Walkie-Talkie: Αυτόματη Δημιουργία Κλειδιών με Βάση την Κίνηση για Ασφαλή Επικοινωνία Συσκευών στο Σώμα

Ονοματεπώνυμο: Κυριακού Ανδρόνικος
Έτος: 5ο
Email: kyriakou@ceid.upatras.gr

1. Εισαγωγή – Πρόβλημα που μελετάται

Η αύξηση του όγκου των ασύρματων δικτύων αισθητήρων έχει επιφέρει την ραγδαία αύξηση του αριθμού των συσκευών που αλληλοεπιδρούν με το ανθρώπινο σώμα όπως τα έξυπνα κινητά και τα έξυπνα ρολόγια. Παράλληλα, όλο και συχνότερες γίνονται οι εμφυτεύσιμες ιατρικές συσκευές (IMD) οι οποίες μπορούν να χρησιμοποιηθούν για συνεχή παρακολούθηση της υγείας του ατόμου και θεραπεία χρόνιων ασθενειών. Αυτή η τεχνολογική επανάσταση αναδεικνύει την σημασία της ασφαλούς επικοινωνίας μεταξύ IoT συσκευών για την ανταλλαγή δεδομένων. Για παράδειγμα τα έξυπνα κινητά πρέπει συνεχώς να διαβάζουν πληροφορίες σχετικά με την υγεία από τις IMDs και είτε να τις επεξεργάζονται είτε να τις προωθούν σε κάποια άλλη συσκευή όπως έξυπνο ρολόι. Η ασύρματη μορφή αυτής της επικοινωνίας δίνει το έναυσμα για προβληματισμούς ασφαλείας. Για να ανταπεξέλθουμε σε αυτό, παραδοσιακοί μηχανισμοί ασφαλείας για την ανταλλαγή κοινών μυστικών κλειδιών από τις συσκευές έχουν προταθεί, αλλά μια έμπιστη τρίτη οντότητα η οποία εποπτεύει την διαδικασία της ανταλλαγής δεν είναι πάντα διαθέσιμη και έτσι πρέπει να δοθεί προτεραιότητα στην διαδικασία δημιουργίας κλειδιών με βάση τον εκάστοτε χρήστη. Πιο συγκεκριμένα, στην εργασία που μελετάμε, προτείνεται ένα σύστημα το οποίο εκμεταλλεύεται τα μοναδικά χαρακτηριστικά του βαδίσματος ενός χρήστη και τα χρησιμοποιεί για την δημιουργία κλειδιών τα οποία χρησιμοποιούνται από όλες τις συσκευές στο σώμα.

Τα πλεονεκτήματα της μεθόδου αυτής είναι τρίπτυχα. Αρχικά, απαλείφεται ο ενεργός ρόλος του χρήστη αφού οι συσκευές που βρίσκονται πάνω στο σώμα αλληλοεπιδρούν μεταξύ τους χωρίς να χρειάζεται η χρήση κωδικών ή δαχτυλικών αποτυπωμάτων. Έτσι, δημιουργείται μια πολλά υποσχόμενη τεχνική η οποία θα κάνει ελαφριά συνεχή αυθεντικοποίηση για συσκευές IoT. Παράλληλα, η αυτόματη διασύνδεση και δημιουργία κλειδιών των συσκευών καθιστούν μη απαραίτητη την χρήση κρυπτογραφικών πρωτοκόλλων ανταλλαγής κλειδιών τα οποία αποτελούν υπολογιστικά δύσκολα προβλήματα και δεν ευθυγραμμίζονται με την ανάγκη για χαμηλή κατανάλωσης ενέργειας. Τέλος, ένα βασικό συστατικό της διαδικασίας διανομής κλειδιών είναι η πολιτική ανάκλησης και ανανέωσης τους. Η στατική αποθήκευση τοπικά κρύβει πιθανούς κινδύνους όποτε η αυτόματη δημιουργία μόνο κατά την ανάγκη επικοινωνίας αποτελεί μονόδρομο.

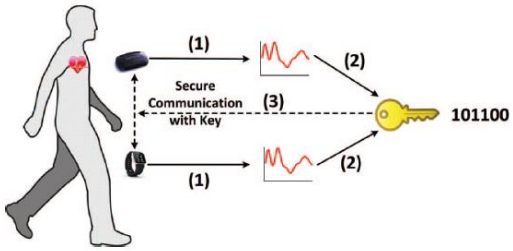
Η προσέγγιση της εργασίας χρησιμοποιεί το βάδισμα, που αποτελεί ένα μοναδικό χαρακτηριστικό του ατόμου, για την δημιουργία των κρυπτογραφικών κλειδιών. Αυτό είναι εφικτό καθώς οι αισθητήρες σε διαφορετικά μέρη του σώματος του ατόμου καταγράφουν το ίδιο σήμα. Βέβαια, λόγω της πολυπλοκότητας των κινήσεων του σώματος, αισθητήρες οι οποίοι βρίσκονται σε διαφορετικά σημεία θα καταγράφουν διαφορετικές επιταχύνσεις λόγω και άλλων κινήσεων που συμβαίνουν ταυτόχρονα όπως αυτή των χεριών. Αυτό αποτελεί μια από τις κύριες προκλήσεις του προς ανάπτυξη συστήματος και παρακάτω θα αναλύσουμε την τεχνική Blind Source Separation (BSS) που χρησιμοποιείται. Σημαντικό είναι να παρατηρηθεί ότι οι μετρήσεις τις επιτάχυνσης στον κορμό ενός ατόμου (μέση και στήθος) είναι παρόμοιες ενώ αυτές οι οποίες λαμβάνονται από τα χέρια διαφέρουν σημαντικά και συνεισφέρουν και θόρυβο.

Μια άλλη πρόκληση η οποία πρέπει να ληφθεί υπόψιν είναι η περιορισμένη υπολογιστική ισχύς και η κατανάλωση ενέργειας. Το προτεινόμενο πρωτόκολλο χρειάζεται μόνο ελαφριούς υπολογισμούς και τεχνικές επεξεργασίας σήματος καθώς και κλήσεις του αλγορίθμου Advanced Encryption Standard (AES) και υπολογισμούς κατακερματισμού από τις συσκευές.

2. Μοντέλο Χρήσης

A. Μοντέλο Χρήστη

Ένα τυπικό μοντέλο χρήσης παρουσιάζεται στο Σχήμα 1. Ο χρήστης θέλει να ζευγαρώσει το έξυπνο ρολόι του (Alice) με τον βηματοδότη του (Bob). Για να το επιτύχει αυτό εκκινεί την εφαρμογή Walkie-Talkie και περπατάει μερικά βήματα. Έτσι και τα δύο συμβαλλόμενα μέρη δημιουργούν ένα κρυφό συμμετρικό κλειδί μετρώντας τιμές από τα βήματα του χρήστη.



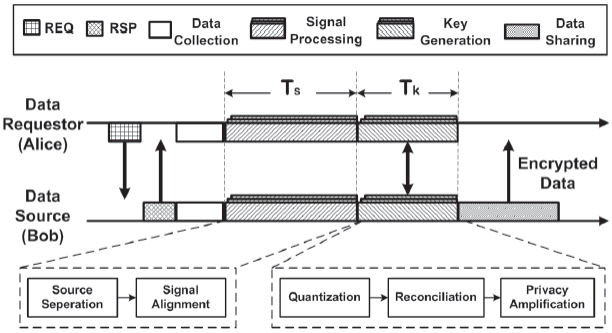
Σχήμα 1: Δημιουργία ζεύγους κλειδιών από τις δύο αυτόνομες συσκευές.

B. Μοντέλο Αντιπάλου

Για την επίτευξη ασφαλούς επικοινωνίας θα υποτεθεί ένας αντίπαλος, η Eve, η οποία θα προσπαθήσει να κάνει μια επίθεση πλαστοπροσωπίας, δηλαδή να φερθεί σαν μια συσκευή και να προσπαθήσει να κλέψει ιδιωτικές πληροφορίες. Θα αναλυθούν δύο είδη επιθέσεων, η παθητική παρακολούθηση του καναλιού και η ενεργητική επίθεση. Στην πρώτη περίπτωση, η Eve ξέρει τον αλγόριθμο δημιουργίας των κλειδιών και μπορεί να ακούσει τα μηνύματα τα οποία ανταλλάσσουν η Alice και ο Bob. Στην δεύτερη περίπτωση η Eve προσπαθεί να μιμηθεί το στυλ βαδίσματος του χρήστη και έτσι να μπορέσει να ζευγαρώσει με τις συσκευές. Είναι σημαντικό να αναφερθεί ότι η Eve δεν μπορεί να επηρεάσει ή να υπολογίσει τις μετρήσεις από τις νόμιμες συσκευές καθώς και ότι δεν μπορεί να τοποθετήσει μια κακόβουλη συσκευή πάνω στον χρήστη, περιπτώσεις στις οποίες θα ήταν αδύνατη η ασφάλεια του συστήματος.

3. Σχεδιασμός Συστήματος

Όπως φαίνεται και στο Σχήμα 2, όταν η Alice θέλει να επικοινωνήσει με τον Bob αρχικοποιεί την σύνδεση στέλνοντας ένα σήμα REQ. Ο Bob απαντάει με ένα σήμα RSP, στιγμή από την οποία και έπειτα οι δύο συσκευές συλλέγουν δεδομένα από τον αισθητήρα τους και επεξεργάζονται κατάλληλα το παραγόμενο σήμα για να δημιουργήσουν το κοινό κλειδί τους.



Σχήμα 2: Διαδικασία Δημιουργίας Κλειδιού.

Τα δύο στάδια επεξεργασίας του σήματος και δημιουργία του κλειδιού παρουσιάζονται στις επόμενες ενότητες.

4. Επεξεργασία Σήματος

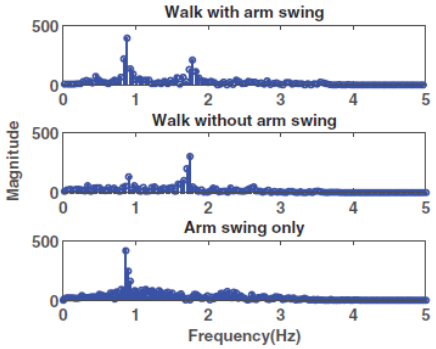
Η επεξεργασία του σήματος χωρίζεται σε δύο στάδια. Στο πρώτο γίνεται διαχωρισμός του σήματος και έπειτα γίνεται ευθυγράμμιση των παραγόμενων σημάτων. Ο διαχωρισμός του σήματος γίνεται για

να εξαχθούν τα χρήσιμα επιμέρους σήματα που προκύπτουν από το βάδισμα και να αφαιρεθεί ο θόρυβος, ενώ η ευθυγράμμιση γίνεται για να μην ληφθεί υπόψιν η θέση της εκάστοτε συσκευής και να υπάρχει η ίδια βάση για την δημιουργία των κλειδιών.

Επεξεργασία Σήματος

Η τεχνική που χρησιμοποιείται για να διαχωριστούν οι διάφορες συνιστώσες του σήματος είναι η ανάλυση ανεξάρτητης συνιστώσας (independent component analysis (ICA)). Η μέθοδος αυτή αποτελεί μια BSS μέθοδο που λαμβάνει πολύ λίγη προηγούμενη πληροφορία για την πηγή των σημάτων. Οι προϋποθέσεις για να λειτουργήσει η μέθοδος ικανοποιούνται και είναι σημαντικό να αναφερθεί ότι για κάθε τοποθεσία μέτρησης λαμβάνουμε μετρήσεις από τρία κανάλια κυρίως από την κίνηση των χεριών και το βάδισμα.

Παρατηρώντας το Σχήμα 3, είναι προφανές ότι υπάρχουν διαφορές στο συχνοτικό φάσμα όταν ένας χρήστης περπατάει κουνώντας και μη τα χέρια του καθώς και ότι η κύρια συχνότητα του βαδίσματος είναι δυο φορές της κίνησης των χεριών το οποίο προκύπτει λογικά αν αναλογιστούμε ότι ένας κύκλος βαδίσματος αποτελείται από δύο βήματα και μία κίνηση των χεριών. Συνεπώς κάθε βήμα (αριστερό ή δεξί) καταγράφεται σαν ένα δυνατό επαναληπτικό σήμα επιτάχυνσης το οποίο μεταφέρεται από τα πόδια σε όλο το σώμα (λόγω συμμετρίας του σώματος τα σήματα από το δεξί και το αριστερό βήμα θεωρούνται όμοια). Παράλληλα, η κίνηση του χεριού επαναλαμβάνεται κάθε δύο βήματα καθώς ο αισθητήρας βρίσκεται σε ένα χέρι.



Σχήμα 3: Συχνότητες περπατήματος με και χωρίς κίνηση χεριών καθώς και αυτόνομη κίνηση χεριών.

Για να υπολογιστούν οι ανεξάρτητες συνιστώσες των κινήσεων θα χρησιμοποιηθεί ο τύπος: $\tilde{S}(t) = W * Acc(t)$, όπου W είναι ένα μητρώο το οποίο διαχωρίζει τις συνιστώσες και $Acc(t) = A * S(t)$ όπου A το μητρώο το οποίο συγχέει τις συνιστώσες και $S(t)$ οι ανεξάρτητες μετρήσεις. Ουσιαστικά $W = A^{-1}$ και για τον υπολογισμό του χρησιμοποιείται ο αλγόριθμος FastICA. Στο αποτέλεσμα του αλγορίθμου εφαρμόζεται ο Fast Fourier Transform (FFT) σε κάθε ανεξάρτητη συνιστώσα και Προκειμένου να μην ληφθεί υπόψιν το σήμα που προκύπτει από την κίνηση του χεριού αρκεί να μηδενιστεί η συνιστώσα η οποία αντιστοιχεί σε αυτό (δεύτερη γραμμή του μητρώου $\tilde{S}(t)$).

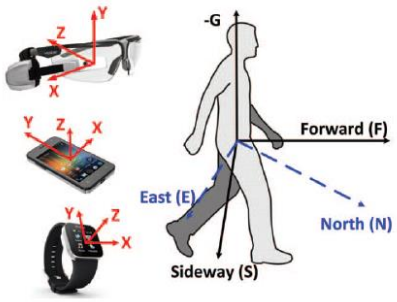
Ευθυγράμμιση Σήματος

Οι μετρημένες τιμές της επιτάχυνσης δεν μπορούν να χρησιμοποιηθούν απ' ευθείας για την δημιουργία κλειδιών καθώς είναι επηρεασμένες από την τοποθεσία και τον προσανατολισμό των μετρητών τους. Παράλληλα, οι διαφορετικές συσκευές δεν είναι συγχρονισμένες χρονικά και άρα τίθεται και αυτό το θέμα προς επίλυση.

Ο χρονικός συγχρονισμός των συσκευών επιλύεται χρησιμοποιώντας ένα γεγονός ως σημείο αναφοράς. Πιο συγκεκριμένα, κάθε συσκευή αυτόνομα εντοπίζει τη χρονική στιγμή που το πέλμα ακουμπάει στο έδαφος και το χρησιμοποιεί ως σημείο αναφοράς. Η λογική πίσω από αυτή τη θεώρηση είναι ότι οι τιμές της επιτάχυνσης φτάνουν στο μέγιστο τους ταυτόχρονα όταν το πόδι ακουμπάει στο έδαφος, χωρίς να θεωρείται ότι υπάρχει χρονική καθυστέρηση για την διάδοση του σήματος στο σώμα. Για να εντοπιστεί ένα πάτημα χρησιμοποιείται ένα κατωπερατό φίλτρο στην διεύθυνση της βαρύτητας με συχνότητα αποκοπής 3Hz καθώς η συχνότητα ενός βήματος είναι

μεταξύ 1.6 – 2.8 Hz. Πρακτικά, όταν η Alice δέχεται ένα RSVP σήμα, συμφωνεί με τον Bob να ξεκινήσουν τις μετρήσεις τους από το επόμενο $n - αρχικό$ βήμα και να τις σταματήσουν στο επόμενο $n - τελικό$ βήμα.

Ο χωρικός συγχρονισμός είναι αναγκαίος καθώς το βάδισμα είναι μια τρισδιάστατη κίνηση και κάθε συσκευή έχει το δικό της σύστημα αναφοράς. Η λύση είναι η δημιουργία ενός κοινού συστήματος αναφοράς βασισμένο στο σώμα και η μετατροπή των μετρήσεων των συσκευών σε αυτό. Πιο συγκεκριμένα, όπως φαίνεται και στο Σχήμα 4 χρησιμοποιείται το σύστημα Μπροστά (Forward (F)), Πλάγια (Sideways (S)) (το οποίο είναι δεξιά από την εμπρός κίνηση του χρήστη) και Αντίθετη Βαρύτητα (-G). Κάθε συσκευή χρησιμοποιεί το σύστημα (X,Y,Z) και η μετατροπή μπορεί να γίνει με κατάλληλους μετασχηματισμούς-περιστροφές του μητρώου που τις περιέχει. Τελικά θα υπολογιστούν τρεις τιμές επιτάχυνσης, Acc_G, Acc_F $και$ Acc_S για την δημιουργία των κλειδιών.



Σχήμα 4: Τα διαφορετικά συστήματα συντεταγμένων.

5. Δημιουργία Κρυπτογραφικών Κλειδιών

Η διαδικασία της δημιουργίας κλειδιών απαρτίζεται από τα εξής βασικά στάδια: κβάντιση, συμφωνία και βελτίωση ιδιωτικότητας. Στο πρώτο στάδιο οι δυο χρήστες μετατρέπουν τα δείγματα της επιτάχυνσης σε bits αν βρίσκονται στο ίδιο σώμα. Στο στάδιο της συμφωνίας ανταλλάσσουν μηνύματα διόρθωσης λαθών πάνω από δημόσια κανάλια για να καταλήξουν στο κοινό κλειδί. Τέλος, λόγω της δημόσιας ανταλλαγής πληροφορίας είναι αναγκαία η βελτίωση ιδιωτικότητας. Αναλυτικά τα βήματα παρουσιάζονται παρακάτω.

Κβάντιση

Η κβάντιση και το φιλτράρισμα του σήματος γίνεται για κάθε διεύθυνση ξεχωριστά. Αρχικά εφαρμόζεται ένα χαμηλοπερατό φίλτρο με συχνότητα αποκοπής τα 10 Hz όπου βρίσκεται και το χρήσιμο σήμα. Έπειτα οι τιμές κανονικοποιούνται για να έχουν μηδενική μέση τιμή και μοναδιαίο μήκος με σκοπό να μην παίζει ρόλο η θέση του αισθητήρα στο σώμα. Η μετατροπή των σημάτων σε bits γίνεται θέτοντας τιμές κατωφλίου (που υπολογίζονται από ένα σύνολο δειγμάτων) και ορίζοντας τις τιμές πάνω και κάτω από αυτό σε 1 και 0 αντίστοιχα. Τελικά για κάθε κατεύθυνση παράγεται μία ακολουθία bits και η συνένωση των τριών δημιουργούν το τελικό κλειδί.

Συμφωνία Κλειδιού

Η παραπάνω διαδικασία εκτελείται τόσο από την Alice όσο και από τον Bob και μπορεί να δώσει διαφορετικά αποτελέσματα λόγω θορύβου. Ο κάθε αισθητήρας στέλνει δειγματοληπτικά bits στον άλλον και μόνο τα κοινά διατηρούνται και από τους δύο για να καταλήξουν στο τελικό κλειδί. Παράλληλα, λόγω διαφορετικής δειγματοληψίας, ένας παράγοντας που πρέπει να αναφερθεί είναι το διαφορετικό μήκος του κάθε κλειδιού που έχει παραχθεί και άρα αυτός είναι ακόμα ένας λόγος για να διαπραχθεί η διαδικασία της συμφωνίας. Ένα δυνητικό πρόβλημα είναι ότι η ανταλλαγή των bits γίνεται πάνω από μη ασφαλές κανάλι και άρα η Eve μπορεί να παρεμβληθεί και να τροποποιήσει το περιεχόμενο των μηνυμάτων. Η λύση σε αυτό είναι η χρήση Message Authentication Code (MAC) για να εγγυηθεί ότι ένα μήνυμα δεν είναι τροποποιημένο.

Βελτίωση της Ιδιωτικότητας

Ο τρόπος δημιουργίας του κλειδιού δεν εξασφαλίζει ένα αρκετά ισχυρό και ανθεκτικό μυστικό κλειδί. Για να επιλυθεί το πρόβλημα αυτό χρησιμοποιείται μια XOR ανά bit για να αναμίξει τα

κλειδιά από τις διάφορες κατευθύνσεις και να εξαλείψει την συσχέτιση μεταξύ τους. Μετά και από αυτό το βήμα έχει πλέον δημιουργηθεί ένα συμμετρικό κλειδί το οποίο μπορεί να χρησιμοποιηθεί από αντίστοιχους αλγορίθμους όπως ο AES. Αν το μήκος του κλειδιού είναι μεγαλύτερο από 128 bits τότε κρατούνται τα πρώτα που δημιουργήθηκαν.

6.Αξιολόγηση

Στόχοι, Μετρικές και Μεθοδολογία

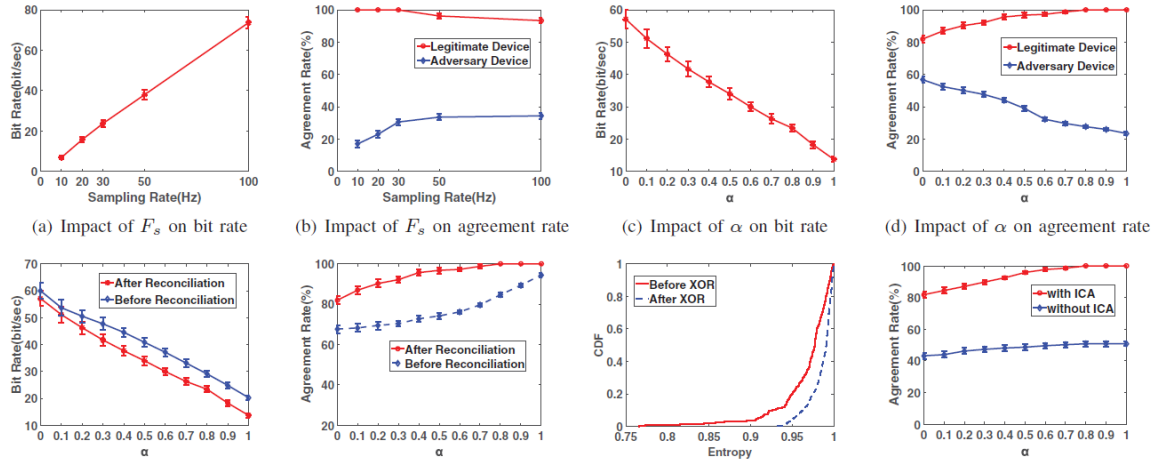
Για τους στόχους της παρούσας ενότητας συλλέχθηκαν δεδομένα από 20 άτομα (14 άνδρες και 6 γυναίκες) που είχαν αισθητήρες τοποθετημένους στο κεφάλι, το στήθος, την μέση και τον καρπό. Η δειγματοληψία έγινε με συχνότητα 100 Hz. Οι συμμετέχοντες βάδισαν για 5 λεπτά σε κανονική ταχύτητα τόσο σε εσωτερικό όσο και σε εξωτερικό περιβάλλον.

Οι μετρικές που χρησιμοποιήθηκαν είναι το ποσοστό της συμφωνίας των κλειδιών μεταξύ των δυο μερών, ο ρυθμός bit, δηλαδή ο μέσος όρος του αριθμού των bits που μπορούν να δημιουργηθούν από τα δείγματα της επιτάχυνσης ανά μονάδα χρόνου και η εντροπία, δηλαδή το μέτρο της αβεβαιότητας που αντιστοιχεί σε δημιουργούμενες συμβολοσειρές bit.

Οι παράγοντες οι οποίοι μελετήθηκαν εκτενώς είναι το W, ο αριθμός των δειγμάτων από τα οποία προκύπτει ένας αριθμός bits, το a, μια παράμετρος για τον υπολογισμό του κατωφλίου στην κβάντιση και το F_s , η συχνότητα δειγματοληψίας. Μετά από πειράματα βρέθηκε ότι ο βέλτιστος συνδυασμός είναι $W = 10, a = 0.8, F_s = 30$. Με βάση αυτά κρατήθηκαν σταθερές οι δύο παράμετροι και η τρίτη μεταβλήθηκε για να φανεί η επίδραση στον ρυθμό bit και στο ποσοστό συμφωνίας των κλειδιών.

Επιλογή Παραμέτρων

Τα αποτελέσματα παρουσιάζονται στο Σχήμα 5 και αναλύονται παρακάτω.



(a) Impact of F_s on bit rate (b) Impact of F_s on agreement rate (c) Impact of α on bit rate (d) Impact of α on agreement rate

(e) Impact of reconciliation on bit rate (f) Impact of reconciliation on agreement rate (g) Impact of privacy amplification (h) Impact of ICA

Σχήμα 5: Αποτελέσματα ανάλυσης

- Στο Σχήμα 5a και 5b παρατηρείται ότι όσο αυξάνεται το F_s η σχέση ρυθμού bit και συμφωνίας είναι αντίστροφη. Από τη μία μεγαλύτερη συχνότητα δίνει παραπάνω bits στην ίδια μονάδα χρόνου και βελτιώνει το ρυθμό bit αλλά μειώνει τη συμφωνία καθώς καταγράφονται τιμές επιτάχυνσης με μεγαλύτερη ακρίβεια με αποτέλεσμα να διαφέρουν από συσκευή σε συσκευή.
- Η αύξηση της παραμέτρου a μειώνει το φάσμα των τιμών της επιτάχυνσης που κρατούνται και συνεπώς επιφέρει μείωση του ρυθμού bit. Παράλληλα παρατηρείται ότι ο ρυθμός συμφωνίας για ένα νόμιμο χρήστη αυξάνεται καθώς αυξάνεται ο αριθμός των μετρήσεων που εξαιρούνται. Αντίθετα ο ρυθμός συμφωνίας για έναν αντίπαλο μειώνεται καθώς δεν ξέρει ποιοι δείκτες κρατούνται και άρα δεν μπορεί να συσχετίσει τις ακολουθίες του με τις νόμιμες. Αυτή η συμπεριφορά φαίνεται στα Σχήματα 5 c και d.

- Σύμφωνα με τα Σχήμα 5 e και f, η διαδικασία της συμφωνίας του κλειδιού μειώνει τον ρυθμό bit ενώ αυξάνει την ρυθμό συμφωνίας. Δεδομένου ότι σκοπός του πρωτοκόλλου είναι να δημιουργήσει κρυπτογραφικό κλειδί, η συμφωνία είναι απαραίτητη ως διαδικασία.
- Στο Σχήμα 5g παρουσιάζεται η επίδραση της διαδικασίας της ιδιωτικότητας και πιο συγκεκριμένα της συνάρτησης XOR. Παρατηρείται ότι η εντροπία είναι πιο κοντά στο 1 μετά την εφαρμογή της συνάρτησης και άρα πετυχαίνεται ο σχεδιαστικός στόχος.
- Η εφαρμογή ICA, σύμφωνα με το Σχήμα 5h προσφέρει τεράστια βελτίωση στον ρυθμό συμφωνίας καθώς και ότι πριν την εφαρμογή του ο ρυθμός ήταν της τάξης του 50% και άρα σαν να διενεργούταν τυχαία επιλογή.
- Τέλος, άλλα πειράματα που δεν παρουσιάζονται έδειξαν ότι οι αισθητήρες που βρίσκονται στον κορμό του σώματος και πιο συγκεκριμένα τα ζεύγη μέση-στήθος και στήθος-κεφάλι έχουν καλύτερο ρυθμό συμφωνίας bit.

Ανάλυση Ασφάλειας

Η τυχαιότητα του δημιουργούμενου κλειδιού είναι κρίσιμης σημασίας καθώς πρόκειται για κρυπτογραφική εφαρμογή. Για τον έλεγχο αυτής της ιδιότητας χρησιμοποιήθηκε το σύνολο στατιστικών ελέγχων του NIST και ολοκληρώθηκαν όλα με επιτυχία.

Μια πιθανή επίθεση η οποία ελέγχθηκε είναι αυτή της μίμησης είτε ενεργητικά είτε παθητικά. Στην ενεργητική εκδοχή ο επιτιθέμενος προσπαθεί να μιμηθεί το βάδισμα ενός νόμιμου χρήστη με σκοπό να ζευγαρώσει την συσκευή του με τη δική του. Στην παθητική εκδοχή ο σκοπός παραμένει ο ίδιος αλλά ο επιτιθέμενος προσπαθεί να χρησιμοποιήσει το δικό του βάδισμα. Τα πειραματικά αποτελέσματα έδειξαν ότι για δεδομένα a=0.8 μπορεί να επιτευχθεί 50% και 30% ρυθμός συμφωνίας και άρα το βάδισμα ενός χρήστη προσφέρει αρκετή μοναδικότητα για την δημιουργία κλειδιών.

Τέλος, στη φάση της συμφωνίας η χρήση MAC μεθόδων προφυλάσσει από την εισαγωγή λανθασμένων τιμών από ένα κακόβουλο παράγοντα.

7. Υλοποίηση του Συστήματος

Στα πλαίσια της ερευνητικής διαδικασίας έγινε μια υλοποίηση του συστήματος σε ένα έξυπνο κινητό Moto E2. Το λειτουργικό σύστημα που χρησιμοποιήθηκε ήταν Android και έγινε υλοποίηση του συστήματος σε Java με την χρήση βιβλιοθηκών για τους αλγορίθμους που παρουσιάστηκαν. Η συχνότητα δειγματοληψίας τέθηκε στα 30Hz και για την ασύρματη επικοινωνία χρησιμοποιήθηκε Bluetooth Low Energy (BLE). Το συγκριμένο μοντέλο κινητού έχει χωρητικότητα μπαταρίας 2390 mAh (30.1 kJ) και θεωρήθηκε ότι έχει προσδόκιμο ζωής 1 ημέρα ή 1.25 kJ/ώρα.

	Υπολογιστικός Χρόνος (ms)	Κατανάλωση Ενέργειας (mJ)
ICA	105.7	71.2
Αναγνώριση Συνιστώσας	2.6	1.5
Δημιουργία Κλειδιού	208.1	12.7
AES Κρυπτογράφηση	0.2	0.1
AES Αποκρυπτογράφηση	0.2	0.1
Συνολικά	316.8	85.6

Σχήμα 6: Επιβάρυνση Συστήματος στο Moto E2

Όπως φαίνεται και στο Σχήμα 6 το ενεργειακό αποτύπωμα της εφαρμογής είναι πολύ μικρό και μπορεί να γίνει χρήση στην καθημερινότητα.

8. Επίλογος

Εν κατακλείδι, παρουσιάστηκε ένα πρωτόκολλο για την δημιουργία κρυπτογραφικών κλειδιών το οποίο χρησιμοποιεί τιμές επιτάχυνσης που προκύπτουν από το βάδισμα ενός χρήστη. Η συγκεκριμένη μέθοδος εκμεταλλεύεται την μοναδικότητα του βαδίσματος του κάθε ανθρώπου. Πειραματικά αποτελέσματα έδειξαν ότι τα κλειδιά που δημιουργούνται από ανεξάρτητες πηγές στο σώμα μπορούν να φτάσουν μέχρι και σε 100% συμφωνία καθώς και ότι η συγκεκριμένη εφαρμογή χαρακτηρίζεται από ενδογενή ασφάλεια και χαμηλή επιβάρυνση σε ένα σύστημα που υλοποιείται.