnesses, αλλά μόνο την απόφασή τους και το πόσο έμπιστα είναι για την CA. Σε περίπτωση που ο verifier έχει επιστρατεύσει ένα έμπιστο witness, τότε μπορεί να δει την ταυτότητά του χωρίς να υφίσταται παραβίαση ιδιωτικότητας.

Τα παραπάνω δύο αναλύονται και με την έννοια της αδυναμίας συσχετισμού.
Η αδυναμία συσχετισμού επιτυγχάνεται με τις διαφορετικές δεσμεύσεις που χρησιμοποιούν οι συμμετέχοντες σε κάθε συνεδρία, καθώς και με την κρυπτογραφία όπου αυτή είναι απαραίτητη. Συγκεκριμένα, έχουμε για τις εξής περιπτώσεις:

Αδυναμία συσχετισμού prover (στάδιο A)
Ναι: Σε κάθε αίτηση ο prover χρησιμοποιεί διαφορετικό τυχαίο αριθμό για την παραγωγή της κρυπτογραφικής δέσμευσης. Επίσης, η υπογραφή του εμφανίζεται κατακερματισμένη.

Τα παραπάνω εμποδίζουν τα witnesses ή κάποιον που «κρυφακούει» (eavesdropper) από το να καταλάβουν ότι δύο αιτήσεις προέρχονται από τον ίδιο χρήστη.

Αδυναμία συσχετισμού witness (στάδιο Α)
Ναι: Παρόμοια, η χρήση κρυπτογραφικών δεσμεύσεων με διαφορετικούς τυχαίους αριθμούς κάθε φορά καθώς και ο κατακερματισμός της υπογραφής καθιστούν ασυσχέτιστες δύο διαφορετικές συμμετοχές ενός witness σε διαφορετικές συνεδρίες. Ακόμα και αν το witness στείλει δύο TAT (LPS) μέσα στην ίδια συνεδρία (πράγμα λάθος), οι χρήστες δεν μπορούν να τα συσχετίσουν καθώς αυτά είναι κρυπτογραφημένα με το δημόσιο κλειδί της CA.

Αδυναμία συσχετισμού prover (στάδιο Β)
Ναι: Μόνο ο verifier και η CA μαθαίνουν την πραγματική ταυτότητα του prover και συνεπώς μπορούν να γνωρίζουν ότι δύο AT ανήκουν στον ίδιο.

Αδυναμία συσχετισμού witness (στάδιο Β)
Ναι: Ο μόνος φορέας που γνωρίζει αν δύο LPS προήλθαν από το ίδιο witness είναι η CA, καθώς τα LPS είναι κρυπτογραφημένα με το δημόσιο κλειδί της. Ο λόγος που η CA μαθαίνει τις ταυτότητες των witnesses είναι για να εφαρμόσει έλεγχο των υπογραφών τους και να τα αξιολογήσει με βάση το σχήμα εμπιστοσύνης που χρησιμοποιεί.

3. Ιδιωτικότητα τοποθεσίας witness
Ναι: Τα witnesses δεν αποκαλύπτουν ποτέ την τοποθεσία τους. Ελέγχουν μόνο αν η τοποθεσία που δηλώνει ο prover βρίσκεται σε μία εφικτή απόσταση για το φυσικό στρώμα επικοινωνίας που χρησιμοποιείται (στην περίπτωσή μας υπέρηχοι).

4. Ιδιωτικότητα τοποθεσίας prover
Ναι: Μόνο τα witnesses μαθαίνουν την ακριβή τοποθεσία του prover, προκειμένου να την ελέγξουν. Με τη χρήση της αλυσίδας κατακερματισμού τοποθεσίας, ο verifier μαθαίνει την τοποθεσία του prover με την ακρίβεια που αυτός επιθυμεί.

5. Ιδιοκτησία AT
Ναι: Αφού ο prover λάβει όλα τα μηνύματα από τα witnesses, κατασκευάζει το LPA και το αποθηκεύει στη μνήμη του. Όταν κληθεί ή επιλέξει να επιβεβαιώσει την τοποθεσία του στον verifier, εκκινεί τη διαδικασία επικοινωνίας με την CA. Δεν υποχρεώνεται να εκθέσει στοιχεία σε άλλους φορείς πριν ξεκινήσει η διαδικασία επιβεβαίωσης.

5 Υλοποίηση του προτεινόμενου πρωτοκόλλου

Το προτεινόμενο πρωτόκολλο υλοποιήθηκε ως εφαρμογή για συσκευές με λειτουργικό σύστημα Android. Χρησιμοποιήθηκε η γλώσσα προγραμματισμού Java και το Ολοκληρωμένο Περιβάλλον Ανάπτυξης (Integrated Development Environment) Android Studio.

Δόθηκε έμφαση στην μορφή και την ανταλλαγή των μηνυμάτων μέσω υπερήχων, καθώς και στις απαιτούμενες κρυπτογραφικές διαδικασίες. Η καταγραφή βίντεο δεν υλοποιήθηκε.

Ο κώδικας της εφαρμογής είναι διαθέσιμος στην ιστοσελίδα: https://github.com/jimcoun/QuietPlace.

Όλα τα αρχεία κώδικα που παράχθηκαν βρίσκονται στη διαδρομή: /app/src/main/java/com/example/user/test.

5.1 Ζητήματα υλοποίησης

5.1.1 Επικοινωνία μεταξύ prover – witness

Η επικοινωνία μεταξύ prover και witness γίνεται μέσω υπερήχων, κάνοντας χρήση της βιβλιοθήκης Quiet for Android [80].

Το Quiet for Android ανήκει σε μία οικογένεια υλοποιήσεων της βιβλιοθήκης Quiet [87] και βασίζεται στον ανοιχτού κώδικα επεξεργαστή σημάτων liquid-dsp [88].

Ως προς τα μηνύματα που ανταλλάσσονται, το Quiet μπορεί να χρησιμοποιηθεί με δύο τρόπους, είτε σε λειτουργία στρώματος πλαισίων (frame layer mode), είτε σε λειτουργία UDP/TCP. Στην πρώτη περίπτωση γίνεται απλή αποστολή μηνυμάτων στο κοινό μέσο (αέρας), ενώ στη δεύτερη υλοποιείται πλήρης στοίβα TCP/IP, παρέχοντας στους κόμβους διευθύνσεις IP. Στην περίπτωση που χρησιμοποιείται TCP, παρέχονται τα χαρακτηριστικά του πρωτοκόλλου, όπως επιβεβαιώσεις και αναμεταδόσεις. Στο πλαίσιο της εργασίας χρησιμοποιήθηκε η λειτουργία πλαισίων καθώς μας ενδιαφέρει η μετάδοση απλών μηνυμάτων.

Ως προς το φυσικό στρώμα, το Quiet υποστηρίζει διάφορα προφίλ ήχου. Οι ρυθμίσεις για το κάθε προφίλ ορίζονται στο αρχείο “quiet-profiles.json”, το οποίο βρίσκεται στη διαδρομή quiet/src/main/res/raw/. Επιπλέον, δίνεται η δυνατότητα δοκιμής και παραγωγής νέων προφίλ, μέσω της ιστοσελίδας “Quiet Profile Lab” [89]. Στο πλαίσιο της εργασίας χρησιμοποιήθηκε το προφίλ “ultrasound-experimental”. Προτιμήθηκε έναντι των υπόλοιπων “ultrasound” καθώς παρατηρήθηκε μεγαλύτερη εμβέλεια και μικρότερη κατευθυντικότητα σε σχέση με τα υπόλοιπα προφίλ, όπως παρουσιάζεται στο επόμενο κεφάλαιο. Η μοναδική αλλαγή που έγινε ήταν η αύξηση του μέγιστου μήκους των πλαισίων στα 2000 bytes, προκειμένου να μπορούν να υποστηριχθούν τα μηνύματα του πρωτοκόλλου. Η αλλαγή αυτή έγινε με την τροποποίηση της γραμμής "frame_length": 2000 στο αρχείο “quiet-profiles.json”.

5.1.2 Μορφή μηνυμάτων

Τόσο τα μηνύματα που ανταλλάσσονται μεταξύ prover και witness, όσο και αυτά που ανταλλάσσει ο prover με την CA και τον verifier είναι στη μορφή JSON [90]. Τα μηνύματα κατασκευάζονται ως αντικείμενα Java και μετατρέπονται σε μορφή JSON προκειμένου να αποσταλούν. Αντίστροφα, τα μηνύματα λαμβάνονται σε μορφή JSON και μετατρέπονται σε αντικείμενα Java, προκειμένου να μπορεί να χρησιμοποιηθεί το κάθε πεδίο τους. Για την μετατροπή των μηνυμάτων από και προς τη μορφή JSON χρησιμοποιήθηκε η βιβλιοθήκη Jackson [91], έκδοση 2.9.8 και συγκεκριμένα τα τρία .jar αρχεία:

- jackson-core

(http://central.maven.org/maven2/com/fasterxml/jackson/core/jackson-core/2.9.8/jackson-core-2.9.8.jar)
- jackson-databind
(http://central.maven.org/maven2/com/fasterxml/jackson/core/jackson-databind/2.9.8/jackson-databind-2.9.8.jar)
- jackson-annotations
(http://central.maven.org/maven2/com/fasterxml/jackson/core/jackson-annotations/2.9.8/jackson-annotations-2.9.8.jar)

Η σχετική κλάση που παρέχει τη διασύνδεση της εφαρμογής με τη βιβλιοθήκη Jackson ονομάζεται ParseJSON και διαθέτει τις εξής δύο μεθόδους:

- String toJSON(Object object)
Μετατρέπει ένα αντικείμενο object σε κείμενο μορφής JSON.
- Object fromJSON(String jsonString, Class classType)
Μετατρέπει το κείμενο jsonString, το οποίο είναι σε μορφή JSON, σε ένα αντικείμενο της κλάσης classType.

5.1.3 Κωδικοποίηση τοποθεσίας

Για την κωδικοποίηση της τοποθεσίας χρησιμοποιήθηκε η έκδοση Java της βιβλιοθήκης Open Location Code (Plus Codes) που βρίσκεται στην ιστοσελίδα [92]. Το αρχείο OpenLocationCode.java(https://github.com/google/open-location-code/blob/master/java/src/main/java/com/google/openlocationcode/OpenLocationCode.java) μετατράπηκε σε αρχείο .jar και εισήχθη στο Android Studio.

Από τη βιβλιοθήκη αυτή χρησιμοποιήθηκε μόνο η μέθοδος που επιστρέφει πλήρη κωδικό plus code 10 χαρακτήρων (περιοχή 14x14 μέτρα), δοθέντος ενός ζεύγους συντεταγμένων.

Το απόσπασμα κώδικα που χρησιμοποιήθηκε είναι το εξής:

```
OpenLocationCode code = new OpenLocationCode(latitude, longitude);
String plusCode = code.getCode();
```

Όπου latitude, longitude το ζεύγος συντεταγμένων και plusCode ο κωδικός που επιστρέφεται.

5.1.4 Κωδικοποίηση δυαδικών σε κείμενο

Σε αρκετά σημεία είναι απαραίτητη η κωδικοποίηση δυαδικών ακολουθιών σε κείμενο, προκειμένου να είναι δυνατή η αποστολή τους μεταξύ των κόμβων. Δυαδικές ακολουθίες αποτελούν τα κρυπτογραφικά κλειδιά, τα κρυπτογραφημένα μηνύματα, οι κατακερματισμοί και οι υπογραφές.

Χρησιμοποιήθηκε κωδικοποίηση Base64 [93] από την κλάση android.util.Base64, η οποία περιέχεται στο Android.

Συγκεκριμένα, έγινε χρήση των παρακάτω δύο μεθόδων:

- String encodeToString(byte[] data, Base64.DEFAULT)
Κωδικοποιεί τη δυαδική ακολουθία “data” σε κείμενο Base64.
- byte[] decode(String data, Base64.DEFAULT)
Αποκωδικοποιεί το κωδικοποιημένο σε Base64 κείμενο “data” σε δυαδική ακολουθία.

5.1.5 Βιβλιοθήκη Crypto (Κρυπτογραφία, κατακερματισμοί, τυχαίοι αριθμοί)

Για την υποστήριξη των απαραίτητων διαδικασιών κρυπτογράφησης κατασκευάστηκε η κλάση Crypto.java, η οποία έχει όλες τις απαραίτητες μεθόδους. Οι διαδικασίες που απαιτεί το πρωτόκολλο υλοποιούνται ως εξής:

5.1.5.1 Κατακερματισμός (hashing)

Για τον κατακερματισμό χρησιμοποιήθηκε ο αλγόριθμος SHA-256 [94] και συγκεκριμένα η υλοποίησή του στην κλάση java.security.MessageDigest. Η σχετική μέθοδος είναι:

- String sha256Base64(String data)
  Επιστρέφει τον κατακερματισμό του κειμένου "data" σε κωδικοποίηση Base64.

5.1.5.2 Τυχαίος αριθμός

Για την παραγωγή τυχαίων αριθμών χρησιμοποιείται η μέθοδος:

- String random256Base64()
  Παράγει έναν τυχαίο αριθμό των 256 bit και τον επιστρέφει σε κωδικοποίηση Base64.

5.1.5.3 Δεσμεύσεις (Commitments)

Στην υλοποίηση χρησιμοποιήθηκε το απλό σχήμα δέσμευσης που περιγράφεται στην ενότητα 4.5.2. Το πρωτόκολλο υποστηρίζει οποιοδήποτε σχήμα δέσμευσης.

Για την υποστήριξη κρυπτογραφικών δεσμεύσεων παρέχονται οι παρακάτω δύο μέθοδοι:

- String commit(String message, String random)
  Επιστρέφει τη δέσμευση του μηνύματος "message" με τυχαίο αριθμό "random".
- boolean deCommit(String commitment, String message, String random)
  Επιστρέφει το δυαδικό αποτέλεσμα (true ή false) του ελέγχου της δέσμευσης "commitment" του μηνύματος "message" με τυχαίο αριθμό "random". Υποδεικνύει δηλαδή αν η δεδομένη δέσμευση αντιστοιχεί στο συνδυασμό του μηνύματος και του τυχαίου αριθμού.

Σημείωση: Οι παραπάνω τυχαίοι αριθμοί "random" είναι της μορφής String, καθώς αναπαρίστανται με κωδικοποίηση Base64.

5.1.5.4 Ασύμμετρη κρυπτογραφία

Για τις ανάγκες ασύμμετρης κρυπτογραφίας χρησιμοποιείται το σύστημα RSA [95], [96] με μέγεθος κλειδιού 1024 bits. Για την παραγωγή του ζεύγους ιδιωτικού-δημόσιου κλειδιού η υλοποίηση στηρίζεται στην κλάση java.security.KeyPairGenerator, ενώ για την κρυπτογράφηση και αποκρυπτογράφηση στην κλάση javax.crypto.Cipher.

Οι μέθοδοι που εξυπηρετούν τις ανάγκες ασύμμετρης κρυπτογραφίας είναι:

- void keyPairGenerator(String fileName)
  Παράγει ζεύγος ιδιωτικού-δημόσιου κλειδιού, κωδικοποιεί τα κλειδιά σε Base64, τα εμφανίζει στην κονσόλα και τα αποθηκεύει σε αρχείο με όνομα "fileName".
- PrivateKey getPrivateFromString(String pvt)
  Διαβάζει το ιδιωτικό κλειδί "pvt" σε κωδικοποίηση Base64 και το επιστρέφει ως αντικείμενο PrivateKey.

- PublicKey getPublicFromString(String pub)
  Διαβάζει το δημόσιο κλειδί "pub" σε κωδικοποίηση Base64 και το επιστρέφει ως αντικείμενο PublicKey.
- String encryptText(String msg, Key key)
  Κρυπτογραφεί το μήνυμα "msg" με χρήση του κλειδιού "key" και επιστρέφει το αποτέλεσμα κωδικοποιημένο σε Base64.
- String decryptText(String msg, Key key)
  Αποκρυπτογραφεί το κωδικοποιημένο σε Base64 κρυπτογραφημένο μήνυμα "msg" με χρήση του κλειδιού "key" και επιστρέφει το αποτέλεσμα.

5.1.5.5 Συμμετρική κρυπτογραφία

Για τη συμμετρική κρυπτογράφηση μηνυμάτων χρησιμοποιήθηκε ο αλγόριθμος AES [97], [98] και συγκεκριμένα η υλοποίησή του στην κλάση javax.crypto.Cipher.

Οι σχετικές μέθοδοι που αναπτύχθηκαν είναι οι εξής:

- SecretKey getKey()
  Δημιουργεί και επιστρέφει συμμετρικό κλειδί.
- IvParameterSpec getIvSpec()
  Δημιουργεί και επιστρέφει διάνυσμα αρχικοποίησης (initialization vector) [99], απαραίτητο για την κρυπτογράφηση/αποκρυπτογράφηση του μηνύματος.
- String symmetricEncrypt(String data, SecretKey key, IvParameterSpec ivSpec)
  Κρυπτογραφεί το μήνυμα "data" με χρήση του συμμετρικού κλειδιού "key" και του διανύσματος αρχικοποίησης "ivSpec" και επιστρέφει το αποτέλεσμα κωδικοποιημένο σε Base64.
- String symmetricDecrypt(String data, SecretKey key, IvParameterSpec ivSpec)
  Αποκρυπτογραφεί το κωδικοποιημένο σε Base64 κρυπτογραφημένο μήνυμα "data" με χρήση του συμμετρικού κλειδιού "key" και του διανύσματος αρχικοποίησης "ivSpec" και επιστρέφει το αποτέλεσμα.

5.1.5.6 Ψηφιακές υπογραφές

Για την παραγωγή και επιβεβαίωση υπογραφών χρησιμοποιείται ο αλγόριθμος SHA-256 with RSA, που υλοποιείται στην κλάση java.security.Signature.

Οι λειτουργίες που κατασκευάστηκαν αφορούν τη δημιουργία και επιβεβαίωση μίας υπογραφής και υλοποιούνται με τις παρακάτω μεθόδους:

- String signBase64(String message, PrivateKey privateKey)
  Παράγει την υπογραφή του μηνύματος "message" με χρήση του ιδιωτικού κλειδιού "privateKey" και επιστρέφει το αποτέλεσμα κωδικοποιημένο σε Base64.
- boolean signVerifyBase64(String message, String signature, PublicKey publicKey)
  Ελέγχει την εγκυρότητα της κωδικοποιημένης σε Base64 υπογραφής "signature"ως προς το μήνυμα "message" με χρήση του δημοσίου κλειδιού "publicKey" και επιστρέφει το δυαδικό αποτέλεσμα (true ή false). Υποδεικνύει δηλαδή αν η υπογραφή ανήκει στον ιδιοκτήτη του δημόσιου κλειδιού και αντιστοιχεί στο συγκεκριμένο μήνυμα.

5.1.6 Αλυσίδα τοποθεσίας

Στην υλοποίηση για ευκολία χρησιμοποιήθηκαν οι απλές αλυσίδες τοποθεσίας που περιγράφηκαν στην προηγούμενη ενότητα. Ωστόσο, η κρυπτογραφική βιβλιοθήκη Crypto.java

δίνει τη δυνατότητα κατασκευής διαφορετικών εκδόσεων αλυσίδων τοποθεσίας με χρήση δεσμεύσεων ή συμμετρικής κρυπτογραφίας.

Οι απαραίτητες λειτουργίες υλοποιούνται από τις παρακάτω μεθόδους:

- String random()
  Παράγει και επιστρέφει τον τυχαίο αριθμό κατάλληλα κωδικοποιημένο σε Base64, με βάση τη βιβλιοθήκη Crypto.
- String[] buildChain(String K0, String L0)
  Με εισόδους τον τυχαίο αριθμό K_0 και την τοποθεσία L_0 σε μέγιστη ακρίβεια κωδικοποιημένη σε Plus Code υπολογίζει και επιστρέφει τα μέλη K_i ($0 \leq i \leq 5$) της αλυσίδας τοποθεσίας.
- boolean checkChain(String Ki, String Li, String K)
  Ελέγχει το κατά πόσον η κεφαλή της αλυσίδας τοποθεσίας K αντιστοιχεί στο μέλος της αλυσίδας K_i και την τοποθεσία L_i εκφρασμένη σε Plus Code, όπου i το επίπεδο ακρίβειας τοποθεσίας. Επιστρέφει το αποτέλεσμα (true ή false).
- String shortenPlusCode(String plusCode, int level)
  Υπολογίζει και επιστρέφει την τοποθεσία που περιγράφει ο πλήρης κωδικός "plusCode" σε επίπεδο ακρίβειας "level". Πρακτικά «κόβει» 2*level χαρακτήρες από το δεξί μέλος του πλήρους κωδικού.

5.2 Διαδικασία κατασκευής της εφαρμογής

Αφού παρουσιάστηκαν τα δομικά στοιχεία με τα οποία κατασκευάστηκε η εφαρμογή, περιγράφεται συνοπτικά η διαδικασία που ακολουθήθηκε για την κατασκευή της.

- Αρχικά έγιναν δοκιμές του "Quiet for Android" με τη βοήθεια της εφαρμογής QuietShare [100], όπως περιγράφεται στο επόμενο κεφάλαιο. Σκοπός ήταν να επιλεχθεί το καταλληλότερο προφίλ υπερήχων. Το Quiet τοποθετήθηκε στο φάκελο /quiet της εφαρμογής.
- Στη συνέχεια υλοποιήθηκαν οι κρυπτογραφικές απαιτήσεις καθώς και οι απαραίτητες διαδικασίες για την αλυσίδα κατακερματισμού τοποθεσίας. Τα αντίστοιχα αρχεία είναι τα Crypto.java και LocationChain.java.
- Αναπαραστάθηκαν τα απαραίτητα μηνύματα ως απλές κλάσεις της Java και τοποθετήθηκαν στο αρχείο Messages.java.
- Εισήχθησαν στο Android Studio τα απαραίτητα αρχεία .jar που αφορούν τη μετατροπή αντικειμένων σε JSON και αντίστροφα (βιβλιοθήκη Jackson), καθώς και τη μετατροπή συντεταγμένων σε plus code (βιβλιοθήκη OpenLocationCode). Τα αρχεία αυτά βρίσκονται στο φάκελο /app/libs.
- Κατασκευάστηκε η βοηθητική κλάση ParseJSON (αρχείο ParseJSON.java), η οποία αποτελεί τη διεπαφή μεταξύ της εφαρμογής και του Jackson.
- Εισήχθη κομμάτι κώδικα από το QuietShare για την ασύγχρονη ανταπόκριση του δέκτη στη λήψη μηνύματος. Ο κώδικας αυτός βρίσκεται στο αρχείο FrameReceiverObservable.java.
- Δημιουργήθηκε η αρχική οθόνη της εφαρμογής (MainActivity.java), η οποία λαμβάνει την τοποθεσία της συσκευής με βάση το λειτουργικό σύστημα και τη μετατρέπει σε μορφή Plus code.
- Δημιουργήθηκε η δεύτερη οθόνη της εφαρμογής (RequestProof.java), η οποία περιέχει τα κουμπιά για την εκτέλεση των λειτουργιών του πρωτοκόλλου.
- Οι λειτουργίες του Prover και του Witness υλοποιούνται από τρεις κλάσεις: Η αφηρημένη (abstract) κλάση Protocol θέτει σε λειτουργία τον πομπό και το δέκτη υπερήχων

και παρέχει μεθόδους που είναι κοινές τόσο για τον Prover όσο για το Witness. Επιπλέον, φορτώνει τα κλειδιά του χρήστη καθώς και το δημόσιο κλειδί της CA από το αρχείο /app/src/main/res/raw/protocol_config.json. Οι άλλες δύο κλάσεις είναι οι ProverProtocol και WitnessProtocol, που εκτελούν το πρωτόκολλο από την πλευρά του Prover και του Witness αντίστοιχα.

- Προσομοιώθηκαν οι λειτουργίες της Certificate Authority στο αρχείο CertificateAuthority.java. Με είσοδο το μήνυμα LPA παράγεται το VS το οποίο στη συνέχεια επεξεργάζεται ο Prover.
- Υλοποιήθηκε η παραγωγή της τελικής απόδειξης τοποθεσίας LP με τη μέθοδο LpGenerator. Αυτή, με βάση το VS, το δημόσιο κλειδί του Verifier και κάποιες επιπρόσθετες πληροφορίες (επίπεδο ακρίβειας τοποθεσίας, αντίστοιχο κομμάτι αλυσίδας τοποθεσίας, δέσμευση) παράγει το μήνυμα LP προς έλεγχο από τον Verifier.
- Η λειτουργία του Verifier προσομοιώνεται με την ομώνυμη μέθοδο (αρχείο Verifier.java), όπου ελέγχεται το μήνυμα LP.

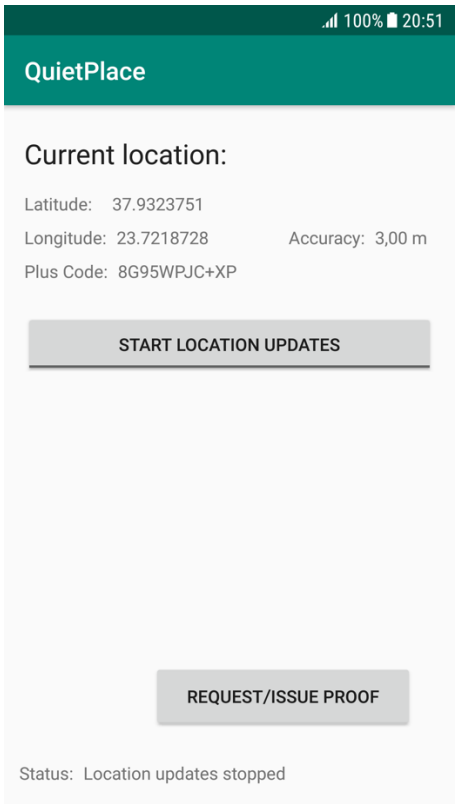
5.3 Χρήση της εφαρμογής

Προκειμένου να χρησιμοποιήσει την εφαρμογή, ο χρήστης πρέπει να δώσει σε αυτήν δικαίωμα χρήσης της τοποθεσίας και εγγραφής ήχου. Επίσης, ο χρήστης πρέπει να ενεργοποιήσει το δέκτη GPS της συσκευής, προκειμένου να επιτευχθεί η επιθυμητή ακρίβεια.

Με την ενσωμάτωση της λειτουργίας εγγραφής βίντεο, η οποία προς το παρόν δεν υλοποιείται, θα απαιτείται επιπλέον η άδεια χρήσης της κάμερας της συσκευής.

Η εφαρμογή δεν απαιτεί ύπαρξη δικτύου κινητής τηλεφωνίας ούτε σύνδεση στο διαδίκτυο.

Ανοίγοντας την εφαρμογή, ο χρήστης βλέπει την αρχική οθόνη, όπως φαίνεται παρακάτω.

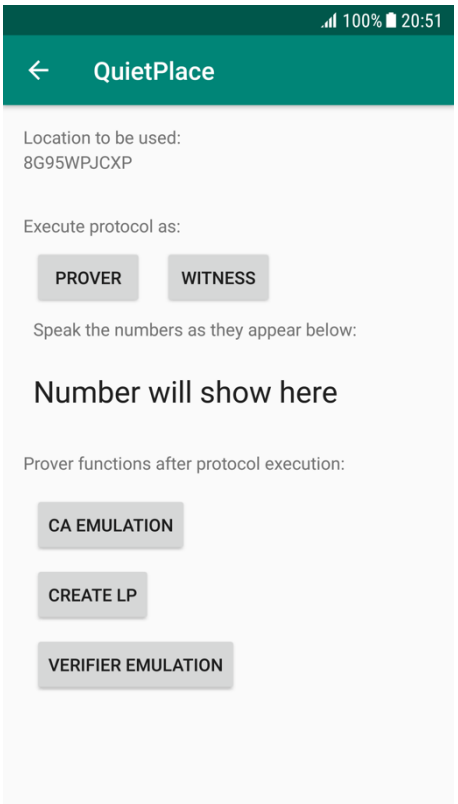


Σχήμα 5.1: Η αρχική οθόνη της εφαρμογής.

Σε πρώτη φάση η εφαρμογή υπολογίζει την τοποθεσία του χρήστη. Αυτό γίνεται πατώντας το κουμπί “Start Location Updates”. Εμφανίζεται η τοποθεσία σε μορφή συντεταγμένων, καθώς και σε plus code μήκους 10 χαρακτήρων. Επιπλέον, εμφανίζεται η ακρίβεια με την οποία έχει υπολογιστεί η τοποθεσία. Ο χρήστης περιμένει να αποκτήσει η συσκευή την κατάλληλη ακρίβεια τοποθεσίας, γιατί θα πρέπει prover και witness να έχουν το ίδιο plus code, προκειμένου να εκτελεστεί με επιτυχία το πρωτόκολλο. Με δεδομένο ότι οι περιοχές που ορίζουν τα Plus Codes μήκους 10 χαρακτήρων είναι 14x14 μέτρα, η ακρίβεια θα πρέπει να είναι το πολύ 14 μέτρα.

Αφού ο χρήστης θεωρεί ότι η ακρίβεια είναι ικανοποιητική, πατάει “Stop Location Updates” και προχωράει προς την εκτέλεση του πρωτοκόλλου, πατώντας το κουμπί “Request/Issue Proof”.

Μεταβαίνει στην οθόνη που φαίνεται παρακάτω.



Σχήμα 5.2: Η δεύτερη οθόνη της εφαρμογής με τις λειτουργίες του πρωτοκόλλου.

Τώρα μπορεί να εκτελέσει το πρωτόκολλο ως prover ή witness.

Αν εκτελεί το πρωτόκολλο ως prover, κατά την έλευση του μηνύματος Challenge θα εμφανιστεί στο πεδίο “Number will show here” ένας τυχαίος τριψήφιος αριθμός που παράχθηκε από το witness. Αυτός ο αριθμός πρέπει να διαβαστεί από τον χρήστη σε περίπτωση που ζητείται ισχυρή ταυτότητα με καταγραφή βίντεο (δεν υλοποιείται).

Με το τέλος της εκτέλεσης του πρωτοκόλλου ως prover, η συσκευή κατασκευάζει το μήνυμα LPA. Στο κάτω μέρος της οθόνης υπάρχουν τρία κουμπιά που αφορούν τις μετέπειτα λειτουργίες του prover. Με το κουμπί “CA Emulation” προσομοιώνεται η λειτουργία της CA, η οποία παραλαμβάνει το μήνυμα LPA, εκτελεί ελέγχους και παράγει το μήνυμα VS. Με το κουμπί “Create LP” κατασκευάζεται το μήνυμα LP με βάση το VS και κάποιες επιπρόσθετες

πληροφορίες (επίπεδο ακρίβειας τοποθεσίας, αντίστοιχο κομμάτι αλυσίδας τοποθεσίας, δέσμευση). Τέλος, με το κουμπί “Verifier Emulation” προσομοιώνεται η λειτουργία του verifier, ο οποίος παραλαμβάνει το LP του prover και εκτελεί ελέγχους.

Η όλη διαδικασία παρακολουθείται προς το παρόν με τη λειτουργία debugging και συγκεκριμένα με το Logcat του Android Studio. Η συσκευή πρέπει να είναι συνδεδεμένη με τον υπολογιστή μέσω καλωδίου USB.

6 Πειραματικές μετρήσεις και σχόλια

Τα δύο πρώτα πειράματα διερευνούν περαιτέρω τις δυνατότητες του Quiet ως προς τη μέγιστη απόσταση στην οποία λαμβάνεται μήνυμα και ως προς την κατευθυντικότητα πομπού-δέκτη (ηχείου-μικροφώνου). Συγκρίνονται τα προφίλ που παρέχει το Quiet από προεπιλογή, εκτός από το "cable-64k", το οποίο προορίζεται για χρήση μέσω καλωδίου ήχου. Πραγματοποιήθηκαν με την εφαρμογή Quietshare [100], η οποία αποτελεί μία υλοποίηση του Quiet σε λειτουργία πλαισιών.

Το τρίτο πείραμα έχει ως σκοπό να αποτιμήσει τη λειτουργία της εφαρμογής που υλοποιήθηκε ως προς το χρόνο που χρειάζεται για να παραχθεί και να επιβεβαιωθεί μία απόδειξη τοποθεσίας με την παρουσία ενός witness.

6.1 Μέγιστη απόσταση για τη λήψη μηνύματος

Όπως αναφέρθηκε, το quiet διαθέτει διάφορα προφίλ ήχου. Έχει ενδιαφέρον η μέτρηση της μέγιστης απόστασης για την οποία είναι δυνατή η λήψη ενός μηνύματος, ανάλογα με το προφίλ το οποίο χρησιμοποιείται.

Για το πείραμα αυτό ως πομπός χρησιμοποιήθηκε ένα Xiaomi Redmi Note 5 και ως δέκτης ένα Samsung Galaxy S6. Η ένταση του ηχείου ορίστηκε στο επίπεδο 14 από τα 15 που ορίζει η συσκευή, προς αποφυγήν παραμορφώσεων.

Για κάθε προφίλ, απομακρύνουμε σταδιακά τον πομπό από το δέκτη στέλνοντας κάθε φορά το μήνυμα "testmessage", μέχρι να μην υπάρχει λήψη. Καταγράφουμε τη μέγιστη απόσταση μεταξύ του ηχείου του πομπού και του μικροφώνου του δέκτη για την οποία έγινε επιτυχής λήψη του μηνύματος. Καθ' όλη τη διάρκεια του πειράματος τα δύο τηλέφωνα τοποθετούνται με τρόπο ώστε το ηχείο του πομπού να στοχεύει το μικρόφωνο του δέκτη.

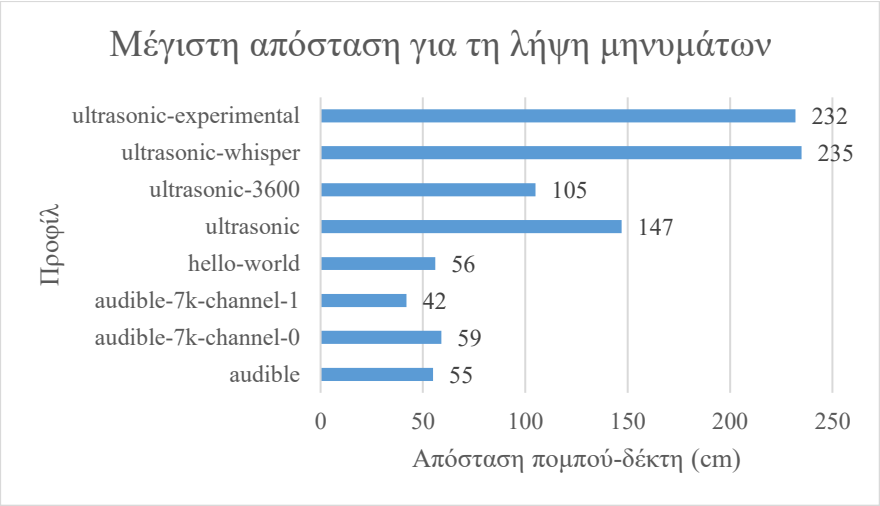
Τα αποτελέσματα που λάβαμε φαίνονται στον παρακάτω πίνακα.

Προφίλ	**Μέγιστη απόσταση (cm)**
audible	55
audible-7k-channel-0	59
audible-7k-channel-1	42
hello-world	56
ultrasonic	147
ultrasonic-3600	105
ultrasonic-whisper	235
ultrasonic-experimental	232

Πίνακας 6: Μέγιστη απόσταση λήψης για κάθε προφίλ του Quiet.

Παρατηρήθηκε πως τα προφίλ που βασίζονται σε υπέρηχους παρουσιάζουν μεγαλύτερη ανοχή στην απόσταση για την ίδια ένταση του ηχείου.

Οπτικά τα αποτελέσματα φαίνονται στο παρακάτω διάγραμμα.



Σχήμα 6.1: Διάγραμμα μέγιστης απόστασης λήψης για κάθε προφίλ του Quiet.

6.2 Κατευθυντικότητα

Οι συσκευές που χρησιμοποιήθηκαν είναι ίδιες με το προηγούμενο πείραμα. Χαμηλώσαμε την ένταση του ηχείου του πομπού στη στάθμη 10/15, καθώς οι αποστάσεις είναι μικρότερες. Άλλωστε, μας ενδιαφέρει η σύγκριση μεταξύ των διαφορετικών προφίλ για τις ίδιες συνθήκες.

Ο δέκτης παραμένει σταθερός καθ' όλη τη διάρκεια του πειράματος. Περιστρέφουμε τον πομπό γύρω από το δέκτη, φροντίζοντας το ηχείο του να στοχεύει συνέχεια τον δέκτη. Η απόσταση μεταξύ του ηχείου του πομπού και του μικροφώνου του δέκτη παραμένει ίδια και περίπου 30 cm.

Ως 0° θεωρείται η διάταξη των συσκευών όταν το ηχείο του πομπού στοχεύει το μικρόφωνο του δέκτη, το οποίο βρίσκεται στο κάτω μέρος της συσκευής, ενώ ως 180 θεωρείται° η διάταξη όταν το ηχείο του πομπού στοχεύει το πάνω μέρος της συσκευής του δέκτη.

Για κάθε προφίλ, περιστρέφουμε τον πομπό γύρω από το δέκτη ανά 10 μοίρες, στέλνοντας κάθε φορά το μήνυμα "testmessage". Σημειώνουμε τις γωνίες στις οποίες έγινε λήψη με τον αριθμό 1, ενώ αυτές στις οποίες δεν έγινε λήψη με τον αριθμό 0.

Τα αποτελέσματα που προέκυψαν παρατίθενται στον ακόλουθο πίνακα:

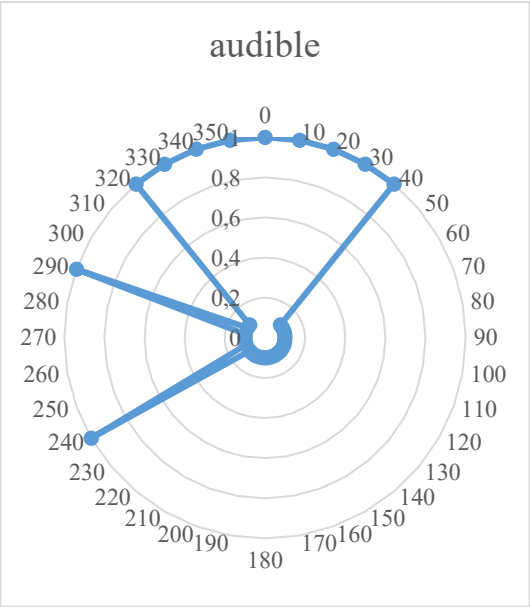
Γωνία(°)	audible	audible-7k-channel-0	audible-7k-channel-1	hello-world	ultrasonic	ultrasonic-3600	ultrasonic-whisper	ultrasonic-experimental
0	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1
20	1	1	1	1	1	1	1	1
30	1	1	1	1	1	1	1	1
40	1	1	1	1	1	1	1	1
50	0	1	1	1	1	1	1	1
60	0	0	0	1	1	1	1	1
70	0	0	1	0	1	1	1	1
80	0	0	0	1	1	1	1	1
90	0	0	0	0	1	0	1	1
100	0	0	0	0	1	0	1	1
110	0	0	0	1	1	0	1	1
120	0	0	0	0	0	0	1	1
130	0	0	0	1	0	0	0	1
140	0	0	0	0	0	0	0	0
150	0	0	0	0	0	0	0	1
160	0	0	0	0	0	0	0	0
170	0	0	0	0	0	0	0	0
180	0	0	0	0	0	0	0	1
190	0	0	0	0	0	0	0	0
200	0	0	0	0	0	0	0	1
210	0	0	0	0	0	0	0	1
220	0	0	0	0	0	0	0	1
230	0	0	0	0	0	0	1	1
240	1	0	0	0	1	0	1	1
250	0	0	0	0	0	0	1	1
260	0	0	0	0	1	0	1	1
270	0	0	0	0	1	0	1	1
280	0	0	0	1	1	1	1	1
290	1	0	0	1	1	1	1	1
300	0	0	0	0	1	1	1	1
310	0	1	1	1	1	1	1	1
320	1	1	1	1	1	1	1	1
330	1	1	1	1	1	1	1	1
340	1	1	1	1	1	1	1	1
350	1	1	1	1	1	1	1	1
Σημεία λήψης	11	11	12	17	23	17	26	32

Πίνακας 7: Μετρήσεις κατευθυντικότητας για τα διάφορα προφίλ του Quiet.

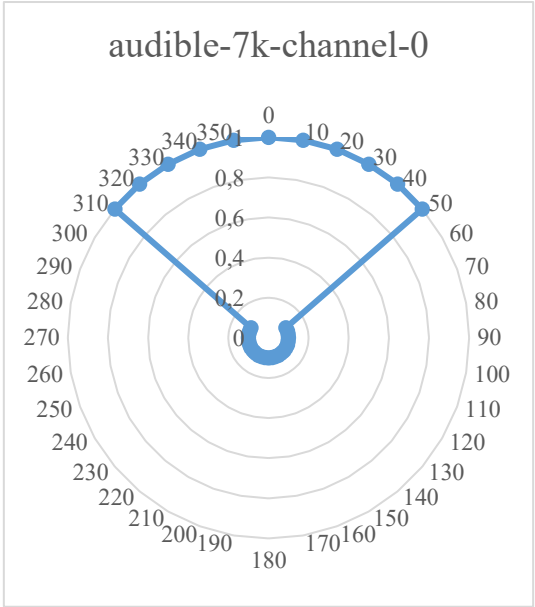
Παρατηρούμε ότι το προφίλ με τα περισσότερα σημεία λήψης είναι το “ultrasonic-experimental”.

Τοποθετούμε τις τιμές σε κυκλικά διαγράμματα, για να οπτικοποιήσουμε τα σημεία όπου πραγματοποιήθηκε λήψη με επιτυχία. Καταχρηστικά θα ονομάσουμε μέγεθος του κύριου λοβού τη μέγιστη γωνία όπου έχουμε συνεχόμενα σημεία λήψης.

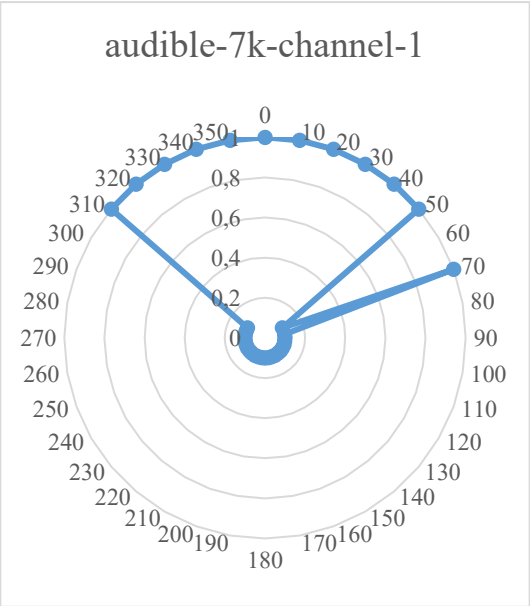
Προκύπτουν τα παρακάτω διαγράμματα:



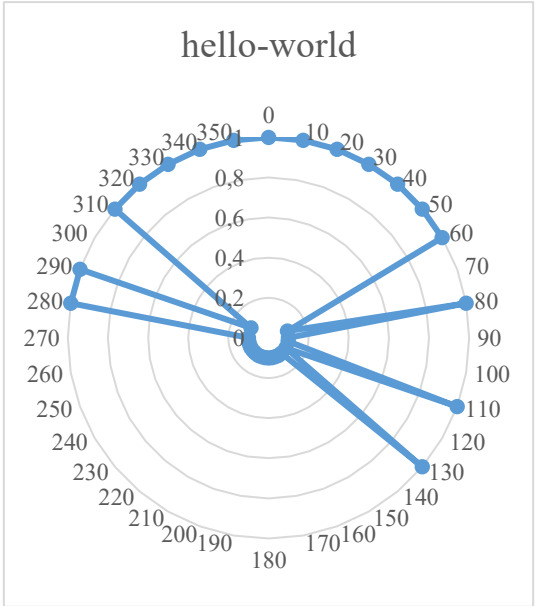
Σχήμα 6.2: Διάγραμμα λήψης για το προφίλ "audible".



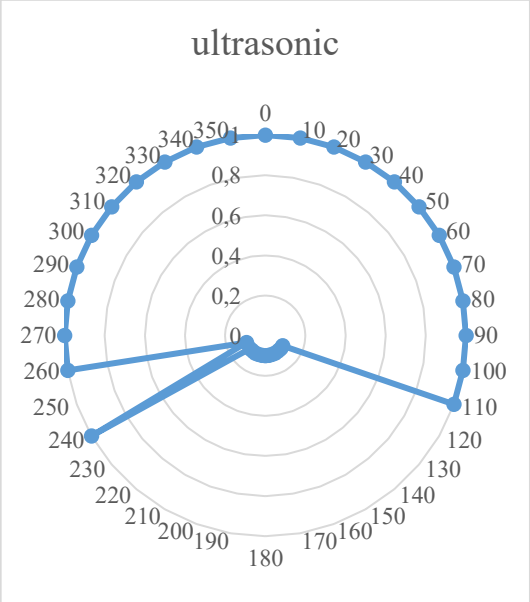
Σχήμα 6.3: Διάγραμμα λήψης για το προφίλ "audible-7k-channel-0".



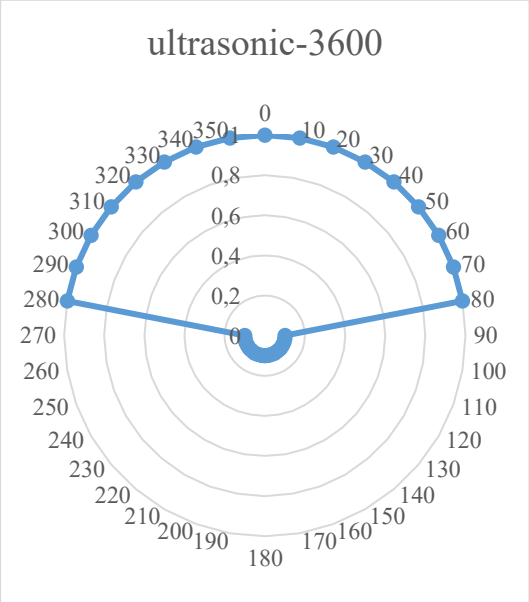
Σχήμα 6.4: Διάγραμμα λήψης για το προφίλ "audible-7k-channel-1".



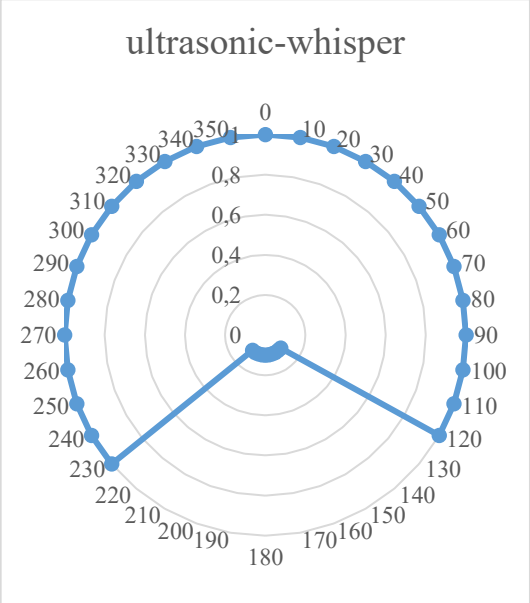
Σχήμα 6.5: Διάγραμμα λήψης για το προφίλ "hello-world".



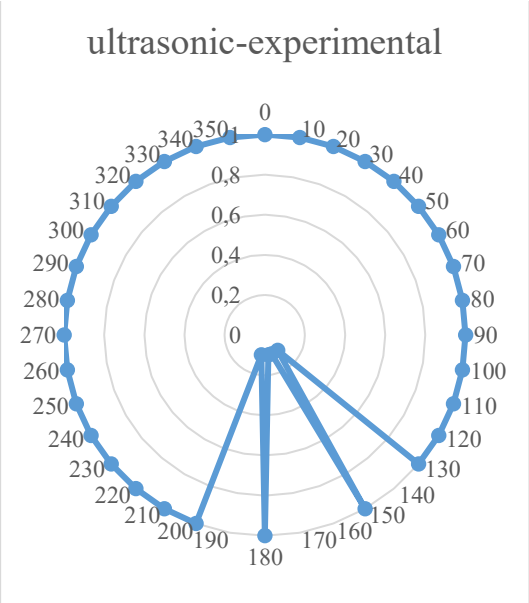
Σχήμα 6.6: Διάγραμμα λήψης για το προφίλ "ultrasonic".



Σχήμα 6.7: Διάγραμμα λήψης για το προφίλ "ultrasonic-3600".



Σχήμα 6.8: Διάγραμμα λήψης για το προφίλ "ultrasonic-whisper".



Σχήμα 6.9: Διάγραμμα λήψης για το προφίλ "ultrasonic-experimental".

Το περισσότερο κατευθυντικό προφίλ είναι το "audible" με άνοιγμα κύριου λοβού 80 μοίρες, ενώ το λιγότερο κατευθυντικό είναι το "ultrasonic-experimental" με άνοιγμα κύριου λοβού 290 μοίρες.

Σημείωση: Στα παραπάνω διαγράμματα τα μηδενικά σημεία (εκεί όπου δεν έχουμε λήψη) αντικαταστάθηκαν με την τιμή 0,1 για οπτικά καλύτερο αποτέλεσμα.

6.3 Απαιτούμενος χρόνος για την εκτέλεση του πρωτοκόλλου

Το πρωτόκολλο εκτελέστηκε με prover το Samsung Galaxy S6 που χρησιμοποιήθηκε προηγουμένως και με witness το Samsung Galaxy J5 2017. Διαπιστώθηκε πως το Xiaomi

Redmi Note 5 για άγνωστο λόγο αδυνατούσε να λάβει μηνύματα είτε με την εφαρμογή QuietPlace είτε με την εφαρμογή Quietshare.

Η αρχική σκέψη ήταν να μετρηθεί ο χρόνος που διαρκεί η αποστολή κάθε μηνύματος προγραμματιστικά, καταγράφοντας τη χρονική στιγμή έναρξης και λήξης της αποστολής του μηνύματος και υπολογίζοντας τη διαφορά. Ωστόσο, λόγω της ασύγχρονης λειτουργίας του Quiet, κάτι τέτοιο είναι αδύνατο να πραγματοποιηθεί δίχως να γίνει επέμβαση στον κώδικα του Quiet.

Μία δεύτερη σκέψη ήταν να μετρηθεί ο συνολικός χρόνος αποστολής και λήψης του κάθε μηνύματος, υπολογίζοντας τη διαφορά μεταξύ της χρονικής στιγμής που το μήνυμα ελήφθη από το δέκτη και της χρονικής στιγμής που το μήνυμα στάλθηκε από τον πομπό. Και αυτή η σκέψη απορρίφθηκε, καθώς εμπλέκονταν ρολόγια διαφορετικών συσκευών, τα οποία δεν είναι απόλυτα συγχρονισμένα.

Τελικά, λόγω του σχετικά μεγάλου χρονικού διαστήματος που απαιτεί η αποστολή κάθε μηνύματος καθώς και του γεγονότος πως τα μηνύματα είναι δυνατόν να «ακουστούν», χρησιμοποιήθηκε χρονόμετρο κατά την εκτέλεση του πρωτοκόλλου. Το πρωτόκολλο εκτελέστηκε τρεις φορές και λήφθηκε η μέση τιμή των χρονικών διαστημάτων που χρειάστηκε κάθε μήνυμα για να αποσταλεί.

Τα αποτελέσματα παρουσιάζονται στον παρακάτω πίνακα.

Μήνυμα	**1η μέτρηση**	**2η μέτρηση**	**3η μέτρηση**	**Χρονικό διάστημα (s) (μέσος όρος)**
Prover Request	2,75	2,73	2,53	2,67
Witness Presence	1,33	1,33	1,13	1,26
Start	2,69	2,71	2,68	2,69
Challenge	1,9	1,73	1,63	1,75
Response	1,66	1,65	1,72	1,68
Video Hash	1,87	1,82	1,96	1,88
LPS	14,37	14,29	14,03	14,23
LIST	6,33	6,45	6,26	6,35
Συνολικός χρόνος μηνυμάτων	**32,9**	**32,71**	**31,94**	**32,52**

Πίνακας 8: Χρονική διάρκεια για την αποστολή μηνυμάτων.

Στα παραπάνω αποτελέσματα δεν περιλαμβάνονται τα χρονικά διαστήματα όπου ο prover περιμένει την πιθανή εμφάνιση και άλλων witnesses πριν στείλει το επόμενο μήνυμα, καθώς και οι χρόνοι επεξεργασίας και προετοιμασίας των μηνυμάτων από τους κόμβους.

Ο **συνολικός χρόνος εκτέλεσης της παρούσας υλοποίησης του πρωτοκόλλου** από την αποστολή του μηνύματος Prover Request μέχρι και τον υπολογισμό του LPA μετρήθηκε περίπου στα **50 δευτερόλεπτα**.

Τα χρονικά διαστήματα είναι αρκετά μεγάλα για να μπορεί η εφαρμογή να χρησιμοποιηθεί στην πράξη. Στην περίπτωση που υπάρχει μόνο ένα witness, η αποστολή του μηνύματος LPS απαιτεί το 44% του συνολικού χρονικού διαστήματος για την αποστολή όλων των μηνυμάτων. Για κάθε επιπλέον witness, το συνολικό χρονικό διάστημα για την αποστολή μηνυμάτων αυξάνεται κατά περίπου 25 δευτερόλεπτα, αφού απαιτούνται επιπλέον μηνύματα witness Presence, Challenge, Response, LPS, LIST.

Στο επόμενο κεφάλαιο γίνονται προτάσεις για τη μείωση του χρονικού διαστήματος που απαιτείται για την εκτέλεση του πρωτοκόλλου.

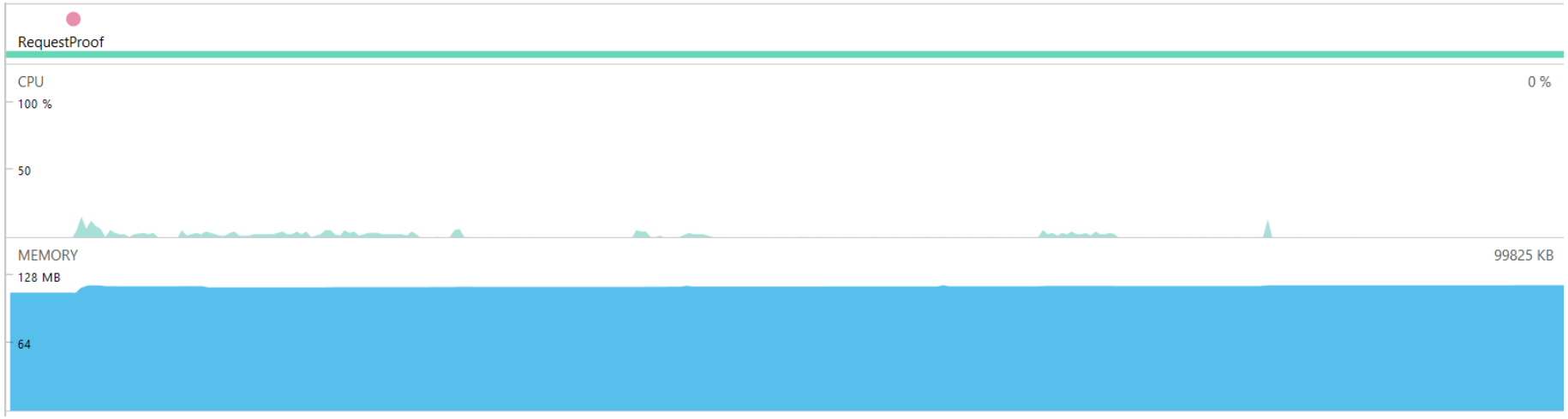
6.4 Χρησιμοποίηση πόρων

Με το εργαλείο Profiler του Android Studio μετρήθηκε η επίπτωση της εφαρμογής στον επεξεργαστή και τη μνήμη της συσκευής Galaxy S6. Δυστυχώς δεν κατέστη δυνατή η μέτρηση της κατανάλωσης ισχύος, καθώς απαιτεί έκδοση Android 8 και μεγαλύτερη, που δεν υποστηρίζεται από τις συσκευές που είχαμε στη διάθεσή μας.

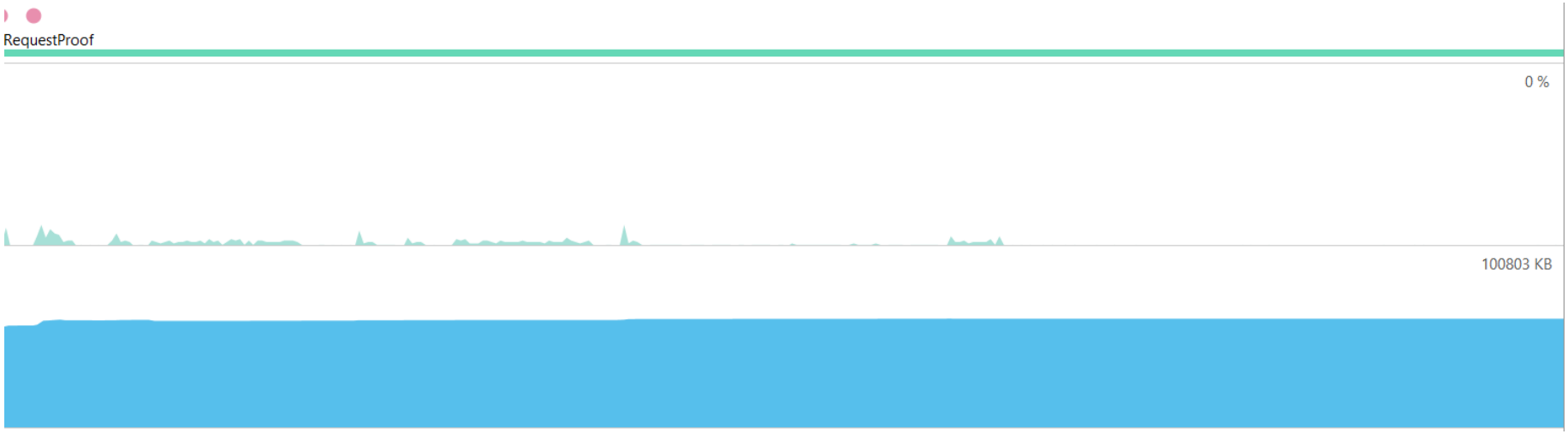
Σε λειτουργία αδράνειας, η εφαρμογή χρησιμοποιεί περίπου 90 MB μνήμης RAM. Αφού εκκινείται το πρωτόκολλο και κατά τη διάρκεια εκτέλεσής του, είτε ως prover είτε ως witness, η χρησιμοποίηση της RAM αυξάνεται περίπου στα 97-98 MB. Σε καμία περίπτωση δεν υπερβαίνει τα 100 MB. Αξίζει να σημειωθεί ότι τα 65 MB καταναλώνονται από τα γραφικά, συνεπώς το υπόλοιπο κομμάτι της εφαρμογής καταναλώνει περίπου 30 MB. Η επίπτωση της εφαρμογής στη μνήμη της συσκευής είναι ελάχιστη.

Η χρήση του επεξεργαστή παρατηρείται κατά την αποστολή και λήψη μηνυμάτων, καθώς και κατά την κατασκευή αυτών. Κατά μέγιστο τόσο στη λειτουργία prover όσο και στη λειτουργία witness φτάνει στιγμιαία το 15%, όμως τις περισσότερες στιγμές κυμαίνεται στο 4%, ενώ υπάρχουν χρονικές στιγμές που αυτή είναι μηδενική.

Υπενθυμίζεται πως δεν έχει υλοποιηθεί η καταγραφή βίντεο, η οποία θα έχει σημαντική επίπτωση στις παραπάνω μετρήσεις καθώς και στην κατανάλωση ενέργειας. Αυτή όμως είναι απαραίτητη μόνο όταν απαιτούνται ισχυρές ταυτότητες.



Σχήμα 6.10: Χρήση πόρων κατά την εκτέλεση του πρωτοκόλλου ως prover.



Σχήμα 6.11: Χρήση πόρων κατά την εκτέλεση του πρωτοκόλλου ως witness.

7 Μελλοντική εργασία και προτάσεις

Στην παρούσα εργασία αναπτύχθηκε και υλοποιήθηκε ένα πρωτόκολλο απόδειξης τοποθεσίας με υποστήριξη ισχυρών ταυτοτήτων.

Στην αρχή έγινε αναφορά στις τεχνικές και μεθόδους γεωεντοπισμού, ώστε να γίνει κατανοητός ο τρόπος με τον οποίο οι συσκευές σήμερα προσδιορίζουν την τοποθεσία τους. Στη συνέχεια, εξηγήθηκε η ανάγκη για πρωτόκολλα απόδειξης τοποθεσίας, παρουσιάστηκαν τα πεδία στα οποία αυτά μπορούν να έχουν εφαρμογή καθώς και τα χαρακτηριστικά, οι προδιαγραφές τους και η διαδικασία που ακολουθούν. Εντοπίστηκαν ενδιαφέροντα ζητήματα στα οποία δεν έχει δοθεί ικανοποιητική λύση και έγινε προσπάθεια για την επίλυσή τους. Προσεγγίστηκε ιδιαίτερα το ζήτημα των ισχυρών ταυτοτήτων, δηλαδή της απόδειξης της παρουσίας του χρήστη μαζί με τη συσκευή που χρησιμοποιεί. Έγινε προσπάθεια για τη διατήρηση της ιδιωτικότητας και την επιβεβαίωση της ταυτότητας διαιρώντας τη γνώση των ταυτοτήτων και της τοποθεσίας. Συγκεκριμένα, η CA ασχολείται με την ταυτότητα ενώ ο verifier με την τοποθεσία του χρήστη. Επιπλέον, έγιναν προτάσεις για την αποτροπή συνεργασιών μεταξύ κάθε τύπου χρήστη που μπορεί να συμμετάσχει στο σύστημα.

Σε αντίθεση με τα περισσότερα υπάρχοντα πρωτόκολλα απόδειξης τοποθεσίας, για την επικοινωνία των κόμβων χρησιμοποιούνται υπέρηχοι. Έτσι δυσκολεύουν επιθέσεις αναμετάδοσης και παράλληλα η όλη συνεδρία μπορεί να καταγραφεί σε βίντεο, το οποίο απεικονίζει το χρήστη.

Διαμορφώθηκε στη συνέχεια το είδος και το περιεχόμενο των απαιτούμενων μηνυμάτων, έχοντας κατά νου την απλότητα και αποφεύγοντας τεχνικές που απαιτούν ειδικό εξοπλισμό και επιφέρουν υπολογιστικό φόρτο, όπως η distance-bounding [77], [48]. Το προτεινόμενο πρωτόκολλο υλοποιήθηκε σε Java για συσκευές με λειτουργικό σύστημα Android και δοκιμάστηκε για τη λειτουργία του.

Ωστόσο, αφενός παρουσιάστηκαν προβλήματα που απαιτούν επίλυση, αφετέρου υπάρχει περιθώριο βελτιώσεων και παράλληλα η εργασία αυτή μπορεί να έχει περαιτέρω επεκτάσεις. Οι διαπιστώσεις αυτές παρουσιάζονται στη συνέχεια.

7.1 Επίλυση προβλημάτων

- Με την παρούσα εφαρμογή, ένα witness δεν μπορεί να γνωρίζει αν κάποιο άλλο witness αποστέλλει μήνυμα κάποια στιγμή, ώστε να αποφύγει να «μιλήσει» μαζί του, καθιστώντας τη λήψη από τον prover αδύνατη. Με άλλα λόγια, δεν εφαρμόζεται κάποια τεχνική Ελέγχου Πρόσβασης Μέσου (Medium Access Control). Για τη χρήση του πρωτοκόλλου με περισσότερα του ενός witness πρέπει να αντιμετωπιστούν οι πιθανές συγκρούσεις (collisions).
- Είναι ανάγκη να αναπτυχθεί τεχνική ώστε να μπορεί το witness να αντιλαμβάνεται πότε κάποιος prover ζητά την έκδοση απόδειξης τοποθεσίας, χωρίς να υπάρχει ανάγκη για συνεχή ακρόαση μέσω του μικροφώνου. Στην παρούσα φάση το witness ξεκινά χειροκίνητα την εκτέλεση του δικού του κώδικα.

7.2 Βελτιώσεις

- Στο πρωτότυπο που υλοποιήθηκε, η λειτουργία της CA και του verifier προσομοιώνεται στη συσκευή του prover, αφού αυτός ολοκληρώσει την εκτέλεση του πρωτοκόλλου και δημιουργήσει το μήνυμα LPA. Σε ένα πραγματικό περιβάλλον οι λειτουργίες αυτές

πρέπει να εκτελούνται από διακομιστές οι οποίοι διατηρούν βάση με τους χρήστες και τα δημόσια κλειδιά τους, ενώ παράλληλα διαθέτουν διεπαφή προγραμματισμού εφαρμογών (API), ώστε να δέχονται μηνύματα από τους χρήστες και να απαντούν κατάλληλα.

- Αξίζει περαιτέρω έρευνας ο τρόπος με τον οποίο μπορεί να επιτευχθεί επικοινωνία μέσω υπερήχων με μεγαλύτερη κατευθυντικότητα και σε μεγαλύτερη απόσταση. Κάτι τέτοιο μπορεί να γίνει δυνατό με τη δημιουργία νέων προφίλ στο Quiet ή με την διερεύνηση της λειτουργίας και των δυνατοτήτων τροποποίησης που δίνει το liquid-dsp.
- Για την επιτάχυνση της εκτέλεσης του πρωτοκόλλου μεταξύ prover και witness είναι επιθυμητό να διερευνηθούν εναλλακτικές μορφές μηνυμάτων και κωδικοποιήσεων, ώστε να παράγονται μηνύματα μικρότερου μεγέθους.

7.3 Επεκτάσεις

- Μεγάλο ερευνητικό ενδιαφέρον έχουν τα σχήματα εμπιστοσύνης με βάση τα οποία μπορεί η CA να αξιολογεί την ειλικρίνεια των provers και των witnesses που συμμετέχουν στο σύστημα αποδείξεων τοποθεσίας. Ανάλογα με τη συμπεριφορά τους οι χρήστες του συστήματος αξιολογούνται ώστε να αποφευχθούν κακόβουλες συμπεριφορές. Σε παρόμοιο πλαίσιο, είναι δυνατόν να παρακολουθούνται οι αλληλεπιδράσεις των χρηστών ώστε να εντοπίζονται κόμβοι που πιθανώς συνεργάζονται για την παραγωγή ψευδών αποδείξεων τοποθεσίας.
- Αξίζει η διερεύνηση συνδυαστικών μεθόδων για την επιβεβαίωση της τοποθεσίας. Με χρήση δεδομένων από διαφορετικές πηγές, όπως για παράδειγμα γειτονικά δίκτυα Wi-Fi, κεραίες κινητής τηλεφωνίας, επίπεδα θορύβου ή φωτεινής έντασης, είναι δυνατόν να επιβεβαιωθεί τόσο η γειτνίαση των κόμβων (prover, witness) μεταξύ τους, όσο και με σημεία γνωστής τοποθεσίας. Θα είχε ενδιαφέρον η ενσωμάτωση των δεδομένων αυτών σε ένα μήνυμα και η αφαιρετική τους σύγκριση (fuzzy matching) ώστε να εντοπιστεί το κατά πόσον αυτά ταιριάζουν και συνεπώς να μπορεί να εξαχθεί αποτέλεσμα για το πόσο κοντά βρίσκονται οι χρήστες που τα παρουσιάζουν.

Παράρτημα: Σχετικές μελέτες

Στο παράρτημα αυτό γίνεται αναφορά σε ενδιαφέροντα σημεία που εντοπίστηκαν κατά τη μελέτη κάθε μίας από τις παρακάτω δημοσιεύσεις και όχι πλήρης σχολιασμός τους.

FOAM [68]**,** [79]

Πρωταρχικός του σκοπός είναι η δημιουργία ενός συλλογικού καταλόγου από σημεία ενδιαφέροντος (Points Of Interest). Η τοποθεσία των POIs επιβεβαιώνεται από χρήστες, οι οποίοι τα επισκέπτονται. Αυτή είναι η **στατική ΑΤ** που παρέχει το FOAM.

Υπάρχουν 3 ομάδες χρηστών:
1. Καταναλωτές: Θέλουν να αποκτούν πρόσβαση σε λίστες με POIs.
2. Υποψήφιοι: Θέλουν να συμπεριληφθούν σε μία λίστα με POI.
3. Χαρτογράφοι: Επιβεβαιώνουν την παρουσία των POI, δηλαδή συντηρούν τις λίστες.

Πέραν της στατικής ΑΤ, το FOAM παρέχει και **δυναμική ΑΤ**, δηλαδή ΑΤ κόμβων χωρίς σταθερή θέση. Η τοποθεσία αυτών δεν προσδιορίζεται από GPS, αλλά μέσω ενός δικτύου κόμβων που διατηρούν συγχρονισμένο ρολόι και συμμετέχουν στον προσδιορισμό θέσεων.

Αρνητικό είναι πως απαιτείται καινούργια υποδομή για γεωεντοπισμό, η οποία χρηματοδοτείται από χρήστες. Επίσης, απαιτείται προσπάθεια από τους χρήστες για να επιβεβαιώσουν την παρουσία αναφερόμενων σημείων ενδιαφέροντος. Αυτοί που αναλαμβάνουν τα παραπάνω ανταμείβονται με κρυπτονόμισμα.

Η βιωσιμότητα του συστήματος αυτού εξαρτάται σε μεγάλο βαθμό από την ειλικρίνεια των παραπάνω ομάδων χρηστών.

Οι συγγραφείς διατηρούν αμφιβολίες για το αν το σύστημα θα μπορεί να χρησιμοποιηθεί για τη δημιουργία ΑΤ για χρήστες. Βασικό πρόβλημα θεωρείται η ανάγκη για επέκταση του δικτύου γεωεντοπισμού που χρησιμοποιεί.

Στη συνέχεια, αναφερόμαστε στις δυναμικές ΑΤ, όπως περιγράφονται στο [79].

Το FOAM προορίζεται για αποκεντρωμένα περιβάλλοντα, όπως π.χ. για μία οικονομία βασισμένη στο blockchain, έναν στόλο αυτόνομων οχημάτων, ή κόμβους Internet Of Things.

Για τον εντοπισμό της τοποθεσίας των κόμβων απαιτείται η ύπαρξη σταθερών σημείων αναφοράς, που ονομάζονται **Zone Anchors**. Διαθέτουν υποδομή ασύρματης επικοινωνίας, τοπικό ρολόι και δημόσιο κλειδί. Αυτές πρέπει να συνδεθούν με μία πύλη και να διατηρούν το ρολόι τους συγχρονισμένο.

Η **Zone Authority** είναι μία πύλη με πρόσβαση στο διαδίκτυο, υπεύθυνη για την διατήρηση της μηχανής κοινής κατάστασης (Shared State Machine).

Τέσσερις ή περισσότερες Zone Authorities σχηματίζουν μία **Zone,** δηλαδή ένα σύνολο κόμβων με συγχρονισμένο ρολόι σε μία περιοχή. Η Zone μπορεί να υπολογίσει την τοποθεσία ενός κόμβου χρησιμοποιώντας τεχνική TOA με τριγωνισμό.

Η **Μηχανή Κοινής Κατάστασης (Shared State Machine)** διατηρείται από τις Zone Authorities που ανήκουν στη συγκεκριμένη Zone και τηρεί τον συγχρονισμό μεταξύ τους. Η Μηχανή αυτή έχει τη μορφή κλάδου της Ριζικής Αλυσίδας.

Το FOAM χρησιμοποιεί blockchain για να καταγράφει τις συναλλαγές υπηρεσιών και νομισμάτων (tokens) μεταξύ των χρηστών του (π.χ. συμφωνίες, καταθέσεις, ανταμοιβές και ποινές). Αυτό αποτελεί την **Ριζική Αλυσίδα (Root Chain)**.

Ένα **Νόμισμα FOAM** (FOAM token) χρησιμοποιείται ως κατάθεση ασφαλείας (εγγύηση) για τη συμμετοχή στο πρωτόκολλο με ορθότητα και ασφάλεια. Το «ποντάρισμα» νομισμάτων στην Root Chain απαιτείται για την πρόσβαση στην Shared State Machine.

Μία **Συμφωνία σε Επίπεδο Υπηρεσιών (Service Level Agreement)** αποτελεί τη μορφή του «πονταρίσματος» με το οποίο δεσμεύονται οι Zone Anchors και Zone Authorities προκειμένου να προσφέρουν υπηρεσίες απόδειξης τοποθεσίας.

Ένα **Δημόσιο Κλειδί Φάρου (Beacon Public Key - BPK)** είναι το γνωστό δημόσιο κλειδί μίας συσκευής που επιθυμεί να αγοράσει Αίτηση Παρουσίας από τις Zones. Αποτελεί ουσιαστικά τον prover.

Ένας **Ισχυρισμός Παρουσίας (Presence Claim)** είναι ένα σύνολο υπογεγραμμένων αιτήσεων που δίνουν πληροφορίες για ακριβή γεωεντοπισμό του φάρου (χρήστη). Εκδίδονται από τους συμμετέχοντες σε μία Ζώνη έναντι κάποιας τιμής. Ο Ισχυρισμός πρέπει να ελεγχθεί προκειμένου να αποτελέσει ΑΤ.

Οι **Επιβεβαιωτές (Verifiers)** έχουν κίνητρο να ελέγχουν τα χρονολόγια καταγραφής (time logs) των Ζωνών για απάτη και να παρέχουν ΑΤ. Οι Επιβεβαιωτές πρέπει να έχουν τουλάχιστον την ίδια υπολογιστική ισχύ με την Zone Authority μίας Ζώνης.

Οι **Δριμείς Καταστάσεις (Slashing Conditions)** είναι σφάλματα που αποτελούν παραβίαση των κανόνων του πρωτοκόλλου εκ μέρους των συμμετεχόντων στη Ζώνη. Έχουν ως αποτέλεσμα την απώλεια των νομισμάτων που έχουν κατατεθεί.

Η **Απόδειξη Τοποθεσίας (Proof of Location)** είναι ένα πιστοποιητικό ανθεκτικό στην απάτη, το οποίο πιστοποιεί ότι ένας χρήστης βρισκόταν σε μία τοποθεσία κάποιο ορισμένη χρονική στιγμή. Η ΑΤ αποτελεί αντικείμενο στο blockchain.

Όπως έχουμε αναφέρει, η τεχνική TOA (Time Of Arrival) απαιτεί τον συγχρονισμό των ρολογιών των κόμβων του δικτύου. Το FOAM χρησιμοποιεί αλγόριθμο για τον συγχρονισμό των ρολογιών των κατανεμημένων κόμβων της Ζώνης, ο οποίος έχει ανεκτικότητα ακόμα και αν δυσλειτουργεί το 1/3 αυτών (byzantine fault tolerance).

Το FOAM βασίζεται στην ομοφωνία (consensus) των κόμβων με τρεις τρόπους. Όπως αναφέρθηκε, χρειάζεται Σύγχρονη ομοφωνία (synchronous consensus) των ρολογιών των κόμβων της Ζώνης. Επιπλέον, χρειάζεται Μερικώς Σύγχρονη ομοφωνία (partially synchronous consensus) για τη διατήρηση της Μηχανής Κοινής Κατάστασης. Τέλος, οι συναλλαγές που καταγράφονται στη Ριζική Αλυσίδα διέπονται από αλγορίθμους Ασύγχρονης ομοφωνίας (Asynchronous consensus algorithms), όπως στα blockchains.

Το FOAM ενσωματώνει στο αποκεντρωμένο περιβάλλον του ένα μηχανισμό κινήτρου προς τους παρόχους της υπηρεσίας. Ο μηχανισμός αυτός βασίζεται στο «κρυπτονόμισμα» που χρησιμοποιεί, τα FOAM tokens.

Παράλληλα με την Root Chain, κάθε Zone διατηρεί μια πλευρική αλυσίδα (side chain), στην οποία αποτυπώνεται η Shared State Machine της Zone.

Οι πάροχοι υποδομής και υπηρεσιών (zone anchors, zone authorities και validators) διαθέτουν tokens ώστε να μπορούν να συμμετέχουν στο σύστημα. Τα tokens είναι σπάνιος πόρος και οι πάροχοι έχουν κίνητρο να συμπεριφερθούν σύμφωνα με το πρωτόκολλο προκειμένου να αυξήσουν το υπόλοιπό τους με ανταμοιβές. Σε περίπτωση που δεν ακολουθούν το πρωτόκολλο, επιβάλλεται ποινή και μειώνεται το υπόλοιπό τους.

Τόσο για τη δημιουργία μιας Zone όσο και για την λειτουργία ως verifier, οι πάροχοι πρέπει να καταθέσουν ορισμένα tokens εκ των προτέρων. Αυτό λειτουργεί ως εγγύηση για τη σωστή λειτουργία τους.

Η διαδικασία δημιουργίας ΑΤ έχει συνοπτικά ως εξής:

1. Ο prover εισέρχεται σε μία Zone και προσφέρει μία αμοιβή σε αυτή, σε νόμισμα που η Zone δέχεται. Στέλνει την τοποθεσία του και έναν τυχαίο αριθμό (nonce).

2. Οι κόμβοι της ζώνης με μέθοδο TDOA υπολογίζουν τη θέση του prover. Κάθε Zone Anchor τοποθετεί στο χρονολόγιο (shared state machine) της Zone την εκτιμώμενη θέση του prover, και στέλνει μήνυμα στον prover. Στην παρούσα φάση έχει δημιουργηθεί η Presence Claim, που πρέπει να ελεγχθεί από τον verifier.
3. Ο verifier, ο οποίος έχει πρόσβαση στη shared state machine της Zone, ελέγχει την Presence Claim και παράγει την AT.

Η AT περιέχει:
1. Ένα geohash με αξιολόγηση ακρίβειας από όσους έχουν ελέγξει την τοποθεσία του prover.
2. Αναφορά στην Zone Authority που εξέδωσε την Presence Claim.
3. Αναφορά στην Presence Claim.
4. Μία υπολογιστική απόδειξη της ορθότητας της Presence Claim.

Σε περίπτωση σωστής λειτουργίας τους, οι συμμετέχοντες στις Zones καθώς και οι verifiers μοιράζονται την αμοιβή του prover.

Εκτός από την αμοιβή του prover, οι συμμετέχοντες που λειτουργούν σωστά, συμμετέχουν στη διαδικασία εξόρυξης (mining) νέων tokens που εισέρχονται στο σύστημα.

Vproof [69]

Στο έργο αυτό αναπτύσσεται ένα πρωτόκολλο απόδειξης τοποθεσίας για εφαρμογή σε Συστήματα Έξυπνων Μετακινήσεων (Intelligent Transportation System - ITS).

Τα συστήματα αυτά βασίζονται σε αναφορές οδηγών για την κίνηση στους δρόμους ή για έργα που εκτελούνται. Αν οι οδηγοί αυτοί αναφέρουν ψευδή γεγονότα για τοποθεσίες στις οποίες δεν έχουν υπάρξει, τότε θέτουν σε κίνδυνο τη λειτουργία του συστήματος.

Οι συγγραφείς προτείνουν ένα σύστημα κατά το οποίο ο χρήστης καταγράφει τις μεταβολές της λαμβανόμενης ισχύος σήματος – RSS (Received Signal Strength) καθώς ο χρήστης οδηγεί σε ένα δρόμο εφοδιασμένο με πλευρικές μονάδες εκπομπής – RSU (Road Side Units). Με αυτόν τον τρόπο εμποδίζεται ένας στατικός παρατηρητής από το να καταγράψει τα εκπεμπόμενα δεδομένα και να προσφέρει σε κάποιον άλλο την απόδειξη της τοποθεσίας. Μόνο αν ο χρήστης έχει πράγματι οδηγήσει στη συγκεκριμένη διαδρομή θα είναι δυνατόν να έχει παρατηρήσει τις μεταβολές αυτές.

Σε μία βάση δεδομένων έχουν αποθηκευτεί από πριν οι πιθανές κυματομορφές που θα καταγράψει ο χρήστης οδηγώντας κοντά σε ένα σταθμό εκπομπής, για κάθε πιθανή τροχιά που μπορεί αυτός να ακολουθήσει!

Αυτό σημαίνει ότι για M σταθμούς εκπομπής και για N τροχιές κοντά σε κάθε σταθμό, απαιτούνται M*N καταγραφές, πριν το σύστημα τεθεί σε λειτουργία.

Ο σταθμός που βρίσκεται στην άκρη του δρόμου στέλνει πακέτα με τυχαία ενέργεια, σε καθένα από τα οποία τοποθετεί κρυπτογραφημένα το επίπεδο ενέργειας που χρησιμοποίησε. Ο χρήστης λαμβάνει τα πακέτα και τα αποστέλλει στο server. Ο server αποκρυπτογραφεί τα επίπεδα ενέργειας για να ανακατασκευάσει την κυματομορφή που θα λάμβανε ο χρήστης αν τα πακέτα είχαν αποσταλεί με μέγιστη ενέργεια από το σταθμό. Συγκρίνει αυτή την κυματομορφή με αυτές που έχει στη βάση δεδομένων, για να συμπεράνει αν ο χρήστης κινήθηκε πράγματι κοντά από τον συγκεκριμένο σταθμό.

Για να ανιχνεύσει τις ψευδείς αναφορές τοποθεσίας, το πρωτόκολλο απαιτεί κάθε φορά που ο prover θέλει να στείλει μία AT, να στέλνει και όλες τις προηγούμενες μέχρι την τελευταία υποβολή που έκανε στον verifier. Αυτό το χαρακτηριστικό μπορεί αφενός να μην τηρείται από τους χρήστες, ενώ αν τηρείται θέτει σε κίνδυνο την ιδιωτικότητα της τοποθεσίας του.

Αρνητικά:

- Απαιτείται ο χρήστης να κινείται κοντά σε ειδικά διαμορφωμένους σταθμούς εκπομπής.
- Απαιτείται εγκατάσταση επιπλέον υποδομής.
- Μπορεί κάποιος με ένα jammer να μπλοκάρει τα σήματα του πλευρικού σταθμού καθιστώντας το σύστημα άχρηστο.
- Οι πλευρικοί σταθμοί εκπομπής ελέγχονται από κεντρικοποιημένη αρχή.

APPLAUS [49]

Σύμφωνα με τους συγγραφείς, η ανάγκη για απόδειξη τοποθεσίας δημιουργείται σε τρεις βασικές περιπτώσεις. Πρώτον, όταν δίνεται κάποιο προνόμιο σε κάποιον που βρίσκεται σε μία συγκεκριμένη τοποθεσία. Δεύτερον, για μεγαλύτερη ασφάλεια στον εντοπισμό τοποθεσίας, καθώς θα μπορούσε κάποιος τρίτος σκόπιμα να προκαλέσει πρόβλημα στο σύστημα εντοπισμού τοποθεσίας. Τρίτον, για επιβεβαίωση της ειλικρίνειας του χρήστη.

Στην πρώτη ομάδα ανήκουν περιπτώσεις όπως πρόσβαση σε ορισμένες πληροφορίες με βάση την τοποθεσία, ή η απόδειξη προς την ασφαλιστική εταιρεία ότι δεν βρισκόταν ο πελάτης της στο χώρο του ατυχήματος τη δεδομένη χρονική στιγμή.

Στη δεύτερη ομάδα ανήκουν περιπτώσεις όπου η επιβεβαίωση της τοποθεσίας είναι πιο χρήσιμη για τον ίδιο το χρήστη, ο οποίος μπορεί να έχει πέσει θύμα κάποιου επιτιθέμενου που θέλει να τον κατευθύνει εκεί που αυτός θέλει.

Στην τρίτη ομάδα ανήκουν περιπτώσεις που κυμαίνονται από έναν απλό διαμοιρασμό της τοποθεσίας του χρήστη σε ένα κοινωνικό δίκτυο μέχρι και την επιβεβαίωση της τοποθεσίας ενός υπόπτου από την Αστυνομία κατά τη διάρκεια ενός εγκλήματος.

Σχετικά με τις μεθόδους εντοπισμού τοποθεσίας που βασίζονται στο δίκτυο, οι συγγραφείς εντοπίζουν πως οι πάροχοι κινητής τηλεφωνίας μπορούν να επιβεβαιώσουν την τοποθεσία των χρηστών τους, ωστόσο η ακρίβεια είναι μη ικανοποιητική και επιπλέον δεν γίνεται να επιβεβαιωθεί το ιστορικό τοποθεσίας ενός χρήστη.

Το APPLAUS χρησιμοποιεί ψευδώνυμα για τον κάθε χρήστη, τα οποία αλλάζουν συνεχώς, ώστε να διαφυλάξει την ανωνυμία τους. Η χρήση ψευδωνύμων συμβάλλει στην ανωνυμία, ωστόσο καθιστά πιο εύκολη τη χρήση του ίδιου ψευδωνύμου (προσωρινής ταυτότητας) από συνεργαζόμενους provers.

Ο location proof server κρατάει τα ζεύγη [τοποθεσία, ψευδώνυμο] ενώ η CA κρατάει τα ζεύγη [ψευδώνυμα, ταυτότητα χρήστη]. Ο LP server στέλνει τα hash των τοποθεσιών στην CA, την οποία και ο verifier ρωτά. Αν κάποιος αποκτήσει πρόσβαση στον LP server και την CA ή αν αυτοί συνεργαστούν τότε η ανωνυμία του συστήματος καταρρίπτεται.

Ένα αρνητικό είναι πως ο verifier ρωτά την CA δίνοντας το hash της τοποθεσίας και την ταυτότητα του prover. Αυτό σημαίνει ότι ο verifier πρέπει να γνωρίζει εκ των προτέρων σε ποια τοποθεσία αναμένεται να είναι ο χρήστης.

Οι συγγραφείς του STAMP [56] αναφέρονται στα εξής αρνητικά του APPLAUS:

1. Τα ψευδώνυμα που αλλάζουν συμβάλλουν σε υπολογιστικό φόρτο.
2. Το σύστημα ψευδωνύμων που χρησιμοποιεί απαιτεί από τον prover να στέλνει αποδείξεις τοποθεσίας ανά τακτά χρονικά διαστήματα, ώστε να εμφανίζεται με διαφορετικά ψευδώνυμα και να μην μπορεί κάποιος κακόβουλος να συσχετίσει τα ψευδώνυμα με την αληθινή του ταυτότητα. Ακόμα και αν δεν υπάρχουν γειτονικά witnesses, ο

prover πρέπει να υποβάλλει στον LP server μία άδεια (dummy) AT. Οι άδειες AT επιβαρύνουν επιπλέον το σύστημα.
3. Για να εντοπίσει πιθανές συνεργασίες, απαιτείται να στέλνονται οι AT στον server αμέσως αφού δημιουργηθούν. Αυτό παραβιάζει την ιδιοκτησία AT και απαιτεί από τον prover να έχει σύνδεση στο διαδίκτυο.

PROPS [47]

Το PROPS παρέχει αρκετές πληροφορίες σχετικά με τους κακόβουλους χρήστες και τις επιθέσεις στα πρωτόκολλα απόδειξης τοποθεσίας.

Οι κακόβουλοι χρήστες που προσδιορίζονται είναι οι εξής:
1. Υποκλοπή της ταυτότητας των χρηστών από κάποιον κακόβουλο χρήστη που κρυφακούει.
2. Ένας prover ο οποίος θέλει να παρουσιάσει ψεύτικο πιστοποιητικό, χωρίς να βρίσκεται πράγματι στη ζητούμενη τοποθεσία. Είτε παρουσιάζει ψεύτικη πληροφορία στον verifier σχετικά με την τοποθεσία του, είτε αλλάζει τις επιβεβαιώσεις που δέχεται από τους μάρτυρες.
3. Ένας verifier ο οποίος προσπαθεί να αποκτήσει περισσότερη πληροφορία για τον prover, ή χρησιμοποιεί τα πιστοποιητικά σαν να εκδόθηκαν για αυτόν.
4. Ένας μάρτυρας που είτε δίνει λάθος βεβαιώσεις στον prover, είτε συνεργάζεται με τον prover για να του εκδώσει περισσότερες από μία βεβαιώσεις.
5. Συνεργασία μεταξύ δύο provers (terrorist fraud). Ένας prover συνεργάζεται με κάποιον άλλον prover, ώστε να εκδώσει AT για λογαριασμό του.

Οι συγγραφείς αναφέρουν πως το πρόβλημα της συνεργασίας μεταξύ πολλών (unbounded size) κακόβουλων χρηστών είναι πολύ δύσκολο να λυθεί χωρίς την αποθήκευση των AT σε κάποια Τρίτη Έμπιστη Οντότητα (π.χ. location proof server στο APPLAUS).

Εντοπίζονται επιπλέον τα παρακάτω είδη επιθέσεων:
- Distance fraud: Ένας κακόβουλος prover προσπαθεί να πείσει ένα ειλικρινή witness ότι βρίσκεται πιο κοντά του από ότι στην πραγματικότητα.
- Mafia fraud (man in the middle): Ο στόχος του επιτιθέμενου είναι να αναπαράγει μια συνεδρία που περιλαμβάνει έναν ειλικρινή P και έναν ειλικρινή W, με σκοπό να εξαπατήσει τον W ότι ο P βρίσκεται πράγματι κοντά του.
- Distance hijacking: Ένας κακόβουλος χρήστης M προσπαθεί να υποκλέψει μία συνεδρία ενός ειλικρινούς prover P. Ο M περιμένει από τον P να επιβεβαιώσει ότι γειτνιάζει με τα witnesses W_i, και έπειτα προσπαθεί να υποκλέψει από αυτόν τα LPS που συλλέγει.

Στο PROPS τα witnesses χρησιμοποιούν Μοναδική Ομαδική Υπογραφή (Unique Group Signature). Κάθε μέλος μίας ομάδας μπορεί να υπογράψει ένα μήνυμα χρησιμοποιώντας μία ομαδική υπογραφή. Δεν μπορεί κάποιος να προσδιορίσει την ταυτότητα του χρήστη που υπέγραψε ένα μήνυμα, εκτός αν διαθέτει ειδικό κλειδί (opening key).

Το κλειδί αυτό διαθέτει ο Ανυψωτής Ανωνυμίας – AL (Anonymity Lifter). Αυτή είναι μία τρίτη έμπιστη οντότητα που έχει τη δυνατότητα να αποκρυπτογραφήσει προσωπικά στοιχεία των χρηστών που συμμετέχουν στη δημιουργία μιας AT, αν για παράδειγμα απαιτηθεί από το Νόμο. Αν και αυτό το χαρακτηριστικό μπορεί να φανεί πολύ χρήσιμο, θα μπορούσε να θέσει σε κίνδυνο την ιδιωτικότητα των χρηστών αν χρησιμοποιούνταν χωρίς να υπάρχει νόμιμη οδηγία ή από κάποιον κακόβουλο που απέκτησε πρόσβαση.

Το PROPS χρησιμοποιεί επίσης Αρχή Πιστοποίησης μόνο για την εγγραφή των χρηστών, η οποία μπορεί να αποτελέσει μοναδικό σημείο αποτυχίας μόνο στην περίπτωση που κάποιος χρήστης δεν είναι ήδη εγγεγραμμένος στο σύστημα. Επιπλέον, η CA είναι υπεύθυνη για το διαμοιρασμό των δημοσίων κλειδιών των χρηστών στον AL, πράγμα που σημαίνει ότι οι χρήστες δεν μπορούν να είναι βέβαιοι για το ποιος μπορεί να έχει πρόσβαση στα προσωπικά τους δεδομένα.

STAMP [56]

Οι συγγραφείς πιστεύουν πως το να βασιστούμε σε WiFi APs δεν μπορεί να έχει εφαρμογή πάντα, όπως για παράδειγμα σε απομακρυσμένες περιοχές ή στο πεδίο μιας μάχης. Γι' αυτό το STAMP σχεδιάζεται κατανεμημένα, για χρήση μακριά από έμπιστο εξοπλισμό (π.χ. trusted witness).

Για να αντιμετωπίσει τη συνεργασία P-W, χρησιμοποιεί σχήμα εμπιστοσύνης βασισμένο στην εντροπία (entropy-based trust model) με σκοπό τον εντοπισμό συνεργασιών. Αυτή τη διαδικασία αναλαμβάνει η CA, η οποία παρέχει και τα κλειδιά στους χρήστες του συστήματος.

Επίσης, υπάρχει η σκέψη να εντοπίζονται ανωμαλίες, αν για παράδειγμα κάποιος χρήστης φαίνεται να έχει μετακινηθεί κατά μία μεγάλη απόσταση σε μικρό χρονικό διάστημα. Ωστόσο, αυτή η τεχνική προϋποθέτει να στέλνει ο χρήστης περιοδικά την τοποθεσία του, κάτι που δεν είναι επιθυμητό. Μόνο όταν υπάρχει λόγος θα πρέπει ο χρήστης να μπορεί να εκδώσει βεβαίωση τοποθεσίας.

Τέλος, όπως άλλα πρωτόκολλα, θεωρεί ότι οι χρήστες δε θα δώσουν τη συσκευή τους ή τα κλειδιά τους σε άλλους. Αυτό όμως μπορεί να γίνει σκόπιμα στο πλαίσιο συνεργασίας.

Blockchain PoL [67]

Χρησιμοποιεί blockchain στο οποίο αποθηκεύονται οι αποδείξεις τοποθεσίας.

Η αποκεντρωμένη φύση των peer-to-peer δικτύων εξασφαλίζει μεγαλύτερα επίπεδα ιδιωτικότητας, καθώς αφαιρεί την ανάγκη για μια κεντρική αρχή (certificate authority) η οποία γνωρίζει την ταυτότητα και την τοποθεσία του χρήστη, καθώς και τα δεδομένα που αυτός ανταλλάσσει.

Χωρίζουν τις προτεινόμενες λύσεις σε δύο κατηγορίες:

- Εξαρτώμενες από εξοπλισμό, όπου η τοποθεσία των χρηστών επιβεβαιώνεται από σημεία πρόσβασης WiFi ή κεραίες δικτύων κινητής τηλεφωνίας.
- Μη Εξαρτώμενες από εξοπλισμό, όπου η τοποθεσία των χρηστών επιβεβαιώνεται από γειτονικούς κόμβους.

Φυσικά, υπάρχουν και υβριδικές λύσεις, οι οποίες συνδυάζουν σταθερούς κόμβους αναφοράς με γνωστή τοποθεσία και έμπιστη συμπεριφορά καθώς και γειτονικούς κόμβους.

Οι συγγραφείς υποστηρίζουν ότι δεν μπορεί κάποιος να δηλώσει ψευδή τοποθεσία, αφού γίνεται έλεγχος αν η τοποθεσία είναι μέσα στην εμβέλεια του πρωτοκόλλου επικοινωνίας. Ωστόσο, εφόσον δεν γίνεται έλεγχος εγγύτητας θα μπορούσε κάποιος prover να αναμεταδίδει το σήμα του ώστε να φαίνεται πιο κοντά στο witness.

Σε ένα περιβάλλον blockchain, όλες οι «συναλλαγές», στην περίπτωσή μας οι AT μπορούν και πρέπει να ελεγχθούν από όλους τους κόμβους. Για το λόγο αυτό, προτείνεται η χρήση διαφορετικών ταυτοτήτων από κάθε χρήστη, προκειμένου να διασφαλίζεται η ανωνυμία του.

Ωστόσο, με μία τέτοια υλοποίηση δεν μπορεί να μετρηθεί η αξιοπιστία των χρηστών με μοντέλα εμπιστοσύνης. Επίσης, είναι δυσκολότερο να παρατηρηθούν συνεργασίες μεταξύ των συμμετεχόντων στο σύστημα. Έχουμε λοιπόν να κάνουμε με ισορροπία (tradeoff) ανάμεσα σε ανωνυμία και εμπιστοσύνη.

Επιπλέον, στο πρωτόκολλο αυτό, για να δημιουργηθεί συμφωνία στο blockchain, ορίζεται πως το επόμενο block προστίθεται στο blockchain από το χρήστη που έλαβε τις περισσότερες ΑΤ στα τελευταία Τ blocks. Τα τελευταία Τ blocks δεν μπορούν να περιέχουν πάνω από ένα block που προστέθηκε από τον ίδιο χρήστη. Η μέθοδος αυτή ονομάζεται proof-of-stake. Η χρήση ψευδωνύμων όμως δυσκολεύει την εφαρμογή της μεθόδου αυτής, καθώς οι χρήστες αλλάζουν συνεχώς ταυτότητες.

Alice in Wonderland [57]

Το πρωτόκολλο αυτό βασίζεται σε δύο τεχνικές.

- Η πρώτη είναι η **παρακολούθηση των Πληροφοριών Κατάστασης Καναλιού** (Channel State Information - CSI) ενός δικτύου WiFi, που βρίσκεται κοντά στον κόμβο που θέλει να εκδώσει απόδειξη τοποθεσίας.
- Η δεύτερη τεχνική ονομάζεται **Fuzzy Vault** και επιτρέπει σε έναν κόμβο Α να κρύψει κάποιες πληροφορίες από ένα σύνολο δεδομένων. Ένας άλλος κόμβος Β μπορεί να ανακτήσει αυτή την πληροφορία μόνο αν το δικό του σύνολο δεδομένων ταιριάζει σε κάποιο ικανοποιητικό βαθμό με το σύνολο του κόμβου Α.

Σκοπός δεν είναι να προσδιορίσει την ακριβή θέση του χρήστη, αλλά να αποδείξει ότι ο χρήστης βρίσκεται όντως κοντά στο AP. Αφορά την εκτίμηση της τοποθεσίας του χρήστη σε εσωτερικό χώρο, όπου δεν υπάρχει κάλυψη GPS.

Περισσότερο ένα πρωτόκολλο ασφαλούς εύρεσης τοποθεσίας (secure localization), αντιμετωπίζει ορισμένες επιθέσεις (π.χ. MITM attack) με τη χρήση χρόνου απόκρισης, ώστε να εντοπίζει ενδιάμεσο κόμβο σε περίπτωση που ο χρόνος αυτός είναι μεγάλος. Ωστόσο, δεν ανταποκρίνεται καλά σε απαιτήσεις ιδιωτικότητας καθώς και στην απάτη απόστασης. Ένας επιτιθέμενος θα μπορούσε να χρησιμοποιεί αναμεταδότη ώστε να εξαπατήσει το AP ότι βρίσκεται πιο κοντά σε αυτό από ότι στην πραγματικότητα. Επίσης, η ταυτοποίηση του χρήστη γίνεται μόνο με το πρώτο μήνυμα, το οποίο περιέχει την υπογραφή του. Αν καταφέρει κάποιος να αποκτήσει αυτό το μήνυμα και να το προωθήσει στο witness (Access Point) θα μπορέσει να λάβει ΑΤ για λογαριασμό άλλου χρήστη.

Location Based Handshake [66]

Επιτρέπει στο χρήστη να βρει από ένα σύνολο κόμβων εκείνους που βρίσκονται κοντά του, με τη βοήθεια ημι-εμπιστευόμενου εξυπηρετητή (semi-trusted server). Η τοποθεσία του χρήστη δε γίνεται γνωστή ούτε στον server, ούτε σε άλλους χρήστες που βρίσκονται εκτός της γειτονιάς του χρήστη.

Το πρωτόκολλο δεν επικεντρώνεται τόσο στην δημιουργία μιας ΑΤ, αλλά στον εντοπισμό γειτονικών κόμβων. Ο χρήστης που αναζητά άλλους λειτουργεί ως verifier, που καλείται να επιβεβαιώσει ότι ορισμένοι κόμβοι βρίσκονται πράγματι κοντά του. Οι υπόλοιποι χρήστες δρουν ως provers, οι οποίοι καλούνται να αποδείξουν τη γειτνίασή τους με τον verifier. Για να το επιτύχουν αυτό, πρέπει να παρουσιάσουν μία χωροχρονική ετικέτα τοποθεσίας.

Η χωροχρονική ετικέτα τοποθεσίας (spatial-temporal location tag) είναι μία συλλογή σημάτων που παρατηρούνται σε μία συγκεκριμένη περιοχή, ένα συγκεκριμένο χρονικό διάστημα. Δημιουργείται από τα σήματα που προέρχονται από το περιβάλλον του χρήστη, όπως WiFi και LTE.

Οι χρήστες-provers συλλέγουν τα location tags του περιβάλλοντος και τα συγκρίνουν με αυτό του verifier με διαδικασία ιδιωτικού ταιριάσματος (private matching).

Με τον τρόπο αυτό επιτυγχάνεται ο έλεγχος γειτνίασης (proximity test) μεταξύ ενός χρήστη (verifier) και πολλών άλλων (provers) ταυτόχρονα. Υπό το πρίσμα αυτό, **δεν υφίσταται η έννοια του witness**.

Για να εντοπιστούν κακόβουλοι χρήστες, κάθε prover ενσωματώνει στα μηνύματά του και όλους τους άλλους provers που βλέπει στη γειτονιά του. Ο server συσχετίζει τους κόμβους που βλέπει κάθε prover και δημιουργεί ένα γράφο, ανιχνεύοντας έτσι provers που ψεύδονται.

Η βασική ιδέα είναι ότι ο verifier δημιουργεί ένα προσωρινό ζεύγος ιδιωτικού/δημόσιου κλειδιού. Οι provers μπορούν να βρουν το δημόσιο κλειδί του verifier μόνον αν έχουν παρόμοιο location tag, δηλαδή αν βρίσκονται κοντά του. Με αυτό τον τρόπο αποφεύγεται η πολυπλοκότητα της διαχείρισης κλειδιών, αφού δεν χρησιμοποιούνται εκ των προτέρων γνωστά κλειδιά – PSK (Pre-shared Keys).

Οι ετικέτες τοποθεσίας πρέπει να διέπονται από δύο χαρακτηριστικά:

1. Αναπαραγωγιμότητα: Δύο ετικέτες που έχουν συλλεχθεί από γειτονικούς κόμβους πρέπει να έχουν μεγάλο ποσοστό ομοιότητας.
2. Μη προβλεψιμότητα: Ένας κακόβουλος χρήστης που δεν βρίσκεται στη ζητούμενη τοποθεσία τη συγκεκριμένη χρονική στιγμή, δεν μπορεί να δημιουργήσει παρόμοια ετικέτα τοποθεσίας.

Για να επιτευχθούν τα παραπάνω είναι απαραίτητο να επιλεχθούν χαρακτηριστικά σημάτων που παρουσιάζουν υψηλή τυχαιότητα (εντροπία) και να μεταβάλλονται με το χρόνο.

Για το πρωτόκολλο αυτό ως Στάδιο Α θεωρείται η δημιουργία των location tags από τους provers και η σύγκριση αυτών με το location tag του verifier, προκειμένου να αποκτήσουν το προσωρινό δημόσιο κλειδί του verifier αν και μόνο αν γειτνιάζουν με αυτόν. Ως Στάδιο Β θεωρείται η υποβολή των τοποθεσιών των provers στον server και η επαλήθευση της γειτνίασής τους με τον verifier.

Ένα αρνητικό του πρωτοκόλλου είναι πως οι χρήστες πρέπει να έχουν σύνδεση με τον server κατά τη διαδικασία εύρεσης γειτόνων.

Επίσης, τόσο τα location tags όσο και οι τοποθεσίες σε κωδικοποίηση location grid τοποθετούνται σε bloom filters, τα οποία ως γνωστόν υποφέρουν από ψευδώς θετικές απαντήσεις (false positives). Αυτό σημαίνει πως υπάρχει πάντα η πιθανότητα ένας prover να εμφανίζεται ως γείτονας του verifier χωρίς να είναι.

CLIP [78]

Μία αλληλουχία παλαιών σημείων τοποθεσίας ενός χρήστη στις αντίστοιχες χρονικές στιγμές ονομάζεται **Ίχνος κινητικότητας του χρήστη**.

Ένα ίχνος κινητικότητας περιέχει n σημεία τοποθεσίας για n χρονικά διαστήματα, όπου n>1.

Οι συγγραφείς αναφέρουν πως είναι δυνατόν να παραχθούν AT με χρήση έμπιστου (trusted) hardware, όπως για παράδειγμα το “Trusted Platform Module (TPM)”. Αυτό είναι ένα έμπιστο κομμάτι υλικού που αναλαμβάνει να υπογράψει την τοποθεσία που παρέχει ο αισθητήρας GPS. Μια τέτοια υλοποίηση έχει μεγάλο κόστος και εισάγει υπολογιστικό φόρτο και καθυστέρηση.

Επίσης, υποστηρίζουν πως δεν υπάρχει άλλο πρωτόκολλο ικανό να παρέχει συνεχείς AT καθώς ο χρήστης κινείται (continuous location provenance).

Στην πρώτη φάση, το πρωτόκολλο απαιτεί από τον prover να επιλέξει τον προορισμό του και να προβλέψει το ίχνος κινητικότητάς του, είτε βασιζόμενος σε οδικούς χάρτες και πληροφορίες μέσων μεταφοράς, είτε κατασκευάζοντας μια πιθανολογική εκτίμηση. Η πρόβλεψη του ίχνους πρέπει να υποβληθεί σε ένα γειτονικό έμπιστο σημείο πρόσβασης (Trusted Access Point). Η απαίτηση αυτή καθιστά το πρωτόκολλο δύσχρηστο, καθώς ο χρήστης οφείλει να γνωρίζει εκ των προτέρων τη διαδρομή που θα ακολουθήσει, η μία εκτίμηση αυτής. Επιπλέον, απαιτεί να υπάρχει ένα διαθέσιμο Trusted Access Point κοντά στο σημείο έναρξης της διαδρομής του prover.

Ιδιαίτερα στην περίπτωση που η διαδρομή που θα ακολουθήσει ο χρήστης βασίζεται σε πιθανολογική εκτίμηση, το πρωτόκολλο εισάγει επιπλέον υπολογιστικό φόρτο στη συσκευή του prover.

Enabling New Mobile Applications with Location Proofs [46]

Στο πρωτόκολλο αυτό, ο prover συλλέγει ΑΤ από WiFi access points ή κεραίες κινητής τηλεφωνίας που είναι έμπιστα από τον verifier.

Όταν ο prover αποκτήσει μία ΑΤ από κάποια συσκευή (π.χ. WiFi access point), θεωρείται πως βρισκόταν εντός της εμβέλειας της. Έτσι, το WiFi μπορεί να χρησιμοποιηθεί για μικρότερη εμβέλεια (της τάξης των 100 μέτρων), ενώ οι κεραίες κινητής τηλεφωνίας για μεγαλύτερη (της τάξης ορισμένων χιλιομέτρων). Η έρευνα επικεντρώνεται στα WiFi Access Points.

Ένα ζήτημα που θίγεται είναι η ανάγκη για χειροκίνητο ορισμό της τοποθεσίας των WiFi Access Points, τα οποία λειτουργούν ως witnesses. Αυτά ενσωματώνουν την τοποθεσία τους στα ΤΑΤ που στέλνουν στον prover. Όμως, επειδή τα APs τοποθετούνται συνήθως σε εσωτερικό χώρο, η ακριβής τους τοποθεσία είναι δύσκολο να προσδιοριστεί με ακρίβεια. Οι συγγραφείς προτείνουν την εύρεση της τοποθεσίας τους από τον πλησιέστερο σε αυτά εξωτερικό χώρο, με τη βοήθεια GPS.

Μία επιπλέον δυσκολία παρουσιάζεται στην περίπτωση που κάποιο AP πρέπει να μετακινηθεί. Οι συγγραφείς προτείνουν τον εντοπισμό της κίνησης με αισθητήρες επιτάχυνσης. Όταν ανιχνευτεί ότι το AP μετακινήθηκε, τότε ο χειριστής θα πρέπει να ρυθμίσει ξανά τη νέα τοποθεσία.

Οι συγγραφείς τονίζουν πως οι witnesses έχουν τη δυνατότητα να παρακολουθούν τους χρήστες, αν το επιθυμούν. Το γεγονός αυτό μπορεί να θέσει σε κίνδυνο την ιδιωτικότητα των χρηστών, αν οι witnesses ναι μεν συμπεριφέρονται σωστά αλλά είναι «περίεργοι» να μάθουν περισσότερα για τους provers (honest but curious).

Στη δημοσίευση αυτή αναλύεται περισσότερο από κάθε άλλη το ζήτημα των ισχυρών ταυτοτήτων. Συγκεκριμένα, οι συγγραφείς αναζητούν έναν τρόπο να επιβεβαιωθεί ότι στην τοποθεσία που αναφέρει η ΑΤ βρίσκεται ο ιδιοκτήτης της συσκευής και όχι απλά η συσκευή του.

Για να επιλύσουν το πρόβλημα αυτό, προτείνουν την εφαρμογή διαδικασίας πρόκλησης-απάντησης (challenge-response) ανάμεσα στον prover και το AP.

Για παράδειγμα, το AP στέλνει στον prover έναν τυχαίο αριθμό (nonce). Ο χρήστης καλείται να βγάλει μια φωτογραφία στην οποία να φαίνεται το πρόσωπό του καθώς και ένα χαρτί στο οποίο έχει γράψει τον τυχαίο αριθμό. Η φωτογραφία αυτή ενσωματώνεται στην ΑΤ και στέλνεται στη συνέχεια στον verifier. Η μέθοδος αυτή δεν παρέχει απόλυτη βεβαιότητα, καθώς ένας κακόβουλος χρήστης μπορεί να χρησιμοποιήσει μία παλαιότερη φωτογραφία στην οποία προσθέτει τον τυχαίο αριθμό με χρήση προγράμματος επεξεργασίας εικόνας.

Οι συγγραφείς προτείνουν μία δεύτερη μέθοδο. Το AP στέλνει μία πρόταση ως πρόκληση στον prover. Ο χρήστης πρέπει να ηχογραφήσει τον εαυτό του να διαβάζει την πρόταση αυτή. Και σε αυτή την περίπτωση μπορεί να εφαρμοστεί επεξεργασία φωνής ώστε ένας τρίτος να παρουσιάζει τη φωνή του ως αυτή του ιδιοκτήτη της συσκευής. Επίσης, είναι δυνατόν να

έχουν προηχογραφηθεί οι λέξεις, όμως στη συνένωσή τους το αποτέλεσμα θα είναι φανερά αφύσικο.

Στις παραπάνω περιπτώσεις πρέπει να λαμβάνεται υπόψη η περίπτωση που ένας τρίτος, ο οποίος έχει στα χέρια του τη συσκευή του νόμιμου χρήστη, μεταβιβάζει σε αυτόν τις προκλήσεις του AP και λαμβάνει τις απαντήσεις, λειτουργώντας ως ενδιάμεσος (man-in-the-middle). Για την αντιμετώπιση της περίπτωσης αυτής, είναι δυνατόν να τίθενται χρονικοί περιορισμοί μεταξύ της πρόκλησης και της απάντησης.

Proving Your Location Without Giving up Your Privacy [48]

Οι συγγραφείς χωρίζουν τις ΑΤ σε δύο κατηγορίες:

- Αντιδραστική ΑΤ (Retroactive Location Proof): Παράγεται από τον prover μετά από αίτημα ενός συγκεκριμένου verifier.
- Προληπτική ΑΤ (Proactive Location Proof): Ένας prover κατασκευάζει μια ΑΤ χωρίς να του ζητηθεί, με δυνατότητα να τη χρησιμοποιήσει μελλοντικά για να επιβεβαιώσει την τοποθεσία του. Ο verifier στον οποίο απευθύνεται μπορεί να μην είναι γνωστός εκ των προτέρων.

Ιδιαίτερα σημαντική είναι η δυνατότητα να παράγει ο χρήστης ΑΤ προληπτικά, πριν του ζητηθούν από κάποιον verifier.

Αυτό έχει τις εξής δυσκολίες:

- Οι witnesses μπορούν να παρακολουθούν τον prover χωρίς να υπάρχει ανάγκη να επιβεβαιωθεί η τοποθεσία του από κάποιον.
- Διαφορετικές εφαρμογές έχουν διαφορετικές απαιτήσεις ως προς την ακρίβεια της τοποθεσίας που περιλαμβάνεται στην ΑΤ. Θα μπορούσαν όλες οι ΑΤ να περιλαμβάνουν την τοποθεσία με τη μεγαλύτερη δυνατή ακρίβεια. Τότε όμως ο verifier πιθανόν να μάθαινε περισσότερη πληροφορία από όση είναι απαραίτητη.
- Πρέπει να δημιουργηθεί ένα γενικό σχήμα ΑΤ, ανεξάρτητα από εφαρμογή- verifier (Application-Agnostic Location Proof). Δε θα πρέπει να περιλαμβάνονται σε αυτές πληροφορίες που αφορούν συγκεκριμένους verifiers (π.χ. δημόσιο κλείδί). Το στοιχείο αυτό είναι προϋπόθεση για την πλήρη υποστήριξη προληπτικών ΑΤ.

LINK

Οι συγγραφείς δίνουν μεγαλύτερη βαρύτητα στο μοντέλο εμπιστοσύνης μεταξύ των συμμετεχόντων, παρά στο σύστημα Αποδείξεων Τοποθεσίας.

Στο πρωτόκολλο αυτό, όλοι οι provers είναι εγγεγραμμένοι σε μία Τρίτη Έμπιστη Οντότητα, την Τοπική Αρχή Πιστοποίησης (Location Certificate Authority - LCA). Αυτή είναι υπεύθυνη να παραλάβει τα ΤΑΤ, να ελέγξει την εγκυρότητά τους καθώς και την αξιοπιστία των witnesses που τα υποβάλλουν και αναλόγως να εγκρίνει ή να απορρίψει την ΑΤ.

Η LCA είναι υπεύθυνη να μεταβιβάσει την απόφασή της στον πάροχο των υπηρεσιών τοποθεσίας (verifier).

Το πρωτόκολλο απαιτεί την επικοινωνία του prover με τον verifier και την LCA κατά τη δημιουργία της ΑΤ, κάτι που μπορεί να μην είναι πάντα εφικτό. Παράλληλα, κάθε ΑΤ που παράγεται απευθύνεται σε συγκεκριμένο verifier, καθιστώντας έτσι αδύνατη την υποστήριξη verifier-agnostic ΑΤ.

Δεν λαμβάνονται υπόψη σημαντικές προδιαγραφές ασφαλείας σχετικά με την ανοχή σε επιθέσεις (distance fraud, mafia fraud, distance hijacking).

Η LCA διαδραματίζει το σημαντικότερο ρόλο στο σύστημα, καθώς εφαρμόζει το μοντέλο εμπιστοσύνης που οι συγγραφείς έχουν αναπτύξει. Είναι υπεύθυνη για την παρακολούθηση

της συμπεριφοράς και του ιστορικού των χρηστών, καθώς και των μεταξύ τους σχέσεων (π.χ. κόμβοι που αλληλοβοηθούνται συχνά).

Η πληροφορία που συγκεντρώνει η LCA θέτει όμως σε κίνδυνο την ιδιωτικότητα των χρηστών. Συγκεκριμένα, η LCA γνωρίζει τόσο τις τοποθεσίες τους όσο και τις ταυτότητές τους. Το χαρακτηριστικό αυτό αποτελεί και το αδύναμο σημείο του πρωτοκόλλου.

Σημείωση: Στη δημοσίευση αυτή ως verifiers νοούνται οι witnesses των περισσότερων πρωτοκόλλων, ενώ ως Location-based Service νοείται ο verifier των περισσότερων πρωτοκόλλων.

Veriplace [1]

Οι συγγραφείς δίνουν βαρύτητα στην προστασία της ιδιωτικότητας των χρηστών (provers), καθώς και στην ανίχνευση χρηστών που προσπαθούν να εξαπατήσουν το σύστημα.

Η ανίχνευση χρηστών που εξαπατούν το σύστημα βασίζεται στο γεγονός πως ένας χρήστης δεν μπορεί να βρεθεί σε δύο απομακρυσμένες τοποθεσίες μεταξύ δύο κοντινών χρονικών στιγμών. Ωστόσο, το VeriPlace αποτυγχάνει να εντοπίσει απάτες που συμβαίνουν σε ένα μεγάλο χρονικό διάστημα. Συνεπώς, το πρωτόκολλο αυτό δεν προσφέρει υψηλό επίπεδο αντοχής σε απάτες, αλλά περισσότερο από άλλα πρωτόκολλα. Οι συγγραφείς προτείνουν πως οι υπηρεσίες τοποθεσίας μεγάλης αξίας (π.χ. πρόσβαση σε ιατρικά δεδομένα) θα πρέπει να εφαρμόζουν επιπλέον ασφάλεια, όπως πιστοποίηση των χρηστών (user authentication), και όχι απλά απόδειξης της τοποθεσίας.

Το πρωτόκολλο χρησιμοποιεί τρεις Έμπιστες Οντότητες:

1. Τρίτη Έμπιστη Οντότητα για τη διαχείριση πληροφορίας τοποθεσίας (Trusted Third Party for managing Location information - TTPL):
   Υπεύθυνη για την έκδοση των τελικών ΑΤ. Λαμβάνει την προσωρινή ΑΤ και αν το witness – Access Point είναι έγκυρο, τότε αντικαθιστά την ταυτότητά του με την τοποθεσία του. Επίσης, διατηρεί τις σχέσεις Ταυτότητα ΑΡ – Γεωγραφική Θέση ΑΡ και τις δημοσιεύει στο διαδίκτυο.
2. Τρίτη Έμπιστη Οντότητα για τη διαχείριση πληροφοριών χρήστη (Trusted Third Party for managing User information - TTPU):
   Αποθηκεύει την κρυπτογραφημένη τοποθεσία που σχετίζεται με τους provers.
3. Αρχή Εντοπισμού Απάτης (Cheating Detection Authority - CDA):
   Πραγματοποιεί έλεγχο χρηστών που συνεργάζονται.

Για να ζητήσει την έκδοση μίας ΑΤ, ο prover πρέπει να επικοινωνήσει πρώτα με την TTPU. Έπειτα, επικοινωνεί με το ΑΡ, το οποίο παρέχει μια προσωρινή ΑΤ. Αυτήν την παρουσιάζει ο prover στην TTPL, η οποία ελέγχει αν το ΑΡ είναι έμπιστο, και αντικαθιστά το ID του με την τοποθεσία του, στέλνοντας έτσι την τελική ΑΤ στον prover.

Η απαίτηση να επικοινωνεί ο prover με την TTPU προκειμένου να ζητήσει την έκδοση ΑΤ είναι αδύνατον να εκπληρωθεί σε απομακρυσμένες τοποθεσίες χωρίς πρόσβαση στο διαδίκτυο. Επιπλέον, υπομονεύει την ιδιωτικότητα του prover, καθώς οι πληροφορίες που αποστέλλονται μπορούν να εκθέσουν την τοποθεσία και την ταυτότητά του πριν αποκτήσει ΑΤ.

Το πρωτόκολλο χωρίζει τη γνώση της ταυτότητας και της τοποθεσίας ανάμεσα στις παραπάνω Έμπιστες Οντότητες. Αυτό έχει ως αποτέλεσμα να εκτίθενται προσωπικά δεδομένα των χρηστών, καθιστώντας το πρωτόκολλο αδύναμο ως προς την ανωνυμία.

OTIT [59]

Οι Αποδείξεις Τοποθεσίας είναι δυνατόν να αποθηκεύονται σε μία χρονολογική αλυσίδα, με βάση τη χρονική στιγμή που δημιουργήθηκαν. Έτσι, ένας verifier μπορεί να γνωρίζει τις διαδοχικές τοποθεσίες που επισκέφθηκε ο prover.

Το OTIT μοντελοποιεί την ασφαλή δημιουργία, αποθήκευση και επιβεβαίωση αλυσίδων AT. Οι συγγραφείς θέτουν ορισμένες προδιαγραφές και προτείνουν εναλλακτικές υλοποιήσεις που καλούνται να τις ικανοποιήσουν.

Οι βασικές προδιαγραφές που θέτουν είναι οι εξής:

1. Χρονολόγηση (Chronological): Οι AT θα πρέπει να εισάγονται στην αλυσίδα με τη σειρά που αποκτήθηκαν. Ένας κακόβουλος χρήστης θα πρέπει να μην μπορεί να δημιουργήσει ψευδείς αλυσίδες με διαφορετική σειρά.
2. Διατήρηση σειράς (Order Preserving): Η αλυσίδα αυτή, που βρίσκεται αποθηκευμένη στη συσκευή του prover, θα πρέπει να διατηρεί αναλλοίωτη τη σειρά των AT που περιέχει.
3. Επιβεβαιωσιμότητα (Verifiable): Ένας verifier πρέπει να μπορεί να επιβεβαιώσει τις AT που βρίσκονται μέσα στην αλυσίδα, καθώς και το ότι είναι τοποθετημένες με τη σωστή σειρά.
4. Εμφανής αλλοίωση (Tamper Evident): Οποιαδήποτε αλλοίωση προκαλείται στην αλυσίδα από τον prover ή από κάποιο τρίτο πρέπει να είναι εμφανής στο verifier.
5. Διατήρηση ιδιωτικότητας (Privacy Preserved): Ο prover έχει τον έλεγχο των πληροφοριών που αποκαλύπτει στον verifier. Όταν ο verifier λαμβάνει μια αλυσίδα AT, δεν αποκτά περισσότερη γνώση από το επίπεδο που έχει ορίσει ο prover.
6. Επιλεκτική ιδιωτικότητα αλυσίδας (Selective In-Sequence Privacy): Όσο ο prover συλλέγει AT, η αλυσίδα μεγαλώνει. Συνεπώς, θα πρέπει να έχει τη δυνατότητα να επιλέξει ποιο υποσύνολο της αλυσίδας (ποιες AT) θα παρουσιάσει στον verifier και ποιο θα μπορεί αυτός να «ανοίξει».
7. Ιδιωτική προστασία χρονολογίας (Privacy Protected Chronology): Αν ο prover επιλέξει να κρύψει ορισμένες AT από μία αλληλουχία στην αλυσίδα, τότε ο verifier θα πρέπει να μπορεί να δει την ύπαρξη των κρυμμένων AT, αλλά όχι το περιεχόμενό τους.
8. Ευκολία και παραγωγικότητα (Convenience and Derivability): Ο prover δεν πρέπει να επιβαρύνει τον verifier στέλνοντας μεγάλο όγκο δεδομένων. Αντιθέτως, πρέπει να αποστέλλει τα ελάχιστα απαραίτητα δεδομένα που χρειάζεται ο verifier για να συνδέσει τα κομμάτια της αλυσίδας και να εξάγει τα συμπεράσματά του.

Οι υλοποιήσεις που προτείνουν περιλαμβάνουν Hash Chains, Block Hash Chains, Bloom Filters, Shadow Hash Chains, Multi-Link Hash Chains, καθώς και RSA chaining. Αξίζει να σημειωθεί πως καμία από τις παραπάνω υλοποιήσεις δεν ικανοποιεί όλες τις προδιαγραφές που τίθενται.

Where have you been? [73]

Για την επιβεβαίωση της παρουσίας του prover σε μία τοποθεσία, το πρωτόκολλο χρησιμοποιεί τις τεχνικές distance-bounding. Δίνεται βαρύτητα στην διατήρηση μιας χρονολογικής αλυσίδας αποδείξεων τοποθεσίας, την οποία ο χρήστης δε θα μπορεί αν αλλοιώσει. Παράλληλα, θα πρέπει να είναι σε θέση να παρουσιάσει ένα μέρος της, ώστε να προστατεύσει την ιδιωτικότητά του.

Θίγεται επίσης η δυσκολία επιβεβαίωσης της χρονικής σειράς των Αποδείξεων Τοποθεσίας, καθώς κάθε μία μπορεί να προέρχεται από κόμβους με διαφορετικό ρολόι. Από την

άλλη, η χρήση ενός καθολικού ρολογιού για όλο το σύστημα δεν είναι κλιμακώσιμη (scalable) και αποτελεί Single Point of Failure.

Για τη διατήρηση της σειράς των ΑΤ μέσα στην αλυσίδα το πρωτόκολλο χρησιμοποιεί hash chains και Bloom filters.

Οι αλυσίδες ΑΤ μας ενδιαφέρουν στις περιπτώσεις όπου απαιτείται γνώση της διαδρομής ενός χρήστη-συσκευής και όχι απλά της παρουσίας του. Για παράδειγμα, αν θέλουμε να επιβεβαιώσουμε την προέλευση κρεάτων που μεταφέρονται με ένα φορτηγό, χρειάζεται να έχουμε γνώση της διαδρομής που το φορτηγό ακολούθησε, και όχι απλά της αφετηρίας του ή κάποιας ενδιάμεσης τοποθεσίας.

Το πρωτόκολλο χρησιμοποιεί επιπλέον των witnesses και την Αρχή Τοποθεσίας (Location Authority). Αυτή είναι υπεύθυνη για την παροχή ΑΤ για μια συγκεκριμένη τοποθεσία (μία περιοχή με ορισμένη επιφάνεια). Τα witnesses επιβεβαιώνουν (endorse) την παρουσία του prover υπό τη συγκεκριμένη Location Authority. Τόσο η Location Authority όσο και τα witnesses δεν θεωρούνται έμπιστα (not trustworthy).

Από τη στιγμή που οι Αλυσίδες ΑΤ είναι αποθηκευμένες στη συσκευή του χρήστη, αυτός μπορεί να τις αλλοιώσει. Οι συγγραφείς σκοπεύουν να καταστήσουν την αλλοίωση εμφανή (tamper-evident) και όχι αδύνατη (tamper-proof).

Secure verification of location claims (Echo) [51]

Στη δημοσίευση αυτή παρουσιάζεται ένα πρωτόκολλο ονόματι Echo.

Το Echo δεν απαιτεί τη χρήση κρυπτογραφίας, συγχρονισμού, ή προηγούμενης συμφωνίας μεταξύ prover και verifier (π.χ. ανταλλαγή κλειδιών).

Προϋποθέτει ότι ο verifier βρίσκεται στην ίδια περιοχή με τον prover. Χρησιμοποιεί σήματα RF (radio frequency) καθώς και υπέρηχους, για να επιβεβαιώσει την παρουσία του prover στην περιοχή του verifier. Επικεντρώνεται περισσότερο στην επιβεβαίωση της γειτνίασης prover-verifier και δεν εκδίδει Αποδείξεις Τοποθεσίας.

Είναι ειδικά σχεδιασμένο για συσκευές με περιορισμένους πόρους, όπως για παράδειγμα αισθητήρες (π.χ. θερμόμετρο) που μετέχουν σε δίκτυα αισθητήρων.

Η λειτουργία του είναι σχετικά απλή:

Έστω verifier V και prover P. Ο verifier έχει μια σφαίρα εμβέλειας η οποία και αποτελεί την περιοχή R (σφαίρα ακτίνας R) μέσα στην οποία θέλουμε να βρίσκεται ο P.

Αν ο P ισχυρίζεται ότι βρίσκεται εκτός της R, τότε ο V απορρίπτει απευθείας το αίτημα.

Αν ο P ισχυρίζεται ότι βρίσκεται σε σημείο l εντός της R, τότε ξεκινά το πρωτόκολλο.

Ο V στέλνει στον P ένα τυχαίο αριθμό (nonce) με RF. Ο P πρέπει να στείλει πίσω στον V τον αριθμό αυτό μέσω υπερήχων.

Αν d(V, l) η απόσταση μεταξύ V και της τοποθεσίας που ισχυρίζεται ο P, s η ταχύτητα του ήχου και c η ταχύτητα του φωτός, τότε η παραπάνω διαδικασία χρειάζεται συνολικό χρόνο

$$\Delta t_{ref} = \frac{d(V,l)}{c} + \frac{d(V,l)}{s}$$

Όπου c η ταχύτητα του φωτός και s η ταχύτητα του ήχου.

Ο V μετράει το χρόνο Δt από τη στιγμή που ξεκινάει την αποστολή του μηνύματος μέχρι τη στιγμή που αρχίζει να λαμβάνει την απάντηση.

Αν $\Delta t > \Delta t_{ref}$ τότε απορρίπτει τον ισχυρισμό του P, αλλιώς τον επιβεβαιώνει.

Ωστόσο, στην πραγματικότητα υπάρχει επιπλέον καθυστέρηση Δt_p, η οποία οφείλεται στο χρόνο που χρειάζεται ο P για να λάβει, να επεξεργαστεί το μήνυμα και να ετοιμάσει την απάντησή του.

Ο P πρέπει μαζί με το αίτημά του προς τον V να γνωστοποιήσει και την καθυστέρηση Δt_p.
Ο V θα πρέπει να ελέγξει ότι είναι $\Delta t_p \geq \frac{n}{bc} + \frac{n}{bs}$
όπου n το μήκος του nonce σε bits, bc η ταχύτητα μετάδοσης για το σήμα RF σε bps και bs η ταχύτητα μετάδοσης για το σήμα υπερήχου σε bps.

Με λίγα λόγια, προσθέτουμε στους χρόνους διάδοσης και τους χρόνους μετάδοσης που απαιτούνται, συν την άλλες πιθανές καθυστερήσεις του P.
Δίνοντας τη δυνατότητα στον P να ορίσει την καθυστέρηση Δt_p, θα μπορούσε να κλέψει το σύστημα. Έστω ότι ο P δηλώνει πως βρίσκεται σε τοποθεσία l στο άκρο της περιοχής R, και πως έχει μεγάλη καθυστέρηση Δt_p, ενώ στην πραγματικότητα έχει περίπου μηδενική. Τότε, θα μπορούσε να βρίσκεται σε απόσταση

$$d_{lie} = \frac{\Delta t_p}{\left(\frac{1}{c} + \frac{1}{s}\right)} \approx \Delta t_p \cdot s$$

εκτός της περιοχής R.

Συνεπώς, ο V θα κάνει αποδεκτές αιτήσεις για τοποθεσίες που βρίσκονται σε σφαίρα ROA (Region Of Acceptance) ακτίνας $ROA=R-\Delta t_p \cdot s$ και για τις οποίες μέτρησε χρόνο

$$\Delta t \leq \Delta t_{ref} = \frac{d(V,l)}{c} + \frac{d(V,l)}{s} + \Delta t_p$$

Ενδιαφέρον παρουσιάζει ο λόγος για τον οποίο χρησιμοποιείται RF σήμα στην κατεύθυνση V->P και υπέρηχος στην P->V (radio, sound).
Αν το σύστημα χρησιμοποιούσε (radio, radio), τότε θα προέκυπτε μεγάλο σφάλμα λόγω της καθυστέρησης Δt_p, ίσως μεγαλύτερο και από την ακτίνα R. Τότε το πρωτόκολλο δε θα λειτουργούσε. Συνεπώς, πρέπει τουλάχιστον η μία κατεύθυνση να χρησιμοποιεί ήχο

Αν το σύστημα χρησιμοποιούσε (sound, radio), τότε θα μπορούσε ένας κακόβουλος χρήστης να έχει τοποθετήσει κοντά στον V συσκευή που μετατρέπει τις ηχητικές δονήσεις σε ραδιοκύματα, ώστε να στείλει το nonce πιο γρήγορα στον P, που βρίσκεται εκτός R.

WORAL [70]

Το WORAL χρησιμοποιεί το μηχανισμό για AT που περιγράφεται στο [101], δίνοντας έμφαση στη διατήρηση ιστορικού τοποθεσιών σε μορφή αλυσίδας σύμφωνα με το OTIT [59].
Είναι από τις λίγες δημοσιεύσεις που αναφέρονται στην εφαρμογή κινήτρου συμμετοχής. Συγκεκριμένα, προτείνεται ανταμοιβή των witnesses από τον πάροχο των υπηρεσιών τοποθεσίας για τις έγκυρες αναφορές τους, παρέχοντας για παράδειγμα προνόμια στη συνδρομή τους.

Γίνονται οι εξής παραδοχές, οι οποίες όμως είναι δύσκολο να αποφευχθούν στην πραγματικότητα:

1. Οι χρήστες δεν μοιράζονται τα ιδιωτικά κλειδιά τους.
2. Οι χρήστες δεν δίνουν σε άλλους τις κινητές συσκευές τους.

Αν οι παραδοχές αυτές δεν ισχύουν, είναι δυνατόν να δημιουργηθούν AT για πρόσωπα που δεν βρέθηκαν στην αναφερόμενη τοποθεσία τη συγκεκριμένη χρονική στιγμή.

Απαιτούνται τρεις οντότητες για την δημιουργία της AT: Ο prover, η Location Authority (LA) και ένα witness. Η LA πραγματοποιεί επιπλέον ελέγχους και συμβάλλει σε μεγαλύτερη αξιοπιστία του πρωτοκόλλου. Ωστόσο, πιθανώς να χρειάζεται AT σε περιοχή που δεν βρίσκεται διαθέσιμη LA. Επιπλέον, η LA διατηρεί λίστα με τα witnesses που είναι εγγεγραμμένα σε αυτή και δημοσιεύει πληροφορίες σχετικά με τις AT που έχει εκδώσει. Αυτό συμβαίνει για την αποτροπή κακόβουλων AT που αναφέρονται σε λανθασμένες χρονικές στιγμές. Ωστόσο, εκθέτει πληροφορίες σχετικά με τους provers και τους witnesses. Ενδιαφέρον παρουσιάζει η δήλωση στο [101] πως τόσο η LA όσο και ο χρήστης μπορούν να δημιουργήσουν ένα εικονικό witness για τη δημιουργία ψευδών AT. Συνεπώς, αμφισβητείται η σημασία της ύπαρξης της LA.

Για την προστασία της ιδιωτικότητας των provers και witnesses, το WORAL χρησιμοποιεί ψευδώνυμα, τα Crypto-IDs. Η υλοποίηση αυτή έχει δύο σημαντικά μειονεκτήματα. Αφενός, ο χρήστης ενημερώνει την κεντρικοποιημένη αρχή που ονομάζεται Service Provider για τα Crypto-IDs που χρησιμοποιεί. Οι συγγραφείς αναφέρουν στο [101] πως όλοι οι συμμετέχοντες στο σύστημα μπορούν να εξάγουν το δημόσιο κλειδί από το Crypto-ID. Συνεπώς, η ταυτότητά του δεν είναι πλήρως προστατευμένη. Αφετέρου, είναι πιο εύκολο για ένα χρήστη να μοιραστεί το ψευδώνυμό του παρά το ιδιωτικό κλειδί του προκειμένου κάποιος άλλος να συλλέξει AT για λογαριασμό του.

Για τον εντοπισμό relay attacks, οι συμμετέχοντες στο πρωτόκολλο μετρούν τους χρόνους μεταξύ αποστολής και λήψης μηνυμάτων (timeout-based). Θεωρώντας κάποιο κατώφλι, υποθέτουν πως αν ο χρόνος το ξεπερνά τότε η άλλη πλευρά χρησιμοποιεί ενδιάμεσο proxy. Αν και η απλοϊκή αυτή προσέγγιση έχει καλά αποτελέσματα (υψηλά ποσοστά εντοπισμού επίθεσης ενδιάμεσου και χαμηλά false positives) χρειάζεται βαθμονόμηση, καθώς ο χρόνος επεξεργασίας και αποστολής των μηνυμάτων επηρεάζεται τόσο από την απόσταση των κόμβων, όσο και από την επεξεργαστική ισχύ τους.

SMILE [102]

Το πρωτόκολλο αυτό αγγίζει τους τομείς των αποδείξεων τοποθεσίας (proofs of location), της ιδιωτικότητας τοποθεσίας (location privacy) και της ανώνυμης επικοινωνίας (anonymized communication).

Το SMILE επιτρέπει σε ανθρώπους που είχαν συναντηθεί στο παρελθόν αλλά δεν γνωρίζονται μεταξύ τους να επικοινωνήσουν ξανά. Είναι εμπνευσμένο από υπηρεσίες γνωριμιών τύπου «σε είδα». Σε αυτές ένας χρήστης Α δημοσιεύει αγγελία αναφέροντας ότι είδε κάποιον άλλον χρήστη Β. Ο Β κοιτά τις αγγελίες και αν βρει κάποια που αναφέρεται σε αυτόν, ξεκινά επικοινωνία με τον Α, ο οποίος στη συνέχεια θα ζητήσει επιβεβαίωση ότι πράγματι ο Β είναι αυτός που ψάχνει. Αυτό γίνεται συνήθως με ορισμένες ερωτήσεις που αφορούσαν τη συνάντηση (π.χ. «τι κρατούσα»).

Στην περίπτωση του SMILE, τη διαδικασία αυτή διεκπεραιώνουν οι κινητές συσκευές των χρηστών, με τη βοήθεια ενός κεντρικού εξυπηρετητή (server). Στόχος είναι να δημιουργηθεί κοινή γνώση (κρυπτογραφικό κλειδί) που μόνο οι παρευρισκόμενοι στη συνάντηση μπορούν να έχουν. Οι κόμβοι ανεβάζουν στον server κατακερματισμένα κλειδιά (hashed keys) ώστε

αυτός να μην μπορεί να αποκτήσει γνώση των κλειδιών. Φροντίζοντας ώστε να δημιουργηθούν διενέξεις των hash (key-hash collisions), επιτυγχάνεται οι επικοινωνία μεταξύ όσων διαθέτουν το σωστό κλειδί.

Η διαδικασία έχει αναλυτικά ως εξής:

1. Κάθε κόμβος-συσκευή αναζητά γειτονικούς κόμβους μέσω Bluetooth.
2. Όταν βρεθούν γειτονικοί κόμβοι, κάποιος από αυτούς δημιουργεί τυχαίο κλειδί x και το μοιράζει στους γείτονές του.
3. Οι κόμβοι κατακερματίζουν (hash) το κλειδί με συνάρτηση κατακερματισμού H() και στέλνουν το hashed key H(x) στον server. Στη μνήμη τους αποθηκεύουν το ζεύγος {x, H(x)} καθώς και άλλες πληροφορίες για τη συνάντηση (π.χ. τοποθεσία, φωτογραφίες).
4. Έστω ότι κάποιος θέλει να επικοινωνήσει με κάποιον που συνάντησε. Στέλνει στον server το $\{H(x), E_x(m|t)\}$ που αντιστοιχεί στη συνάντηση που τον ενδιαφέρει. Στο παραπάνω m είναι το μήνυμα που θέλει να στείλει, t το χρονόσημο (timestamp) και E_x κρυπτογράφηση με το κλειδί x.
5. Ο server στέλνει το παραπάνω μήνυμα σε όσους έχουν ανεβάσει το ίδιο H(x), το οποίο σκόπιμα μπορεί να αντιστοιχεί σε πολλά κλειδιά (hash collision).
6. Οι clients βρίσκουν τις καταχωρήσεις που έχουν με το ίδιο hash και προσπαθούν να αποκρυπτογραφήσουν το μήνυμα με βάση το αντίστοιχο κλειδί. Αν καταφέρουν να αποκρυπτογραφήσουν το μήνυμα τότε μπορούν να απαντήσουν κατασκευάζοντας αντίστοιχη απάντηση $\{H(x), E_x(m|t+1)\}$.

Αξίζει να σημειωθεί πως ο χρήστης μπορεί να επιλέξει να στείλει πρόθεμα ορισμένου μεγέθους l από το H(x), ώστε να αυξήσει τα επίπεδα ανωνυμίας, αυξάνοντας όμως τον υπολογιστικό φόρτο, καθώς το μήνυμα θα πρέπει να σταλθεί σε περισσότερους κόμβους από τον server.

Το πρωτόκολλο είναι απλό και λειτουργικό, ωστόσο έχει αδύναμα σημεία.

- Αρχικά, όλοι οι κόμβοι που διαθέτουν το κλειδί x, δηλαδή οι παρευρισκόμενοι στη συνάντηση μπορούν να αποκρυπτογραφήσουν τα μηνύματα. Ορισμένες φορές όμως ενδιαφέρει η συνομιλία μεταξύ δύο κόμβων, όπως στην περίπτωση των γνωριμιών που αναφέρουν οι συγγραφείς. Το πρωτόκολλο δεν μπορεί να βοηθήσει περαιτέρω, καθώς οι κόμβοι πρέπει μεταξύ τους να επιβεβαιώσουν ποιοι ακριβώς είναι, μέσω ερωτήσεων αναγνώρισης.
- Επιπλέον, είναι δυνατή η συνεργασία ενός κόμβου με τον server και η αποστολή σε αυτόν του κλειδιού x. Σε αυτή την περίπτωση καταρρίπτεται η ιδιωτικότητα των υπόλοιπων κόμβων που παρευρίσκονταν στη συνάντηση.
- Ακόμα, είναι δυνατόν να «μαντέψει» κανείς το κλειδί x, δοθέντος ενός hash H(x), έχοντας προηγουμένως υπολογίσει μία λίστα ζευγών {key, H(key)}.

Privacy-Preserving Alibi Systems [50]

Το πρωτόκολλο αυτό επικεντρώνεται στη δημιουργία ΑΤ που λειτουργούν ως άλλοθι για τον prover (ονομάζεται owner). Βασικός στόχος των συγγραφέων είναι να παραμένει ανώνυμος ο prover κατά τη δημιουργία των ΑΤ, αλλά να εμφανίζει την ταυτότητά του όταν παρουσιάζει την ΑΤ σε κάποια δικαστική αρχή.

Από την άλλη, ο witness (ονομάζεται corroborator) μπορεί να είναι μία δημόσια οντότητα ή κάποιος ιδιώτης. Στην πρώτη περίπτωση δεν ενδιαφέρει η ιδιωτικότητά του, ενώ στη δεύτερη είναι κρίσιμη η προστασία της και η εμφάνισή της μόνο όταν αυτός αποφασίσει να

βοηθήσει τον prover ενώπιον της δικαστικής αρχής. Για το λόγο αυτό, παρουσιάζονται δύο σχεδιαστικές προσεγγίσεις.

Όπως πολλά πρωτόκολλα, θεωρεί ότι ο χρήστης δεν μοιράζεται το ιδιωτικό του κλειδί, το οποίο είναι συνδεδεμένο με το φυσικό πρόσωπο που έχει τη συσκευή (δεν ασχολείται με το πρόβλημα strong identities).

Οι συγγραφείς έχουν προσομοιώσει τον πραγματικό τρόπο λειτουργίας των άλλοθι σε ένα δικαστήριο, παρουσία μάρτυρα. Έχουν καταφέρει καλές επιδόσεις ιδιωτικότητας, ωστόσο δεν έχουν ληφθεί υπόψη προδιαγραφές ασφαλείας. Για την παραγωγή ενός άλλοθι απαιτείται ένα witness, με το οποίο ο prover μπορεί να έχει συνεργαστεί. Αυτό θα μπορούσε να είχε αποφευχθεί με την απαίτηση να υπάρχουν περισσότερα witnesses.

Επιπλέον, δεν πραγματοποιείται έλεγχος εγγύτητας και δεν έχουν αντιμετωπιστεί επιθέσεις ενδιάμεσου (man in the middle). Αυτές οι ελλείψεις καθιστούν ευκολότερη την δημιουργία ψευδών άλλοθι. Οι συγγραφείς θεωρούν πως η δικαστική αρχή είναι υπεύθυνη να κρίνει την αξιοπιστία του witness, όπως με τα πραγματικά άλλοθι.

Επιπλέον, στην υλοποίηση του πρωτοκόλλου όπου το witness διατηρεί κρυφή την ταυτότητά του κατά τη δημιουργία της AT (άλλοθι), προκύπτουν ορισμένα ζητήματα. Σύμφωνα με το πρωτόκολλο, όταν ο prover χρειαστεί να επιβεβαιώσει την AT του, πρέπει να επικοινωνήσει με το witness, ώστε αυτό να αποκαλύψει την ταυτότητά του. Ωστόσο, ο prover ενδέχεται να μην γνωρίζει το witness και συνεπώς πρέπει να χρησιμοποιήσει έναν μηχανισμό όπως περιγράφεται στο [102] προκειμένου να επικοινωνήσει ανώνυμα μαζί του και να ζητήσει τη συμβολή του ενώπιον της δικαστικής αρχής. Ανεξάρτητα από το αν γνωρίζει ή όχι το witness, αυτό μπορεί να αρνηθεί να συνεργαστεί (π.χ. συγκάλυψη εγκλήματος) ή μπορεί να μη συμμετέχει πλέον στο σύστημα. Εκτός αυτού, απουσιάζει μηχανισμός που να ενημερώνει το witness ότι πράγματι κάποια δικαστική αρχή ζήτησε την εξέταση του άλλοθι. Ο prover μπορεί αυθαίρετα να ζητήσει από το witness να βοηθήσει αποκαλύπτοντας την ταυτότητά του, χωρίς να έχει ζητηθεί κάτι τέτοιο από τη δικαστική αρχή. Το κενό αυτό μπορεί να χρησιμοποιηθεί από κακόβουλους χρήστες (provers) που επιθυμούν να αποκτήσουν πληροφορίες για την ταυτότητα άλλων χρηστών.

I Know Where You Are [77]

Ένας τρόπος για την επιβεβαίωση της γειτνίασης δύο κόμβων είναι η ανταλλαγή σημάτων μεταξύ τους ή συλλογή στοιχείων του περιβάλλοντος τα οποία χαρακτηρίζονται από μεγάλη τυχαιότητα (εντροπία), όπως για παράδειγμα ακουστικά κύματα, ένταση φωτός, ατμοσφαιρικά αέρια, θερμοκρασία, υγρασία και πίεση, καθώς και ηλεκτρομαγνητικά κύματα (π.χ. GPS, Bluetooth, WiFi).

Στο paper αυτό θεωρείται πως ο έλεγχος γειτνίασης πραγματοποιείται μεταξύ prover και verifier, ώστε να υπάρχει απευθείας επιβεβαίωση πως βρίσκονται κοντά. Ωστόσο, η μέθοδος αυτή μπορεί να χρησιμοποιηθεί μεταξύ prover και witness για τη δημιουργία μίας AT, η οποία θα επιβεβαιωθεί στη συνέχεια από τον verifier.

Ο έλεγχος γειτνίασης αυτού του είδους μπορεί να πραγματοποιηθεί με δύο τρόπους:

- **Beaconing:** Ο verifier (ή witness) εκπέμπει ορισμένα σήματα, τα οποία μπορεί να συλλάβει μόνο κάποιος ο οποίος βρίσκεται κοντά του. Το αρνητικό στην περίπτωση αυτή είναι πως ο verifier (ή witness) κάνουν αισθητή την παρουσία τους, κάτι που μπορεί να παραβιάζει την ιδιωτικότητά τους.

- **Context-based:** Ο verifier (ή witness) και ο prover συλλέγουν ταυτόχρονα στοιχεία του περιβάλλοντος, τα οποία μεταβάλλονται διαρκώς και παρουσιάζουν μεγάλη τυχαιότητα. Πραγματοποιούν στη συνέχεια σύγκριση των στοιχείων που συνέλεξαν και αν ταιριάζουν, τότε προκύπτει το συμπέρασμα πως βρίσκονται κοντά.

Οι συγγραφείς ασχολούνται με τη δεύτερη τεχνική και επικεντρώνονται στις επιθέσεις εκτίμησης περιβάλλοντος (context-guessing attacks), όπου ο επιτιθέμενος «μαντεύει» τα τρέχοντα στοιχεία του περιβάλλοντος και εξαπατά τον verifier (ή witness) ότι βρίσκεται κοντά του.

Για την αντιμετώπιση τέτοιου είδους επιθέσεων, πρέπει ο verifier να είναι σε θέση να εκτιμήσει την πιθανότητα να εξαπατηθεί, με άλλα λόγια να συμπεράνει το επίπεδο της τυχαιότητας των τρεχουσών περιβαλλοντικών συνθηκών. Αν η τυχαιότητα είναι μικρή, είναι ευκολότερο για τον επιτιθέμενο να δημιουργήσει (μαντέψει) πλαστές μετρήσεις. Σε αυτή την περίπτωση χρειάζεται προσθήκη τυχαίων χαρακτηριστικών, ώστε να γίνει δυσκολότερη η εξαπάτηση του verifier.

Συγκεκριμένα, αναπτύσσονται δύο μέθοδοι για την αύξηση της δυσκολίας (hardening) ενός prover να εξαπατήσει έναν verifier:

- **Φίλτρο «έκπληξης» (surprisal filtering):**

  Η έννοια της έκπληξης σχετίζεται με συγκεκριμένες παρατηρήσεις του περιβάλλοντος. Ενώ η εντροπία αφορά τη μέση τιμή της αβεβαιότητας των στοιχείων του περιβάλλοντος, η έκπληξη αφορά την αβεβαιότητα μίας συγκεκριμένης μέτρησης των περιβαλλοντικών στοιχείων.

  Ο επιτιθέμενος prover έχει σκοπό να παρουσιάσει ένα σύνολο μετρήσεων το οποίο θα συμπίπτει με αυτό που παρατηρεί ο verifier. Ο verifier γνωρίζει ποιες μετρήσεις είναι πιο συχνές και συνεπώς μπορεί να θεωρήσει πως είναι πιθανότερο αυτές να χρησιμοποιηθούν από έναν επιτιθέμενο που είχε επισκεφθεί παλαιότερα την τοποθεσία. Αντίθετα, σπάνιες μετρήσεις προκαλούν «έκπληξη» στον verifier, ο οποίος τις θεωρεί περισσότερο αξιόπιστες όταν παρουσιάζονται από τον prover. Συνεπώς, ο verifier κάνει αποδεκτές μόνο όσες παρατηρήσεις ξεπερνούν ένα επίπεδο «έκπληξης», δηλαδή τυχαιότητας.

- **Μακροχρόνιες μετρήσεις περιβάλλοντος (longitudinal ambient modalities):**

  Τα στοιχεία που παρατηρούνται στο περιβάλλον διακρίνονται από τους συγγραφείς σε στατικά και δυναμικά. **Στατικά** είναι τα στοιχεία που παρουσιάζουν μικρή τυχαιότητα, ενώ **δυναμικά** είναι εκείνα που μεταβάλλονται διαρκώς. Για παράδειγμα, στατικό στοιχείο θεωρούνται οι συνδεδεμένες συσκευές σε ένα οικιακό WiFi hotspot. Δυναμικό στοιχείο θεωρούνται τα ηχητικά κύματα σε μία καφετέρια.

  Το παραπάνω φίλτρο «έκπληξης» δεν έχει καλή απόδοση σε στατικά περιβάλλοντα, καθώς δεν υπάρχει τυχαιότητα.

  Τυχαιότητα μπορεί να προστεθεί αν συμπεριληφθούν δυναμικά δεδομένα που αφορούν τη φωτεινότητα του περιβάλλοντος καθώς και τα ηχητικά κύματα (στάθμη θορύβου) που υπάρχουν σε αυτό. Συγκεκριμένα, οι συγγραφείς προτείνουν την καταγραφή μεταβολών φωτός και θορύβου για ένα λεπτό. Πετυχαίνουν καλά αποτελέσματα, ωστόσο το χρονικό διάστημα του ενός λεπτού είναι ακατάλληλο για ορισμένες εφαρμογές. Επιπλέον, η συσκευή πρέπει να είναι εκτεθειμένη στο περιβάλλον ώστε να λάβει αυτές τις μετρήσεις, δηλαδή δεν θα λειτουργήσει καλά αν βρίσκεται για παράδειγμα στην τσέπη ή την τσάντα του χρήστη.

Βιβλιογραφία

[1] W. Luo και U. Hengartner, «VeriPlace: A Privacy-Aware Location Proof Architecture,» σε Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems (pp. 23-32), 2010.

[2] Techopedia, «What is Geolocation? - Definition from Techopedia,» Techopedia Inc., [Ηλεκτρονικό]. Available: https://www.techopedia.com/definition/1935/geolocation. [Πρόσβαση 15 March 2019].

[3] A.-M. Roxin, J. Gaber, M. Wack και A. Nait Sidi Moh, «Survey of Wireless Geolocation Techniques,» σε IEEE Globecom Workshops, Washington, DC, United States, 2007.

[4] Α. Πασιάς, «Συστήματα προσδιορισμού θέσης σε εσωτερικούς χώρους,» Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής, 2015.

[5] S. Cole, «Securing military GPS from spoofing and jamming vulnerabilities,» 30 November 2015. [Ηλεκτρονικό]. Available: http://mil-embedded.com/articles/securing-military-gps-spoofing-jamming-vulnerabilities/. [Πρόσβαση 2 March 2019].

[6] Encyclopædia Britannica, Inc., «Triangulation | trigonometry | Britannica.com,» [Ηλεκτρονικό]. Available: https://www.britannica.com/science/triangulation-trigonometry. [Πρόσβαση 3 March 2019].

[7] Encyclopædia Britannica, Inc. , «Trilateration | measurement | Britannica.com,» [Ηλεκτρονικό]. Available: https://www.britannica.com/science/trilateration. [Πρόσβαση 3 March 2019].

[8] «WiFi RSS based trilateration with MATLAB,» 9 March 2016. [Ηλεκτρονικό]. Available: https://github.com/joaodias/WiFi-RSS-based-trilateration-with-MATLAB. [Πρόσβαση 5 August 2018].

[9] M. Shchekotov, «Indoor localization method based on Wi-Fi trilateration technique.,» Proceeding of the 16th conference of fruct association., pp. 177-179, October 2014.

[10] GPS.gov, «Other Global Navigation Satellite Systems (GNSS),» 18 December 2017. [Ηλεκτρονικό]. Available: https://www.gps.gov/systems/gnss/. [Πρόσβαση 3 March 2019].

[11] U.S.A. Department of Transportation & Federal Aviation Administration, «GLOBAL POSITIONING SYSTEM WIDE AREA AUGMENTATION SYSTEM (WAAS) PERFORMANCE STANDARD,» 31 October 2008. [Ηλεκτρονικό]. Available: https://www.gps.gov/technical/ps/2008-WAAS-performance-standard.pdf. [Πρόσβαση 24 June 2018].

[12] Information and Analysis Center for Positioning, Navigation and Timing,, «Information analytical centre of GLONASS and GPS controlling,» 2019. [Ηλεκτρονικό]. Available: https://www.glonass-iac.ru/en/. [Πρόσβαση 3 March 2019].

[13] European Global Navigation Satellite Systems Agency, «European GNSS Service Centre,» 1 March 2019. [Ηλεκτρονικό]. Available: https://www.gsc-europa.eu/. [Πρόσβαση 3 March 2019].

[14] Government of China, «BeiDou Navigation Satellite System,» 2019. [Ηλεκτρονικό]. Available: http://en.beidou.gov.cn/. [Πρόσβαση 3 March 2019].

[15] Indian Space Research Organization (ISRO), «IRNSS Programme,» 2017. [Ηλεκτρονικό]. Available: https://www.isro.gov.in/irnss-programme. [Πρόσβαση 3 March 2019].

[16] Cabinet Office, Government Of Japan, «Quasi-Zenith Satellite System (QZSS),» 2019. [Ηλεκτρονικό]. Available: http://qzss.go.jp/en/. [Πρόσβαση 3 March 2019].

[17] Grindgis.com, «50 Uses or Applications of GPS,» Grindgis.com, [Ηλεκτρονικό]. Available: https://grindgis.com/gps/50-uses-or-applications-of-gps. [Πρόσβαση 15 September 2018].

[18] T. Humphreys, «GPS Spoofing and the Financial Sector,» June 2011. [Ηλεκτρονικό]. Available: https://repositories.lib.utexas.edu/handle/2152/63513. [Πρόσβαση 22 August 2018].

[19] Resilient Navigation and Timing Foundation, «Prioritizing Dangers to the United States from Threats to GPS,» 2016. [Ηλεκτρονικό]. [Πρόσβαση 22 August 2018].

[20] B. Markle, «Loran---staging for a comeback,» Marine Electronics, 2 November 2015. [Ηλεκτρονικό]. Available: https://www.marineelectronicsjournal.com/content/newsm/news.asp?show=VIEW&a=116. [Πρόσβαση 11 September 2018].

[21] Wikipedia, «LORAN,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/LORAN. [Πρόσβαση 17 September 2018].

[22] E. Collier, «eLoran: More accurate & less vulnerable but not a done deal yet, Part 1,» Marine Electronics Journal, 2 January 2017. [Ηλεκτρονικό]. Available: https://www.marineelectronicsjournal.com/content/newsm/news.asp?show=VIEW&a=178. [Πρόσβαση 10 September 2018].

[23] C. James, «GPS Backup: Is eLoran the Answer?,» aviationtoday.com, 12 April 2012. [Ηλεκτρονικό]. Available: https://www.aviationtoday.com/2012/04/12/gps-backup-is-eloran-the-answer/. [Πρόσβαση 10 September 2018].

[24] GrindGIS, «Difference Between GPS and DGPS,» 17 July 2017. [Ηλεκτρονικό]. Available: https://grindgis.com/blog/difference-between-gps-and-dgps. [Πρόσβαση 11 September 2018].

[25] F. Zahradnik, «An Explanation of Wi-Fi Triangulation,» LifeWire.com, 30 April 2018. [Ηλεκτρονικό]. Available: https://www.lifewire.com/wifi-positioning-system-1683343. [Πρόσβαση 14 September 2018].

[26] S. J. Vaughan-Nichols, «How Google--and everyone else--gets Wi-Fi location data,» ZDnet, 16 November 2011. [Ηλεκτρονικό]. Available: https://www.zdnet.com/article/how-google-and-everyone-else-gets-wi-fi-location-data/. [Πρόσβαση 14 September 2018].

[27] Wikipedia, «Geocoding,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Geocoding. [Πρόσβαση 4 March 2019].

[28] Google and other contributors, «An Evaluation of Location Encoding Systems,» 10 December 2018. [Ηλεκτρονικό]. Available: https://github.com/google/open-location-code/wiki/Evaluation-of-Location-Encoding-Systems#geohash36. [Πρόσβαση 3 March 2019].

[29] Wikipedia, «List of geocoding systems,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/List_of_geocoding_systems. [Πρόσβαση 4 March 2019].

[30] The New York Times, «The Numbering of Houses,» 16 July 1898. [Ηλεκτρονικό]. [Πρόσβαση 24 August 2018].

[31] what3words Ltd. , «what3words | Addressing the world,» what3words Ltd. , [Ηλεκτρονικό]. Available: https://what3words.com/. [Πρόσβαση 15 7 2018].

[32] «About | what3words,» what3words Ltd., [Ηλεκτρονικό]. Available: https://what3words.com/about/. [Πρόσβαση 26 August 2018].

[33] geohash.org, «Geohash,» [Ηλεκτρονικό]. Available: http://geohash.org. [Πρόσβαση 18 September 2018].

[34] Wikipedia, «Geohash,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Geohash. [Πρόσβαση 18 September 2018].

[35] Wikipedia, «Geohash-36,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Geohash-36. [Πρόσβαση 18 September 2018].

[36] Stichting Mapcode Foundation, «Welcome to Mapcode | mapcode.com,» [Ηλεκτρονικό]. Available: http://www.mapcode.com/. [Πρόσβαση 27 August 2018].

[37] Open Post Code, «Ireland's Free Any-Location Postcode,» [Ηλεκτρονικό]. Available: http://www.openpostcode.org/. [Πρόσβαση 18 September 2018].

[38] NAC Geographic Products Inc., «NacGeo.com,» [Ηλεκτρονικό]. Available: http://www.nacgeo.com/. [Πρόσβαση 27 August 2018].

[39] NAC Geographic Products Inc., «The Natural Area Coding System,» [Ηλεκτρονικό]. Available: http://www.nacgeo.com/nacsite/documents/nac.asp. [Πρόσβαση 27 August 2018].

[40] Wikipedia, «Maidenhead Locator System,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Maidenhead_Locator_System. [Πρόσβαση 18 September 2018].

[41] Wikipedia, «World Geographic Reference System,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/World_Geographic_Reference_System. [Πρόσβαση 18 September 2018].

[42] Wikipedia, «Global Area Reference System,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Global_Area_Reference_System. [Πρόσβαση 18 September 2018].

[43] Wikipedia, «Universal Transverse Mercator coordinate system,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Universal_Transverse_Mercator_coordinate_system. [Πρόσβαση 18 September 2018].

[44] Wikipedia, «World Meteorological Organization squares,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/World_Meteorological_Organization_squares. [Πρόσβαση 18 September 2018].

[45] «Plus codes,» [Ηλεκτρονικό]. Available: https://plus.codes/. [Πρόσβαση 12 December 2018].

[46] S. Saroiu και A. Wolman, «Saroiu, Stefan, and Alec Wolman. "Enabling new mobile applications with location proofs.,» σε Proceedings of the 10th workshop on Mobile Computing Systems and Applications. , 2009.

[47] S. Gambs, M.-O. Killijian, M. Roy και M. Traoré, «PROPS: A PRivacy-Preserving Location Proof System,» σε 2014 IEEE 33rd International Symposium on Reliable Distributed Systems, 2014.

[48] W. Luo και U. Hengartner, «Proving your location without giving up your privacy.,» σε Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, 2010.

[49] Z. Zhu και G. Cao, «Applaus: A privacy-preserving location proof updating system for location-based services.,» σε 2011 Proceedings IEEE INFOCOM, 2011.

[50] B. Davis, H. Chen και M. Franklin, «Privacy-Preserving Alibi Systems,» σε Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security., 2012.

[51] N. Sastry, U. Shankar και D. Wagner, «Secure verification of location claims.,» σε Proceedings of the 2nd ACM workshop on Wireless security., 2003.

[52] M. Talasila, R. Curtmola και C. Borcea, «LINK: Location verification through Immediate Neighbors Knowledge,» σε International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services, 2010.

[53] M. Bond και P. Landrock, «The Trusted Platform Module Explained,» 12 September 2011. [Ηλεκτρονικό]. Available: https://www.cryptomathic.com/news-events/blog/the-trusted-platform-module-explained. [Πρόσβαση 17 September 2018].

[54] Wikipedia, «Trusted Platform Module,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Trusted_Platform_Module. [Πρόσβαση 17 September 2018].

[55] Foursquare, «Mayorships,» [Ηλεκτρονικό]. Available: https://support.foursquare.com/hc/en-us/articles/201065220-Mayorships. [Πρόσβαση 28 September 2018].

[56] X. Wang, A. Pande, J. Zhu και P. & Mohapatra, «STAMP: enabling privacy-preserving location proofs for mobile users.,» IEEE/ACM transactions on networking, τόμ. 24, αρ. 6, pp. 3276-3289, 2016.

[57] C. Javali, G. Revadigar, K. B. Rasmussen, W. Hu και S. Jha, «I am Alice, I was in wonderland: secure location proof generation and verification protocol.,» σε 2016 IEEE 41st conference on local computer networks (LCN)., 2016.

[58] J. R. Douceur, "The sybil attack," in International workshop on peer-to-peer systems, 2002.

[59] R. Khan, S. Zawoad, M. M. Haque και R. Hasan, «OTIT: Towards Secure Provenance Modeling for Location Proofs,» σε Proceedings of the 9th ACM symposium on Information, computer and communications security., 2014.

[60] «Why use smart cards to store private keys,» ANZ Banking Group Ltd., [Ηλεκτρονικό]. Available: http://www.anz.com/corporate/products-services/transaction-services/public-key-infrastructure/anz-pki/why-use-smart/. [Πρόσβαση 20 September 2018].

[61] J. Marchi, «Private Key Protection- Steps to keeping your keys private,» GlobalSign, Inc., 30 September 2015. [Ηλεκτρονικό]. Available: https://www.globalsign.com/en/blog/private-key-protection/. [Πρόσβαση 20 September 2018].

[62] Android Developers, «Best practices for unique identifiers,» [Ηλεκτρονικό]. Available: https://developer.android.com/training/articles/user-data-ids. [Πρόσβαση 21 September 2018].

[63] Apple Developers, «UIDevice: A representation of the current device.,» Apple Inc., [Ηλεκτρονικό]. Available: https://developer.apple.com/documentation/uikit/uidevice. [Πρόσβαση 21 September 2018].

[64] The iPhone Wiki, «UDID,» 30 March 2017. [Ηλεκτρονικό]. Available: https://www.theiphonewiki.com/wiki/UDID. [Πρόσβαση 21 September 2018].

[65] V. Brik, S. Banerjee, M. Gruteser και S. Oh, «Wireless device identification with radiometric signatures.,» σε Proceedings of the 14th ACM international conference on Mobile computing and networking., 2008.

[66] Y. Zheng and W. Lou, "Location based handshake and private proximity test with location tags.," IEEE Transactions on Dependable and Secure Computing 14.4, pp. 406-419, 2017.

[67] G. Brambilla, M. Amoretti και F. Zanichelli, Using Blockchain for Peer-to-Peer Proof-of-Location, arXiv preprint arXiv:1607.00174, 2016.

[68] Foamspace Corp, «FOAM Whitepaper,» 5 January 2018. [Ηλεκτρονικό]. Available: https://foam.space/publicAssets/FOAM_Whitepaper.pdf. [Πρόσβαση 4 March 2019].

[69] Y. Zhang, C. C. Tan, F. Xu, H. Han και Q. Li, «Vproof: Lightweight privacy-preserving vehicle location proofs,» IEEE Transactions on Vehicular Technology, τόμ. 64, αρ. 1, pp. 378-385, 2015.

[70] R. Khan, S. Zawoad, M. M. Haque και R. Hasan, «WORAL: A Witness Oriented Secure Location Provenance Framework for Mobile Devices,» σε IEEE Transactions on Emerging Topics in Computing, 2016.

[71] S. Halevi και S. Micali, «Practical and provably-secure commitment schemes from collision-free hashing.,» σε Annual International Cryptology Conference., 1996.

[72] T. P. Pedersen, «Non-interactive and information-theoretic secure verifiable secret sharing.,» σε Annual International Cryptology Conference, 1991.

[73] R. Hasan και R. Burns, «Where have you been? secure location provenance for mobile devices.,» arXiv preprint arXiv:1107.1821, 2011.

[74] D. Chaum και E. Van Heyst, «Group signatures,» σε Workshop on the Theory and Application of of Cryptographic Techniques, Berlin, Heidelberg, 1991.

[75] S. Brands και D. Chaum, «Distance-bounding protocols,» σε Workshop on the Theory and Application of of Cryptographic Techniques, Berlin, Heidelberg.

[76] L. Bussard και W. Bagga, «Distance-bounding proof of knowledge to avoid real-time attacks,» σε IFIP International Information Security Conference, Boston, MA, 2005.

[77] M. Miettinen, N. Asokan, F. Koushanfar, T. D. Nguyen, J. Rios, A.-R. Sadeghi, M. Sobhani και S. Yellapantula, «I know where you are: Proofs of presence resilient to malicious provers,» σε Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, 2015.

[78] C. Lyu, A. Pande, X. Wang, J. Zhu, D. Gu και P. Mohapatra, «CLIP: Continuous location integrity and provenance for mobile phones,» σε 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, 2015.

[79] Foamspace Corp, «FOAM Technical Whitepaper Draft 0.4,» 4 May 2018. [Ηλεκτρονικό]. Available: https://github.com/f-o-a-m/public-research/raw/master/FOAM%20Techincal%20Whitepaper%20Draft.pdf. [Πρόσβαση 4 March 2019].

[80] B. Armstrong, «Quiet for Android - TCP over sound,» [Ηλεκτρονικό]. Available: https://github.com/quiet/org.quietmodem.Quiet. [Πρόσβαση 7 March 2019].

[81] GPS.gov, «GPS Accuracy,» 5 December 2017. [Ηλεκτρονικό]. Available: https://www.gps.gov/systems/gps/performance/accuracy/#how-accurate. [Πρόσβαση 11 September 2018].

[82] P. Oechslin, «Making a faster cryptanalytic time-memory trade-off.,» σε Annual International Cryptology Conference, 2003.

[83] Wikipedia, «Rainbow table,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Rainbow_table. [Πρόσβαση 11 December 2018].

[84] Wikipedia, «Hash chain,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Hash_chain. [Πρόσβαση 11 December 2018].

[85] G. Lenzini, S. Mauw και J. Pang, «Selective location blinding using hash chains.,» σε International Workshop on Security Protocols, 2011.

[86] Κ. Λιμνιώτης, «Κρυπτογραφία 5 - Τεχνικές πιστοποίησης μηνύματος και αποστολέα,» [Ηλεκτρονικό]. Available: http://cgi.di.uoa.gr/~klimn/cryptography/chapter_5-message_and_entity_authenication.pdf. [Πρόσβαση 12 December 2018].

[87] B. Armstrong, «Quiet Modem Project,» [Ηλεκτρονικό]. Available: https://github.com/quiet. [Πρόσβαση 7 March 2019].

[88] J. D. Gaeddert, «liquidsdr.org - making software radio portable since 2007,» 2018. [Ηλεκτρονικό]. Available: http://liquidsdr.org/. [Πρόσβαση 7 March 2019].

[89] B. Armstrong, «Quiet Profile Lab,» [Ηλεκτρονικό]. Available: https://quiet.github.io/quiet-profile-lab/. [Πρόσβαση 7 March 2019].

[90] json.org, «Introducing JSON,» [Ηλεκτρονικό]. Available: http://www.json.org. [Πρόσβαση 7 March 2019].

[91] FasterXML, «Jackson Project Home @github,» [Ηλεκτρονικό]. Available: https://github.com/FasterXML/jackson. [Πρόσβαση 7 March 2019].

[92] Google and other contributors, «Open Location Code,» [Ηλεκτρονικό]. Available: https://github.com/google/open-location-code. [Πρόσβαση 7 March 2019].

[93] Wikipedia, «Base64,» Wikipedia, [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Base64. [Πρόσβαση 7 March 2019].

[94] Wikipedia, «SHA-2,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/SHA-2. [Πρόσβαση 7 March 2019].

[95] R. L. Rivest, A. Shamir και L. Adleman, «A method for obtaining digital signatures and public-key cryptosystems,» Communications of the ACM, τόμ. 21, αρ. 2, pp. 120-126, 1978.

[96] Wikipedia, «RSA (cryptosystem),» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/RSA_(cryptosystem). [Πρόσβαση 7 March 2019].

[97] J. Daemen και V. Rijmen, The design of Rijndael: AES-the advanced encryption standard, Springer Science & Business Media, 2013.

[98] Wikipedia, «Advanced Encryption Standard,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard. [Πρόσβαση 7 March 2019].

[99] Wikipedia, «Initialization vector,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Initialization_vector. [Πρόσβαση 7 March 2019].

[100] A. Birkett, «QuietShare,» 4 April 2019. [Ηλεκτρονικό]. Available: https://github.com/alexbirkett/QuietShare. [Πρόσβαση 12 March 2019].

[101] R. Khan, S. Zawoad, M. M. Haque και R. Hasan, «'Who, When, and Where?'Location Proof Assertion for Mobile Devices.,» σε IFIP Annual Conference on Data and Applications Security and Privacy., 2014.

[102] J. Manweiler, R. Scudellari και L. P. Cox, «SMILE: encounter-based trust for mobile social services.,» σε Proceedings of the 16th ACM conference on Computer and communications security., 2009.

[103] T. Fernholz, «The entire global financial system depends on GPS, and it's shockingly vulnerable to attack,» Quartz, 22 October 2017. [Ηλεκτρονικό]. Available: https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack/. [Πρόσβαση 24 June 2018].