Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Συστήματα Ασύρματης επικοινωνίας*

Μεταπτυχιακή Διατριβή

Ενισχυμένη εμπειρία χρήστη μέσω RFID σε συνωστισμένους χώρους στη Κύπρο

Γεώργιος Κρέκος

Επιβλέπουσα Καθηγήτρια

Αδαμαντίνη Περατικού

Μάιος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Συστήματα Ασύρματης επικοινωνίας*

Μεταπτυχιακή Διατριβή

Ενισχυμένη εμπειρία χρήστη μέσω RFID σε συνωστισμένους χώρους στη Κύπρο

Γεώργιος Κρέκος

Επιβλέπουσα Καθηγήτρια

Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών
στον Γεώργιο Κρέκο

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Πανεπιστημίου Κύπρου

Μάιος 2020

Περίληψη

Εδώ και αρκετά χρόνια η χρήση και ανάπτυξη τεχνολογικών συστημάτων αποτελεί συστατικό κάθε επιχείρησης που εδράζεται στο χώρο του λιανικού εμπορίου και όχι μόνο. Η RFID τεχνολογία αποτελεί μια μέθοδο ανίχνευσης και παρακολούθησης ανθρώπων, ζώων ή αντικειμένων με την ανάγνωση των δεδομένων που αποθηκεύονται σε ετικέτες. Η δυνατότητα ανίχνευσης μέσω ραδιοσυχνοτήτων, σε συνδυασμό με τη αναγνώριση μεμονωμένου προϊόντος και την αποθήκευση αρκετών δεδομένων, άνοιξε νέους ορίζοντες για τη διαχείριση της εφοδιαστικής και καταναλωτικής αλυσίδας.

Με την υιοθέτηση RFID τεχνολογιών, οι επιχειρήσεις και βιομηχανίες επιδιώκουν να λειτουργήσουν πιο γρήγορα , πιο αποδοτικά,όσον αφορά τον καταναλωτή και με μεγαλύτερη αξιοπιστία και αυτό γίνεται με τη βελτίωση του επίπεδου των υπηρεσιών που προσφέρουν στους πελάτες τους, τη καλύτερη διαχείριση των αποθεμάτων και τον περιορισμό του κόστους που είναι ελκυστικό «πακέτο» για κάθε πελάτη- καταναλωτή

Αρχικά λοιπόν, η τεχνολογία RFID προωθήθηκε ως λύση για τα προβλήματα του εφοδιαστικού κύκλου. Όμως, μέσα από πιλοτικές εφαρμογές στην Κύπρο και παγκοσμίως, οι επιχειρήσεις αρχίζουν να καταλαβαίνουν τις δυνατότητες της μεθόδου RFID στις πραγματικές τους διαστάσεις. Οι σύγχρονες επιχειρήσεις δεν αρκούνται πλέον μόνο στον έλεγχο των εσωτερικών τους διαδικασιών, αλλά προχωρούν σε συνεργασίες με πελάτες και άλλες επιχειρήσεις για τη δημιουργία ενός ολοκληρωμένου εφοδιαστικού κύκλου, όπου παρακολουθείται η πορεία του προϊόντος, από την παραγωγή στην κατανάλωση.

Η παρούσα μεταπτυχιακή εργασία περιλαμβάνει την έρευνα για το ποσό αποδοχής που θα υπάρχει από τις κυπριακές εταιρίες κατά την εισδοχή των συστημάτων RFID και επίσης το σχέδιο για ανάπτυξη μίας εφαρμογής για Android smartphones που θα αποσκοπεί στην περεταίρω εξυπηρέτηση των πελατών στα διάφορα καταστήματα ή υπεραγορές.

Summary

For decades, the use and development of technology systems has been an integral part of any business in retail. RFID technology is a method of directly detecting and tracking people, animals or objects by reading data stored on RFID tags. The ability to detect radio frequencies, combined with unique product recognition and data storage, has opened new horizons for supply chain management. By adapting RFID technologies, companies seek to operate faster, more efficiently and with greater reliability towards the customer. Through improving the level of services, they provide to their customers, better inventory management and reduction of costs.

Initially, RFID technology had been promoted as a solution to supply chain problems. However, through pilot applications in Cyprus and internationally, the companies have begun realising the potential of RFID technologies in its true dimensions. Modern businesses are no longer content with just controlling their internal processes but are working with customers and suppliers to create a complete supply chain, which monitors the product's full life cycle, from production to final consumption.

This postgraduate thesis encloses research regarding the extent to which the admission of RFID systems will be accepted from Cypriot companies, as well as a plan for development of an RFID technology adapted application for Android smartphone systems, that will aim at improving customer service in various stores or supermarkets.

Ευχαριστίες

Η παρούσα εργασία αποτελεί μεταπτυχιακή εργασία στα πλαίσια του μεταπτυχιακού προγράμματος σπουδών «Συστήματα Ασύρματης επικοινωνίας » του τμήματος Θετικών και Εφαρμοσμένων Επιστημών. Πριν την παρουσίαση των αποτελεσμάτων της παρούσας μεταπτυχιακή εργασίας, αισθάνομαι την υποχρέωση να ευχαριστήσω την επόπτρια μου, Αδαμαντίνη Περατικού για την πολύτιμη καθοδήγηση της ,την εμπιστοσύνη και εκτίμηση που μου έδειξε.

Στη συνέχεια θα ήθελα να ευχαριστήσω τις υπεραγορές Αλφαμέγα και Olympic για την φιλοξενία και την παραχώρηση του χώρου τους για τη διεξαγωγή συλλογής δεδομένων και πληροφοριών από τους πελάτες τους.

Τέλος, θέλω να ευχαριστήσω τους γονείς και τα αδέρφια μου, που με υπομονή και κουράγιο πρόσφεραν την απαραίτητη ηθική συμπαράσταση για την ολοκλήρωση της μεταπτυχιακής μου εργασίας.

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

1.1. Αντικείμενο της εργασίας

Η τεχνολογία Ραδιοσυχνικής Αναγνώρισης ή αλλιώς Radio Frequency Identification (RFID) αποτελεί μια τεχνολογία που χρησιμοποιεί τις ραδιοσυχνότητες για την αναγνώριση ανθρώπων ή αντικειμένων. Ανήκει στις τεχνολογίες αυτόματης αναγνώρισης και μάλιστα θεωρείται η μετεξέλιξη της τεχνολογίας των ραβδωτών κωδικών.

Ένα RFID σύστημα χρησιμοποιεί αναγνώστες για την συλλογή δεδομένων από ετικέτες . Τα δεδομένα αυτά μπορούν να συσχετιστούν με άλλα δεδομένα που βρίσκονται καταχωρημένα σε μια βάση δεδομένων. Για την RFID τεχνολογία έχουν αναπτυχθεί διάφορα πρότυπα από οργανισμούς όπου και χρησιμοποιούν την αναγνώριση μέσω ραδιοσυχνοτήτων με σκοπό να επιτρέψει και να διευκολύνει την ορατότητα πληροφοριών σχετικά με τα αντικείμενα και τα άτομα αλλά και τον διαμοιρασμό των πληροφοριών αυτών .

Τα RFID συστήματα αντιμετωπίζουν παράλληλα διάφορες απειλές και επιθέσεις. Σημαντικά είναι τα ζητήματα που προκύπτουν όσον αφορά την ιδιωτικότητα αφού μπορεί να γίνει λαθραία παρακολούθηση ατόμων και αντικειμένων και αποκάλυψη προσωπικών δεδομένων καθώς και ζητήματα που αφορούν την αυθεντικοποίηση αφού οι ετικέτες μπορούν να κλωνοποιηθούν ή να παραποιηθούν τα δεδομένα τους.

Η τεχνολογία Ραδιοσυχνικής Αναγνώρισης είναι πλέον κατανοητό ότι βρίσκεται σε ένα ώριμο στάδιο. Υπάρχει πληθώρα κατασκευαστών και προϊόντων που μπορούν να καλύψουν οποιαδήποτε ανάγκη. Καθημερινά συναντάμε την RFID στην ζωή μας και η πρακτική αξιοποίηση της συγκεκριμένης τεχνολογίας είναι γεγονός αδιαμφισβήτητο. Η βελτιστοποίηση της ήδη υπάρχουσας τεχνολογίας για μια ευκολότερη και αποτελεσματικότερη χρήση κυρίως σε χώρους που χρησιμοποιείται ευρέως π.χ. αεροδρόμια , εμπορικά κέντρα κτλ. θα ήταν ευχής έργο.

2. Η ΤΕΧΝΟΛΟΓΙΑ RFID

2.1. Ιστορική αναδρομή

Τα πρώτα συστήματα RFID, αναφέρετε να έχουν ξεκινήσει από την εποχή του Β παγκοσμίου πολέμου. Την εποχή εκείνη γινόταν χρήση της τεχνολογίας των ραντάρ για την ανίχνευση των αεροπλάνων που πλησίαζαν, έστελναν παλμούς ραδιοκυμάτων και λάμβαναν τις ηχώ που δημιουργούνταν από τα αεροσκάφη. Όμως μόνο με την οπτική επαφή μπορούσαν να εξακριβώσουν αν το αεροπλάνο ήταν εχθρικό ή συμμαχικό. Οι Γερμανοί βρήκαν λύση σε αυτό το πρόβλημα, οι πιλότοι κατά την επιστροφή τους στην βάση έκαναν μια συγκεκριμένη μανούβρα η οποία επηρέαζε την απεικόνιση του σήματός τους στο ραντάρ. Με αυτή την παρατήρηση το Γερμανικό προσωπικό ελέγχου, ξεχώριζε τα εχθρικά του αεροπλάνα από αυτά τα συμμαχικά. Αυτό ουσιαστικά ήταν και το πρώτο παθητικό σύστημα RFID.

Αργότερα, ο βρετανικός στρατός εισήγαγε ένα πιο εξελιγμένο σύστημα που το ονόμασαν Identify Friend or Foe (IFF). Η τεχνολογία αυτή πλησιάζει περισσότερο στα σημερινά συστήματα RFID στην οποία, κάθε αεροσκάφος ήταν εξοπλισμένο με ένα αναμεταδότη που ρύθμιζε το σήμα των ραντάρ, επιτρέποντας έτσι την αναγνώριση του συμμαχικού αεροσκάφους. Η συγκεκριμένη τεχνολογία λόγω της απλότητας αλλά και την ανθεκτικότητας της έχει παραμένει και γίνεται χρήση της από τον κλάδο της αεροπορίας μέχρι και σήμερα, κρατώντας τα αεροπλάνα ανιχνεύσιμα. Ωστόσο, η αναγνώριση ενός μη συμμαχικού αεροπλάνου, θα πρέπει να αντιμετωπίζεται με προσοχή , αφού δεν υπάρχει καμιά απόδειξη ότι είναι εχθρικό. Προφανώς, αυτή η ανακρίβεια έχει προκαλέσει ατυχήματα, για παράδειγμα, το 1983, ο στρατός της Σοβιετικής Ένωσης πυροβόλησε ένα κορεατικό επιβατικό αεροπλάνο που είχε θεωρηθεί κατασκοπικό. Ομοίως, ένα επιβατικό αεροπλάνο από το Ιράν, καταρρίφθηκε το 1988 από το στρατό των Ηνωμένων Πολιτειών, με αποτέλεσμα πλήρωμα και επιβάτες να σκοτωθούν.

Καθώς οι εξελίξεις σε συστήματα επικοινωνιών ραδιοσυχνοτήτων και σε χαμηλού κόστους ενσωματωμένους υπολογιστές συνεχίστηκαν τη δεκαετία του 1950, 1960 και 1970, αναπτύχθηκαν αρκετές τεχνολογίες που σχετίζονται με ραδιοκύματα (π.χ. Electronic Article Surveillance application (EAS) που έχουνσχεδιαστεί για την αποφυγή κλοπής προϊόντων από καταστήματα

λιανικής πώλησης). Παρ 'όλα αυτά, το πρώτο δίπλωμα ευρεσιτεχνίας για τις παθητικές ετικέτες RFID (ανάγνωσης-εγγραφής) λήφθηκε από τον Mario Cardullo το 1973. Αυτό το σύστημα θεωρείται ο πρώτος αληθινός πρόγονος της σύγχρονης RFID τεχνολογίας, καθώς ήταν ένας παθητικός ραδιοφωνικός αναμεταδότης με μνήμη. Εκ τότε τα συστήματα RFID δεν είναι ιδιαίτερα ευδιάκριτα, αφού οι μοντέρνες RFID ετικέτες έχουν το μέγεθος ενός κόκκου ρυζιού αλλά μπορεί να έχουν δυνατότητες ενός υπολογιστή, όπως: μνήμη μόνο για ανάγνωση (Read-Only Memory (ROM)), Electrically Erasable Programmable Read-Only Memory (EEPROM), μπορεί να λειτουργεί με χρήση μπαταριών αντί της ισχύος των αναγνωστών RFID κ.λπ.

Κατά συνέπεια, με την πάροδο των ετών, ο αριθμός των λύσεων βασισμένων στην τεχνολογία RFID έχει αναπτυχθεί σημαντικά. Στην πραγματικότητα, τα συστήματα RFID είναι πλέον περισσότερο συνδεδεμένα με την βιομηχανία και τις επιχειρήσεις από ότι με το στρατό. Για παράδειγμα στις δεκαετίες του 1980 και 1990, εμφανίστηκαν εφαρμογές RFID στους τομείς των μεταφορών, τον έλεγχο πρόσβασης, την ταυτοποίηση των ζώων, την παρακολούθηση πυρηνικών υλικών, των φορτηγών και την ηλεκτρονική είσπραξη διοδίων [1].Η τάση αυτή αυξήθηκε κατά την διάρκεια του 21ου αιώνα με την μείωση των τιμών των RFID ετικετών καθώς και της τυποποίησης RFID.

2.2. Συστήματα RFID

Γενικά, τα συστήματα RFID εντοπίζουν και παρακολουθούν αντικείμενα χρησιμοποιώντας τα ραδιοκύματα, παρόμοια με άλλα συστήματα αναγνώρισης όπως οι ραβδωτοί κώδικες, δακτυλικά αποτυπώματα ή αναγνώριση της ίριδας των ματιών. Ο αναγνώστης RFID (RFID reader) διαβάζει από κάποια πηγή δεδομένων ταυτοποίησης, τις ετικέτες RFID (RFID tag), στην συνέχεια τα δεδομένα ταυτοποίησης, επεξεργάζονται από ένα υποσύστημα ή έναν σέρβερ.

Αυτό που κάνει τα συστήματα RFID να ξεχωρίζουν από τα υπόλοιπα συστήματα αναγνώρισης είναι ότι, μπορούν να είναι εξίσου φθηνά με τα συστήματα ραβδωτού κώδικα αλλά ταυτόχρονα να χρησιμοποιούν ασύρματο κανάλι όπως το GPS ή το GSM και να έχουν και κάποιες υπολογιστικές δυνατότητες αντίστοιχες των μαγνητικών καρτών. Γι 'αυτό έχει δοθεί περισσότερη προσοχή σε αυτήν την τεχνολογία.

Με πιο τεχνικούς όρους το RFID σύστημα αποτελείται από τρία βασικά στοιχεία :

1. ***Την ετικέτα RFID*** (RFID tag) ή αναμεταδότη, που περιέχει πληροφορίες και στοιχεία αναγνώρισης.
2. ***Τον αναγνώστη RFID*** (RFID reader) ή πομποδέκτη, που λαμβάνει από τους αναμεταδότες τις πληροφορίες που είναι αποθηκευμένες σε αυτούς. Αυτές οι πληροφορίες μπορούν να κυμαίνονται από στατικούς αριθμούς αναγνώρισης έως δεδομένα χρήστη ή δεδομένα τα οποία λαμβάνονται από αισθητήρες.
3. ***Το υποσύστημα επεξεργασίας δεδομένων*** ή το ***σέρβερ*** που επεξεργάζεται τα δεδομένα που λαμβάνονται από τους αναγνώστες RFID.

Διαισθητικά, όλα τα αντικείμενα που θα πρέπει να ταυτοποιηθούν, φέρουν την φυσική ετικέτα RFID. Στην συνέχεια οι αναγνώστες RFID θα πρέπει να διανέμονται με στρατηγικό τρόπο έτσι ώστε να ανακτούν τα απαιτούμενα δεδομένα από τις ετικέτες. Παραδείγματος χάριν, ένα σύστημα χρονομέτρησης αγώνων ποδηλάτου πρέπει να τοποθετήσει τουλάχιστον έναν αναγνώστη στην αφετηρία και ακόμα έναν στην γραμμή τερματισμού. Άλλες ιδιότητες των αναγνωστών, δηλαδή το μέγεθος πεδίου ανταπόκρισης, οι υπολογιστικές δυνατότητες καθώς και το μέγεθος μνήμης των ετικετών, διαφέρουν από εφαρμογή σε εφαρμογή.

2.3. Ετικέτες RFID

Συνήθως, οι αναμεταδότες ή οι ετικέτες RFID αποτελούνται από ολοκληρωμένα κυκλώματα συνδεδεμένα σε μια κεραία. Η μνήμη χρησιμεύει ως χώρος αποθήκευσης δεδομένων, εγγράψιμος και μη εγγράψιμος, ο οποίος μπορεί να κυμαίνεται μεταξύ μερικών bytes μέχρι και αρκετών kilobytes. Οι ετικέτες μπορούν να σχεδιαστούν για διάφορες χρήσεις, όπως μόνο για ανάγνωση (read-only), για εγγραφή μόνο μια φορά (write-once), για πολλαπλή ανάγνωση (read-many) ή για πλήρη επανεγγραφή (fully rewritable). Επομένως, ο προγραμματισμός ετικετών μπορεί να πραγματοποιηθεί σε επίπεδο παραγωγής ή σε επίπεδο εφαρμογής.

Μια ετικέτα μπορεί να λάβει ενέργεια από το σήμα που έλαβε από τον αναγνώστη ή μπορεί να έχει τη δική της εσωτερική πηγή ισχύος. Ο τρόπος που οι ετικέτες λαμβάνουν ενέργεια καθορίζει γενικά την κατηγορία τους:

- ***Οι παθητικές ετικέτες*** , χρησιμοποιούν την ισχύ που παρέχεται από τον αναγνώστη μέσω ηλεκτρομαγνητικών κυμάτων. Η απώλεια τροφοδοσίας σημαίνει ότι η συσκευή μπορεί να είναι αρκετά μικρή και φθηνή.
- ***Οι ημι-παθητικές ετικέτες*** φέρουν μια μπαταρία για να μπορούν να θέσουν σε ισχύ το κύκλωμα του μικροτσίπ, αλλά η επικοινωνία επιτυγχάνεται συλλέγοντας ισχύ από το σήμα του αναγνώστη, όπως και οι παθητικές.
- ***Οι ενεργητικές ετικέτες*** έχουν τη δική τους εσωτερική πηγή τροφοδοσίας, συνήθως μια μπαταρία, η οποία χρησιμοποιείται για να τροφοδοτήσει το εξερχόμενο σήμα.

Οι ετικέτες RFID μπορούν επίσης να ταξινομηθούν ανάλογα με την ισχύ επεξεργασίας τους. Υπάρχουν οι ετικέτες που, δεν έχουν σημαντική ισχύ επεξεργασίας, υπάρχουν και οι πιο "έξυπνες" ετικέτες οι οποίες έχουν ενσωματωμένους επεξεργαστές οι οποίοι μπορούν να εκτελέσουν λειτουργίες με κρυπτογραφημένο κώδικα [2]. Οι ετικέτες χωρίς τους επεξεργαστές αποτελούν την καρδιά των συστημάτων RFID, αφού λόγω του χαμηλού κόστους τους έχουν αρκετές εφαρμογές σε εργοστάσια και καταστήματα λιανικής πώλησης. Επίσης σε διάφορες χώρες, απαιτούν από τους ιδιοκτήτες κατοικίδιων ζώων να εμφυτεύσουν μια ετικέτα RFID τα κατοικίδια ζώα τους.

Αυτές οι ετικέτες περιέχουν πληροφορίες που επιτρέπουν γρήγορο και αποτελεσματικό εντοπισμό ιδιοκτητών κατοικίδιων ζώων σε περίπτωση απώλειας των κατοικίδιων ζώων τους. Ο λόγος που κάνει τις ετικέτες αυτής της κατηγορίας κατάλληλες και πιο πρακτικές για τον εντοπισμό κατοικίδιων είναι το ότι δεν υπάρχει κίνδυνος παραχάραξης της ταυτότητας ενός κατοικίδιου. Με τη σειρά τους, οι "έξυπνες" ετικέτες χρησιμοποιούνται για τις εφαρμογές που απαιτούν κάποιο επίπεδο ασφάλειας ή/και ιδιωτικότητας, συγκεκριμένα για ηλεκτρονικά διαβατήρια, για διαχείριση εφοδιαστικής αλυσίδας (ΔΕΑ) ή έλεγχο πρόσβασης.

Λαμβάνοντας υπόψη ότι τα συστήματα RFID βασίζονται σε ραδιοκύματα, οι ετικέτες λειτουργούν με μια καθορισμένη συχνότητα. Υπάρχουν τέσσερα κύρια εύρη συχνοτήτων: χαμηλή συχνότητα (LF), υψηλή συχνότητα (HF),κατεξοχήν υψηλή συχνότητα (UHF) και τα μικροκύματα. Η ακριβής

συχνότητα ποικίλλει ανάλογα με την εφαρμογή και τους κανονισμούς σε διάφορες χώρες. Οι συχνότητες που συνηθίζονται να χρησιμοποιούνται συχνά για τα συστήματα RFID παρατίθενται στον πίνακα (1).

Frequency Band	**Operating Range**	**Applications**
125kHz to 134kHz (LF)	≈ 0.5 Meters	Access control and Animal identification
13.56MHz (HF)	≈ 1 Meters	Library books and Smart cards
860MHz to 930MHz (UHF)	≈ 3 Meters	Logistic and Parking access
2.4GHz (Microwave)	≈ 10 Meters	Electronic toll collection and Airline baggage tracking

Πίνακας 1

2.4. Αναγνώστες RFID

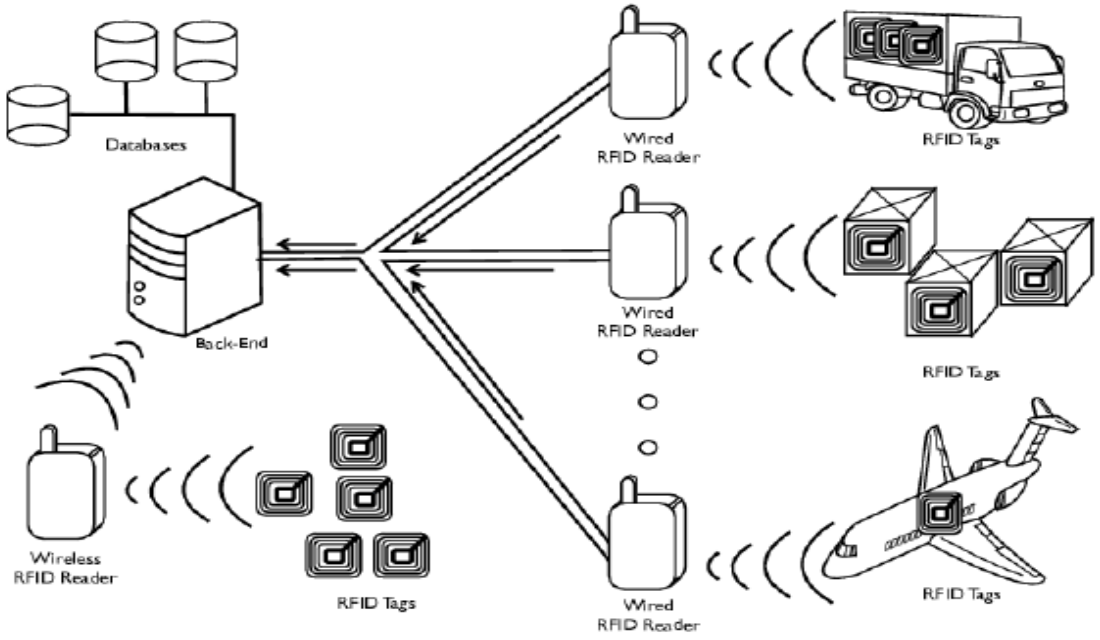
Γενικά οι πομποδέκτες ή οι συσκευές ανάγνωσης RFID αποτελούνται από μια μονάδα ραδιοσυχνοτήτων, μια μονάδα ελέγχου και ένα στοιχείο ζεύξης για τον εντοπισμό ετικετών RFID επικοινωνώντας με ραδιοσυχνότητες. Οι αναγνώστες μπορούν να εκτελέσουν δύο τύπους κλήσεων: multicast και unicast. Οι κλήσεις πολλαπλής διανομής (multicast) απευθύνονται σε όλες τις ετικέτες στο εύρος ενός αναγνώστη, ενώ οι κλήσεις μονής διανομής (unicast) απευθύνονται σε συγκεκριμένες ετικέτες. Προκειμένου να διατηρηθούν οι αναγνώστες όσο το δυνατόν πιο απλοί, έχουν συνήθως μια διεπαφή που τους επιτρέπει να προωθούν τα ληφθέντα δεδομένα σε ένα υποσύστημα επεξεργασίας δεδομένων ή μια βάση δεδομένων ή σε έναν σέρβερ. Με αυτόν τον τρόπο, οι αναγνώστες μεταβιβάζουν το μεγαλύτερο μέρος της υπολογιστικής επεξεργασίας και υπολογισμών σε άλλες πιο ισχυρές συσκευές επεξεργασίας δεδομένων, έτσι ώστε να επιτευχθεί η διατήρηση της απλότητας των συσκευών αναγνώρισης.

2.5.Υποσύστημα επεξεργασίας δεδομένων

Το υποσύστημα επεξεργασίας δεδομένων ή ο σέρβερ, χρησιμοποιείται για να ξεπεράσει τους περιορισμούς υπολογιστικής επεξεργασίας των ετικετών και των αναγνωστών. Και τα δύο μέρη του συστήματος χρειάζεται να συνδεθούν σε ένα υποσύστημα επεξεργασίας, επειδή από την μια

οι ετικέτες στέλνουν πληροφορίες που χρειάζονται οι αναγνώστες και έτσι αυτές οι πληροφορίες συνήθως αποθηκεύονται σε βάσεις δεδομένων. Από την άλλη έχοντας επιπλέον στόχο και τη μείωση του κόστους των αναγνωστών RFID, οι κρυπτογραφικές συναρτήσεις ή οι αλγόριθμοι επεξεργασίας δεδομένων πρέπει να βασίζονται σε ένα υποσύστημα επεξεργασίας δεδομένων ή σέρβερ, διατηρώντας έτσι το χαμηλό κόστος τους.

Πρέπει να σημειωθεί ότι γενικά θεωρείται ασφαλής η σύνδεση μεταξύ αναγνωστών και βάσεων δεδομένων, έτσι η επικοινωνία αναγνώστη με συστήματα επεξεργασίας ή η επικοινωνία ετικέτας με συστήματα επεξεργασίας δεν ανήκει στα προβλήματα που αντιμετωπίζει η τεχνολογία RFID.



Εικόνα 1 Γραφική αναπαράσταση των μερών και μελών που αποτελούν ένα σύστημα RFID και των βασικών σχέσεων/συνδέσεων τους.

2.6. Εφαρμογές

Η τεχνολογία RFID χαρακτηρίζεται από την αυξανόμενη δημοτικότητά της. Κατά συνέπεια, ένας μεγάλος αριθμός λύσεων RFID χρησιμοποιούνται από όλο και περισσότερες επιχειρήσεις και βιομηχανίες. Δεν αποτελεί έκπληξη, ότι οι κυβερνήσεις έχουν επίσης παρατηρήσει τα οφέλη των συστημάτων RFID στις συνήθεις εργασίες, δηλαδή τον έλεγχο διαβατηρίων και την

παρακολούθηση εγγράφων. Επομένως, είναι δύσκολο να πούμε ακριβώς πόσα συστήματα RFID έχουν ήδη αναπτυχθεί παγκοσμίως. Ωστόσο, είναι σαφές ότι αυτά τα συστήματα γίνονται όλο και πιο δημοφιλή με την πάροδο του χρόνου.

2.6.1.Ταυτοποίηση

Από την αρχή της τεχνολογίας RFID κατά τον Δεύτερο Παγκόσμιο Πόλεμο, η ταυτοποίηση ήταν ο πρωταρχικός της στόχος και μια από τις πρώτες εφαρμογές. Ακόμα και σήμερα τα πράγματα δεν έχουν αλλάξει και πολύ αφού από τις πιο συχνές εφαρμογές της τεχνολογίας RFID είναι, η ταυτοποίηση ζώων, συστήματα απογραφής, ανθρώπινα εμφυτεύματα, ταυτοποίηση ασθενών και έλεγχος φαρμάκων, είναι μόνο μερικά παραδείγματα αναγνώρισης με ραδιοσυχνότητα.

(α) (β)

Εικόνα 2 :(α) Θέση με την προγραμματισμένη θέση του τσιπ RFID (β) Χέρι με εμφύτευμα RFID τσιπ. Το κίτρινο είναι η απολύμανση πριν παρεμβάλει το τσιπ.

2.6.2. Παρακολούθηση

Υπάρχουν πολλά σενάρια στα οποία τα συστήματα RFID είναι τα πιο κατάλληλα για παρακολούθηση (π.χ. εσωτερικούς χώρους ή για επιτήρηση ζώων). Επίσης, σε σύγκριση με άλλα συστήματα παρακολούθησης όπως το GPS ή το GSM, η τεχνολογία RFID θεωρείται πολύ λιγότερο δαπανηρή. Αυτός είναι ο λόγος για τον οποίο η παρακολούθηση, μαζί με την αναγνώριση, θεωρείται ένας από τους πρωταρχικούς στόχους των συστημάτων RFID. Για παρακολούθηση, απαιτούνται συνήθως ετικέτες που λειτουργούν σε υψηλή συχνότητα επειδή έχουν μεγαλύτερο εύρος ανάγνωσης. Αυτοί οι τύποι ετικετών χρησιμοποιούνται για

παρακολούθηση σε βιβλιοθήκες ή βιβλιοπωλεία, έλεγχος πρόσβασης κτιρίων, παρακολούθηση αποσκευών αεροπορικών εταιρειών και παρακολούθηση ειδών ένδυσης και φαρμακευτικών προϊόντων.

2.6.3. Ιατροφαρμακευτική Περίθαλψη

Η βιομηχανία της ιατροφαρμακευτικής περίθαλψης έχει επενδύσει σε μεγάλο βαθμό στο RFID. Η αλυσίδα εφοδιασμού γενικά στον τομέα της υγείας, η πρόληψη της παραχάραξης των φαρμάκων ή η ασφάλεια των ασθενών, είναι μόνο μερικά παραδείγματα κρίσιμων διαδικασιών που παρακολουθούνται από το RFID. Με αυτόν τον τρόπο, οι ασθενείς ενός νοσοκομείου στην Αγγλία θα μπορούσαν να αποφύγουν την έκθεση σε ασθένειες που προκαλούνται από μολυσμένο εξοπλισμό που δεν εντοπίστηκε και ταξινομήθηκε σωστά [6]. Επιπλέον, οι απορριφθείσες συσκευασίες φαρμάκων δεν θα μπορούν να επαναχρησιμοποιηθούν από εταιρείες που προσπαθούν να πουλήσουν πλαστά φαρμακευτικά προϊόντα, όπως σημειώνεται από την κολομβιανή φαρμακευτική αλυσίδα Medicarte [7].

Εικόνα 3 Έλεγχος και προσδιορισμός των φαρμάκων

2.6.4. Ηλεκτρονικά διαβατήρια

Ηλεκτρονικά διαβατήρια (ηλεκτρονικά διαβατήρια) ή διαβατήρια με ενσωματωμένη ετικέτα RFID έχουν εισαχθεί σε πολλές χώρες, όπως και στην Κύπρο. Σε αντίθεση με τις περισσότερες εφαρμογές RFID, οι ετικέτες RFID στα διαβατήρια είναι ένα είδος έξυπνης κάρτας και όχι μιας ετικέτας χαμηλού κόστους. Είναι σε θέση να εκτελέσουν υπολογιστικά πολύπλοκα κρυπτο-συστήματα και επίσης είναι αναλλοίωτες. Επιπλέον, πολλές πληροφορίες μπορεί να αποθηκευτούν στη μνήμη της ετικέτας, όπως όνομα, ημερομηνία γέννησης, βιομετρικές πληροφορίες, φωτογραφία και άλλα. Αυτές οι πληροφορίες μπορεί να αντιπαραβληθούν με τις διαθέσιμες πληροφορίες σε χαρτί, μειώνοντας έτσι τον κίνδυνο πλαστογραφίας και απάτης διαβατηρίου.

Ωστόσο, έχουν εντοπιστεί πολλές αδυναμίες στα ηλεκτρονικά διαβατήρια [8]. Ιδιαίτερα ανησυχητικές είναι αυτές που επιτρέπουν στην αποτελεσματική κλωνοποίηση ενός ηλεκτρονικού διαβατήριου, έτσι ώστε ο αναγνώστης RFID να μην μπορεί να διακρίνει το νόμιμο διαβατήριο.[9,10]. Εν πάση περίπτωσή, οι κυβερνήσεις ισχυρίζονται ότι η κλωνοποίηση δεν είναι μεγάλο πρόβλημα, καθώς οι ηλεκτρονικές πληροφορίες που είναι αποθηκευμένες στην μνήμη της ετικέτας πρέπει να ταιριάζουν με τα φυσικά χαρακτηριστικά των χρηστών. Επιπλέον, έχει κυκλοφόρησει η τρίτη γενιά ηλεκτρονικών διαβατηρίων που, ακόμη δεν έχει γίνει οποιαδήποτε αναφορά για επίθεση κλωνοποίησης.

Εικόνα 4 Έλεγχος παλαιού τύπου διαβατηρίου με χρήση RFID

2.6.5. Πληρωμές μέσων μαζικής μεταφοράς

Οι πληρωμές σε δημόσια μέσα μεταφοράς με κάρτες RFID είναι πιθανώς μια από τις πρώτες αξιοπρόσεκτες επαφές που έχουμε με αυτήν την τεχνολογία. Με αυτήν τη λύση δεν γίνεται τόσο συχνή χρήση κερμάτων από τους επιβάτες και η αλλαγή μετρητών από τους οδηγούς. Ως εκ τούτου, μειώνεται ο φόρτος εργασίας των οδηγών λεωφορείων, μειώνοντας έτσι τον κίνδυνο τροχαίου ατυχήματος λόγω περισπασμών και τηρώντας έτσι το χρονοδιάγραμμα των διαδρομών λόγω καθυστέρησης στις εισπράξεις.

Σύμφωνα με το διεθνές πρότυπο Calypso3 (RFID), αρκετές χώρες στην Ευρώπη και την Αμερική χρησιμοποιούν κάρτες RFID για συστήματα δημόσιων μεταφορών. Στην Ασία, ιδίως στο Χονγκ Κονγκ, άλλοι τύποι καρτών RFID, που ονομάζονται Octopus Cards, χρησιμοποιούνται επίσης για συστήματα μεταφοράς. Αυτές οι κάρτες χρησιμοποιούνται σαν πιστωτικές κάρτες μπορεί να

χρησιμοποιοηθούν σε μηχανήματα αυτόματης πώλησης, εστιατόρια «φάστ φούντ» και σουπερμάρκετ. Υπάρχουν πολλές άλλες πληρωμές με μέσα μαζικής μεταφοράς με βάση το RFID, όπως είναι και το σύστημα πληρωμών μετρό της Μόσχας ή το σύστημα χρήσης δημόσιων ποδηλάτων στη Βαρκελώνη που επίσης αποτρέπει την κλοπή τους.

Εικόνα 5 Ηλεκτρονική πληρωμή στην εταιρία McDonalds

Εικόνα 6 RFID κάρτες για ηλεκτρονική πληρωμή

2.7. Πλεονεκτήματα και μειονεκτήματα της τεχνολογίας RFID

2.7.1.Πλεονεκτήματα τεχνολογίας RFID

Τα πλεονεκτήματά της τεχνολογίας RFID σχετικά με άλλους τρόπους συλλογής δεδομένων είναι οι εξής (Goldman & Crawford, 2003; Mortensen & Pedersen, 2004; Μαστορίδου, 2007):

- Η τεχνολογία RFID επιτρέπει την παρακολούθηση και τη συλλογή δεδομένων σε περιβάλλοντα που είναι ακατάλληλα για εργαζομένους, επειδή η ανάγνωση ετικετών δεν απαιτεί την ύπαρξη εργατικού δυναμικού
- Αποδεικνύεται αξιόπιστη λειτουργιά ακόμα και σε «σκληρά» περιβάλλοντα και εφαρμογές όπου είναι πιθανό να υπάρχουν δονήσεις, χτυπήματα και κραδασμοί
- Απομακρύνει κρίσιμα λάθη από καταγεγραμμένα δεδομένα
- Τα δεδομένα της ετικέτας RFID μπορούν να μεταβληθούν συνεχώς
- Δεν απαιτείται άμεση οπτική επαφή μεταξύ της ετικέτας και του αναγνώστη

- Επιτάχυνση της συλλογής δεδομένων και λειτουργία χωρίς επαφή.
- Πάρα πολλοί οργανισμοί και επιχειρήσεις έχουν εκμεταλλευτεί τα οφέλη που προσφέρει η τεχνολογία RFID έτσι ώστε να παρακολουθούν τις διαδικασίες τους, να παρέχουν ακριβή δεδομένα σε πραγματικό χρόνο, να ιχνηλατούν και να παρατηρούν το απόθεμα μειώνοντας έτσι απαιτήσεις εργασίας
- Η τεχνολογία RFID δύναται να χρησιμοποιηθεί σε συνδυασμό σε συστήματα barcode και Wi-Fi δίκτυο
- Οι κατασκευαστές μπορούν να εντοπίζουν από που προέρχεται ένα προϊόν και έτσι, να αντιλαμβάνονται καλύτερα πότε δημιουργείται ένα επιτυχημένο προϊόν και πότε ένα ελαττωματικό.
- Οι επιχειρήσεις θα πληροφορούνται καλύτερα σχετικά με την απόδοση των προϊόντων μετά την πώλησή τους
- Οι ετικέτες διασφαλίζουν την παραγωγή μείωσης σφαλμάτων εντός εργοστασίου
- Οι ετικέτες RFID διασφαλίζουν την βελτίωση των logistics μιας βιομηχανίας
- Η τεχνολογία RFID είναι δυνατόν να εξαλείψει προβλήματα τύπου εξάντλησης αποθεμάτων, τα οποία μπορούν να δημιουργηθούν από την χρήση της Just-in-time(JIT)

2.7.2.Μειονεκτήματα της τεχνολογίας RFID

Με τη χρήση της τεχνολογίας RFID δεν υπάρχουν μόνο πλεονεκτήματα αλλά και μειονεκτήματα (Goldman & Crawford, 2003; Mortensen & Pedersen, 2004):

- Προβλήματα αναφορικά με την ασφάλεια και στην ιδιωτικότητα
- Το κόστος υλοποίησης της τεχνολογίας RFID είναι αρκετά ψηλό
- Ο τρόπος που λειτουργεί η τεχνολογία RFID απαιτεί και την ύπαρξη εναλλακτικών τρόπων απόκτησης των πληροφοριών
- Οι ετικέτες RFID παρουσιάζουν προβλήματα κατά την ανάγνωσή τους μέσω αγώγιμων υλικών
- Υπάρχουν διάφορα ανταγωνιστικά πρότυπα

- Η τεχνολογία RFID είναι λειτουργίσιμη σε περιβάλλον ραδιοσυχνοτήτων (RF), που επηρεάζεται από διάφορες συνθήκες και καταστάσεις. Το εύρος ανάγνωσης ή και εγγραφής μπορεί να διαφέρει αναλόγως καιρικών συνθηκών που επικρατούν
- Συνεχής εκπαίδευση για την χρήση των εντολών της γλώσσας προγραμματισμού των εφαρμογών για την τεχνολογία RFID (RFID command language) λόγω των αλλαγών που υπάρχουν χρόνο με τον χρόνο
- Δεν υπάρχει κάποια γενικού τύπου ετικέτα αλλά μία για κάθε εφαρμογή

3. ΠΡΩΤΟΚΟΛΛΑ RFID

Στις μέρες μας οποιαδήποτε τεχνολογία χρησιμοποιείται διέπεται από πρότυπα. Βασικά, αυτά ορίζουν τις ελάχιστες απαιτήσεις ορισμένης τεχνολογίας προκειμένου να επιτευχθεί διαλειτουργικότητα, η οποία είναι ιδιαίτερα σημαντική στα συστήματα RFID. Για την απεικόνιση της ανάγκης διαλειτουργικότητας στην τεχνολογία RFID, είναι σημαντικό να κατανοήσουμε τα προβλήματα των αλυσίδων εφοδιασμού, όπου γίνεται και η πιο συχνή χρήση του συστήματος RFID. Για παράδειγμα, η διαχείριση της εφοδιαστικής αλυσίδας ξεκινά από ένα ορυχείο ή ένα αγρόκτημα και τελειώνει σε μια μονάδα ανακύκλωσης ή σκουπιδιών [3], και στα ενδιάμεσα στάδια το αρχικό υλικό τροποποιείται ή υποβάλλεται σε επεξεργασία όπως μπορεί επίσης να αλλάξει και ιδιοκτήτη.

Με την παγκοσμιοποίηση του εμπορίου και γενικά της αλυσίδας εφοδιασμού, ένα υλικό ή αντικείμενο, συνδεδεμένο με μια ετικέτα RFID, πιθανόν να μπορεί ταξιδέψει σε όλο τον κόσμο , για παράδειγμα, από τους κατασκευαστές έως τις αποθήκες, από τις αποθήκες έως τα σημεία πώλησης, από τα σημεία πώλησης έως τους πωλητές, από τους πωλητές στους πελάτες και από πελάτες σε πελάτες. Αυτό σημαίνει ότι οι ετικέτες RFID πρέπει να διαβάζονται σωστά από όλους και παντού, στο παρόν και στο μέλλον, και χωρίς περιορισμένη πρόσβαση ή συγκεκριμένη εφαρμογή, δηλαδή τα συστήματα RFID πρέπει να είναι διαλειτουργικά. Με το παραπάνω παράδειγμα παρουσιάζεται η σημασία και η σημαντικότητα της διαλειτουργικότητας στα συστήματα RFID.

Ένα πρωτόκολλο επικοινωνίας ορίζει τον τρόπο με τον οποίο οι συσκευές επικοινωνίας καταφέρνουν να επικοινωνούν με επιτυχία. Στην περίπτωση πρωτοκόλλων RFID, το πρωτόκολλο καθορίζει τον τρόπο με τον οποίο επικοινωνούν οι αναγνώστες και οι ετικέτες. Το πρωτόκολλο ορίζει:

- Τη διεπαφή αέρα, η οποία περιλαμβάνει πληροφορίες, όπως ποια διαμόρφωση χρησιμοποιείται από τον αναγνώστη για τον ορισμό ενός δυαδικού, πόσο γρήγορα μεταφέρεται η πληροφορία, ο τρόπος με τον οποίο χειρίζονται τα πακέτα ή τι είδους σήμα αποστέλλεται από την ετικέτα.

- Το μεσοπρόθεσμο έλεγχο πρόσβασης ο οποίος καθορίζει πότε μια συσκευή είναι υποχρεωμένη να μεταδίδει ή τον τρόπο με τον οποίο επιλύεται η σύγκρουση.
- Τον ορισμό δεδομένων, που είναι η έννοια και το είδος των δεδομένων που σχετίζονται με τις ετικέτες και τους Readers.

Η κατασκευή παθητικών ετικετών RFID είναι φθηνή. Επίσης, η ισχύς εκπομπής τους εξαρτάται από το σήμα μετάδοσης του Reader. Επομένως, η επικοινωνία μεταξύ των ετικετών και των αναγνωστών αντιμετωπίζει προβλήματα που δεν παρατηρούνται σε άλλες ψηφιακές επικοινωνίες. Τροποποιήσεις όπως Quadrature Amplitude Keying (QAM) ή phase-shift keying (PSK) δεν είναι διαθέσιμες, λόγω της ανάληψης κακών συνθηκών καναλιού. Επιπλέον, απορρίπτονται επίσης οι διαμορφώσεις που απενεργοποιούν τη δύναμη του Reader, λόγω της σχέσης μεταξύ της ισχύος μετάδοσης του Reader και της ισχύος εκπομπής των ετικετών. Συνεπώς, για να επιτευχθεί επιτυχής επικοινωνία μεταξύ του Reader και των ετικετών, όλα τα παραπάνω προβλήματα πρέπει να αντιμετωπιστούν και να λυθούν.

3.1. Πρωτόκολλα EPCglobal class 1 Generation 2

3.1.1. EPCglobal RDFID Πρωτόκολλα

Η EPCglobal δημοσίευσε μια σειρά από πρωτόκολλα (EPCglobal class 0,EPCglobal class 1), τα οποία θεωρούνται πρώτης γενιάς. Παρ ’όλα αυτά όμως, τα πρώτης-γενιάς πρότυπα έχουν σημαντικά ελαττώματα, όπως για παράδειγμα την δυσκολία στο να απευθυνθείς σε μια συγκεκριμένη ετικέτα ή προβλήματα με αργή λήψη πληροφοριών όπως όταν η ετικέτα ενωνόταν με τον reader αφού είχε ξεκινήσει ήδη η καταγραφή δεδομένων. Επιπρόσθετα, τα δύο πρότυπα είναι ασύμβατα, ενώ ο κόσμος χρειάζεται ένα παγκόσμιο πρότυπο, έτσι ώστε κάθε αναγνώστης να είναι συμβατός με κάθε ετικέτα. Με σκοπό να επιλυθούν τα παραπάνω προβλήματα, η EPCglobal δημοσίευσε ένα πρότυπο νέας γενιάς που προσφέρει μια επαρκή απόδοση σε χαμηλό κόστος. Το πρωτόκολλο EPCglobal Class 1 Generation 2 επικυρώθηκε το 2005 και επικυρώθηκε επίσης από τον Διεθνή Οργανισμό Τυποποίησης (ISO), ως ISO18000-6C. Το Class 1 Gen2 Protocol αντικατέστησε σταδιακά παλαιότερα πρωτόκολλα UHF και θα συνεχίσει να χρησιμοποιείται σε μεγάλο μέρος της αγοράς, λόγω της χαμηλής απόδοσης κόστους που παρέχει.

[2]. Ο Πίνακας δείχνει την ταξινόμηση των ετικετών RFID σύμφωνα με τον οργανισμό EPCGlobal.

Class	Description
Class 0	Passive, read-only.
Class 0+	Passive, write-once but using class 0 protocols.
Class I	Passive, write-once.
Class II	Passive, write-once with extras such as encryption.
Class III	Rewritable, semi-passive, integrated sensors.
Class IV	Rewritable, active, may communicate with other active tags.
Class V	Rewritable, active, can power and read other tags.

Πίνακας 2

3.2. Φυσικό Υπόστρωμα

Αυτό το κεφάλαιο παρουσιάζει μερικές βασικές έννοιες του πρωτοκόλλου EPC Global RFID Class-1 Gen2, όπως ορίζεται στο [5]. Ένας αναγνώστης στέλνει πληροφορίες σε μία ή περισσότερες ετικέτες διαμορφώνοντας έναν φορέα RF χρησιμοποιώντας πληκτρολόγιο μετατόπισης πλάτους διπλής πλευρικής ζώνης (DSB-ASK), πληκτρολόγηση μετατόπισης πλάτους μονής πλευρικής ζώνης (SSB-ASK) ή μετατόπιση πλάτους αναστροφής φάσης (PRASK) χρησιμοποιώντας παλμό - μορφή κωδικοποίησης ενδιάμεσου (PIE). Οι ετικέτες λαμβάνουν τη λειτουργική τους ενέργεια από τον ίδιο διαμορφωμένο φορέα RF. Ένας αναγνώστης λαμβάνει πληροφορίες από μια ετικέτα, διαβιβάζοντας έναν μη διαμορφωμένο φορέα RF και ακούγοντας μια απάντηση backscatter. Οι ετικέτες επικοινωνούν πληροφορίες ρυθμίζοντας το πλάτος και / ή τη φάση του φορέα RF. Επιλέχθηκε η μορφή κωδικοποίησης ως απόκριση στις εντολές του αναγνώστη, είτε είναι FM) είτε ο υπο-φορέας διαμόρφωσης Miller. Ο σύνδεσμος επικοινωνίας μεταξύ των αναγνωστών και των Tas είναι μισός-διπλός, που σημαίνει ότι οι ετικέτες δεν θα απαιτηθούν για την αποδιαμόρφωση των εντολών του αναγνώστη, ενώ θα υπάρξει backscattering. Μια ετικέτα δεν αποκρίνεται σε μια υποχρεωτική ή προαιρετική εντολή χρησιμοποιώντας επικοινωνίες full-duplex.

3.2.1. Σηματοδότηση

Η επαφή σηματοδότησης μεταξύ αναγνώστη και ετικέτας μπορεί να θεωρηθεί ως το φυσικό επίπεδο του συστήματος δικτύου. Η επαφή σήματος καθορίζει τις συχνότητες λειτουργίας, τις διαμορφώσεις που μπορούν να χρησιμοποιηθούν, την κωδικοποίηση δεδομένων, τον φάκελο RF, τους ρυθμούς δεδομένων και άλλες παραμέτρους. Οι ετικέτες θα λαμβάνουν ισχύ από και θα επικοινωνούν με τους αναγνώστες εντός του εύρους συχνοτήτων από 860 MHz έως 960 MHz. Οι αναγνώστες θα χρησιμοποιούν DSB-ASK, SSB-ASK ή PR-ASK για να διαμορφώσουν την κωδικοποίηση σήματος και PIE. Το Tari, που φαίνεται στο Παράρτημα 3.1, είναι η διάρκεια των δεδομένων-0. Οι υψηλές τιμές αντιπροσωπεύουν CW που μεταδίδονται, ενώ οι χαμηλές τιμές αντιπροσωπεύουν εξασθενημένο CW. Οι τιμές Tari θα κυμαίνονται από 6,25μs έως 25μs με ανοχή +/- 1%.

3.2.2. Προοίμιο του αναγνώστη και συγχρονισμός πλαισίου

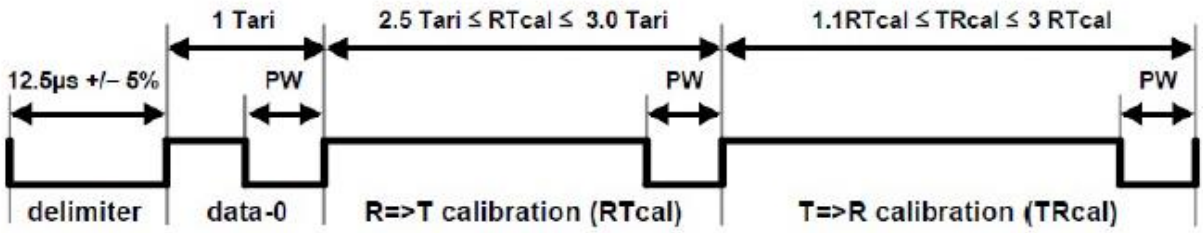
Ένας αναγνώστης ξεκινά ένα σήμα R⇒T προσθέτοντας ένα προοίμιο ή ένα πλαίσιο-συγχρονισμό στο πακέτο που μεταδίδεται. Ένα προοίμιο προηγείται μιας εντολής ερωτήματος και υποδηλώνει την έναρξη ενός γύρου απογραφής. Όλα τα υπόλοιπα που μεταδίδονται από τον ανακριτή ξεκινούν με ένα frame-sync. Η ανοχή που καθορίζεται σε μονάδες Tari είναι +/- 1%. Περιλαμβάνεται ένα προοίμιο ενός καθορισμένου μήκους αρχικού διαμέτρου, ενός συμβόλου δεδομένων-0, ενός συμβόλου βαθμονόμησης R⇒T (RTcal) και ενός συμβόλου βαθμονόμησης T⇒R (TRcal).

- Ένας αναγνώστης ορίζει το σύμβολο RTcal ίσο με το μήκος ενός συμβόλου δεδομένων-0, συν το μήκος ενός συμβόλου δεδομένων-1. Η ετικέτα μετρά το μήκος RTcal και υπολογίζει το pivot = RT cal 2. Στη συνέχεια, η ετικέτα αποκωδικοποιεί σύμβολα μακρύτερα από το περιστρεφόμενο ως δεδομένα-1 και μικρότερο από το περιστρεφόμενο ως δεδομένα-0. Σύμβολα μεγαλύτερα από 4 RTcals ερμηνεύονται από την ετικέτα ως μη έγκυρα. Πριν αλλάξει το RTcal, ένας αναγνώστης μεταδίδει CW για τουλάχιστον 8 RTcals.
- Ένας αναγνώστης καθορίζει μια συχνότητα συνδέσμου backscatter μιας ετικέτας (FM0 datarate ή τη συχνότητα του φορέα της Miller) χρησιμοποιώντας την αναλογία TRcal και divide, που βρίσκεται στο προοίμιο και το ωφέλιμο φορτίο, αντίστοιχα, μιας εντολής

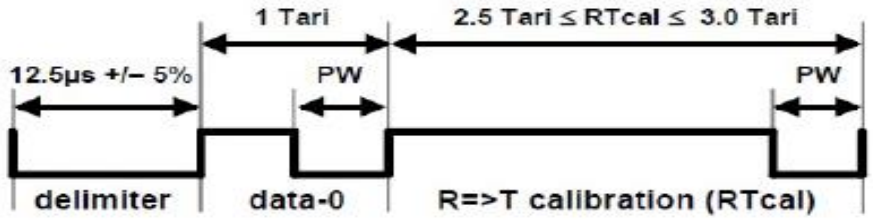
ερωτήματος, που ξεκινά έναν γύρο αποθέματος. Μια ετικέτα προσαρμόζει τη συχνότητα του συνδέσμου backscattering σύμφωνα με την εξίσωση (1):

BLF = DR T Rcal (3.1) 1.1 × RT cal ≤ T Rcal ≤ 3 × RT cal (1)

Ένας αναγνώστης, κατά τη διάρκεια ενός γύρου απογραφής, θα χρησιμοποιεί το ίδιο μήκος RTcal σε ένα πλαίσιο-συγχρονισμό, όπως χρησιμοποιήθηκε στο προοίμιο που ξεκίνησε τον γύρο. Οι συγχρονισμοί καρέ είναι πανομοιότυποι με τα προοίμια, μείον το σύμβολο TRcal. Ένα προοίμιο και ένας συγχρονισμός πλαισίου φαίνονται στις εικόνες 6 και 7, αντίστοιχα.



Εικόνα 6 Παράδειγμα προοιμίου



Εικόνα 7 Παράδειγμα frame-sync.

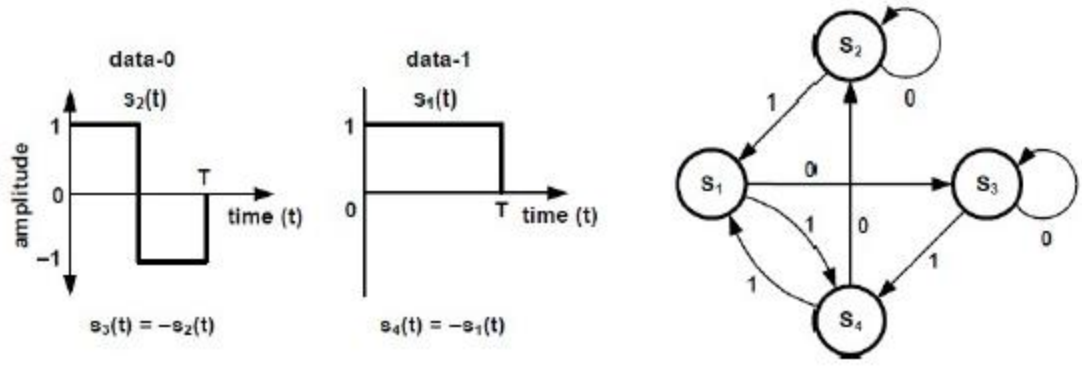
3.3. Επικοινωνία ετικέτας προς τον αναγνώστη

Μια ετικέτα επικοινωνεί, με ένα αναγνώστη, χρησιμοποιώντας διαμόρφωση backscatter. Πρακτικά, αλλάζει τον συντελεστή ανάκλασης της κεραίας του μεταξύ δύο καταστάσεων, ανάλογα με τα δεδομένα που αποστέλλονται. Μια ετικέτα κάνει backscatter χρησιμοποιώντας

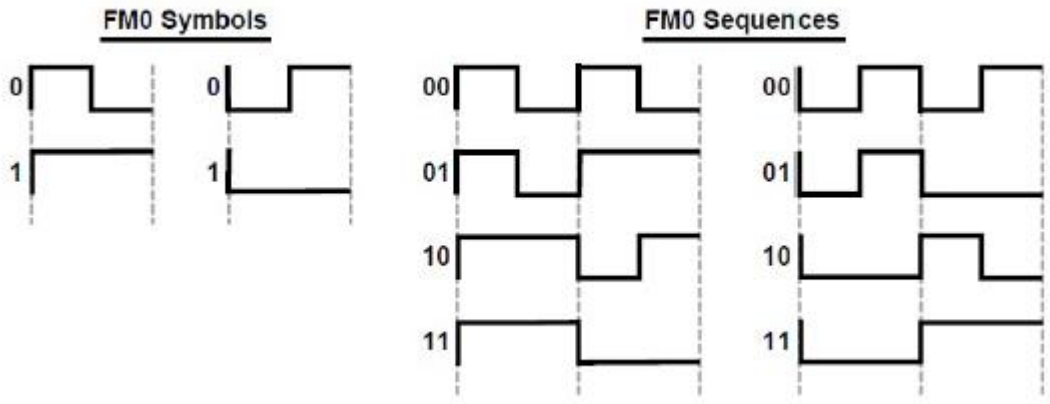
σταθερή μορφή διαμόρφωσης, κωδικοποίηση δεδομένων και ρυθμό δεδομένων κατά τη διάρκεια ενός γύρου απογραφής. Οι ετικέτες επιλέγουν τη μορφή διαμόρφωσης, ενώ ο αναγνώστης επιλέγει κωδικοποίηση και ρυθμό δεδομένων χρησιμοποιώντας μια εντολή ερωτήματος. Οι ετικέτες χρησιμοποιούν διαμόρφωση ASK ή / και PSK και χρησιμοποιούν είτε διαμόρφωση FM0 baseband είτε Miller για έναν υπο-φορέα μέσω του ρυθμού δεδομένων.

3.3.1. FM0 baseband

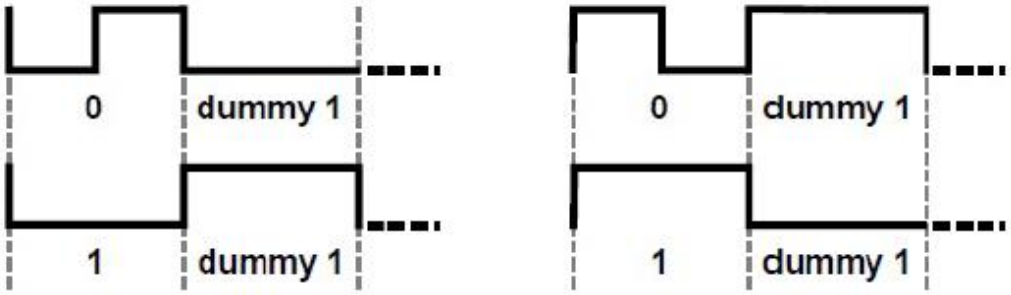
Η κωδικοποίηση FM0 αντιστρέφει τη φάση της βασικής ζώνης σε κάθε όριο συμβόλων, ενώ ένα δεδομένο-0 έχει μια επιπλέον αντιστροφή φάσης μεσαίου συμβόλου. Η αριστερή πλευρά της εικόνας 8 δείχνει τις βασικές λειτουργίες FM0 που μεταδίδονται. Τα δεδομένα-0 μεταδίδονται είτε με συνάρτηση s2 (t) ή s3 (t), ανάλογα με το bit δεδομένων που είχε προηγουμένως μεταδοθεί. Το ίδιο ισχύει και για τα δεδομένα1, είτε μεταδίδεται με μια λειτουργία s1 (t) ή s4 (t), ανάλογα με το προηγουμένως μεταδιδόμενο bit, που σημαίνει ότι η κωδικοποίηση FM0 έχει μνήμη. Όλες οι μεταβάσεις μεταξύ των λειτουργιών της κωδικοποίησης FM0 φαίνονται στην εικόνα 8. Για παράδειγμα, μια μετάβαση από την κατάσταση S2 στην κατάσταση S3 δεν επιτρέπεται, επειδή η μετάδοση που προκύπτει δεν θα είχε αντιστροφή φάσης σε όριο συμβόλων. Παραδείγματα ακολουθιών FM0 φαίνονται στην εικόνα 9. Η κωδικοποίηση FM0 «τελειώνει» πάντα με εικονικό bit-1 bit, όπως φαίνεται στην εικόνα 10.



Εικόνα 8 Βασικές λειτουργίες FM0 και διάγραμμα κατάστασης



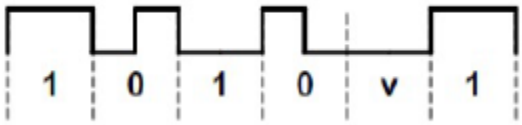
Εικόνα 9 Σύμβολα και αλληλουχία FM0



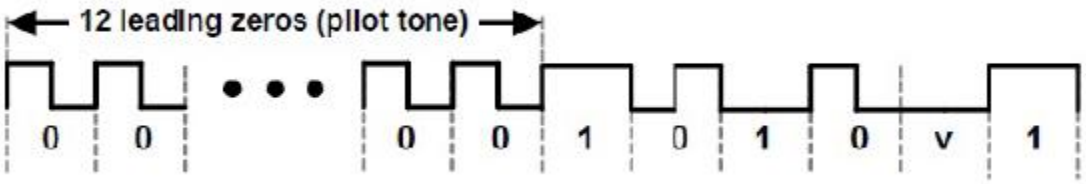
Εικόνα 10 Τέλος σηματοδότησης

3.3.2. Προοίμιο FM0

Η σηματοδότηση FM0 ξεκινά με ένα από τα προοίμια, που φαίνονται στις εικόνες 11 και 12, αντίστοιχα. Η επιλογή εξαρτάται από την τιμή του TRext bit που βρίσκεται στην εντολή Query, που ξεκίνησε τον γύρο του αποθέματος, εκτός αν μια ετικέτα απαντά σε μια εντολή που γράφει στη μνήμη, οπότε η ετικέτα θα χρησιμοποιεί το εκτεταμένο προοίμιο, ανεξάρτητα από το TRext. Το "v", που φαίνεται και στις δυο αυτές εικόνες υποδεικνύει μια παραβίαση FM0 (δηλ. μια αντιστροφή φάσης θα έπρεπε να είχε συμβεί αλλά δεν συνέβη).



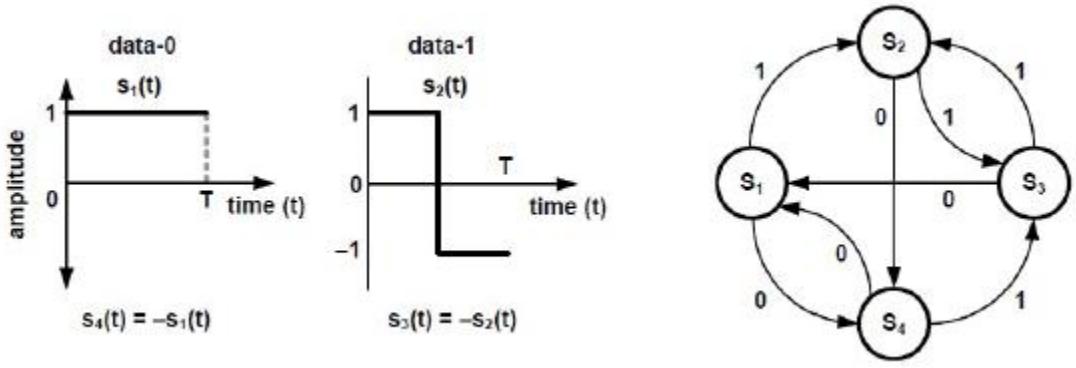
Εικόνα 11 Προοίμια (Trext=0)



Εικόνα 12 Προοίμια (Trext=1)

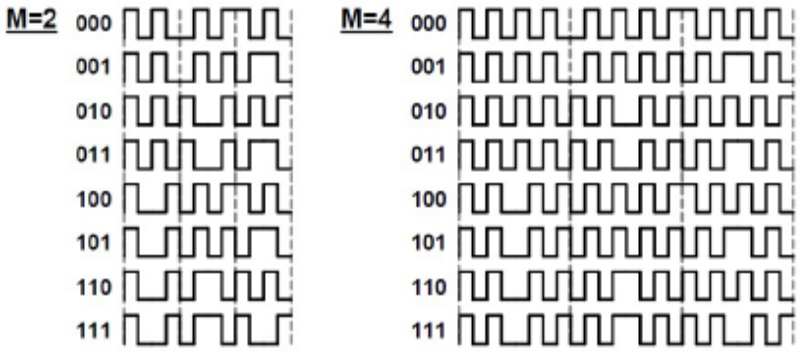
3.3.3. Miller-modulated subcarrier

Το Baseband Miller αντιστρέφει τη στάση του ανάμεσα σε δύο δεδομένα-0s διαδοχικά, επίσης τοποθετεί μια αντιστροφή φάσης στη μέση ενός συμβόλου δεδομένων-1. Την εικόνα 13 αντιπροσωπεύει τις βασικές λειτουργίες της κωδικοποίησης Miller καθώς και το διάγραμμα κατάστασης. Οι ετικέτες κατάστασης S1 - S4 υποδεικνύουν όλες τις πιθανές λειτουργίες που επιτρέπονται σε αυτήν την κωδικοποίηση, που αντιπροσωπεύονται από τις δύο όψεις καθεμιάς από τις συναρτήσεις βάσης Miller, ενώ τα βέλη δείχνουν τις μεταβάσεις μεταξύ τους, δηλαδή η μετάβαση από την κατάσταση S3 στην κατάσταση S4 δεν επιτρέπεται, επειδή δεν υπάρχει μετατόπιση φάσης μεταξύ δεδομένων-0 και δεδομένων-1.

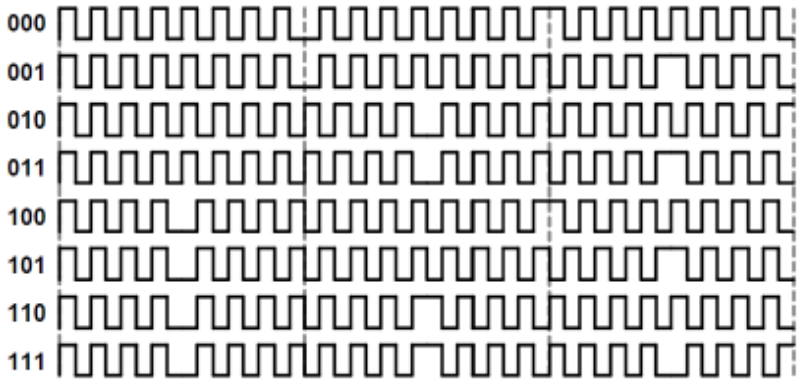


Εικόνα 13 Βασικές λειτουργίες Miller και διάγραμμα κατάστασηw

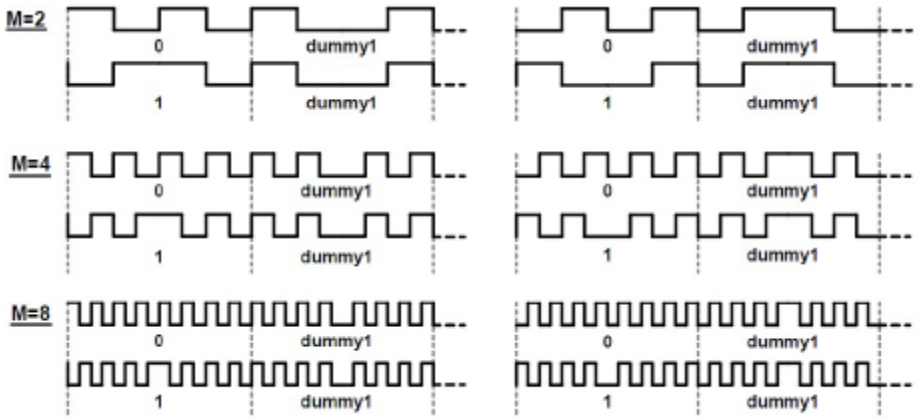
Από την άλλη πλευρά, είναι δυνατή η μετάβαση μεταξύ S2 και S3, εάν το επόμενο σύμβολο της ακολουθίας είναι ένα data-1. Οι ετικέτες κατάστασης, επίσης, αντιπροσωπεύουν την κυματομορφή βασικής ζώνης Miller, που δημιουργείται κατά την είσοδο στην κατάσταση. Η κυματομορφή που εκπέμπεται από την κατάσταση είναι η κυματομορφή της βασικής ζώνης, πολλαπλασιαζόμενη με ένα τετράγωνο κύμα σε M επί τη συχνότητα του συμβόλου. Η ακολουθία Miller θα περιέχει ακριβώς δύο, τέσσερις ή οκτώ κύκλους υπο-φορέα ανά bit, ανάλογα με την τιμή M, που βρίσκεται στην εντολή Query, που ξεκίνησε τον γύρο απογραφής, όπως φαίνεται στις εικόνες 14 και 15. Ο κύκλος λειτουργίας ενός συμβόλου 0 ή 1 είναι τουλάχιστον 45% και μέγιστο 55%, με ονομαστική τιμή 50%. Η σηματοδότηση Miller, πάντοτε, τελειώνει με "εικονική" δεδομένα-1 στο τέλος της ακολουθίας, όπως φαίνεται στην εικόνα 16.



Εικόνα 14 Αλληλουχία Miller (για M=2,M=4)



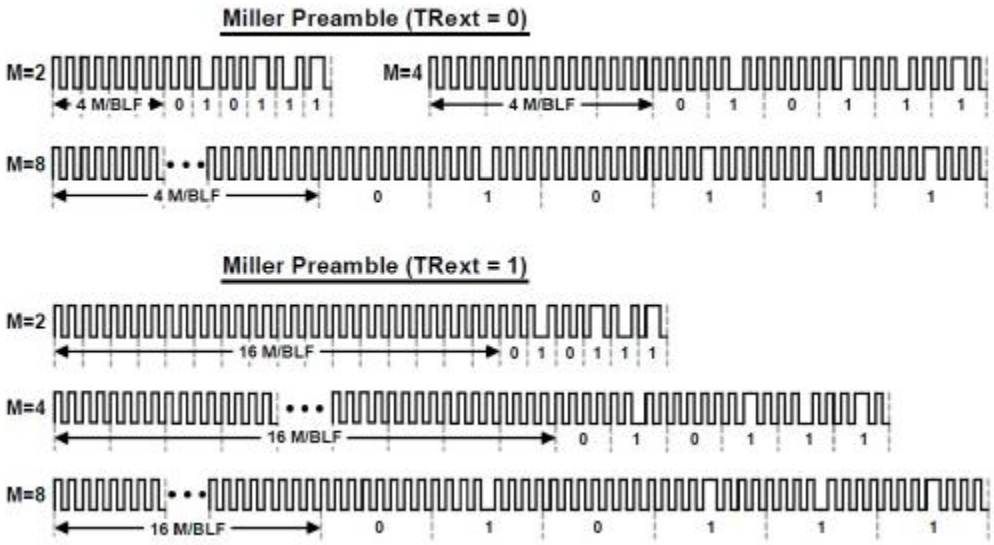
Εικόνα 15 Αλληλουχία Miller (για M=8)



Εικόνα 16 Τέλος σηματοδότηση

3.3.4. Προοίμιο Miller

Η κωδικοποίηση Miller προηγείται πάντοτε από ένα από τα προοίμια, όπως φαίνεται στην εικόνα 17 Η επιλογή εξαρτάται από την τιμή του TRext bit, το οποίο βρίσκεται στην εντολή Query, που ξεκινά τον τρέχοντα γύρο αποθέματος. Ωστόσο, εάν η ετικέτα απαντήσει σε μια εντολή που αναφέρεται στη μνήμη, θα χρησιμοποιήσει το εκτεταμένο προοίμιο, ανεξάρτητα από την τιμή του TRext bit. Οι ετικέτες υποστηρίζουν όλη την τιμή R⇒T Tari, από 6,25μs έως 256,25μs.



Εικόνα 17

3.3.5. Παράμετροι ετικετών

Οι παράμετροι που καθορίζουν τη συχνότητα backscatter, τον τύπο διαμόρφωσης (FM0 ή Miller) και τον ρυθμό δεδομένων T⇒. για τον γύρο είναι DR, M, TRcal και BLF. Το BLF υπολογίζεται χρησιμοποιώντας το 3.1, ενώ οι άλλες παράμετροι βρίσκονται στην εντολή Query. Η εντολή μετάδοσης, και για τις επικοινωνίες R⇒T και T⇒, θα είναι πρώτα το πιο σημαντικό bit (MSB). Σε κάθε λέξη και σε κάθε μήνυμα, το MSB θα μεταδοθεί πρώτα. Επίσης, θα συμπεριληφθεί ένα συγκεκριμένο CRC (κυκλικός έλεγχος πλεονασμού), προκειμένου να διασφαλιστεί η εγκυρότητα ορισμένων R⇒T και ο ανακριτής το χρησιμοποιεί, για να διασφαλίσει την εγκυρότητα ορισμένων απαντήσεων T⇒. Το πρωτόκολλο χρησιμοποιεί δύο τύπους CRC CRC-16 και CRC-5. Το Σχήμα 3.14 δείχνει το χρονοδιάγραμμα μεταξύ των εντολών που αποστέλλονται από τον αναγνώστη και των απαντήσεων που διασκορπίζονται από την ετικέτα που:

- Το T1 είναι ώρα από τη μετάδοση του ερωτηματολογίου στην απόκριση ετικέτας που μετριέται στα τερματικά της κεραίας της ετικέτας. Η τιμή του T1 ορίζεται σύμφωνα με την Εξίσωση 2.
- Απαιτείται χρόνος απόκρισης του ερωτηματολογίου T2, εάν μια ετικέτα πρόκειται να αναδιαμορφώσει το σήμα του αναγνώστης , που μετριέται από το τέλος του τελευταίου bit της απόκρισης της ετικέτας έως το πρώτο μειωμένο άκρο της μετάδοσης των ερωτημάτων (Εξίσωση: 3).
- T3 Ώρα ο αναγνώστης περιμένει, μετά το T1, προτού εκδώσει άλλη εντολή (Εξίσωση: 4).
- T4 Ελάχιστος χρόνος μεταξύ εντολών του ερωτηματολογίου (Εξίσωση: 5).

$$MAX(RTcal, 10{\times}T_{pri}){\times}(1-|FFT|){-}2\mu s \leq T_1 \leq MAX(RTcal, 10\times T_{pri})\times(1+|FFT|)+2\mu s \quad (2)$$

$$3T_{pri} \leq T_2 \leq 20T_{pri} \quad (3)$$

$$T_3 = 0.0T_{pri}, \quad (4)$$

$$T_4 = 2RTcal \quad (5)$$

3.4. Επίπεδο αναγνώρισης ετικέτας

Ο αναγνώστης διαχειρίζεται πληθυσμούς ετικετών χρησιμοποιώντας τρεις βασικές λειτουργίες:

- Επιλεκτική: Η λειτουργία της επιλογής ενός πληθυσμού ετικετών για απόθεμα και πρόσβαση. Μια εντολή επιλογής μπορεί να εφαρμοστεί διαδοχικά για να επιλέξετε έναν συγκεκριμένο πληθυσμό ετικετών βάσει κριτηρίων που καθορίζονται από τον χρήστη. Αυτή η λειτουργία είναι ανάλογη με την επιλογή εγγραφών από μια βάση δεδομένων.

- Αποθέματος: Η λειτουργία αναγνώρισης ετικέτας. Ένας αναγνώστης ξεκινά έναν γύρο απογραφής μεταδίδοντας μια εντολή ερωτήματος σε μία από τις τέσσερις συνεδρίες. Μια ή περισσότερες ετικέτες ενδέχεται να απαντήσουν. Οι αναγνώστες εντοπίζουν μία απλή ετικέτα και ζητούν τις λέξεις PC / XPC, EPC και CRC από την ετικέτα. Το απόθεμα περιλαμβάνει πολλές εντολές. Ένας γύρος αποθέματος λειτουργεί σε μία και μόνο μία συνεδρία κάθε φορά.

- Πρόσβασης: Η λειτουργία της επικοινωνίας με (ανάγνωση ή / και γραφή σε μια ετικέτα. Μια μεμονωμένη ετικέτα πρέπει να αναγνωριστεί με μοναδικό τρόπο πριν από την πρόσβαση. Η πρόσβαση περιλαμβάνει πολλές εντολές, ορισμένες από τις οποίες χρησιμοποιούν κωδικοποίηση κωδικοποίησης με βάση ένα μόνο πληκτρολόγιο του συνδέσμου R⇒T .

3.4.1. Απογραφή ετικετών

Το σύνολο εντολών απογραφής περιλαμβάνει Query, QueryAdjust, QueryRep, ACK και NAK. Η ζήτηση ξεκινά ένα γύρο αποθέματος και αποφασίζει ποιες ετικέτες συμμετέχουν στον γύρο. Ένας γύρος αποθέματος είναι μια περίοδος που ξεκινά από μια εντολή ζήτηση και τερματίζεται είτε από μια νέα εντολή Query (η οποία ξεκινά έναν νέο γύρο αποθέματος) είτε από μια εντολή Select. Η ζήτηση περιέχει μια παράμετρο Q-count-slot. Κατά τη λήψη μιας ζήτησης που συμμετέχουν ετικέτες, επιλέγεται μια τυχαία τιμή στο εύρος (0, 2 Q −1), συμπεριλαμβανομένης και φορτώνει αυτή την τιμή στον μετρητή slot counter. Οι ετικέτες που επιλέγουν μετάβαση μηδενικής τιμής στην κατάσταση απάντησης και απαντούν αμέσως, ενώ ετικέτες που επιλέγουν μετάβαση μη μηδενικής τιμής στην κατάσταση διαιτησίας και περιμένουν μια εντολή QueryAdjust ή QueryRep. Για μια ετικέτα, ο αλγόριθμος προχωρά ως εξής (εικόνα 19):

1. Η ετικέτα οπισθοδρομεί ένα RN16, καθώς μπαίνει απάντηση.
2. Ο Interrogator αναγνωρίζει την ετικέτα με ACK, που περιέχει το ίδιο RN16.
3. Η αναγνωρισμένη ετικέτα μεταβαίνει στην αναγνωρισμένη κατάσταση, διασκορπίζοντας πίσω μια απάντηση που φαίνεται στην εικόνα 19
4. Ο αναγνώστης εκδίδει μια εντολή QueryAdjust ή QueryRep, αναγκάζοντας την αναγνωρισμένη ετικέτα να αντιστρέψει την απογραφείσα σημαία της και να μεταβεί σε έτοιμη, προκαλώντας δυνητικά μια άλλη ετικέτα να ξεκινήσει έναν διάλογο ερωτήσεων-απαντήσεων με τον αναγνώστη, ξεκινώντας από το βήμα (α), παραπάνω.

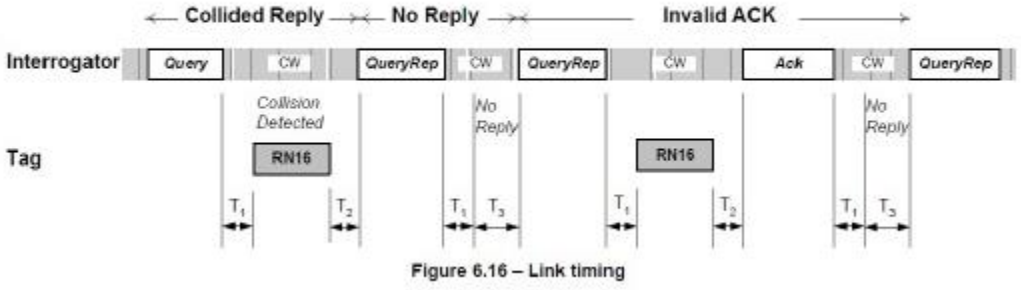
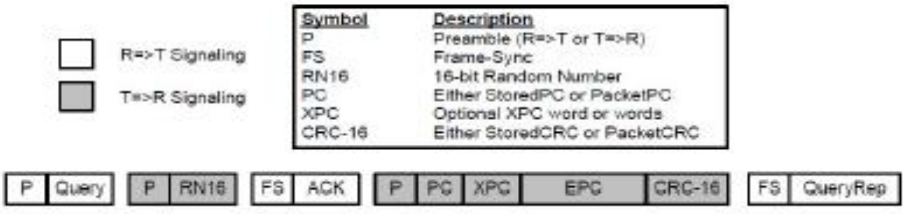


Figure 6.16 – Link timing

Εικόνα 18 Συγχρονισμός συνδέσμων



Εικόνα 19 Για μια ετικέτα

Εάν η ετικέτα αποτύχει να λάβει το ACK στο βήμα (2) εντός του χρονικού διαστήματος T2 (βλ.: εικόνα 18) ή λάβει το ACK με λάθος RN16, επιστρέφει σε αλλαγή. Εάν πολλές ετικέτες απαντήσουν στο βήμα (1) αλλά ο αναγνώστης, ανιχνεύοντας και επιλύοντας συγκρούσεις σε επίπεδο κυματομορφής, μπορεί να επιλύσει ένα RN16 από ένα από τις ετικέτες. Οι άλυτες ετικέτες λαμβάνουν εσφαλμένο RN16, επομένως επιστρέφουν σε κατάσταση slot counter, χωρίς να διασκορπίζουν εκ νέου την απάντηση στο (3). Σε κάποιο σημείο ο αναγνώστης θα εκδώσει ένα νέο ερώτημα, ξεκινώντας έτσι έναν νέο γύρο αποθέματος. Οι ετικέτες στο slot counter μειώνουν τον μετρητή υποδοχών τους κάθε φορά που λαμβάνουν ένα QueryRep, μεταβαίνοντας στην κατάσταση απάντησης και επανασυνδέοντας ένα RN16, όταν ο μετρητής slot counterς τους φτάσει τις 0000 ώρες. Οι ετικέτες των οποίων ο μετρητής slot counter έφτασε τις 0000 ώρες, οι οποίοι απάντησαν και δεν αναγνωρίστηκαν (συμπεριλαμβανομένων των ετικετών που απάντησαν στο αρχικό ερώτημα και δεν αναγνωρίστηκαν) επιστρέφουν σε slot counter με τιμή υποδοχής 0000 ώρες και μειώνουν αυτήν την τιμή υποδοχής από 0000 ώρες έως 7F F Fh στην επόμενη QueryRep,

αποτρέποντας έτσι αποτελεσματικά τις επόμενες απαντήσεις, έως ότου η ετικέτα να φορτώσει μια νέα τυχαία τιμή στην τιμή υποδοχής.

3.5. Καταστάσεις ετικέτας

Ορισμένες από τις καταστάσεις, που χρησιμοποιούνται σε αυτήν τη διατριβή, περιγράφονται σε αυτήν την ενότητα προκειμένου να κατανοηθεί μια βασική γνώση της λειτουργικότητας των ετικετών. Οι καταστάσεις των ετικετών είναι:

- Έτοιμο: Στην κατάσταση ετοιμότητας η ετικέτα περιμένει είτε μια εντολή Select είτε ένα Query. Μετά τη μετάδοση μιας από αυτές τις εντολές από τον αναγνώστη , η ετικέτα παραμένει σε αυτήν την κατάσταση.
- Αλλαγή: Ενώ βρίσκεστε σε αυτήν την κατάσταση, η ετικέτα περιμένει είτε μια εντολή Select, Query ή QueryRep. Εάν η ετικέτα μεταδίδει RN16, μετακινείται στην κατάσταση απάντησης.
- Απάντηση: Στην κατάσταση ετοιμότητας, η ετικέτα περιμένει μια εντολή Query, QueryAdjust ή ACK. Σε περίπτωση εντολής ACK, μεταβαίνει στην κατάσταση αναγνώρισης. Εάν μεταδοθεί ένα ερώτημα, ξεκινά έναν νέο γύρο, επομένως η ετικέτα μετακινείται στην κατάσταση Arbitrate. Εάν μεταδοθεί ένα QueryAdjust, η ετικέτα μεταδίδει ένα νέο RN16.
- Αναγνωρισμένο: Σε αυτήν την κατάσταση η ετικέτα backscatters μια λέξη EPC και μετά παραμένει σιωπηλό για το υπόλοιπο του γύρου αποθέματος.

3.6. Εντολή ερωτήματος

Η εντολή ερωτήματος ξεκινά και καθορίζει έναν γύρο αποθέματος. Το ερώτημα περιλαμβάνει τα ακόλουθα πεδία

- Το DR (TRcal divide ratio) ορίζει τη συχνότητα σύνδεσης T⇒R.
- M (κύκλοι ανά σύμβολο) ορίζει το ρυθμό δεδομένων T⇒ και τη μορφή διαμόρφωσης.
- Το Trext επιλέγει εάν το προοίμιο T⇒ προσποιείται με πιλοτικό τόνο, εκτός εάν μια ετικέτα απαντήσει σε μια εντολή που γράφει στη μνήμη. Σε αυτήν την περίπτωση, πάντα, χρησιμοποιεί πιλοτικό τόνο, ανεξάρτητα από το TRext.

- Η Sel επιλέγει ποιες ετικέτες ανταποκρίνονται στο ερώτημα.
- Η συνεδρία επιλέγει μια συνεδρία για τον γύρο αποθέματος.
- Ο στόχος επιλέγει εάν οι ετικέτες των οποίων η σημαία απογραφής είναι A ή B συμμετέχουν στον γύρο αποθέματος.
- Το Q ορίζει τον αριθμό των κουλοχέρηδων στο γύρο. Το πεδίο της εντολής ερωτήματος παρουσιάζεται στον πίνακα 3.

Οι αναγνώστες προηγούνται μιας εντολής ερωτήματος με ένα προοίμιο (πίνακας 4). Το ερώτημα προστατεύεται από CRC-5, εάν μια ετικέτα λάβει εσφαλμένο CRC-5, θα αγνοήσει την εντολή. Μόλις λάβει ένα ερώτημα, οι ετικέτες με ταίριασμα Sel και Target θα επιλέξουν μια τυχαία τιμή στο εύρος (0, 2 Q - 1) και θα φορτώσουν αυτήν την τιμή στον μετρητή υποδοχών τους. Εάν μια ετικέτα , σε απάντηση στο ερώτημα, φορτώνει τον μετρητή υποδοχής με μηδέν, τότε η απάντησή της εμφανίζεται στον πίνακα 4, διαφορετικά θα παραμείνει σιωπηλή.

3.6.1. QueryRep

Οι αναγνώστες και οι ετικέτες εφαρμόζουν την εντολή QueryRep, όπως φαίνεται στον πίνακα 5. Το QueryRep δίνει εντολή στις ετικέτες να μειώσουν τους μετρητές slot counters τους και εάν το slot counter= 0 μετά τη μείωση, να επανασυνδέσει ένα RN16 στον Ανακριτή. Περιλαμβάνει τα ακόλουθα πεδία:

- Συνεδρία, η οποία δείχνει τον αριθμό περιόδου λειτουργίας για αυτόν τον γύρο. Εάν μια ετικέτα λάβει ένα QueryRep, του οποίου ο αριθμός περιόδου λειτουργίας είναι διαφορετικός από τον αριθμό περιόδου λειτουργίας του ερωτήματος που ξεκίνησε τον γύρο, θα αγνοήσει την εντολή. Πριν από ένα QueryRep προηγείται ένας συγχρονισμός καρέ (πίνακας 5). Εάν μια ετικέτα λάβει ένα QueryRep και μετά τη μείωση, ο μετρητής slot counter του είναι η τιμή μετρητή slot counter, οπισθοδρομεί μια απάντηση που φαίνεται στον πίνακα 6.

	Command	DR	M	TRext	Sel	Session	Target	Q	CRC-5
# of bits	4	1	2	1	2	2	1	4	5
description	1000	$DR = 8$ $DR = 64/3$	$00 : M = 1$ $01 : M = 2$ $10 : M = 4$ $11 : M = 8$	0:No pilot tone 1:Use pilot tone	00:All 01:All 10: SL 11:SL	00:S0 01:S1 10:S2 11:S3	0:A 1:B	0-15	

Πίνακας 3

	Response
# of bits	16
Description	RN16

Πίνακας 4

	Command	Session
# of bits	2	2
Description	00	00:S0 01:S1 10:S2 11:S3

Πίνακας 5

	Response
# of bits	16
Description	RN16

Πίνακας 6

3.7. ACK

Οι αναγνώστες και οι ετικέτες θα εφαρμόσουν την εντολή ACK, όπως φαίνεται στον πίνακα 7. Μετά από ένα επιτυχημένο Query ή QueryRep, ένας αναγνώστης στέλνει μια εντολή ACK για να αναγνωρίσει μια μεμονωμένη ετικέτα. Ο αναγνώστης επαναλαμβάνει το RN16, που είχε σταλεί προηγουμένως από την ετικέτα . Εάν το RN16, που αποστέλλεται από τον Reader, είναι σωστό και η ετικέτα είναι στη σωστή κατάσταση, τότε η ετικέτα θα εμφανίσει ξανά την απάντησή του, όπως φαίνεται στον πίνακα 8. Όλη η διαδικασία εξαγωγής ενός αποθηκευμένου EPC φαίνεται στην εικόνα 19

	Response
# of bits	16
Description	RN16

Πίνακας 7

	Command	RN16
# of bits	2	16
Description	01	Echoed RN16 or handle.

Πίνακας 8

4. ΠΡΟΚΛΗΣΕΙΣ RFID

Υπάρχουν πολλές προκλήσεις σχετικά με την ανάπτυξη συστημάτων RFID (π.χ. ψευδείς ή ελλείψεις ανάγνωσης λόγω αλλοίωσης ραδιοκυμάτων, επεκτασιμότητας, ασφάλειας και απορρήτου, σχεδιασμός κεραίας, κόστος ανάπτυξης, και άλλα). Ωστόσο, υπάρχουν και άλλες προκλήσεις που μπορεί να μην είναι τόσο προφανές.

Για πολλούς κλάδους, η ανάπτυξη RFID θα αλλάξει την επιχειρηματική διαδικασία, αναγκάζοντας νέες επενδύσεις σε προσωπική εκπαίδευση, υποδομές, δοκιμές κλπ. Αυτή η εισαγωγή μιας νέας τάξης πραγμάτων μπορεί να δημιουργήσει μια κρίση αβεβαιότητας στις επιχειρήσεις και στον κόσμο της τεχνολογίας. Οι εταιρείες πρέπει να αξιολογήσουν προσεκτικά την οικονομική βιωσιμότητα του τι μπορεί να αντιπροσωπεύει μια μεγάλη αρχική επένδυση χρημάτων. Για παράδειγμα, το Διεθνές Αεροδρόμιο McCarran στο Λας Βέγκας έπρεπε να επενδύσει περίπου 125 000,000 $ σε RFID-ενεργοποίηση του συστήματος παρακολούθησης αποσκευών [11].

Από την άλλη, παρόλο που ένα σύστημα RFID παρέχει άφθονα δεδομένα απαραίτητα για τον έλεγχο και την κατανόηση των επιχειρηματικών διαδικασιών, εφαρμογές όπως η διαχείριση της αλυσίδας εφοδιασμού ή η παρακολούθηση σε πραγματικό χρόνο μπορεί να παράγουν τόσο μεγάλο όγκο πληροφοριών που δεν θα μπορούσαν να χειριστούν οι τυπικές βάσεις δεδομένων. (προβλέπεται ότι η WalMart μπορεί παράξει πάνω από 7 terabyte λειτουργικών δεδομένων RFID ανά ημέρα [12]). Επομένως, οι αρχιτεκτονικές λογισμικού και οι back-end βάσεις δεδομένων θα πρέπει να επανεξεταστούν για τη συλλογή, συσχέτιση, φιλτράρισμα και καθαρισμό δεδομένων RFID.

Σχετικά στενά με τις τεχνικές λεπτομέρειες και τις λεπτομέρειες ανάπτυξης, τρεις διαφορετικές προκλήσεις, η ασφάλεια, η προστασία της ιδιωτικής ζωής και η δυνατότητα κλιμάκωσης, αποτελούν το κύριο θέμα συζήτησης σε αυτήν την διατριβή. Λόγω της ασύρματης φύσης και των υπολογιστικών περιορισμών των ετικετών RFID, η εγγύηση της ασφάλειας των δεδομένων των ετικετών και του απορρήτου των φορέων ετικετών είναι μια δύσκολη αποστολή. Οι απειλές απορρήτου αυξάνονται αν λάβουμε υπόψη όλα τα προσωπικά δεδομένα που αφορούν τον τεράστιο όγκο πληροφοριών που συλλέγονται από ετικέτες. Εάν αυτά τα δεδομένα δεν

αντιμετωπιστούν σωστά, ενδέχεται να αποκαλυφθούν ευαίσθητες πληροφορίες χωρίς να γνωρίζουν οι χρήστες του RFID. Αυτό σημαίνει ότι η ανάγκη για αποτελεσματικές και επεκτάσιμες μεθόδους διατήρησης της ιδιωτικής ζωής για μικροδεδομένα αυξάνεται με τη μαζική ανάπτυξη RFID.

4.1. Θέματα ασφάλειας, απορρήτου και επεκτασιμότητας στα πρωτόκολλα αναγνώρισης RFID

Γενικά η ανάπτυξη της τεχνολογίας RFID και το πως οι ετικέτες αλληλοεπιδρούν με τους αναγνώστες, τείνει να βοηθήσει και να βελτιώσει την καθημερινή ζωή και την αλληλεπίδραση ανθρώπου και περιβάλλοντος, γεγονός στο οποίο υποστηρίζει το όραμα της πανταχού παρούσας υπολογιστικής δύναμης.

Κατά συνέπεια, στις περισσότερες εφαρμογές, οι αναγνώστες πρέπει να είναι σε θέση να αναγνωρίσουν μία ή περισσότερες ετικέτες σε ένα σύνολο εκατομμυρίων ή δισεκατομμυρίων. Αυτό το σενάριο χαρακτηρίζει μια σημαντική ιδιότητα που πρέπει να πληροί ένα πρωτόκολλο αναγνώρισης RFID: δυνατότητα κλιμάκωσης.

Όσον αφορά τα περισσότερα συστήματα αναγνώρισης, το να είναι ασφαλή και να κρατούν την ιδιωτικότητας τους είναι δύο άλλες ιδιότητες που πρέπει υποχρεωτικά να παρέχουν τα συστήματα RFID. Αυτές οι δύο δυνατότητες είναι συναφή με το πλαίσιο RFID, λόγω του ότι το κανάλι επικοινωνίας μεταξύ ετικετών και αναγνώστη είναι εύκολα προσβάσιμο και όχι τόσο ασφαλές.

Γενικά, ασφάλεια στα συστήματα σημαίνει ότι τα δεδομένα που είναι αποθηκευμένα στη μνήμη μιας ετικέτας πρέπει να έχουν πρόσβαση μόνο από εξουσιοδοτημένα μέρη και ότι η αντιγραφή ή δημιουργία πλαστής ετικέτας θα πρέπει να έχει αμελητέα πιθανότητα να επιτευχθεί. Από την άλλη πλευρά, η διατήρηση του απορρήτου μπορεί να οριστεί ως η ικανότητα των ετικετών να δημιουργούν ασύνδετα μηνύματα αναγνώρισης.

4.2. Ασφάλεια

Η ασφάλεια χαρακτηρίζεται από μια σειρά ιδιοτήτων η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των δεδομένων. Σήμερα είναι δύσκολο να εγγυηθεί κανείς για αυτές τις ιδιότητες, για δυο λόγους. Πρώτος είναι η έλλειψη διαφάνειας, όσον αφορά́ τον τρόπο λειτουργιάς της υπάρχουσας υποδομής που έχει αναπτυχθεί́ κατά́ τρόπο εμπειρικό́. Δεύτερός είναι η εκθετικά́ αυξανόμενη πολυπλοκότητα της. Ο έλεγχος της ποιότητας επιτρέπει την εγγύηση ορισμένων τεχνικών χαρακτηριστικών, όπως τον χρόνο απόκρισης και την παροχή δεδομένων, που είναι απαραίτητα για την σωστή́ και ομαλή λειτουργιά των ενσωματωμένων συσκευών.

Πλέον στην καθημερινότητα μας περιστοιχιζόμαστε από εκατοντάδες επεξεργαστές/υπολογιστικές μονάδες, σε δικτυωμένες συσκευές που θα κάνουν την καθημερινότητα του ανθρώπου πολύ́ πιο απλή αλλά και πιο ενδιαφέρουσα. Η νέα αυτή πραγματικότητα συνοδεύεται με αμέτρητες προσδοκίες ανάπτυξης και βελτίωσης σε όλους τους τομείς, αλλά και ανησυχία για θέματα ασφάλειας και παραβίασης δεδομένων. Κυριότερο πρόβλημα φαίνεται να είναι η έμμεση παρακολούθηση των ατόμων, μεσώ των αντικειμένων που κατέχουν. Ειδικά́ στην περίπτωση του επίγειου οδικού́ δικτυού που παρουσιάστηκε, οι χρήστες των οδών παρακολουθούνται και καταγράφονται οι κινήσεις και επιλογές. Προσδιορίζονται έτσι όλες οι συνήθειες κάθε ατόμου, αγοραστικές και μη. Η πληροφορία αυτή κρίνεται ως μεγάλής αξίας, γι’ αυτό και η διαχείρισή της είναι ένα ζήτημα προς επίλυση.

Είναι συνετό να σημειωθεί́ πως οι απειλές από το RFID σε ένα περιβάλλον τεχνολογικής παρακολούθησης υπάρχουν και μάλιστα σοβαρές. Ήδη είναι γνωστό́ πως οι καταναλωτικές συνήθειες των χρηστών του internet καταγράφονται και τεχνολογίες που παλαιότερα προκάλεσαν έντονη δυσαρέσκεια και προβληματισμό όπως τα cookies, σήμερα αποτελούν αποδεκτές πρακτικές. Παράλληλα αρκετοί οργανισμοί διαθέτουν ήδη ένα μεγάλο όγκο πληροφοριών, που ενδεχομένως να εμπεριέχουν και προσωπικά δεδομένα. Τέτοιοι οργανισμοί́ είναι οι πάροχοι τηλεπικοινωνιακών υπηρεσιών και διαδικτύου, οι τράπεζες μέσω των πιστωτικών καρτών, οι κατασκευαστές όλων των smart cards αλλά και των ετικετών RFID, καθώς και τα κοινωνικά δίκτυα. Η πληροφορία αυτή, σε συνδυασμό με την μείωση του κόστους αποθήκευσης δεδομένων και την αύξηση της διαθέσιμης υπολογιστικής ισχύος, επιτρέπουν την δημιουργία μοντέλων εξαγωγής συμπερασμάτων που είναι πιθανό́ να παραβιάζουν την ιδιωτικότητα του ατόμου.

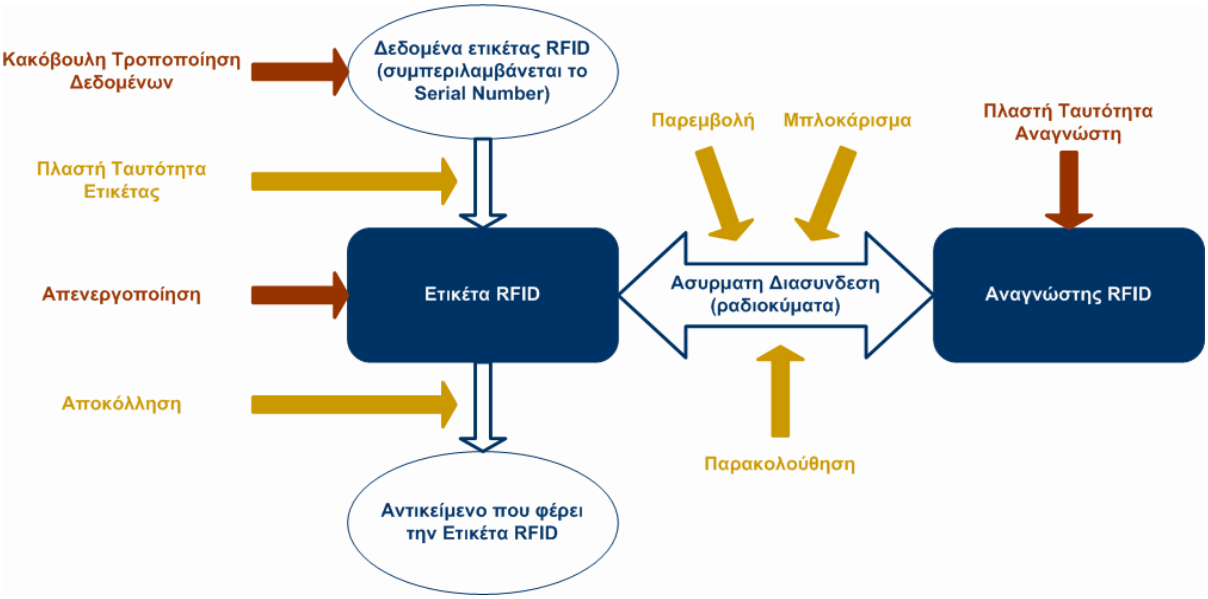
4.3. Ζητήματα Ασφάλειας

Η έννοια της ασφάλειας ενός πληροφοριακού συστήματος σχετίζεται με την ικανότητα ενός οργανισμού

- να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του
- να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν.

Τα συστήματα RFID υπόκεινται σε πολλές επιθέσεις, από επιθέσεις που λειτουργούν στο φυσικό επίπεδο έως επιθέσεις που εκμεταλλεύονται αδυναμίες σε αυτά τα πρωτόκολλα που εκτελούνται στο επίπεδο εφαρμογής [14, 13 , 15]. Οι φυσικές επιθέσεις μπορεί να είναι τόσο απλές όσο το τύλιγμα μιας ετικέτας RFID σε αλουμινόχαρτο, η οποία πιθανόν να προκαλεί άρνηση παροχής υπηρεσιών (DoS), επειδή οι αναγνώστες δεν θα μπορούν να επικοινωνήσουν με μια τέτοια ετικέτα. Άλλες φυσικές επιθέσεις είναι πιο εξελιγμένες, όπως επιθέσεις μπλοκαρίσματος που καταστρέφουν μόνιμα συσκευές ραδιοσυχνοτήτων ή επιθέσεις καναλιών που λαμβάνουν πληροφορίες από τη φυσική εφαρμογή κρυπτοσυστημάτων.

Υπάρχουν όμως και εχθροί που στοχεύουν στη διακοπή των συστημάτων ταυτοποίησης / ελέγχου ταυτότητας χρησιμοποιώντας θεωρητικές αδυναμίες τέτοιων αλγορίθμων. Για να γίνει αυτό, υποθέτουμε ότι ο αντίπαλος μπορεί να παρατηρήσει, να αποκλείσει, να τροποποιήσει και να εισάγει μηνύματα στην επικοινωνία μεταξύ μιας ετικέτας και ενός αναγνώστη. Επιπλέον, καθώς οι ετικέτες δεν είναι ανθεκτικές σε παραβιάσεις, υποθέτουμε ότι ένας αντίπαλος μπορεί να κλωνοποιήσει και να παραβιάσει οποιαδήποτε ετικέτα RFID.



Εικόνα 20: *Σχέσεις μεταξύ στοιχείων RFID και οι απειλές που δέχονται Πηγή: [53,54]:*

Οι απειλές που αντιμετωπίζει ένα σύστημα RFID υφίστανται τόσο στα ίδια τα στοιχεία του συστήματός, όσο και στις σχέσεις μεταξύ αυτών.

4.3.1. Συγκεκριμένα οι απειλές αυτές είναι [53,54]:

- ***Πλαστή Ταυτότητα Ετικέτας***

Η πιο σχετική επίθεση σε συστήματα RFID είναι η λεγόμενη επίθεση πλαστογράφησης. Στην ουσία ο επιτιθέμενος μπορεί να κλωνοποιήσει μια ετικέτα χωρίς να την αναπαράγει φυσικά. Με αυτόν τον τρόπο, ο αντίπαλος αποκτά τα προνόμια μιας τέτοιας ετικέτας, αυτό θεωρείται σημαντική απειλή ασφάλειας για σχεδόν κάθε σύστημα RFID. Η χειρότερη περίπτωση εμφανίζεται όταν ο εχθρός είναι σε θέση να σπάσει το σύστημα κρυπτογράφησης που χρησιμοποιήθηκε κατά τη διαδικασία ελέγχου ταυτότητας. Ο επιτιθέμενος έχει στην κατοχή του σειριακό αριθμό της ετικέτας RFID και άλλα στοιχειά ασφαλείας συστήματος, με σκοπό να εξαπάτηση του αναγνώστη στο να δεχτεί μια άλλη ετικέτα RFID. Μ' άλλα λόγια ο εχθρός αποκτά γνώση των πρωτοκόλλων ελέγχου ταυτότητας και των μυστικών δεδομένων.

Σε πολλές περιπτώσεις, ο αντίπαλος δεν χρειάζεται πολύ χρόνο για να σπάσει πρωτόκολλο της κρυπτογράφησης. Αντίθετα, ο αντίπαλος θα μπορεί να πλαστογραφήσει μια ετικέτα επαναλαμβάνοντας την αναπαραγωγή ή με τον χειρισμό των απαντήσεων ορισμένων ετικετών

που έχουν καταγραφεί από προηγούμενες συναλλαγές (πλαστογράφηση). Παρόλο που αυτές οι επιθέσεις έχουν αποτραπεί με επιτυχία, με την χρήση συμμετρική κρυπτογράφηση κλείδας, κατάλληλη για ετικέτες RFID χαμηλού κόστους [16], εξακολουθούν όμως να υπάρχουν ανοιχτά ζητήματα όταν πρέπει να ληφθεί υπόψη επίσης η προστασία της ιδιωτικής ζωής και της επεκτασιμότητας.

Τέτοιου είδους επιθέσεις εμφανίζονται εφοδιαστικό κύκλο όπου και γίνεται εφικτή η κλοπή προϊόντων με την εξαπάτηση του συστήματος, από κακόβουλα προγράμματα ότι τα προϊόντα υφίστανται ενώ στην πραγματικότητα δεν υπάρχουν.

- ***Κακόβουλη Τροποποίηση Δεδομένων***

Τα δεδομένα των ετικετών RFID, εκτός από τον σειριακό τους αριθμό και άλλα αναγνωριστικά όπως διάφορα κλειδιά διαφοροποιούνται με σκοπό την εξαπάτηση. Αυτού του είδους επιθέσεις παρατηρούνται σε συστήματα ασφάλειας ή/και σε συστήματα ασύρματων πληρωμών, όπου σκοπός είναι η αναγνώριση της ετικέτας RFID από το σύστημα, με τροποποιημένα όμωστα δεδομένα της.

- ***Απενεργοποίηση***

Η ετικέτα δεν αναγνωρίζεται πλέον από το σύστημα ή ακόμα δεν εντοπίζεται από τους αναγνώστες. Η απενεργοποίηση γίνεται από εντολές σβησίματος δεδομένων (delete), νόμιμης απενεργοποίησης (kill) και φυσικής καταστροφής. Σκοπός αυτών των επιθέσεων δεν είναι άλλος από την κακή́ διαχείριση αντικειμένων, αλλά και στην κλοπή αυτών.

- ***Αποκόλληση***

Η ετικέτα αποκολλιέται φυσικά από το προϊόν/αντικείμενο στο οποίο βρισκόταν έτσι ώστε το αντικείμενο αυτό να θεωρείται και να είναι πλέον μην αναγνωρίσιμο. Συχνό φαινόμενο είναι η προσκόλληση διαφορετικής ετικέτας στο αντικείμενο, για την εξαπάτηση του συστήματος .

- ***Παρακολούθηση***

Τα δεδομένα που ανταλλάζουν αναγνώστης και ετικέτα κατά την διάρκεια της επικοινωνίας τους, υποκλέπτονται και αποκωδικοποιούνται.

- ***Μπλοκάρισμα***

Ειδικά κατασκευασμένες ετικέτες, (blocker tags), δημιουργούν την εντύπωση στον αναγνώστη ότι διαβάζεται ταυτόχρονα πολύ μεγάλος αριθμός ετικετών, έτσι που υπάρχει πιθανότητα πρόκλησης μπλόκου στον αναγνώστη λόγω σύγκρουσης που δημιουργείται(collision).

- ***Παρεμβολή***

Η παρεμβολή στην ασύρματη επικοινωνία μεταξύ αναγνώστη και ετικέτας είναι κατά κάποιο τρόπο εύκολη και μπορεί να επιτευχθεί με μέσα, κάλυψη κατάλληλων μέσων των ετικετών ή/και των αναγνωστών. Παραδείγματος χάριν συστήματα εντοπισμού κλοπών σε καταστήματα λιανικού εμπορίου και ειδικότερα ρούχων, αν καλυφθεί η ετικέτα που έχουν τα ρούχα με αλουμίνιο δεν μπορεί να διαβαστεί από αναγνώστες στην έξοδο του καταστήματος οπότε και επιτυγχάνεται η παρεμβολή.

- ***Πλαστή Ταυτότητα Αναγνώστη***

Όταν ο αναγνώστης επιθυμεί να επικοινωνήσει με την ετικέτα, πρέπει να αποδείξει ότι είναι νόμιμος. Αν έναςεπιτιθέμενος επιθυμεί να διαβάσει τα δεδομένα της ετικέτας, το μόνο που χρειάζεται είναι στη ουσία να προσποιηθεί ότι είναι ο πραγματικός αναγνώστης, «δείχνοντας» πλαστή ταυτότητα.

- ***Εμπιστευτικότητα***

Πρόληψη για μη εξουσιοδοτημένης (unauthorized) αποκάλυψης πληροφοριών και δεδομένων , δηλαδή για μη εξουσιοδοτημένη ανάγνωση. Με άλλα λόγια τα δεδομένα αποκαλύπτονται μονό σε εξουσιοδοτημένα, νόμιμα άτομα. Εκδηλώσεις εμπιστευτικότητας είναι η ιδιωτικότητα (privacy) και η μυστικότητα (secrecy).

- ***Μυστικότητα***

Μυστικότητα είναι η προστασία των δεδομένων οργανισμού (Secrecy).

- ***Ακεραιότητα***

Ακεραιότητα είναι η πρόληψη μη εξουσιοδοτημένης αλλοίωσης πληροφοριών. Στον όρο αλλοίωση περιλαμβάνεται η εγγραφή, η διαγραφή αλλά και η δημιουργία δεδομένων.

- ***Διαθεσιμότητα***

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσβάσιμες και χωρίς καθυστερήσεις, οι υπηρεσίες πληροφοριακού συστήματος, όταν χρειάζεται μια εξουσιοδοτημένη οντότητα.

- ***Ευπάθεια***

Ευπάθεια είναι η αδυναμία ή ένα ευάλωτο/τρωτό σημείο στο σύστημα ασφάλειας , που πιθανόν να προκαλέσει απώλειες ή ζημίες, αν αξιοποιηθεί σωστά.

- ***Επίθεση***

Επίθεση ονομάζεται η εκμετάλλευση ευπαθούς σημείου από κάποιο ατόμο.

- ***Απειλή***

Απειλή αποτελεί μια κατάσταση όπου υπάρχει η πιθανότητα να προκληθούν ζημίες στο πληροφοριακό/υπολογιστικό σύστημα. [53,54]

Σχετικά με το μέγεθος και τις φυσικές και άλλες ιδιότητες των ετικετών RFID, λόγω του ότι η ετικέτα πρέπει να είναι μικρή και φθηνή, η ασφάλεια που θα μπορούσε να εξασφαλιστεί σε αυτό το μέρος του συστήματος RFID είναι πολύ περιορισμένη. Εξάλλου, ο ασύρματος τρόπος επικοινωνίας προσθέτει ακόμα μια σειρά κίνδυνων και απειλών σε σχέση με την ενσύρματη επικοινωνία, και επομένως, χρειάζεται επιπρόσθετες απαιτήσεις ασφάλειας.[55]

Είναι γεγονός ότι στις μέρες μας η τεχνολογία RFID γίνεται όλο και πιο προηγμένη και καταρτισμένη, οι καταναλωτές χάνουν κάθε δυνατότητα να αποφύγουν προϊόντα με εμφυτευμένα τσιπς. Ερευνητές, έχουν δημιουργήσει εξαιρετικά μικρά σφαιρίδια γραμμικού κώδικα που είναι αόρατα από τον άνθρωπο. Τα μικροσκοπικά αυτά σφαιρίδια ενσωματώνονται σε μελάνια για τον εντοπισμό χαρτονομισμάτων και άλλων έγγραφων, ή ακόμη και να συνδεθούν με μόρια DNA. Μπορούν επίσης να μπαίνουν σε ουσίες, όπως μπογιές αυτοκίνητων, εκρηκτικές ύλες και άλλα όπου οι υπεύθυνοι επιβολής του νόμου ή οι λιανοπωλητές, ενδιαφέρονται έντονα για την παρακολούθησή.

Οι «εχθροί» της χρήσης των συστημάτων RFID για τον εντοπισμό προϊόντων και προσώπων, έχουν προτείνει μετρά για την παρεμπόδιση της συλλογής πληροφοριών. Από την απενεργοποίηση των ετικετών, έως το απλό μποϋκοτάζ προϊόντων των εταιρειών που χρησιμοποιούν ή σχεδιάζουν να χρησιμοποιήσουν την εφαρμογή της τεχνολογίας RFID, ακόμα και στις σχεδιαστικές/ κατασκευαστικές εταιρίες συστημάτων RFID. Ένας από τους τρόπους για καταστροφή των ετικετών είναι με την τοποθέτηση τους στο φούρνο μικροκυμάτων για μερικά δευτερόλεπτα. Άλλος ένας, διαφορετικός τρόπος είναι η παρεμπόδιση της συγκέντρωσης πληροφοριών από αναγνώστες με τη χρήση RFID tag blocker. Οι tag-blockers με το που μεταφέρονται από τον καταναλωτή, ταυτόχρονα εμποδίζουν τους αναγνώστες λόγω προσομοίωσης πολλών απλών ετικετών RFID ταυτοχρόνως. Ετικέτες τύπου Blocker μπορούν να μπλοκάρουν επιλεκτικά, μόνο μέσω προσομοίωσης συγκεκριμένους κωδικούς ID, αυτοί που εκδίδονται από ένα συγκεκριμένο κατασκευαστή.

4.4. Ιδιωτικότητα

Υπάρχουν δύο βασικά ζητήματα ιδιωτικού απορρήτου στην τεχνολογία RFID: 1) Η διαρροή πληροφοριών και 2) Η δυνατότητα ανίχνευσης. Η διαρροή πληροφοριών είναι κυριολεκτικά επικίνδυνη, εφόσον οι ετικέτες ενδέχεται να αποκαλύπτουν ευαίσθητες πληροφορίες σε σχέση με προϊόντα (π.χ. το όνομα ή την τιμή ακριβών προϊόντων).Τέτοιου είδους δεδομένα μπορούν να χρησιμοποιηθούν για την δημιουργία προφίλ οικονομικών δεδομένων και καταστατικών συγκεκριμένων ατόμων ή βιομηχανιών, κάτι που παραπέμπει στην κατασκοπεία.

Επιπρόσθετα, σύμφωνα με την Γαλλική Αρχή Προστασίας Προσωπικών Δεδομένων, κρίνεται και είναι σκόπιμο να επισημανθούνε οι τέσσερις παγίδες ή απάτες που μπορούν έτσι να μειώσουν τις αρνητικές επιπτώσεις της τεχνολογίας RFID της ιδιωτικής ζωής του καταναλωτή, που περιλαμβάνει και δικαίωμα της ανωνυμίας του ατόμου: [56]

- Παγίδα είναι όταν αφήνεται να νοηθεί ότι τα δεδομένα που αποθηκεύονται στα προϊόντα δεν έχουν σημασία (τι σημασία έχει ο σειριακός αριθμός κουτιού με χυμό;)
- Παγίδα είναι όταν αφήνεται να νοηθεί ότι ετικέτες τοποθετούνται ως επί το πλείστων σε αντικείμενα και όχι σε ανθρώπους

- Παγίδα είναι όταν αφήνεται να νοηθεί ότι οι πλείστες έρευνες για εφαρμογές RFID διεξάγονται σε κέντρα που είναι εγκατεστημένα στις Η.Π.Α., όπου το επίπεδο προστασίας των πολίτων δεν είναι τόσο υψηλό στην Ευρώπη
- Η παγίδα είναι η αόρατη παρουσία εχθρού και αυτόματης ενεργοποίησης του συστήματος RFID, έτσι ώστε ο πολίτης δεν αντιλαμβάνεται την επεξεργασία των πληροφοριών που τον αφορούν.

Πρόκειται πραγματικά για παγίδες διότι :

- Στην πρώτη πτώση αγνοείται το γεγονός δυνατότητας οποιουδήποτε, να συγκεντρώσει πλήθος πληροφοριών για ένα άτομο, από διασταυρωμένη συγκέντρωση και ανάλυση όλων των ετικετών(προϊόντων -αντικειμένων) που φέρει το συγκεκριμένο άτομο.

- Στη δεύτερη περίπτωση παραβλέπει ότι υπάρχει περίπτωση η εξάπλωση χρήσης των ετικετών να συμβεί μελλοντικά και πάνω στον άνθρωπο καθησυχάζοντας το κοινό με λάθος τρόπο.

- Στην Τρίτη περίπτωση δεν λαμβάνεται υπόψη ότι, είναι εξαιρετικά πιθανό σενάριο στην ραγδαία παγκοσμιοποίηση, η χρήση της τεχνολογίας RFID θα εισχωρήσει και στην Ευρώπη, χωρίς να τις λάβει να καλουπωθεί με τα υψηλά πρότυπα ευρωπαϊκής νομοθεσίας για την προστασία των προσωπικών δεδομένων.

- Στην τέταρτη περίπτωση είναι φανερό ότι η αόρατη παρουσία και ενεργοποίηση του συστήματος RFID είναι κάτι παραπάνω από φανερό ότι το πρόσωπο στερείται ατομικής του απόφασης για αυτοπροστασία αφού εν αγνοία του, γίνεται επεξεργασία των προσωπικών του δεδομένων.

5. ΑΠΟΦΥΓΗ ΑΝΙΧΝΕΥΣΙΜΟΤΗΤΑΣ

Η βασική ιδέα για την αποφυγή διαρροής πληροφοριών σε συστήματα RFID είναι η μετακίνηση όλων των δεδομένων των ετικετών σε έναν ή περισσότερους σέρβερ. Με αυτόν τον τρόπο, μόνο εξουσιοδοτημένα μέρη μπορούν να ανακτούν αυτά τα δεδομένα όταν απαιτείται. Ωστόσο, αυτό μπορεί να μην αποτρέψει την ανιχνευσιμότητα. Για παράδειγμα, μια εστία που στέλνει το μοναδικό αναγνωριστικό κωδικό δεν αποκαλύπτει πληροφορίες σχετικά με το αντικείμενο στο οποίο είναι προσαρτημένη, αλλά είναι ανιχνεύσιμη. Για να αποφευχθεί η ανιχνευσιμότητα, οι αναγνώστες και οι ετικέτες πρέπει να ανταλλάσσουν νέες πληροφορίες σε κάθε ταυτοποίηση, ώστε να διακρίνεται η ότι γίνεται απόκριση από δύο διαφορετικές ετικέτες.

Η πρόκληση είναι ότι η διακριτότητα είναι μια έννοια που εξαρτάται από την εφαρμογή όπου πρέπει να ληφθούν υπόψη οι δυνατότητες των αντιπάλων και των κατόχων ετικετών, καθώς και των φυσικών περιορισμών, προκειμένου να παρέχεται ένας υποτυπώδης ορισμός σε σχέση με το απόρρητο για τα συστήματα RFID. Αυτός είναι ο λόγος για τον οποίο έχουν οριστεί διαφορετικά μοντέλα απορρήτου για το RFID [19,18].

Μεταξύ αυτών, παρατίθενται πιο κάτω δύο γνωστές έννοιες περί απορρήτου που πρότεινε η Avoine στο [18]:

- ***Ορισμός 1 :*** (Καθολική ανιχνευσιμότητα). Η καθολική ανιχνευσιμότητα επιτυγχάνεται όταν οποιοδήποτε ζεύγος αποκρίσεων ετικετών, χωρισμένο από μια επιτυχημένη αναγνώριση με έναν νόμιμο αναγνώστη, και δεν μπορεί να συσχετιστεί πλήρη σαφήνεια έναν αντίπαλο.
- ***Ορισμός 2 :*** (Υφιστάμενη ανιχνευσιμότητα). Η υπάρχουσα ανιχνευσιμότητα επιτυγχάνεται όταν οποιοδήποτε ζεύγος αποκρίσεων ετικετών δεν μπορεί να συσχετιστεί πλήρη σαφήνεια από έναν αντίπαλο.

Διαισθητικά, η υφιστάμενη ανιχνευσιμότητα είναι ισχυρότερη από την καθολική ανιχνευσιμότητα. Να σημειωθεί ότι το τελευταίο διασφαλίζει το απόρρητο μόνο έναντι παθητικών αντιπάλων. Αυτός είναι ο λόγος για τον οποίο πρωτόκολλα που επιτυγχάνουν καθολική

ανιχνευσιμότητα αναφέρονται συνήθως ως παθητικά ιδιωτικά, ενώ αυτά τα πρωτόκολλα που επιτυγχάνουν υπαρξιακή ανιχνευσιμότητα αναφέρονται ως ενεργά ιδιωτικά.

Υπάρχουν έννοιες της ιδιωτικής ζωής στα συστήματα RFID όπως η ανιχνευσιμότητα εμπρός και πίσω. Και οι δύο έννοιες βασίζονται στο γεγονός ότι οι ετικέτες RFID δεν είναι ανθεκτικές σε παραβιάσεις και επομένως, ένας αντίπαλος μπορεί να έχει πλήρη πρόσβαση στην εσωτερική κατάσταση μιας ετικέτας. Ανεπίσημα, η ανιχνευσιμότητα εμπρός και πίσω, διασφαλίζουν ότι η αποκαλύπτοντας την εσωτερική κατάσταση μιας ετικέτας δεν μπορεί να βοηθήσει έναν αντίπαλο να εντοπίσει τις προηγούμενες ή τις μελλοντικές συναλλαγές μιας ετικέτας.

5.1. Πρόοδοι στα πρωτόκολλα αναγνώρισης RFID

Όπως αναφέρεται στο [17], μια ετικέτα μπορεί να ταξινομηθεί σύμφωνα με τις λειτουργίες που υποστηρίζει. Οι ετικέτες υψηλού κόστους είναι αυτές που υποστηρίζουν την συμβατική κρυπτογράφηση και η συμμετρική κρυπτογράφηση και η κρυπτογράφηση δημόσιας κλείδας.

Οι απλές ετικέτες θεωρούνται ετικέτες υψηλού κόστους, με την διαφορά ότι υποστηρίζουν μόνο γεννήτορες τυχαίων αριθμών και συναρτήσεις κατατεμαχισμού μονής κατεύθυνσης. Επίσης, οι ετικέτες χαμηλού κόστους μπορούν να ταξινομηθούν ως ετικέτες ελαφράς βαρύτητας ή ετικέτες εξαιρετικά ελαφράς βαρύτητας. Και οι δύο είναι σε θέση να υπολογίσουν απλές λειτουργίες bitwise όπως XOR, AND, OR, αλλά οι πρώτες υποστηρίζουν γεννήτορες τυχαίων αριθμών και πιο απλές λειτουργίες έλεγχος cyclic redundancy code (CRC). Αναμφίβολα, οι χαμηλού κόστους και οι απλές ετικέτες, που προορίζονται ως αντικατάσταση των ετικετών γραμμικού κώδικα, αντιπροσωπεύουν τη μεγαλύτερη πρόκληση σε θέματα ασφάλεια και προστασία της ιδιωτικής ζωής.

5.2. Άλλα ζητήματα στα συστήματα RFID

Η παρακολούθηση και ο εντοπισμός είναι οι κύριοι στόχοι συστήματος RFID. Κατά συνέπεια, αυτές οι προκλήσεις που σχετίζονται με τη διαδικασία αναγνώρισης μπορεί να φαίνονται πολύ πιο σχετικές από άλλες. Ωστόσο, τα συστήματα RFID θα πρέπει να αντιμετωπίσουν πολλές άλλες προκλήσεις ανάλογα με την εφαρμογή τους. Για παράδειγμα, οι λύσεις RFID που αποσκοπούν στον έλεγχο πρόσβασης απαιτούν οι ετικέτες να βρίσκονται κοντά στους αναγνώστες. Ωστόσο, η

τεχνολογία RFID δεν είναι σε θέση να μετρήσει την απόσταση από τους αναγνώστες έως τις ετικέτες όπως μπορεί να κάνει η τεχνολογία GPS. Αυτό κάνει την πρόκληση του σχεδιασμού πρωτοκόλλων οριοθέτησης από απόσταση αφιερωμένων στις ετικέτες RFID μεγαλύτερη [20]. Επιπλέον, η σωστή χρήση δεδομένων RFID εξακολουθεί να είναι ένα ευρύ ζήτημα. Χάρη στην τεχνολογία RFID, οι τροχιές των ατόμων μπορούν εύκολα να συλλεχθούν και να απελευθερωθούν από σουπερμάρκετ, νοσοκομεία ή λούνα παρκ. Επομένως, οι αποτελεσματικοί αλγόριθμοι ανωνυμοποίησης τροχιάς είναι ανάγκη για προστασία του απορρήτου των χρηστών RFID.

5.3. Έλεγχος απόστασης

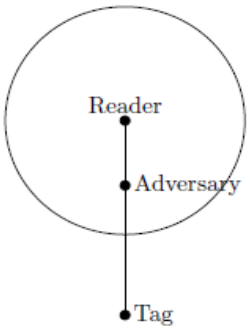
Το 1987, οι Desmedt, Goutier και Bengio [23] παρουσίασαν μια επίθεση που νίκησε οποιοδήποτε πρωτόκολλο ελέγχου ταυτότητας. Σε αυτήν την επίθεση, που ονομάζεται Mafia Fraud, ο αντίπαλος περνά από τη διαδικασία ελέγχου ταυτότητας απλώς μεταδίδοντας τα μηνύματα μεταξύ ενός νόμιμου αναγνώστη (του επαληθευτή) και μιας νόμιμης ετικέτας (ο αποδέκτης). Με αυτόν τον τρόπο, δεν χρειάζεται να τροποποιεί ή να αποκρυπτογραφεί δεδομένα που ανταλλάσσονται. Αρχικά, αυτή η επίθεση θεωρήθηκε μάλλον μη ρεαλιστική, επειδή ο αποδέκτης πρέπει να συμμετέχει ενεργά σε αυτήν. Ωστόσο, οι RFID ετικέτες ανταποκρίνονται σε οποιοδήποτε αίτημα του αναγνώστη χωρίς καμία συμφωνία ή επίγνωση του φορέα τους, ένα χαρακτηριστικό που ανοίγει σαφώς την πόρτα σε αυτόν τον τύπο επίθεσης.

Στην πραγματικότητα, υπάρχουν κάποιες αποδείξεις της έννοιας αυτής, που δείχνουν τη σκοπιμότητα της απάτης Mafia Fraud. Το 2005, ο Hancke έδειξε ότι δύο συμμαχίες που απέχουν 50 μέτρα μπορούν να εκτελέσουν επίθεση απάτης Mafia Fraud μέσω ενός ραδιοφωνικού καναλιού [21]. Αυτό είναι ιδιαίτερα επικίνδυνο επειδή αυτή η απόσταση είναι αρκετά μεγάλη για να προκαλέσει μια επίθεση απάτης Mafia Fraud σε σχεδόν κάθε σύστημα πληρωμών ή ελέγχου πρόσβασης. Δεν αποτελεί έκπληξη ότι αυτή η επίθεση έχει εφαρμοστεί με επιτυχία σε άλλες τεχνολογίες [24] , συγκεκριμένα, Bluetooth, σε ανέπαφες κάρτες και NFC.

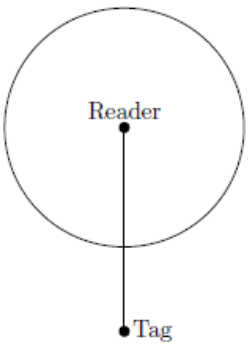
Μια άλλη επίθεση που βασίστηκε στην εξαπάτηση της απόστασης μεταξύ δοκιμαστών και επαληθευτών εισήχθη το 1993 από τους Brands και Chaum [22]. Σε αυτήν την επίθεση, που ονομάζεται Distance Fraud, ένας παράνομος αποδέκτης ισχυρίζεται ότι είναι πιο κοντά στον επαληθευτή από ό, τι είναι στην πραγματικότητα. Οι εικόνες 21 και 22 απεικονίζουν τόσο την μαφία όσο και την απάτη από απόσταση αντίστοιχα. Και για τα δύο σχήματα, ο κύκλος

αντιπροσώπευε τη μέγιστη απόσταση στην οποία πρέπει να επικυρωθεί ένας αποδέκτης. Επισήμως, μπορούμε να ορίσουμε και τις δύο απάτες ως εξής [25]:

- **Ορισμός 3 (Mafia fraud).** Μια απάτη μαφίας είναι μια επίθεση όπου ένας αντίπαλος περνά ένα πρωτόκολλο ελέγχου ταυτότητας χρησιμοποιώντας μια στρατηγική man-in-the-middle μεταξύ του αναγνώστη και μιας έντιμης ετικέτας που βρίσκεται έξω από τη γειτονιά του επαληθευτή.
- **Ορισμός 4 (Distance fraud)**. Η απάτη εξ αποστάσεως είναι μια επίθεση όπου ένας ανέντιμος και μοναχικός υποστηρικτής ισχυρίζεται ότι βρίσκεται στη γειτονιά του επαληθευτή όταν στην πραγματικότητα δεν είναι.



Εικόνα21: Απάτη μαφίας: ένας αντίπαλος που προσπαθεί να επικυρωθεί εφαρμόζοντας μια επίθεση man-in-the-middle.



Εικόνα 22 : Απόσταση απάτης: ένας νόμιμος επαληθευτής είναι πιο μακριά από τον αποδέκτη από το αναμενόμενο.

5.4. Πρωτόκολλα περιορισμού απόστασης RFID

Το 1993, οι Brands και Chaum [22] πρότειναν ένα αντίμετρο που αποτρέπει μια τέτοια επίθεση υπολογίζοντας ένα ανώτερο όριο της απόστασης μεταξύ του αναγνώστη και της ετικέτας για έλεγχο ταυτότητας: το πρωτόκολλο οριοθέτησης απόστασης. Με αυτόν τον τρόπο, τα mafia και distance frauds δεν θα μπορούσαν να αποφευχθούν εντελώς, αλλά αυτά τα πρωτόκολλα ενδέχεται να τις αποτρέψουν. Ωστόσο, μόλις το 2005 εμφανίστηκε το πρώτο πρωτόκολλο οριοθέτησης από απόσταση αφιερωμένο στο RFID [20].

Το πρωτόκολλο χωρίζεται σε δύο φάσεις: μια αργή φάση, στην οποία ο αναγνώστης και η ετικέτα ανταλλάσσουν δύο nonces, και συνεχίζουν την ανταλλαγή πληροφοριών. Ακολούθως υπάρχει γρήγορη φάση χωρισμένη σε n γύρους όπου, σε κάθε έναν, ο αναγνώστης μετρά τον χρόνο μετ ' επιστροφής (RTT) της διαδικασίας πρόκλησης / απόκρισης. Λαμβάνοντας υπόψη ότι τα ραδιοκύματα δεν μπορούν να διαδίδονται γρηγορότερα από το φως, ο αναγνώστης μπορεί να δεσμεύσει την απόσταση μεταξύ αυτού και της ετικέτας. Αυτές οι επικοινωνίες παρέχουν επίσης απόδειξη ταυτότητας της ετικέτας. Δυστυχώς, η πιθανότητα επιτυχίας του αντιπάλου σχετικά με τα mafia και distance frauds είναι $(3/4)_n$ ενώ κάποιος θα υπολόγιζε $(1/2)_n$ (η πιθανότητα επιτυχίας του αντιπάλου σε κάθε γύρο αναμένεται να είναι 1/2). Έκτοτε, έχουν προταθεί αρκετά πρωτόκολλα οριοθέτησης από απόσταση RFID προκειμένου να βελτιωθεί η αντίσταση και στις δύο απάτες. Μεταξύ όλων των πρωτοκόλλων οριοθέτησης RFID, διαφοροποιούμε δύο κύριες οικογένειες.

Εκείνοι που απαιτούν μια επιπλέον αργή φάση μετά τη γρήγορη φάση. Αυτή η τελική φάση μπορεί να χρησιμοποιηθεί για την υπογραφή των μηνυμάτων που μεταδίδονται κατά τη διάρκεια της γρήγορης φάσης ή για τον έλεγχο οποιωνδήποτε άλλων πληροφοριών. Εκείνοι που, πλησιέστερα στην πρόταση Hancke και Kuhn [20], τερματίζουν το πρωτόκολλο μετά τη γρήγορη φάση.

Οι Brands και Chaum [22] πρότειναν το πρώτο πρωτόκολλο οριοθέτησης απόστασης βασισμένο σε μια υπογραφή μετά τη γρήγορη φάση. Στην πρώτη αργή φάση, ο αποδέκτης (verifier) δεσμεύει στον επαληθευτή(prover) μια ακολουθία n bits $m_1, \cdots, m_n$. Στη συνέχεια, κατά τη διάρκεια της γρήγορης φάσης, ο επαληθευτής στέλνει μια πρόκληση ci στον prover, ο οποίος θα πρέπει να απαντήσει με $r_i = c_i \oplus m_i$. Επίσης, ο αποδέκτης συνενώνει και υπογράφει με το ιδιωτικό του κλειδί όλες τις προκλήσεις και τις απαντήσεις, δηλαδή στέλνει στον αποδέκτη Signk ($c_1 \| r_1 \| \cdots$

|| c_n || r_n). Εάν κάποια απόκριση r_i καθυστερήσει περισσότερο από ένα όριο Δt, ο επαληθευτής υποθέτει ότι ο αποδέκτης είναι εκτός επιτρεπόμενης περιοχής. Τέλος, εάν ο επαληθευτής επιτύχει σε όλους τους γύρους, ο αποδέκτης ελέγχει την ληφθείσα υπογραφή προκειμένου να επαληθεύσει την επικύρωση. Αυτό το πρωτόκολλο θεωρείται ισχυρό με την έννοια ότι τόσο mafia όσο και η distance fraud από απόσταση δεν μπορούν να επιτύχουν με πιθανότητα μεγαλύτερη από $(1/2)^n$.

Υπάρχουν και άλλα πρωτόκολλα που καθορίζουν την απόσταση βάσει της πρότασης Brands and Chaum [27]. Δεδομένου ότι τόσο τα mafia και distance frauds δεν μπορούν να βελτιωθούν, αυτά τα πρωτόκολλα στοχεύουν στη βελτίωση της αντίστασης σε έναν νέο τύπο απάτης που ονομάζεται terrorist fraud [25] (βλ. Ορισμό 5), παρόλο που αυτός ο τύπος απάτης είναι εκτός του πεδίου αυτής της διατριβής.

- **Ορισμός 5 (Terrorist fraud).** Μια τρομοκρατική απάτη (terrorist fraud) είναι μια επίθεση όπου ένας αντίπαλος νικά ένα πρωτόκολλο οριοθέτησης από απόσταση χρησιμοποιώντας μια στρατηγική man-in-the-middle μεταξύ του αναγνώστη και μιας παράνομης ετικέτας που βρίσκεται έξω από τη νόμιμη περιοχή, έτσι ώστε η τελευταία να βοηθά ενεργά τον αντίπαλο να μεγιστοποιήσει την πιθανότητα επιτυχία της επίθεσης, χωρίς να της δίνει κανένα πλεονέκτημα για μελλοντικές επιθέσεις.

Στην πράξη, η τελική υπογραφή αντιπροσωπεύει μια επιπλέον καθυστέρηση. Άλλωστε, σύμφωνα με το [26], καθώς ο έλεγχος ταυτότητας βασίζεται εξ ολοκλήρου σε αυτήν τη φάση, εάν η τελευταία διακοπεί ή δεν επιτευχθεί, τότε ολόκληρη η διαδικασία χάνεται. Αυτό σημαίνει ότι προτιμώνται ασφαλή πρωτόκολλα περιορισμού απόστασης που δεν απαιτούν τελική υπογραφή.

Μεταξύ των πρωτοκόλλων χωρίς τελική υπογραφή, το πρωτόκολλο Avoine και Tchamkerten [26] είναι το πιο ανθεκτικό στις mafia και distance frauds. Εισήγαγε την έννοια των πρωτοκόλλων οριακής απόστασης που βασίζονται σε δέντρα. Η ιδέα είναι ότι ο αποδέκτης και ο επαληθευτής συμφωνούν σε ένα δέντρο αποφάσεων βάθους n, το οποίο περιέχει στους κόμβους του τις σωστές απαντήσεις για οποιαδήποτε ακολουθία προκλήσεων $c_1, \cdots, c_i$ $(1 \leq i \leq n)$. Δεδομένου ότι οι τιμές των κόμβων επιλέγονται τυχαία στην αρχή του πρωτοκόλλου, η πιθανότητα δύο διαφορετικές ακολουθίες προκλήσεων $c_1, \cdots, c_i$ και $\tilde{c}_1, \cdots, \tilde{c}_i$ να περιέχουν την ίδια απόκριση είναι $1/2$. Διαισθητικά, αυτή η ιδιοκτησία μειώνει δραματικά την πιθανότητα επιτυχίας των mafia και distance frauds. Ωστόσο, η αποθήκευση ενός δέντρου βάθους n είναι απαγορευτική για τις

περισσότερες ετικέτες RFID. Σε σύγκριση με το πρωτόκολλο Avoine και Tchamkerten [28], το πρωτόκολλο του Kim an Avoine [32, 33] επιτυγχάνει μεγάλη αντίσταση στο mafia fraud. Επιπλέον, το πρωτόκολλο τους απαιτεί μόνο 4_n bits μνήμης στην πλευρά της ετικέτας όπου *n* είναι ο αριθμός των γύρων.

Σε αυτό το πρωτόκολλο, ο αποδέκτης είναι εξοπλισμένος με έναν μηχανισμό για να ανιχνεύσει εάν είναι ο στόχος μιας επίθεσης mafia fraud. Στη συνέχεια, μόλις εντοπιστεί η επίθεση, αποκρίνεται τυχαία στους επόμενους γύρους.

Επομένως, η πιθανότητα επιτυχίας του αντιπάλου μειώνεται σημαντικά. Ωστόσο, όσο πιο αποτελεσματικός είναι ο μηχανισμός, τόσο ασθενέστερο είναι το πρωτόκολλο κατά της επίθεσης distance fraud. Κατά συνέπεια, το πρωτόκολλο Kim και Avoine [32, 33] μπορεί να μην είναι κατάλληλο όταν πρέπει να αποτραπούν τόσο τα mafia όσο και τα distance frauds

5.5. Ανωνυμοποίηση τροχιάς

Η θέση ενός ατόμου μπορεί να προσδιοριστεί με διαφορετικές τεχνικές. Ενδεχομένως, η πιο συμβατική και προγονική από αυτές τις τεχνικές είναι η οπτική ταυτοποίηση αυτού του ατόμου σε ένα δεδομένο μέρος μια δεδομένη στιγμή. Σήμερα, αυτή η εργασία είναι πολύ πιο εύκολη, καθώς δεν υπάρχει ανάγκη για ένα άτομο να παρακολουθεί ή να παρενοχλεί άλλο άτομο. Αντ' αυτού, πολλές τεχνολογίες που υιοθετούνται ευρέως παγκοσμίως μπορούν να εκτελέσουν αυτό το καθήκον για εμάς αυτόματα (π.χ. κάμερες παρακολούθησης, συναλλαγές με πιστωτικές κάρτες, αναγνώριση RFID, μεταξύ άλλων). Επιπλέον, η σημερινή διεισδυτικότητα των συσκευών που γνωρίζουν την τοποθεσία, όπως τα κινητά τηλέφωνα και οι δέκτες GPS, βοηθούν τις εταιρείες και τις κυβερνήσεις να συλλέγουν εύκολα τεράστιες πληροφορίες σχετικά με τις κινήσεις των ανθρώπων.

Η ανάλυση και η εξόρυξη αυτού του τύπου πληροφοριών, επίσης γνωστών ως δεδομένα τροχιάς ή χωροχρονικών δεδομένων, ενδέχεται να αποκαλύψει νέες τάσεις και προηγούμενες άγνωστες γνώσεις που πρέπει να χρησιμοποιούνται στην κυκλοφορία, τη διαχείριση βιώσιμης κινητικότητας, τον αστικό σχεδιασμό, τη διαχείριση της εφοδιαστικής αλυσίδας κ.λπ. Με αυτόν τον τρόπο, οι πόροι μπορούν να βελτιστοποιηθούν και οι επιχειρηματικές και κυβερνητικές αποφάσεις μπορούν να είναι σταθερές και βάσιμες. Ως αποτέλεσμα, θεωρείται ότι τόσο οι

εταιρείες όσο και οι πολίτες επωφελούνται άμεσα από τη δημοσίευση και ανάλυση βάσεων δεδομένων τροχιών. Ωστόσο, υπάρχουν προφανείς απειλές για το απόρρητο των ατόμων εάν οι τροχιές τους δημοσιεύονται με τρόπο που επιτρέπει την επαναπροσδιορισμό του ατόμου πίσω από μια τροχιά.

Μια προσωρινή λύση για τη διατήρηση του απορρήτου των ατόμων είναι η από-ταυτοποίηση, δηλαδή η κατάργηση όλων των αναγνωριστικών χαρακτηριστικών των ατόμων. Ωστόσο, αυτό συχνά δεν επαρκεί για τη διατήρηση της ιδιωτικής ζωής των ατόμων. Ένα άλλο σύνολο χαρακτηριστικών, γνωστοί ως quasi-identifiers, μαζί με εξωτερικές πληροφορίες, μπορεί να χρησιμοποιηθούν για την ταυτοποίηση του ατόμου πίσω από μια εγγραφή. Για παράδειγμα, έχει αποδειχθεί ότι η πλειάδα {ταχυδρομικός κώδικας, φύλο και ημερομηνία γενεθλίων} είναι μοναδική για το 87% του πληθυσμού των Ηνωμένων Πολιτειών [29]. Για παράδειγμα στο πλαίσιο των χωροχρονικών βάσεων δεδομένων, ας εξετάσουμε μια εφαρμογή GPS που καταγράφει τις τροχιές ορισμένων ατόμων. Η καθημερινή ρουτίνα δείχνει ότι η πορεία ενός χρήστη το πρωί είναι πιθανό να ξεκινήσει στο σπίτι και να τελειώσει στο χώρο εργασίας του. Αυτές οι πληροφορίες μπορούν εύκολα να συνδεθούν με έναν μόνο χρήστη, του οποίου η ταυτότητα μπορεί να ληφθεί από μια εξωτερική πηγή πληροφοριών, όπως τηλεφωνικούς καταλόγους ή κοινωνικά δίκτυα.

Η εκτίμηση του αριθμού των εξωτερικών πληροφοριών που είναι διαθέσιμες σε έναν αντίπαλο είναι μια πρόκληση [31]. Επιπλέον, οι πληροφορίες του χρόνου και η σχέση τους με τις χωρικές πληροφορίες δίνουν μια ξεχωριστή φύση στα χωροχρονικά δεδομένα πάνω από τα μικροδεδομένα, δηλαδή πάνω από τις εγγραφές που περιγράφουν τα δεδομένα των χρηστών χωρίς διαδοχική σειρά. Αυτός είναι ο λόγος για τον οποίο οι παραδοσιακές μέθοδοι ανωνυμοποίησης και απολύμανσης για τα μικροδεδομένα [30] δεν είναι κατάλληλες για χωροχρονικά δεδομένα και αντίστροφα. Επομένως, απαιτούνται ολοένα και περισσότεροι αλγόριθμοι ανωνυμοποίησης που αποσκοπούν στην αποτροπή των επιθέσεων απορρήτου σε δημοσιευμένες βάσεις δεδομένων τροχιών.

5.6. *k*- Ανωνυμία και *l*- ποικιλομορφία

Έχουν γίνει πολλές εργασίες σε ανώνυμα μικροδεδομένα και σχεσιακές / συναλλακτικές βάσεις δεδομένων [36]. Ένας συνηθισμένος στόχος στην ανωνυμοποίηση είναι η επίτευξη της *k*-ανωνυμίας [37, 29], η οποία είναι η έννοια της «ασφάλειας σε αριθμούς».

Ένα ανώνυμο σύνολο μικροδεδομένων λέγεται ότι ικανοποιεί την *k*-ανωνυμία, εάν κάθε συνδυασμός τιμών χαρακτηριστικών quasi-identifier κοινοποιείται από τουλάχιστον *k* εγγραφές. Επομένως, αυτή η ιδιότητα εγγυάται ότι ένας αντίπαλος δεν μπορεί να προσδιορίσει το άτομο στο οποίο αντιστοιχεί μια ανώνυμη εγγραφή με πιθανότητα μεγαλύτερη από 1 / *k*.

Μια άλλη χρήσιμη έννοια απορρήτου είναι η *l*-ποικιλομορφία [34], η οποία βελτιώνει την *k*-ανωνυμία διαφοροποιώντας τις τιμές ευαίσθητων χαρακτηριστικών κάθε ομάδας εγγραφών που μπορούν να απομονωθούν από έναν εισβολέα. Αυτή η έννοια απορρήτου οφείλεται στο γεγονός ότι ακόμη και όταν ένας αντίπαλος δεν μπορεί να αναγνωρίσει την εγγραφή του ατόμου σε ένα σύνολο εγγραφών *k* με πιθανότητα μεγαλύτερη από 1 / *k*, θα μπορούσε εύκολα να ανακτήσει τις ευαίσθητες αξίες του ατόμου με υψηλό επίπεδο εμπιστοσύνης, π.χ. εάν οι εγγραφές *k* έχουν τις ίδιες ευαίσθητες αξίες. Στο [34, 35], μπορείτε να βρείτε διαφορετικές εκτιμήσεις σχετικά με την έννοια της ιδιωτικής ζωής «-ποικιλότητας».

5.7. Microaggregation

k- Ανωνυμία δεν μπορεί να επιτευχθεί άμεσα με χωροχρονικά δεδομένα, επειδή οποιοδήποτε σημείο ή χρόνος μπορεί να θεωρηθεί ως χαρακτηριστικό quasi-identifier [41]. Η άμεση *k*-ανωνυμοποίηση θα απαιτούσε να μετατραπεί ένα σύνολο αρχικών τροχιών σε ένα σύνολο ανώνυμων τροχιών έτσι ώστε καθένα από αυτά να είναι πανομοιότυπο με τουλάχιστον *k* - 1 άλλων ανώνυμων τροχιών. Αυτό προφανώς θα προκαλούσε τεράστια απώλεια πληροφοριών.

Η γενίκευση ήταν η υπολογιστική προσέγγιση που προτάθηκε αρχικά για να επιτευχθεί η ονομασία *k* ανωνυμία [37] . Αργότερα, ο Zhang et al. εισήγαγε την προσέγγιση με βάση τη μεταλλαγής [38], η οποία έχει το πλεονέκτημα ότι δεν περιορίζεται από τον τομέα της ιεραρχικής γενίκευσης. Στο [39] αποδείχθηκε ότι η *k*-ανωνυμία θα μπορούσε επίσης να επιτευχθεί μέσω της μικρής συσσωμάτωσης των quasi-identifiers. Η μικρή συσσωμάτωση [40] λειτουργεί σε δύο στάδια:

Ομαδοποίηση-δημιουργία συμπλέγματος. Οι αρχικές εγγραφές χωρίζονται σε ομάδες βάσει κάποιου μέτρου ομοιότητας (κάποιο είδος απόστασης) μεταξύ των εγγραφών με τον περιορισμό ότι κάθε σύμπλεγμα πρέπει να περιέχει τουλάχιστον εγγραφές *k* - *Ανωνυμοποίηση*. Κάθε σύμπλεγμα, είναι ανώνυμα ξεχωριστό. Η ανωνυμοποίηση ενός συμπλέγματος μπορεί να βασίζεται

σε έναν χειριστή συνάθροισης όπως ο μέσος όρος [40] ή ο διάμεσος [39], ο οποίος χρησιμοποιείται για τον υπολογισμό του κεντρικού συμπλέγματος . Κάθε εγγραφή στο σύμπλεγμα στη συνέχεια αντικαθίσταται από το κεντρικό σύμπλεγμα. Η ανωνυμοποίηση ενός συμπλέγματος μπορεί επίσης να επιτευχθεί αντικαθιστώντας τις εγγραφές στο σύμπλεγμα με συνθετικά ή μερικώς συνθετικά δεδομένα. Αυτό ονομάζεται υβριδική μικροσυσσωμάτωση δεδομένων ή συμπύκνωση [43].

5.8. Αλγόριθμοι ομαδοποίησης των τροχιών

Ακριβώς όπως στις εγγραφές μικροδεδομένων, η καταστολή των άμεσων αναγνωριστικών από τις τροχιές δεν αρκεί για την προστασία της ιδιωτικής ζωής . Κατά συνέπεια, έχουν προταθεί αρκετές έννοιες ανωνυμίας και μέθοδοι για τροχιές. Μεταξύ αυτών, εξετάζουμε στη συνέχεια αυτές που προσπαθούν να επιτύχουν κάποιες έννοιες της τροχιάς *k*-ανωνυμίας. Άλλες συγκρίσεις πολλών μεθόδων ανωνυμοποίησης τροχιάς μπορούν να βρεθούν στο [42].

Μια αφελής προσέγγιση για την επίτευξη της *k*-ανωνυμίας είναι με την καταστολή των χαρακτηριστικών τιμών, η οποία χρησιμοποιείται γενικά σε κατηγορηματικά ονομαστικά δεδομένα όπου οι μέθοδοι διαταραχής δεν είναι οι κατάλληλες. Μία από τις πρώτες μεθόδους καταστολής για ανωνυμοποίηση τροχιάς οφείλεται στον Trrovitis και τον Mamoulis [46]. Θεωρούν ότι οι τροχιές είναι ακολουθίες διευθύνσεων που λαμβάνονται από έναν τομέα διευθύνσεων *P* και από αντίπαλους που ελέγχουν υποσύνολα διευθύνσεων του *P*. Έτσι, οι γνώσεις του αντιπάλου μπορούν να αναπαρασταθούν ως βάση δεδομένων των προβολών των αρχικών τροχιών πάνω από τις διευθύνσεις στο *P* που ελέγχει. Στη συνέχεια, προτείνουν έναν άπληστο αλγόριθμο με σκοπό να εγγυηθεί ότι καμία διεύθυνση άγνωστη στον αντίπαλο δεν μπορεί να συνδεθεί με οποιονδήποτε χρήστη με πιθανότητα υψηλότερη από κάποιο όριο. Το κύριο πρόβλημα με αυτήν την προσέγγιση είναι ότι η αντιμετώπιση όλων των πιθανών γνώσεων του αντιπάλου προκαλεί ένα πρόβλημα ανωνυμοποίησης δυσκολότερο από το απλούστερο πρόβλημα *k*-ανωνυμίας σε συνδεόμενες βάσεις δεδομένων, το οποίο είναι ήδη γνωστό ότι είναι NP-Hard [47].

Οι Abul, Bonchi και Nanni πρότειναν την έννοια της τροχιάς της *k*-ανωνυμίας, υποθέτοντας αβεβαιότητα στα δεδομένα που παρέχονται από τεχνολογίες όπως το GPS [41, 42]. Πρότειναν επίσης δύο μεθόδους για την επίτευξη μυστικότητας σύμφωνα με την έννοια της ιδιωτικής ζωής.

Στην αρχική μέθοδο –Never Walk Alone (NWA) [41] , το σύνολο των τροχιών χωρίζεται σε διαχωριστικά υποσύνολα στα οποία οι τροχιές ξεκινούν και τελειώνουν περίπου την ίδια στιγμή.

Στη συνέχεια, οι τροχιές σε κάθε σύνολο συγκεντρώνονται χρησιμοποιώντας την Ευκλείδεια απόσταση. Στη μέθοδο παρακολούθησης –Wait For Me (W4M) [42] , οι αρχικές τροχιές συγκεντρώνονται χρησιμοποιώντας την απόσταση επεξεργασίας σε πραγματικές ακολουθίες (EDR) [48]. Και οι δύο προσεγγίσεις προχωρούν κάνοντας ανώνυμο κάθε σύμπλεγμα ξεχωριστά. Δύο τροχιές *T1* και *T2* λέγεται ότι συν-εντοπίζονται σε σχέση με το δ σε ένα συγκεκριμένο χρονικό διάστημα $[t_1, t_n]$ εάν για κάθε τριπλό (t, x_1, y_1) στο *T1* και κάθε τριπλό (t, x_2, y_2) σε *T2* με $t \in [t_1, t_n]$, υποστηρίζει ότι η χωρική ευκλείδεια απόσταση μεταξύ των δύο τριπλών δεν είναι μεγαλύτερη από δ. Η ανωνυμία σε αυτό το πλαίσιο σημαίνει ότι κάθε τροχιά εντοπίζεται με τουλάχιστον k - 1 άλλες τροχιές ((k, δ) -ανωνυμία).

Η ανωνυμοποίηση επιτυγχάνεται με χωρική μετάφραση τροχιών μέσα σε ένα σύμπλεγμα τουλάχιστον k τροχιών που έχουν το ίδιο χρονικό διάστημα. Στην ειδική περίπτωση όταν $\delta = 0$, η μέθοδος παράγει μία κεντρική/ μέση τροχιά που αντιπροσωπεύει όλες τις τροχιές στο σύμπλεγμα. Η ad hoc προ-επεξεργασία και η απομάκρυνση του εξωτερικού διευκολύνουν τη διαδικασία. Το βοηθητικό πρόγραμμα αξιολογείται ως προς την παραμόρφωση της τροχιάς και τον αντίκτυπο στα αποτελέσματα των ευρύτερων ερωτημάτων. Το πρόβλημα με τη μέθοδο NWA είναι ότι ο διαχωρισμός του συνόλου όλων των τροχιών σε υποσύνολα που μοιράζονται το ίδιο χρονικό διάστημα μπορεί να παράγει πάρα πολλά υποσύνολα με πολύ λίγες τροχιές μέσα σε καθεμία από αυτές. Σαφώς, ένα υποσύνολο με λιγότερες από k τροχιές δεν μπορεί να k-ανωνυμοποιηθεί. Επίσης, ο καθορισμός μιας τιμής για δ μπορεί να είναι περίεργος σε πολλές εφαρμογές (π.χ. τροχιές που καταγράφονται χρησιμοποιώντας τεχνολογία RFID).

Μια άλλη έννοια που βασίζεται στην k-ανωνυμία για τροχιές που αποτελείται από εύρη σημεία και χρόνο. Χρησιμοποιεί ομαδοποίηση για να ελαχιστοποιήσει τη "μέτρηση κόστους καταγραφής", η οποία μετρά το βάρος των χωρικών και χρονικών μεταφράσεων με που παρέχονται από τον χρήστη. Η ελαχιστοποίηση του κόστους καταγραφής μεγιστοποιεί τη χρησιμότητα. Τα συμπλέγματα ανωνυμοποιούνται με αντιστοίχιση σημείων των τροχιών και γενίκευσή τους σε ελάχιστα πλαίσια οριοθέτησης. Τα αταίριαστα σημεία καταστέλλονται όπως και κάποιες τροχιές. Τα ανώνυμα δεδομένα δεν κυκλοφορούν. Αντίθετα, οι συνθετικές «ατομικές» τροχιές (που έχουν μονάδα x-range, y-range και time range) δημιουργούνται με δειγματοληψία

των ορίων οριοθέτησης. Αυτή η προσέγγιση δεν απελευθερώνει τυπικές τροχιές αλλά μόνο τροχιές με εύρος μονάδων.

Στο [50], η *k*-ανωνυμία σημαίνει ότι μια αρχική τροχιά *T* γενικεύεται σε μια τροχιά *g(T)* (χωρίς τις πληροφορίες του χρόνου) με τέτοιο τρόπο ώστε το *g(T)* είναι μια υπο-τροχιά των γενικεύσεων τουλάχιστον *k* - 1 από άλλη αρχική τροχιά. Η παράβλεψη των πληροφοριών του χρόνου κατά τη διάρκεια της ανωνυμοποίησης που χρησιμοποιούνται για την επίτευξη της *k*-ανωνυμίας είναι τα κύρια μειονεκτήματα αυτής της μεθόδου. Το βοηθητικό πρόγραμμα μετριέται συγκρίνοντας τα αποτελέσματα ομαδοποίησης.

Το [49] είναι μια άλλη πρόταση για την επίτευξη της *k*-ανωνυμίας των τροχιών μέσω της γενίκευσης. Η διαφορά έγκειται στον τρόπο εκτέλεσης της γενίκευσης: οι συγγραφείς προτείνουν μια τεχνική που ονομάζεται τοπική διεύρυνση, η οποία εγγυάται ότι οι τοποθεσίες των χρηστών διευρύνονται αρκετά ώστε να φτάσουν στην *k*-ανωνυμία, γεγονός που βελτιώνει τη χρησιμότητα των ανώνυμων τροχιών.

Η προσαρμοσμένη έννοια *k*-ανωνυμίας για τροχιές που αναφέρεται σε ένα διμερές γράφημα επίθεσης που σχετίζεται με πρωτότυπες και ανώνυμες τροχιές έτσι ώστε το γράφημα να είναι συμμετρικό και ο βαθμός κάθε κορυφής που αντιπροσωπεύει ανώνυμη τροχιά είναι τουλάχιστον *k*. Οι quasi-identifiers που χρησιμοποιούνται για τον ορισμό των ταυτοτήτων είναι οι χρόνοι των θέσεων σε μια τροχιά και η ανωνυμία επιτυγχάνεται με τη γενίκευση σημείων τροχιάς σε περιοχές του πλέγματος. Μια μέτρηση απώλειας πληροφοριών που ορίζεται για τέτοιες περιοχές χρησιμοποιείται για την αξιολόγηση της χρησιμότητας των ανώνυμων δεδομένων.

Ορισμένες προσεγγίσεις υποθέτουν ότι η ανώνυμοποίηση της βάσης δεδομένων από τον κάτοχο των δεδομένων, γνωρίζει ακριβώς ποιες είναι οι γνώσεις του αντιπάλου. Εάν ο αντίπαλος υποτίθεται ότι γνωρίζει διαφορετικά μέρη των τροχιών, τότε αυτά αφαιρούνται από τα δημοσιευμένα δεδομένα. Ωστόσο, αυτή η εργασία λαμβάνει υπόψη μόνο τη διαδοχική επίσκεψη στο μέρος χωρίς time-stamps σε πραγματικό χρόνο. Εάν ο αντίπαλος υποτίθεται ότι χρησιμοποιεί κάποια πρόβλεψη για συνέχιση μιας τροχιάς με βάση την προηγούμενη διαδρομή και την ταχύτητα, τότε η απόκρυψη πορείας με γνώμονα την αβεβαιότητα [45, 44] μπορεί να καταστείλει αυτές τις τροχιές. Αυτή η διαδικασία, ωστόσο, οδηγεί σε υψηλή απώλεια πληροφοριών.

Επιπρόσθετες σχετικές εργασίες σχετικά με την ανώνυμοποίηση χωρικών-χρονικών δεδομένων μπορούν να βρεθούν στη βιβλιογραφία σχετικά με το απόρρητο της τοποθεσίας, επικεντρωμένο σε εφαρμογές όπως υπηρεσίες βάσει τοποθεσίας με γνώμονα την προστασία της ιδιωτικής ζωής (LBS) ή παρακολούθηση με γνώμονα το απόρρητο των συνεχώς κινούμενων αντικειμένων. Το απόρρητο της τοποθεσίας στη ρύθμιση LBS προτάθηκε για πρώτη φορά στο [44]. Το απόρρητο της τοποθεσίας επιβάλλεται σε μεμονωμένες ευαίσθητες τοποθεσίες ή σε αποσυνδεδεμένες τοποθεσίες σε λειτουργία on-line. Συχνά, τα δεδομένα ανωνυμοποιούνται βάσει αιτήματος και στο πλαίσιο της απόκτησης μιας υπηρεσίας βάσει τοποθεσίας. Σε αυτή τη διατριβή, εστιάζουμε στην έκδοση εκτός σύνδεσης ολόκληρων βάσεων χωροχρονικών δεδομένων παρά στην προστασία συγκεκριμένων ατόμων από παρόχους LBS ή σε απευθείας σύνδεση παρακολούθησης κινήσεων. Γενικά, μια λύση στο απόρρητο της τοποθεσίας δεν είναι λύση για τη δημοσίευση ανώνυμων τροχιών και το αντίστροφο.

6. ΕΜΠΕΙΡΙΚΗ ΕΡΕΥΝΑ

6.1. Εταιρείες που εφάρμοσαν την τεχνολογία RFID

Ξεκινώντας από την Ελλάδα τα συστήματα RFID έχουν αναπτυχθεί σε ένα περιορισμένο αριθμό για χρόνια. Δύο από τα κυρίαρχα είδη έχουν την μορφή των αναμεταδοτών συλλογής διοδίων και των καρτών ασφαλείας. Οι οδικές αρχές της Ελλάδας έχουν εξοπλίσει τους οδηγούς με ένα αναμεταδότη που συνδέεται με την πιστωτική τους κάρτα. Αυτό επιτρέπει στους οδηγούς να πληρώσουν στα διόδια σε απόσταση 40 μιλίων ανά ώρα, αντί να σταματήσει το όχημα για να πληρώσει απαιτούμενο ποσό και να επιβραδύνει την κυκλοφορία. Οι κονκάρδες αυτές ασφαλείας έχουν εγκατεστημένο τσιπ RFID για να επιτρέψει την πρόσβαση στις εγκαταστάσεις και στα ειδικά δωμάτια στο εσωτερικό των κτιρίων. Αυτά, επίσης, μπορούν να χρησιμοποιηθούν για να παρακολουθούνται οι θέσεις των ανθρώπων σε μία εγκατάσταση.

Αργότερα, η εταιρεία Wal-Mart και το Υπουργείο Αμύνης των Ηνωμένων Πολιτειών της Αμερικής εκτόξευσε την βιομηχανία της τεχνολογίας RFID με υψηλή ταχύτητα, αναγγέλλοντας ότι όλοι οι προμηθευτές θα πρέπει να επισημάνουν τις συσκευές ναυτιλίας (Papadopoulou, 2009;Angeles, 2005). Η Wal-Mart το έχει επιβάλλει στην κορυφή 100 προμηθευτών τους αρχίζοντας τον Ιανουάριο του 2005. Σε αυτό το σημείο, η απαίτηση αυτή ισχύει για δοχεία ναυτιλίας και δεν επεκτείνεται σε μεμονωμένες συσκευασίες προϊόντων. Η επιρροή αυτών των δύο μεγάλων πελατών που προκαλούν όλες τις επιχειρήσεις να αξιολογήσουν, εάν θα πρέπει να αρχίσουν την πρόθεση χρήσης των RFID συστημάτων σήμανσης. Και οι δύο οργανώσεις υποστηρίζουν, ότι οι ετικέτες ηλεκτρονικής ταυτοποίησης θα βελτιώσουν την απόδοσή τους σε κινούμενα προϊόντα, να μειώσει το κόστος διαχείρισής τους και να μειώσει τις απώλειες (Tzelepi, 2013; Smith, 2004).

Περίπου το 97% των παλετών, των οποίων εστάλησαν στο Ιράκ έχουν αποσταλεί με ετικέτες RFID. Η μεγαλύτερη έκταση της έγκρισης είναι στον κλάδο του λιανικού εμπορίου και έχει περίπου 15.000 διπλώματα ευρεσιτεχνίας RFID που έχουν εκδοθεί από το 1997. Ακόμη, η Mobil είχε προωθήσει την «speed pass» την κάρτα καυσίμων το 1997. Τα περισσότερα, τελευταίας

τεχνολογίας, αυτοκίνητα είναι επιπλέον εξοπλισμένα με μία ετικέτα στα κλειδιά των αυτοκινήτων (Tzelepi, 2013; Roberts, 2006).

Η Delta Airlines έχει πραγματοποιήσει ορισμένους ελέγχους σε κάποιες υπηρεσίες για την τοποθέτηση των ετικετών RFID σε 40.000 πινακίδες, καθώς και η Michelin έχει κατασκευάσει ετικέτες RFID, οι οποίες τοποθετήθηκαν στα ελαστικά των οχημάτων. Η ετικέτα αυτή μπορεί να αποθηκεύσει ένα μοναδικό αριθμό για το κάθε ελαστικό, το οποίο σχετίζεται με τον αναγνωριστικό αριθμό του οχήματος (VIN). Η ετικέτα μπορεί να χρησιμοποιηθεί και για την μέτρηση των φθορών των ελαστικών των αυτοκινήτων.

Οι λιμενικοί φορείς, οι οποίοι αντιπροσωπεύουν το 70% του κόσμου στις λιμενικές εργασίες που έχουν συμφωνήσει να αναπτύξουν τις ετικέτες RFID για την παρακολούθηση των 17.000 κιβωτίων εμπορεύματος που φτάνουν στους λιμένες των ΗΠΑ σε καθημερινή βάση (Tzelepi, 2013; Roberts, 2006).

Η τεράστια εταιρία «γρήγορου φαγητού» McDonalds χρησιμοποιεί RFID στα συστήματα πληρωμής για την καλύτερη κι αποτελεσματικότερη εξυπηρέτηση των πελατών. Έξω από το εστιατόριο ο αναμεταδότης που είναι ενσωματωμένος στο εσωτερικό του παρμπρίζ του αυτοκινήτου, διαβάζεται από την κεραία. Ο πελάτης, αφού παραγγείλει στο παράθυρο παραγγελίας, προσπερνά το παράθυρο πληρωμής και πηγαίνει κατευθείαν στο παράθυρο παραλαβής της παραγγελίας χωρίς να χρειάζεται να βγάλει μετρητά ή κάρτα για να πληρώσει, ενώ και οι εργαζόμενοι δεν απασχολούνται με οικονομικές συναλλαγές. (Papadopoulou, 2009; O'Connor, 2006)

Η Metro Group είναι ο τρίτος μεγαλύτερος λιανοπωλητής του κόσμου και ο πρώτος μεγαλύτερος στην Γερμανία, με τα εμπορικά καταστήματα και εγκαταστάσεις σε περισσότερες από 30 χώρες σε Ευρώπη και Ασία. Το 2002 αποφάσισε να σχεδιάσει την εφαρμογή συστήματος RFID κατά μήκος της εφοδιαστικής της αλυσίδας ξεκινώντας με το υποκατάστημα της στο Rheinberg της Γερμανίας. Πρόκειται για ένα σύγχρονο κατάστημα που θα αναπτύσσει και θα εφαρμόζει νέες μορφές διαδικασιών της εφοδιαστικής αλυσίδας, από τις διαδικασίες logistics έως και τα ράφια του καταστήματος, ευελπιστώντας να αποκομίσει μερικά από τα πλεονεκτήματα της τεχνολογίας RFID όπως μείωση του χρόνου των διαδικασιών, μείωση του χρόνου και του κόστους της

εργασίας και μείωση των αποθεμάτων (Papadopoulou, 2009; Metro Group, 2008; Rfidjournal, 2003)

Έπειτα από μία πιλοτική εφαρμογή, η εταιρεία ενθαρρύνθηκε από την απόδοση του συστήματος και του εξοπλισμού της Intermec Technologies Corp, και προχώρησε σε περαιτέρω εφαρμογή της τεχνολογίας RFID στις καθημερινές διαδικασίες της εφοδιαστικής αλυσίδας. Όπως τονίζει και ο CEO της Metro Group Zygmunt Mierdorf, διαπιστώθηκε:

1. Μείωση του χρόνου στη διαδικασία της αποστολής εμπορευμάτων
2. Ουσιαστική βελτίωση στις καθημερινές διαδικασίες εφοδιασμού
3. Σημαντική βελτίωση της αναγνώρισης και της ιχνηλασιμότητας
4. Μείωση των αδυνάτων σημείων των χειρωνακτικών διαδικασιών στην αποθήκη, και κατ' επέκταση βελτίωση στην απόδοση τους
5. Εξάλειψη των φαινομένων έλλειψης αποθέματος.

Έτσι τον Μάρτιο του 2005, η Metro Group σε συνεργασία με τους προμηθευτές εξοπλισμού σχεδίασε την πρώτη εμπορική χρήση του προτύπου EPC Gen 2 RFID για την εφαρμογή σε μια παγκόσμια εφοδιαστική αλυσίδα. Έπειτα από τα επιτυχημένα πιλοτικά προγράμματα, η Metro Group αποφάσισε να εγκαταστήσει, σε πλήρη κλίμακα, το σύστημα ανίχνευσης πελατών μέσω RFID ετικετών σε ένα από τα πιο φορτωμένα κέντρα διανομής (distribution center DC), αυτό στην Unna της Γερμανίας. Εκεί έκανε χρήση πολλαπλών εφαρμογών της τεχνολογίας RFID και σύμφωνα με την Metro, με αυτή την εφαρμογή είναι σε θέση να ταξινομήσει πάνω από 8000 διαφορετικά εμπορεύματα την ώρα.

Τα πρώτα αποτελέσματα για την Metro από την εφαρμογή της τεχνολογίας RFID στην αποθήκη και στο DC, έδειξαν μείωση του χρόνου ελέγχου και εκφόρτωσης των φορτηγών της τάξης των 15 με 20 λεπτών. Η εγκατάσταση του συστήματος RFID στις διαδικασίες αναγνώρισης των πελατών, παραλαβής και αποστολής των παραγγελιών, αλλά και της τοποθέτησης αυτών, μείωσε το χρόνο των εργασιών αυξάνοντας την παραγωγικότητα των εργατών. Οι ελλιπείς αποστολές αναγνωρίζονται άμεσα, γεγονός που βελτίωσε την ακρίβεια των αποθεμάτων και οδήγησε την Metro να μειώσει τα επίπεδα έλλειψης αποθεμάτων στα καταστήματα της κατά 11%.

Η Food Manufacturers Ltd. είναι μεγάλος παραγωγός μιας ευρείας ποικιλίας τροφίμων παγκοσμίως. Η επιχείρηση πωλεί καταναλωτικά προϊόντα με διαφορετικά εμπορικά σήματα. Οι πολλαπλές διαδικασίες που λαμβάνουν μέρος στην εφοδιαστική αλυσίδα των τροφίμων κάνει απαιτητική τη χρήση όλων των ειδών τεχνολογίας που έχει αναπτυχθεί για τα RFID συστήματα. Ενώ η επέκταση του συστήματος RFID από τον αρχικό σχεδιασμό αποτελεί προϋπόθεση για τους παραγωγούς και εμπόρους τροφίμων, καθώς χρόνο με το χρόνο θα επεκτείνεται η χρήση της τεχνολογίας RFID. (Papadopoulou, 2009;Sensap, 2008)

Η εταιρία STAFF Jeans AE με το αρκετά εξελιγμένο σύστημα RFID, εκτός του ότι επιτάχυνε την διαδικασία παραλαβής, συλλογής και αποστολής προϊόντων, θα προσφέρει στην εταιρεία τη δυνατότητα καλύτερης διαχείρισης του αποθέματος στα καταστήματα λιανικής πώλησης, θα μειώσει την πιθανότητα ελλείψεων καθώς επίσης και τον όγκο των επιστρεφόμενων προϊόντων. Επιπρόσθετα οι ετικέτες RFID συμβάλουν στην προστασία του ονόματος της εταιρείας (brand name) μέσω της πιστοποίησης της αυθεντικότητας των επώνυμων προϊόντων STAFF Jeans and Co, ενώ παράλληλα θα επιτρέψουν την εγκατάσταση μιας σειράς ηλεκτρονικών εφαρμογών στα καταστήματα λιανικής πώλησης με σκοπό τη διαφήμιση και την προώθηση των πωλήσεων της εταιρείας. Ένα παράδειγμα είναι "διαδραστικό δοκιμαστήριο", το οποίο δοκιμάζει ο πελάτης, διαφημιστικό υλικό και υλικό πολυμέσων, καθώς και πληροφορίες για σχετικά προϊόντα τα οποία είναι διαθέσιμα στο κατάστημα, όπως gadgets και accessories.

6.2. Μελέτη του ποσοστού αποδοχής και διείσδυση της τεχνολογίας RFID από τις επιχειρήσεις και τους καταναλωτές στον Κυπριακό χώρο

Οι πρώτες υλοποιήσεις RFID στην Κύπρο καταδεικνύουν ότι υπάρχει μεν ενδιαφέρον - και μάλιστα μεγάλο- από τις κυπριακές επιχειρήσεις, παράλληλα όμως υπάρχει και πολύς δισταγμός. Οι κυπριακές εταιρείες προτιμούν να δοκιμάσουν τα πλεονεκτήματα της εν λόγω τεχνολογίας σε συγκεκριμένες εφαρμογές με μικρό ρίσκο και σημαντικά οφέλη σε περίπτωση επιτυχίας. Το κόστος ήταν ένας ανασταλτικός παράγοντας τόσο στην Κύπρο όσο και στη διεθνή χώρο, και εφόσον βρέθηκαν οι φόρμουλες για μειώσεις στα κόστη όσον αφορά στην τοποθέτηση ετικετών - σε κιβώτια, παλέτες και κουτιά ,τα συστήματα RFID αναπτύσσονται ραγδαία. Όπως είναι λογικό και αναμενόμενο, σε καμία περίπτωση το RFID δεν έχει ακόμη αντικαταστήσει πλήρως το

barcode. Οι περισσότεροι αναλυτές μετά από έρευνες θεωρούν πολύ πιθανή την αρμονική συνύπαρξη των δυο μεθόδων ταυτοποίησης για χρόνια.

Όσον αφορά τον χώρο του λιανικού εμπορίου και γενικότερα στον κύκλο προμηθειών και εφοδιασμού της λιανικής πώλησης, αρχίζουν σιγά σιγά να αυξάνονται. Όσοι λοιπόν παρακολουθούν από κοντά τη συγκεκριμένη αγορά επισημαίνουν το πολύ μεγάλο ενδιαφέρον για την εν λόγω τεχνολογία που πολυάριθμες κυπριακές επιχειρήσεις της αγορά του λιανικού εμπορίου εκδηλώνουν . Επιπλέον, τα τελευταία χρόνια έχουν αρχίσει να υλοποιούνται πιλοτικά έργα, τα οποία μπορούν να αποτελέσουν ένα καλό παράδειγμα, στην επιτάχυνση της διείσδυσης της τεχνολογίας RFID στην Κύπρο.

Ενδεικτικό παράδειγμα είναι τα συστήματα αποθηκών. Ένα σύστημα WMS διαχειρίζεται το σύνολο των εργασιών που εκτελούνται σε μία αποθήκη ή σε ένα κέντρο διανομής. Συγκεκριμένα, την εισαγωγή των προϊόντων στην αποθήκη, την κατάλληλη απόθεσή τους, τη διαχείριση αποθεμάτων, την περισυλλογή των προϊόντων, τις διαδικασίες συσκευασίας, τη δρομολόγηση των προϊόντων μίας παραγγελίας και τη διαχείριση του ανθρώπινου δυναμικού της αποθήκης ή του κέντρου διανομής. Συνήθως τα συστήματα WMS συνδέονται με εργαλεία αυτόματης εισαγωγής δεδομένων γραμμωτού κώδικα (barcode) αλλά πλέον με τεχνολογίες ραδιοσυχνοτήτων (Radio Frequency Technology, RFID).

Η Κύπρος σημειώνει αργή πρόοδο. Οι εταιρείες χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης και το ηλεκτρονικό εμπόριο, αλλά είναι λιγότερο πρόθυμες να υιοθετήσουν νέες τεχνολογίες όπως το υπολογιστικό νέφος (cloud computing) και η RFID (Radio-frequency identification). Οι υπηρεσίες των ΜΜΕ για την πραγματοποίηση πωλήσεων μέσω διαδικτύου μειώθηκαν έναντι του προηγούμενου έτους. Αφετέρου, ο κύκλος εργασιών του ηλεκτρονικού εμπορίου αυξήθηκε. Παρόλο που ο κύκλος εργασιών του ηλεκτρονικού εμπορίου αυξήθηκε (6,3%), υπολείπεται αρκετά του μέσου όρου της ΕΕ (10,3%), όπως υπολείπεται του μέσου όρου της ΕΕ (17,2%) και το ποσοστό των ΜΜΕ που πραγματοποιούν πωλήσεις μέσω διαδικτύου (11,4%). [57]

Όπως σημειώνει ο ΣΕΒ (Σύνδεσμος Επιχειρήσεων και Βιομηχανιών) στο νεότερο Special Report του, «ο ψηφιακός και τεχνολογικός μετασχηματισμός αυξάνει την παραγωγική ευελιξία αλλά,

δημιουργεί έντονες ανταγωνιστικές πιέσεις για τις επιχειρήσεις και τις χώρες που δεν ακολουθούν. Συνεπώς, εκτός από προϋπόθεση ενός νέου παραγωγικού προτύπου που συμβάλει στη βιομηχανική αναζωογόνηση και στη δημιουργία περισσότερων διεθνώς εμπορεύσιμων προϊόντων και υπηρεσιών, ο μετασχηματισμός, μπορεί να εξελιχθεί σε παράγοντα επιβίωσης για πολλές επιχειρήσεις. Τη στιγμή που ο διεθνής ανταγωνισμός απολαμβάνει σημαντικά οφέλη από σύγχρονες τεχνολογίες, η Κύπρος έχει πολύ δρόμο να καλύψει σε όρους ψηφιακής ετοιμότητας και δεξιοτήτων».

Η πρώτη έκδοση του Παρατηρητηρίου Ψηφιακού Μετασχηματισμού του ΣΕΒ χαρτογραφεί λεπτομερώς την ωριμότητα της οικονομίας με χρήση 100 δεικτών που δίνουν μια ολοκληρωμένη εικόνα για το σημείο στο οποίο βρισκόμαστε σήμερα. ,Οι επί μέρους παρατηρούμενες επιδόσεις δείχνουν την κατεύθυνση των αναγκαίων παρεμβάσεων, τόσο της πολιτείας, όσο και των επιχειρήσεων. Είναι σημαντικό να αντιμετωπίσουμε ως ευκαιρία τις προκλήσεις της 4ης βιομηχανικής επανάστασης. Έτσι, θα μπορέσουν οι επιχειρήσεις όχι μόνο να ανταποκριθούν στον δυναμισμό μιας οικονομίας που εξέρχεται από την κρίση, αλλά και να αναβαθμίσουν τη συμμετοχή τους στις διεθνείς αλυσίδες αξίας, που δημιουργούνται στη ψηφιακή εποχή».[58]

Αυτό συμβαίνει λόγω κάποιων κρίσιμων παραγόντων αναφορικά με την προοπτική χρήσης της τεχνολογίας RFID στην εφοδιαστική αλυσίδα και που χρειάζεται να ξεπεραστούν έτσι που να διεισδύσει η εν λόγω τεχνολογία στις κυπριακές επιχειρήσεις ομαλά. Θέματα που αφορούν το κόστος αγοράς και εφαρμογής της νέας τεχνολογίας, ο ανασχεδιασμός των ήδη υπαρχουσών διαδικασιών καθώς επίσης τεχνικά ζητήματα σε σχέση πάντα με τη συμβατότητα των αναγνωστών κτλ, αποτελούν τους πιο σημαντικούς πυλώνες που χαρακτηρίζουν την τεχνολογία RFID. Οι κυπριακές επιχειρήσεις φαίνονται ακόμη διστακτικές και προβληματισμένες δεδομένου ότι έχουν ελαχιστοποιηθεί τα περιθώρια λάθους ή εσφαλμένης λειτουργίας (π.χ. θέματα στην εκχώρηση και καταχώρησης ετικετών, ασυμβατότητες λειτουργίας κ.ο.κ.). Σε αυτά τα πλαίσια, πρέπει πρώτα να ξεπεραστούν όλα τα τέτοιου είδους προβλήματα που αναφέρονται στην τεχνολογική αρτιότητα του RFID και σε δεύτερο στάδιο να επιλυθούν θέματα που σχετίζονται με την εφαρμογή της τεχνολογίας στις επιχειρηματικές διαδικασίες.

Συγχρόνως είναι σημαντικό να λεχθεί ότι οι εταιρείες τόσο στο κυπριακό όσο και στον διεθνή στερέωμα αντιλαμβάνονται ότι η εφαρμογή RFID αποτελεί προτεραιότητα, αλλά εξακολουθούν

να προβάλλουν την τεχνολογία περισσότερο ως "επιχειρηματική εντολή" εκπορευόμενη κυρίως από τον πελάτη. Για παράδειγμα, η Wal-Mart ζήτησε από επιλεγμένους σημαντικούς προμηθευτές για χρήση RFID σε πελάτες και κιβώτια. Για να βελτιώσουν τις αλυσίδες αξίας τους, οι εν λόγω προμηθευτές, με τη σειρά τους, θα απαιτήσουν τους προμηθευτές τους να πράξουν το ίδιο, και ούτω καθεξής. Οι εταιρείες που θίγονται άμεσα από αυτές τις "εντολές", δεν έχουν άλλη επιλογή από το να θέσουν σε εφαρμογή την RFID τεχνολογία, αν θέλουν να συνεχίσουν την επιχειρηματική δραστηριότητα με τις εν λόγω εταιρείες.(Papadopoulou, 2009; Angeles, 2007)

6.3. Η αποδοχή τεχνολογίας RFID από τις κυπριακές επιχειρήσεις

Αρκετές κυπριακές επιχειρήσεις δεν είναι εξοικειωμένες με την τεχνολογία αλλά έχουν ενημερωθεί κυρίως μέσω σεμιναρίων, συμμετοχή σε συνέδρια, έντυπα και ηλεκτρονικό τύπο κ.ο.κ. Παρόλα αυτά, αναγνωρίζουν πως η τεχνολογία RFID μπορεί να λειτουργήσει ως επιταχυντής στην αποτελεσματικότερη διαχείριση του εφοδιαστικού κύκλου. Παράλληλα, ιδιαίτερο ενδιαφέρον εξέφρασαν για να ενσωματώσουν την τεχνολογία RFID στις επιχειρηματικές τους δραστηριότητες και διαδικασίες ενώ πολλές είναι αυτές που έχουν αρχίσει δραστηριοποιούνται συμμετέχοντας σε πιλοτικά έργα που χρησιμοποιούν την τεχνολογία RFID. Το τελευταίο χαρακτηριστικό δείχνει και την δυναμική των κυπριακών επιχειρήσεων οι οποίες επιθυμούν σε κάθε περίπτωση να είναι προετοιμασμένες για την ολοκληρωτική μετάβαση τους από το barcode στο RFID.

Στην πλειονότητα τους οι κυπριακές επιχειρήσεις αποδέχονται ότι η τεχνολογία RFID αναμένεται να επιφέρει σημαντικά οφέλη σχεδόν σε όλα τα θέματα που υπήρχαν και υπάρχουν αναφορικά με την εφοδιαστική αλυσίδας με σημαντικότερο το όφελος της αποφυγής λαθών κατά τον έλεγχο και τον υπολογισμό στο απόθεμα του καταστήματος ή της κεντρικής αποθήκης, τον υπολογισμό των επιστροφών, όπως και την έλλειψη διαφάνειας στην εφοδιαστική αλυσίδα, γεγονός που επιβεβαιώνει ότι η τεχνολογία RFID αναμένεται να βελτιώσει κατά κύριο λόγο προβλήματα τα οποία είναι σχετικά με την ιχνηλάτηση και παρατήρηση των προϊόντων.

Ιδιαίτερα ενθαρρυντικό είναι το γεγονός ότι οι κυπριακές επιχειρήσεις είναι διατεθειμένες να πραγματοποιήσουν ενέργειες για εφαρμογή της τεχνολογίας στις επιχειρηματικές τους διαδικασίες. Έχουν εμπεδώσει ότι η αξιοποίηση της τεχνολογίας RFID στη διαχείριση της

εφοδιαστικής αλυσίδας αποτελεί ένα σημαντικό παράγοντα εξέλιξης, επιτυχίας και κυρίως οικονομικού οφέλους . Βέβαια, ένα από τα σημαντικότερα θέματα που εμφανίζεται στην κυπριακή πραγματικότητα είναι η ελλιπής ενημέρωση των κυπριακών επιχειρήσεων (κυρίως μικρών και μικρομεσαίων) όσον αφορά τις δυνατότητες της εν λόγω τεχνολογίας. Το σύστημα RFID δεν πρόκειται σε καμία περίπτωση να αντικαταστήσει πλήρως τουλάχιστον στο άμεσο μέλλον τις υπάρχουσες τεχνολογίες σήμανσης προϊόντων και ιδιαίτερα το barcode. Άλλωστε, όλες οι προσπάθειες που γίνονται σε διεθνές επίπεδο, επικεντρώνονται στην ομαλή αναβάθμιση των συστημάτων διαχείρισης της εφοδιαστικής αλυσίδας έτσι ώστε να υποστηρίζουν και το RFID πέρα από το barcode, για να επιτευχθεί μια ομαλή μετάβαση.

Από τα πιο πάνω εξάγεται ότι παρόλο που η Κύπρος υστερεί σε αρκετούς τομείς, ως εκ τούτου, αναγνωρίστηκε από την Κυβέρνηση ότι απαιτείται σαφής επαναπροσδιορισμός της στρατηγικής και του καθορισμού συγκεκριμένων στόχων με πρόταξη των πλεονεκτημάτων που η χώρα παρουσιάζει. Το καλοκαίρι του 2020 θα είναι έτοιμη η νέα στρατηγική του κράτους για την ψηφιακή αναβάθμιση της χώρας. Η προηγούμενη στρατηγική εκπονήθηκε το 2012, επομένως ήταν αδήριτη ανάγκη ο εκσυγχρονισμός της. Ο διαγωνισμός εκπόνησης μελέτης με στόχο την επικαιροποίηση της ψηφιακής στρατηγικής της Κύπρου έχει επικυρωθεί στον ελεγκτικό οίκο PwC, ο οποίος αναμένεται να παρουσιάσει τη νέα στρατηγική και τους πυλώνες στους οποίους θα βασιστεί το κράτος.

Η μελέτη θα καθορίσει συγκεκριμένους στόχους, μέτρα, δράσεις και τον απαιτούμενο οδικό χάρτη προκειμένου η Κύπρος να συνεχίσει τα επόμενα χρόνια με γοργούς ρυθμούς τη μετάβασή της στην ψηφιακή εποχή, με τη χρήση τεχνολογιών πληροφορικής και επικοινωνιών. [59]

6.4. Η αποδοχή της τεχνολογίας RFID από τους καταναλωτές

Πολλές είναι οι αντιδράσεις και ανησυχίες των καταναλωτών που επακολουθούν την εφαρμογή της τεχνολογίας RFID, λόγω φόβου κυρίως για παραβίαση του ιδιωτικού απορρήτου. Εκφράζονται αντιρρήσεις για το ιδιωτικό απόρρητο σχεδόν παντού. Η αντίθεση για τη χρήση του RFID οφείλεται στη δυνατότητα εφαρμογής της τεχνολογίας σε οτιδήποτε έχει σχέση με τον προσδιορισμό της θέσης χωρίς πρωτύτερη ενημέρωση του καταναλωτή, στην πολύ μεγάλη συλλογή δεδομένων που εκτελεί και στη δικτύωση της τεχνολογίας σε ασύρματα περιβάλλοντα.

Σε έρευνα που διενεργήθηκε σε Γερμανούς καταναλωτές (Papadopoulou,2009;Guthner et al,2005) εκτός από την διαπίστωση ότι στο σύνολο τους εκφράζουν το φόβο της απώλειας και παραβίασης της ιδιωτικής ζωής αναλύθηκε περαιτέρω και το εκπαιδευτικό τους υπόβαθρο σε σχέση με το κατά πόσο αποδέχονται την εν λόγω τεχνολογία. Τα συμπεράσματα αυτής της έρευνας είναι αξιοσημείωτα: καταναλωτές με υψηλότερο εκπαιδευτικό υπόβαθρο αισθάνονται λιγότερο ενημερωμένοι, περισσότερο αδύναμοι και ανίκανοι να κάνουν τις επιλογές τους μπροστά στην ολοκληρωτική εισαγωγή της RFID τεχνολογίας συγκριτικά με καταναλωτές που δεν έχουν τριτοβάθμια εκπαίδευση. Ακόμη και αν τα πιθανά οφέλη των RFID (όπως η βελτιωμένη εξυπηρέτηση μετά την πώληση) είναι ευκόλως κατανοητά από μία μεγάλη πλειοψηφία καταναλωτών, ο φόβος φαίνεται να υπερισχύει των θετικών συναισθημάτων. Η αντιμετώπιση αυτού του φόβου αποτελεί επιτακτική ανάγκη καθώς μόνο με αυτόν τον τρόπο η RFID τεχνολογία θα μπορέσει να χρησιμοποιηθεί ευρέως ως ένα επιχειρηματικό εργαλείο. Ένας ανοικτός διάλογος για τα πλεονεκτήματα της τεχνολογίας και των δυνητικών κινδύνων είναι ένα σημαντικό βήμα προς αυτή την κατεύθυνση.

Επιπρόσθετα, ένας ακόμη παράγοντας, εκτός του εκπαιδευτικού υποβάθρου, που θα πρέπει να ληφθεί υπόψη είναι το κατά πόσο είναι αποδεκτή μια τέτοιου είδους τεχνολογία σε σχέση με την ηλικία των καταναλωτών. Όσο μεγαλύτερη είναι η ηλικία του καταναλωτή τόσο λιγότερο εξοικειωμένος και πρόθυμος είναι να χρησιμοποιήσει τις νέες τεχνολογίες γενικότερα αλλά και την τεχνολογία RFID που περικλείει ένα τόσο μεγάλο όγκο πληροφοριών ειδικότερα. Αυτή η εντύπωση αποτυπώνεται στο μυαλό τόσο του καταναλωτικού κοινού όσο και στο ανθρώπινο δυναμικό (logistics managers) που στελεχώνει τις επιχειρήσεις. Ιδιαίτερα στον κυπριακό τομέα επιχειρήσεων, όπου η ανάπτυξη των logistics και του εφοδιαστικού κύκλου συνεχίζεται σε

έντονους και γοργούς ρυθμούς τα τελευταία χρόνια, παρατηρείται ότι το ανθρώπινο δυναμικό αδυνατεί να προσαρμοστεί με ευκολία στα νέα δεδομένα που προκύπτουν μέσα από την εισχώρηση των τεχνολογιών και συνεχίζουν να λειτουργούν περισσότερο εμπειρικά χωρίς να δίνουν αρκετή σημασία στις τεχνολογικές καινοτομίες.

Μια ακόμη ενδιαφέρουσα έρευνα σχετικά με την αποδοχή της RFID τεχνολογίας από τους καταναλωτές πραγματοποιήθηκε από τους Muhammad Hossain και Victor Prybutok και δημοσιεύθηκε τον Μάιο του 2008. Στόχος αυτής της έρευνας ήταν να διερευνηθούν οι παράγοντες που επηρεάζουν τους καταναλωτές στην αποδοχή της τεχνολογίας RFID. Σύμφωνα με την έρευνα, οι ευκολίες και ανέσεις που προσφέρουν τα συστήματα RFID, η επιρροή της κουλτούρας του εκάστοτε λαού και το πώς καταλαμβαίνουν την ασφάλεια οι καταναλωτές, παίζουν σημαντικό ρόλο στην προθυμία των καταναλωτών να δεχθούν την τεχνολογία RFID. Όσο περισσότερες είναι οι ευκολίες που προσφέρει η τεχνολογία τόσο μεγαλύτερη γίνεται η πρόθεση των καταναλωτών να την χρησιμοποιήσουν προφανώς. Η επιρροή του πολιτισμού στις αντιλήψεις σχετικά με την τεχνολογία γενικότερα και με τα συστήματα RFID ειδικότερα είναι επίσης ένας καθοριστικός παράγοντας της αποδοχής της τεχνολογίας αυτής από τον καταναλωτή. Δηλαδή, το πόσο εύκολα μπορεί να αποδεχτεί ο καταναλωτής την τεχνολογίας RFID επηρεάζεται από κοινωνικές πεποιθήσεις, αξίες, κανόνες, ή συμπεριφορές. Ένας άλλος σημαντικός και καθοριστικός ταυτόχρονα παράγοντας για αποδοχή της τεχνολογίας RFID είναι η κατανόηση της ασφάλειας των προσωπικών πληροφοριών. Όσο μεγαλύτερη σημασία δίνουν οι καταναλωτές στην προσωπική ασφάλεια των πληροφοριών και όσο χαμηλότερη είναι η βούληση του καταναλωτή να θυσιάσει την ασφάλεια των προσωπικών πληροφοριών του, τόσο χαμηλότερη είναι η πρόθεσή του να αποδεχτεί την τεχνολογία αυτή.

7.ΥΛΟΠΟΙΗΣΗ ΕΦΑΡΜΟΓΗΣ “ΤσέκΛιστ»

Αυτή η μεταπτυχιακή διατριβή , καταπιάνεται σε υλοποίηση συνεργασίας με ένα πολυκατάστημα (πολυσύχναστου χώρου) που στόχος του έργου είναι η δημιουργία ενός περιβάλλοντος που να διευκολύνει τους καταναλωτές κατά τη διάρκεια των αγορών στο κατάστημα, λαμβάνοντας υπόψη τις καταναλωτικές τους προτιμήσεις αλλά και την ευκολία στο θέμα εύρεσης του προϊόντος ειδικά

σε περιπτώσεις πανδημίας που πρέπει να κινούνται όλοι σε απόσταση με τη χρήση ασύρματων τεχνολογιών.

Συγκεκριμένα, οι καταναλωτές μπορούν να αλληλεπιδράσουν με το σύστημα μέσα από τις εξής επιλογές:

- Μια περιοχή «Τοποθεσία προϊόντος» που παρουσιάζει αναλυτικές πληροφορίες για το που είναι τοποθετημένα τα προϊόντα μετά από επιλογή του καταναλωτή.
- Μια περιοχή «Απόθεμα στο ράφι» όπου εμφανίζονται όλες οι πληροφορίες σχετικά με το πόσο απόθεμα υπήρχε στην αρχή της ημέρας
- Μια περιοχή «Επιπρόσθετες πληροφορίες για κάθε προϊόν», στην οποία εμφανίζονται περαιτέρω χρήσιμες πληροφορίες, όπως η θρεπτική αξία.
- Μια περιοχή «Εμφάνιση της συνολικής τιμής» των προϊόντων στο καρότσι, συμπεριλαμβανομένων και των πόντων που κερδίζει με τις τυχόν αγορές.

7.1.Έρευνα

Η έρευνα αξιολόγησης του προτεινόμενου μηχανισμού αγορών έλαβε χώρα σε τοπικό κατάστημα σουπερμάρκετ και σε μεγάλη υπεραγορά με πραγματικούς καταναλωτές κατά την περίοδο πανδημίας καρονωιού Μαρτίου-Απριλίου 2020. Σκοπός της έρευνας ήταν να μελετηθεί πως επιδρούν στην παραδοσιακή εμπειρία των καταναλωτών οι νέες τεχνολογίες και, κατ' επέκταση, οι νέοι μηχανισμοί πραγματοποίησης αγορών.

7.1.1.Μεθοδολογία

7.1.1.1. Δειγματοληψία

Η δειγματοληψία σύμφωνα με τους Παπαναστασίου και Παπαναστασίου (2005), θα πρέπει να περιλαμβάνει τα υποκείμενα της έρευνας τη μέθοδο επιλογής τους και τέλος το μέγεθος του δείγματος. Ο ερευνητής θα πρέπει να επιλέξει μεταξύ του πληθυσμού που σχετίζεται με το θέμα του, ένα αριθμό συμμετεχόντων από τους οποίους θα πάρει τα δεδομένα που χρειάζεται. Έπειτα, θα πρέπει να έρθει σε επαφή με τους συμμετέχοντες και να επιλέξει τον τρόπο με τον οποίο θα γίνει η συλλογή των δεδομένων. Στη δειγματοληψία, θα υπάρχει ένας ακριβής ορισμός του

πληθυσμού, έτσι ώστε να είναι δυνατή η επιλογή του δείγματος από τον πληθυσμό στον οποίο απευθύνεται η έρευνα (Παπαναστασίου & Παπαναστασίου**,** 2005).

Στην παρούσα έρευνα, χρησιμοποιήσαμε τη θεωρητική δειγματοληψία (Theoretical sampling) ή αλλιώς θεμελιωμένη θεωρία (Grounded theory). Όπως αναφέρει ο Robson (2010), η θεωρία αυτή ονομάζεται «θεμελιωμένη θεωρία» γιατί «θεμελιώνεται» στα δεδομένα που συγκεντρώνονται κατά τη διάρκεια της μελέτης της, ιδιαίτερα σε ενέργειες και αλληλεπιδράσεις που διαδραματίζονται μεταξύ των εμπλεκόμενων ανθρώπων (Robson, 2010).

Γι' αυτόν ακριβώς το λόγο, η θεωρία αυτή ταιριάζει απόλυτα στη μελέτη μας μιας κι κύριος σκοπός της μελέτης αυτής είναι να δημιουργήσουμε μια αλληλεπίδραση μεταξύ των συμμετεχόντων, από την οποία θα συλλέξουμε τα δεδομένα μας. Αυτό αναφέρεται και στο βιβλίο της Mason (2003), η οποία λέει πως η θεωρητική δειγματοληψία είναι μια διαδικασία που επιλέγει ομάδες ή κατηγορίες έτσι ώστε να χρησιμοποιηθούν στη μελέτη, με κριτήριο τη σχέση που υπάρχει με τα ερευνητικά ερωτήματα, τη θεωρητική προσέγγιση, το αναλυτικό πλαίσιο και την αναλυτική πρακτική. Κύριο κριτήριο είναι η ανάπτυξη που δίνουν οι ερευνητές (Mason, 2003).

Στόχος της συγκεκριμένης δειγματοληψίας λοιπόν, είναι να εξετάσει τη σχέση μεταξύ των συνεντεύξεων και των παρατηρήσεων που θα προκύψουν κατά τη διάρκεια της έρευνας. Βασικό χαρακτηριστικό της θεωρίας είναι πως εξετάζει εις βάθος τη σχέση μεταξύ των όσων λέγονται και των όσων παρατηρούνται. Όπως αναφέρει ο Robson (2010), η συγκεκριμένη δειγματοληψία βοηθά τον ερευνητή να προσθέτει νέες πληροφορίες/ δεδομένα στις επισκέψεις του μέχρι ότου να υπάρξει «κορεσμός» μεταξύ των κατηγοριών που μελετώνται. Επίσης, αναφέρει πως η συλλογή των δεδομένων θεωρείται ολοκληρωμένη όταν οι πληροφορίες φθίνουν και δεν υπάρχουν νέα δεδομένα από αυτά που ήδη έχουμε (Robson, 2010).

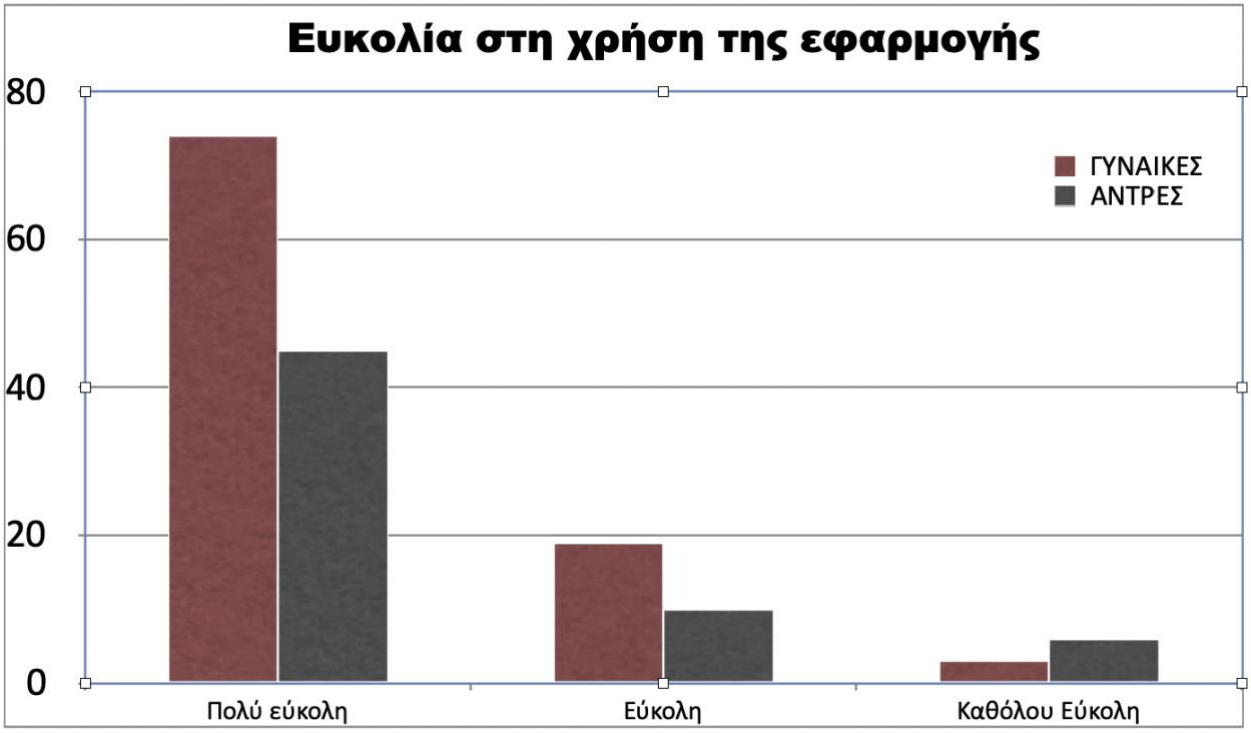
Η θεωρητική δειγματοληψία έχει άμεση σχέση με τη δημιουργία ενός δείγματος, λόγω του ότι η ομάδα συλλέγει κάποια κριτήρια και χαρακτηριστικά που στη συνέχεια διευκολύνει το έργο του ερευνητή τόσο στην ανάπτυξη όσο και στον έλεγχο της θεωρίας που στοχεύει (Mason, 2003). Επομένως, σε αυτή τη δειγματοληψία, στόχος είναι να επιλεγούν άτομα που έχουν συγκεκριμένα χαρακτηριστικά. Όπως αναφέρει και ο Dudovskiy (2013), αντίθετα με την σκόπιμη

δειγματοληψία, η θεωρητική στοχεύει στο να εμπλέξει τα άτομα από τα οποία παίρνει τα δεδομένα, με το θέμα που ερευνά. Το ίδιο αναφέρει και ο Patton (2002), λέγοντας πως η θεωρητική δειγματοληψία είναι διαδικασία επιλογής ατόμων με βάση τις πιθανές εκδηλώσεις που εκφράζουν και τα θεωρητικά πλαίσια που αντιπροσωπεύουν (Patton, 2002).

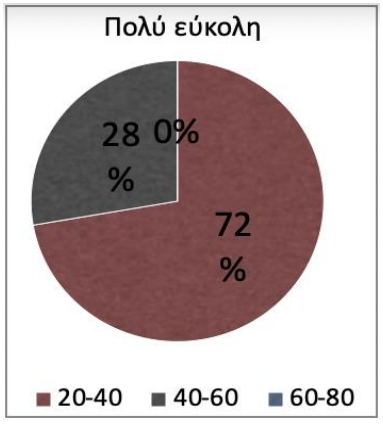
Με άλλα λόγια, η «θεωρητική δειγματοληψία» είναι συνώνυμη με τη σκόπιμη δειγματοληψία, μιας και οι συμμετέχοντες επιλέγονται με βάση κάποια κριτήρια που θα βοηθήσουν τον ερευνητή να εξάγει όσο το δυνατό πιο έγκυρα αποτελέσματα για την έρευνα του. Λαμβάνοντας υπόψη όσα είπαν οι ποιο πάνω, τα προφίλ των ατόμων που επιλέγηκαν για τη δική μας έρευνα είχαν ως βάση: την ηλικία και το επίπεδο μόρφωσης.

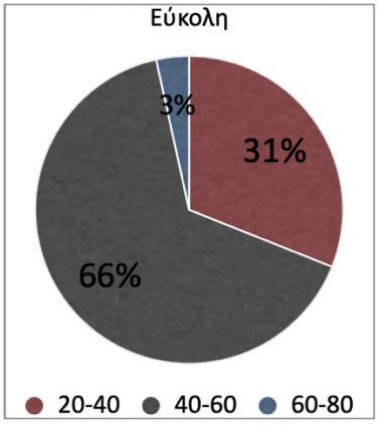
7.1.2. Παρουσίαση της έρευνας μέσω ερωτηματολογίου

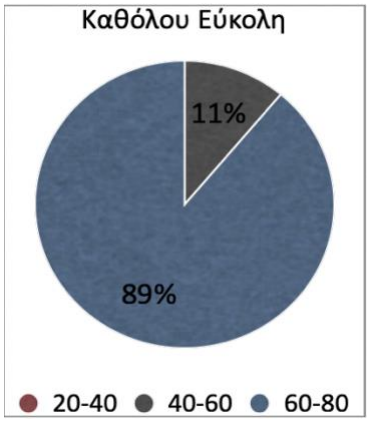
Στην συγκεκριμένη ενότητα θα γίνει παρουσίαση των αποτελεσμάτων που αντλήθηκαν μέσω επεξεργασίας ερωτηματολογίου. Το δείγμα μας ήταν 157 άτομα εκ των οποίων 96 γυναίκες και 61 άντρες . Σκοπός του ερωτηματολογίου είναι να αντληθούν όσες περισσότερες πληροφορίες από τους συμμετέχοντες στην έρευνα. Το ερωτηματολόγιο αποτελείται από ένα και μόνο μέρος , ο χρόνος απάντησης του ερωτηματολογίου ήταν περίπου 3-4 λεπτά συμπεριλαμβανομένου και του χρόνου επίδειξης της εφαρμογής. Με την επίδειξη του δείγματος του προτεινόμενου μηχανισμού σε μορφή κινητό τηλέφωνο οι ερωτήσεις ήταν κατά πόσο θα ήταν εύκολη στην χρήση μια τέτοιου είδους εφαρμογή και κατά ποιο βαθμό θα βοηθούσε στις αγορές και πως. Το αποτέλεσμα του ερωτηματολογίου μετά από επίδειξη του προτεινόμενου μηχανισμού – ιδέα για νέα εμπειρία στις καταναλωτικές παραδοσιακές συνήθειες.



Γράφημα1

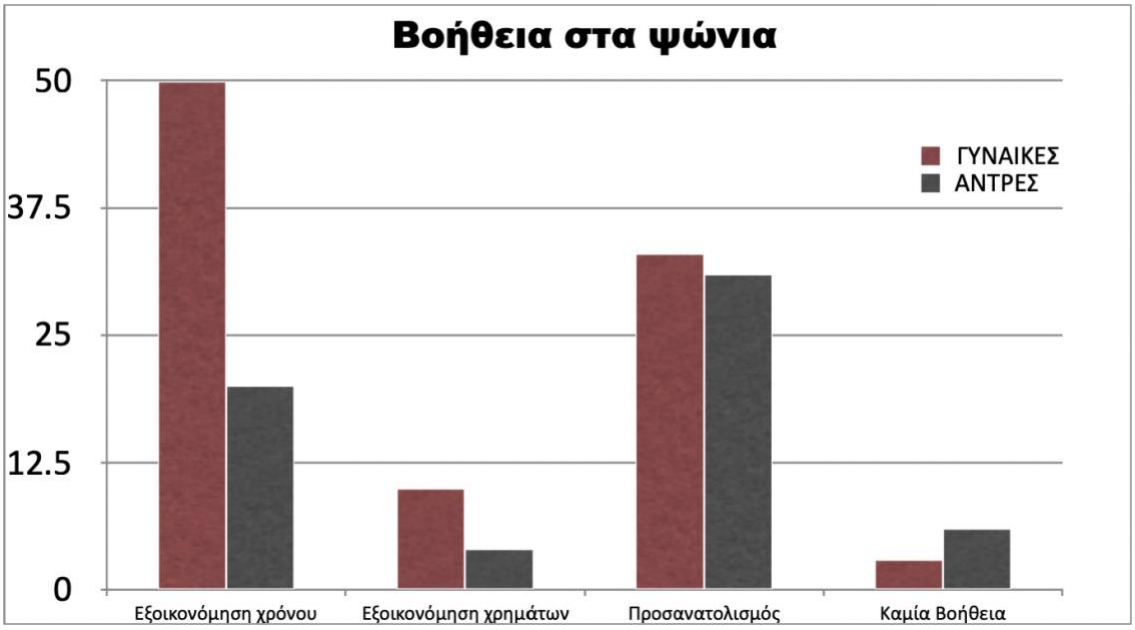




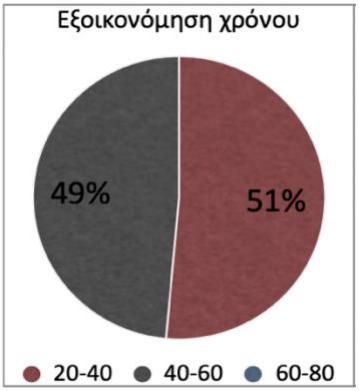


Γράφημα 2 *Γράφημα 3* *Γράφημα 4*

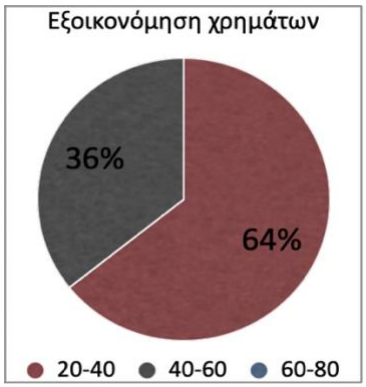
Στα πιο πάνω γραφήματα φαίνεται το ποσοστό των συμμετεχόντων που έχουν απαντήσει κατά πόσο θα ήταν εύκολη στην χρήση η επικείμενη εφαρμογή και σε ποιες ηλικίες αντιστοιχεί κάθε απάντηση.



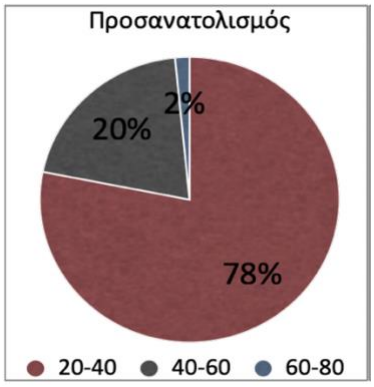
Γράφημα 5



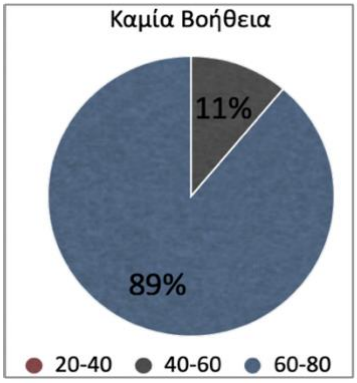
Γράφημα 6



Γράφημα 7



Γράφημα 8



Γράφημα 9

Στα πιο πάνω γραφήματα φαίνεται το ποσοστό των συμμετεχόντων που έχουν απαντήσει κατά πόσο θα τους βοηθούσε στα ψώνια και με πιο τρόπο με την χρήση της επικείμενης εφαρμογής και σε ποιες ηλικίες αντιστοιχεί κάθε απάντηση

Οι συμμετέχοντες στην έρευνα έχουν αναγνωρίσει την δυνατότητα που προσφέρει η νέα αυτή σχετικά με την εξοικονόμηση του χρόνου πρώτα και χρημάτων στην συνέχεια κατά την επίσκεψη στο κατάστημα. Συγκεκριμένα, οι καταναλωτές θεωρούν ότι η μείωση του χρόνου αναμονής στο κατάστημα λόγω δυνατότητας προσανατολισμού και η εμφάνισης της συνολικής αξίας των προϊόντων στη λίστα βλέποντας την εφαρμογή, βελτιώνουνε την αγοραστική τους εμπειρία. Συμπερασματικά, οι καταναλωτές που συμμετείχαν στην έρευνα αναγνώρισαν τον ρόλο αυτής της νέας τεχνολογίας στην πραγματοποίηση αγορών με ταχύτερο τρόπο, πιο εύκολα πιο ποιοτικά και κατά κάποιους και πιο φθηνά.

7.1.3.Το συγκριτικό πλεονέκτημα και η πολυπλοκότητα

Παλαιότερες μελέτες έχουν δείξει ότι, το συγκριτικό πλεονέκτημα και η πολυπλοκότητα είναι οι καλύτεροι δείκτες για αξιολόγηση των οφελών και των προκλήσεων της τεχνολογικής εξέλιξης. Τα αποτελέσματα των συγκριτικών πλεονεκτημάτων και της πολυπλοκότητας καθρεφτίζουν την συμπεριφοράς πρόθεσης χρησιμοποίησης αυτού το είδους της τεχνολογίας RFID.

Με βάση προηγούμενες μελέτες, τα συγκριτικά πλεονεκτήματα της τεχνολογίας RFID μπορούν να ταξινομηθούν σε:

- Αύξηση της αποδοτικότητας του κόστους (μέσω της βελτίωσης της προβολής του ενεργητικού μειώνοντας την απώλεια και την εξοικονόμηση του ανθρώπινου κεφαλαίου) (Tzelepi,2013;Angeles, 2005)
- Βελτίωση της αναπλήρωσης αποθεμάτων (μέσω της καλύτερης παρακολούθησης των αποθεμάτων) (Tzelepi,2013;Smith, 2005)
- Εδραίωση της στρατηγικής μάρκετινγκ (με τη διατύπωση της καλύτερης στρατηγικής μάρκετινγκ και την αύξηση της εξυπηρέτησης των πελατών) (Tzelepi,2013;Jones *et al.*, 2005)

- Αύξηση της ασφάλειας του προϊόντος (με την αύξηση της ακρίβειας των πληροφοριών σχετικά με την κυκλοφορία των υλικών αγαθών) (Tzelepi,2013;Ranky, 2006)

Η πολυπλοκότητα των προκλήσεων μπορεί να περιλαμβάνει τα παρακάτω:

- Η ελάχιστη ή καμία εναρμόνιση των διεπαφών, λόγω της έλλειψης των ενιαίων προδιαγραφών για την τεχνολογία RFID (Tzelepi,2013; Wu *e t a l* , 2006)
- Το μεγάλο κόστος επένδυσης και συντήρησης των συστημάτων RFID
- Η κακή αξιοπιστία του εντοπισμού που οφείλεται στην κακή υποδοχή των ραδιοκυμάτων
- Η μειωμένη ασφάλεια των επιχειρήσεων και των χρηστών (Tzelepi,2013; Ngai *et al.*, 2008)

7.2. Εφαρμογή σε συσκευές Android

Πέρα από τα κινητά τηλέφωνα, τις ταμπλέτες και τα netbooks, το Android έχει επεκταθεί και σε μια πληθώρα συσκευών όπως τα παρακάτω:

- Φωτογραφικές μηχανές
- Τηλεοράσεις
- Συσκευές αναπαραγωγής πολυμέσων (media players)
- Παιχνιδομηχανές
- Συστήματα αυτοματισμού κατοικιών και κτηρίων
- Έξυπνα ρολόγια
- Πλυντήρια κ.α.

7.2.1. Πολυμορφικότητα

Η τεράστια και συνεχής ανάπτυξη του Android , ανά το παγκόσμιο, έχει και το αντίτιμο της, το οποίο παρουσιάζεται κυρίως στην ομάδα των καταναλωτών και των προγραμματιστών. Η ομάδα των καταναλωτών δέχεται συνεχώς βομβαρδισμό, νέων συσκευών, και με την μεγάλη ποικιλία των μοντέλων αλλά και των προσφορών των διαφόρων εταιριών, η αξία των συσκευών απαξιώνετε καθώς αποκτούν εύκολα την ιδιότητα των αναλώσιμων συσκευών. Από την άλλη, στην ομάδα των προγραμματιστών Android, η δυσκολία παρουσιάζεται, στο ότι κάθε συσκευή

έχει τις ιδιαιτερότητες της και διαφορετικά μεγέθη, οπότε για κάθε συσκευή ο κωδικάς θα πρέπει να προσαρμοστεί έτσι ώστε να λειτουργεί σε κάθε είδος συσκευής και μέγεθος οθόνης επιτυγχάνοντας έτσι και την καλή λειτουργία μιας εφαρμογής. Έτσι ένας προγραμματιστής θα πρέπει να σπαταλήσει περισσότερο χρόνο στην ανάπτυξη του κώδικα, για να είναι συμβατή η εφαρμογή στην μεγάλη γκάμα συσκευών και στις διάφορες εκδόσεις λογισμικού.

Επιπρόσθετα, ένα άλλο παράπονο για τους χρήστες Adroid, είναι το γεγονός της μη αναβάθμισης των λειτουργικών συστημάτων ειδικότερα στις συσκευές μικρής και μεσαίας συναμικότητας, εφόσον το κόστος είναι χαμηλό. Με αυτόν τον τρόπο η εταιρίες αυξάνουν πολύ περισσότερο τα κέρδη αναγκάζοντας τον καταναλωτή να αποκτήσει καινούρια συσκευή, αφού δεν του παρέχεται η κατάλληλη συντήρηση καθιστώντας την συσκευή του παρωχημένη πολύ νωρίς. Αντίθετα οι χρήστες Apple, μπορούν να φορτώσουν και να είναι απόλυτα λειτουργικές χωρίς πρόβλημα τις τελευταίες εκδόσεις του λειτουργικού συστήματος. Αυτό είναι εφικτό ακόμα και από συσκευές που βρίσκονται τρεις γενιές πίσω, όπως για παράδειγμά το iPhone 4 μπορεί να τρέξει την έκδοση, iOS9.X

7.2.2. Αγορές Android και διανομή εφαρμογών

Ένας χρήστης για να μπορέσει να διαχειριστεί αλλά και να μεταφορτώσει τις εφαρμογές Android μπορεί να το πετύχει μέσα από το Play store, το οποίο αποτελεί την επίσημη εφαρμογή που προσφέρει αγορά λογισμικού Android, απο την Google, που είναι εγκατεστημένο σε κάθε συσκευή Android. Να σημειωθεί ότι στις πρώτες συσκευές Android ονομαζόταν Android Market. Παρόλο που παρέχεται από την Google η εφαρμογή του play store, έχουν αναπτυχθεί και άλλες εφαρμογές για να γίνονται αγορές λογισμικού εφαρμογών Android. Κάθε μια από αυτές έχει και τους περιορισμούς της. Κάποιες από αυτές είναι:

- SlideMe (αναξάρτητο)
- Amazon App Store (από την Amazon)
- Samsung Apps Store (παρέχει αποκλειστικά μόνο λογισμικό της Samsung)
- Opera Mobile App Store (από την εταιρία Opera, του Opera browser).
- GetJar (ανεξάρτητο)

Ένας χρήστης Android συσκευής έχει δύο τρόπους να εγκαταστήσει εφαρμογή στην συσκευή του

1. Πρώτος τρόπος: εγκατάστασης εφαρμογής είναι οι εφαρμογές αγοράς λογισμικού οι οποίες αναγέρθηκαν και πιο πάνω. Κάθε εφαρμογή αγοράς προσφέρει στους χρήστες πρόσβαση σε διαφορετικές εφαρμογές ανάλογα με την επωνυμία της.

2. Δεύτερος τρόπος: δεν είναι τόσο αυτοματοποιημένος όσο ο πρώτος τρόπος, αφού ο χρήστης πρέπει να μεταφορτώσει ένα εκτελέσιμο αρχείο του οποίου ο τύπος είναι APK. Για να γίνει επιτυχώς η εγκατάσταση της εφαρμογής στην συσκευή σαν πακέτο APK, ο χρήστης πρέπει να κάνει κάποιες αλλαγές στις ρυθμίσεις της συσκευής έτσι ώστε να επιτρέπει την εγκατάσταση πακέτων APK από άγνωστες πηγές . συνήθως ο τρόπος αυτός συνηθίζεται αν ο χρήστης θέλει να εγκαταστήσει πειρατική εφαρμογή οι οποίες δεν διατίθενται στο Play Store, είτε γιατί είναι ιδιωτική είτε επειδή δεν συμφωνεί με τους όρους του marketplace . Αυτή η διαδικασία ονομάζεται «κατά περίπτωση διανομή εφαρμογής» ή αλλιώς ad-hoc app distribution.

7.2.3. Πλατφόρμα Ανάπτυξης Εφαρμογών

Για να δημιουργηθεί μια εφαρμογή κατάλληλη για την πλατφόρμα Android πρέπει να γίνει με προεπιλογή χρησιμοποιώντας java ως γλώσσα προγραμματισμού η οποία πρέπει να συνδυαστεί με το Πακέτο Ανάπτυξης Λογισμικού για Android (Android Software Development Kit). Το πακέτο αυτό δίνει την δυνατότητα στον προγραμματιστή να χρησιμοποιήσει κάποια εργαλεία του όπως :

- εργαλείο για την επιδιόρθωση σφαλμάτων (Debuger)
- βιβλιοθήκες (π.χ.βιβλιοθήκη Facebook και βιβλιοθηκη για game development,)
- προσομοιωτή φυσικής συσκευής (Devtools)
- οδηγίες χρήσης
- compiler
- Integrated Development Environment, IDE, το περιβάλλον που παρέχει το πακέτο για την δημιουργία και ανάπτυξη του κώδικα, για το Android, το οποίο είναι μια τροποποιημένη έκδοση του περιβάλλοντος Eclipse, που ενσωματώνει την τελευταία έκδοση του πακέτου.

Όλα αυτά μαζί ονομάζονται:«Εργαλεία Ανάπτυξης Λογισμικού για Android”, Android

7.2.3.1. Θεμελειώδης αρχές εφαρμογών Android

Ακολουθούν οι θεμελειώδης δομικοί φορείς, που μέσα από την πράξη και την εφαρμογή τους, έχει πραγματοποιηθεί η σύνθεση μιας εφαρμογής Android

7.2.3.2. Δραστηριότητες (Activities)

Οι συγκεκριμένες ενέργειες ενός χρήστη στις εφαρμογές Android ορίζονται ως δραστηριότητες. Η κάθε δραστηριότητα έχει την υπευθυνότητα να δημιουργήσει ένα παράθυρο που θα περιέχει την διεπαφή που θα έχει με τον χρήστη, εφόσον η κάθε δραστηριότητα ορίζει αυτή την διεπαφή.

Κάθε εφαρμογή είναι σύνηθες να αποτελείται από περισσότερες από μια δραστηριότητες. Θα υπάρχει φυσικά αυτή που ονομάζεται «κύρια δραστηριότητα» (main activity), είναι και αυτή που απαρτίζει την οθόνη που θα εμφανιστεί στον χρήστη με την εκκίνηση της εφαρμογής. Επίσης , γίνεται εναλλαγή των δραστηριοτήτων με την εκκίνηση άλλων, για την πραγματοποίηση αυτής της εναλλαγής, με το που θα σταματήσει η εκτέλεση μιας δραστηριότητας, θα τοποθετηθεί από το λειτουργικό σύστημα μέσα σε μια στοίβα την λεγόμενη back stack. Έτσι με αυτόν τον τρόπο, καινούρια δραστηριότητα που θα την αντικαταστήσει, και θα τοποθετηθεί στην κορυφή της στοίβας, και η δραστηριότητα η οποία έτρεχε προηγουμένως να τοποθετηθεί ακριβώς από κάτω της

Είναι σημαντικό να τονιστεί ότι ή μεταφορά του χρήστη από την μια οθόνη στην άλλη σε τόσο μικρό , οφείλεται στην βασική αρχή της στοίβας, αφού ορίζει την ύπαρξη ενός πίσω κουμπιού , back button, το οποίο είναι καθολικό για όλες τις Android συσκευές.

Η κάθε δραστηριότητα αποτελείται από 4 καταστάσεις (states):

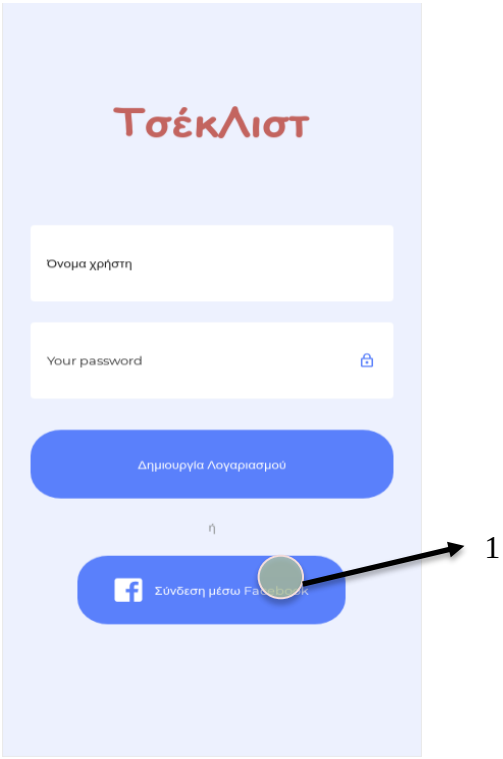
- Ενεργή (active): όταν η δραστηριότητα βρίσκεται στην κορυφή της στοίβας
- Σε παύση (paused): όταν η δραστηριότητα μπορεί να είναι ακόμα ορατή από το σύστημα αλλά έχει χάσει την εστίαση της
- Σταματημένη (stopped): όταν η δραστηριότητα έχει ήδη αντικατασταθεί με μια νέα δραστηριότητα.

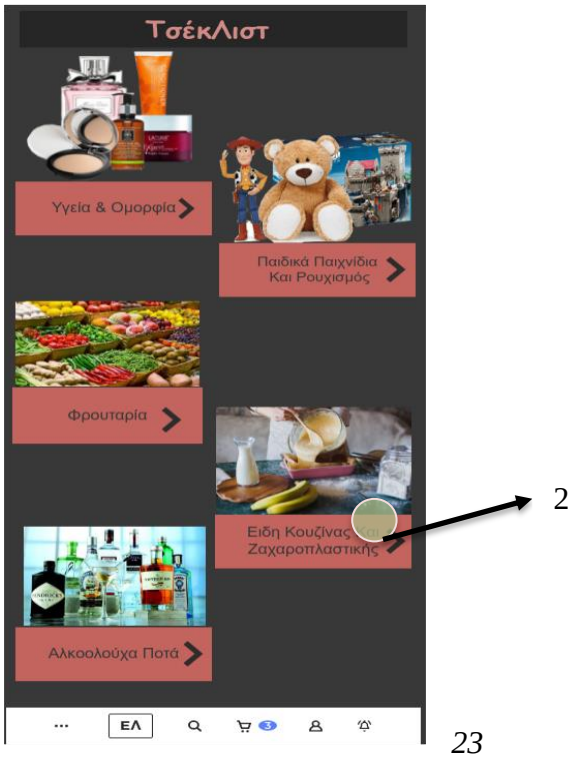
Στις περιπτώσεις όπου η κατάσταση μιας δραστηριότητας είναι σε παύση ή έχει σταματήσει, τότε δίνεται στο λειτουργικό σύστημα η δυνατότητα να αποδεσμεύσει τον χώρο τον οποίο καταλάμβανε μέσα στην μνήμη με τον τερματισμό της κάθε διεργασίας που εκτελεί εκείνη την στιγμή ή απλά σταματώντας την λειτουργία της.

7.3. Προσομοίωση εφαρμογής

Στις εικόνες που ακολουθούν παρουσιάζεται ένα δείγμα για το πως θα μπορούσε να φαίνεται και να λειτουργεί η εφαρμογή «ΤσέκΛιστ» σε συσκευή Android με την χρήση ιδιωτικής ιστοσελίδας https://proto.io.

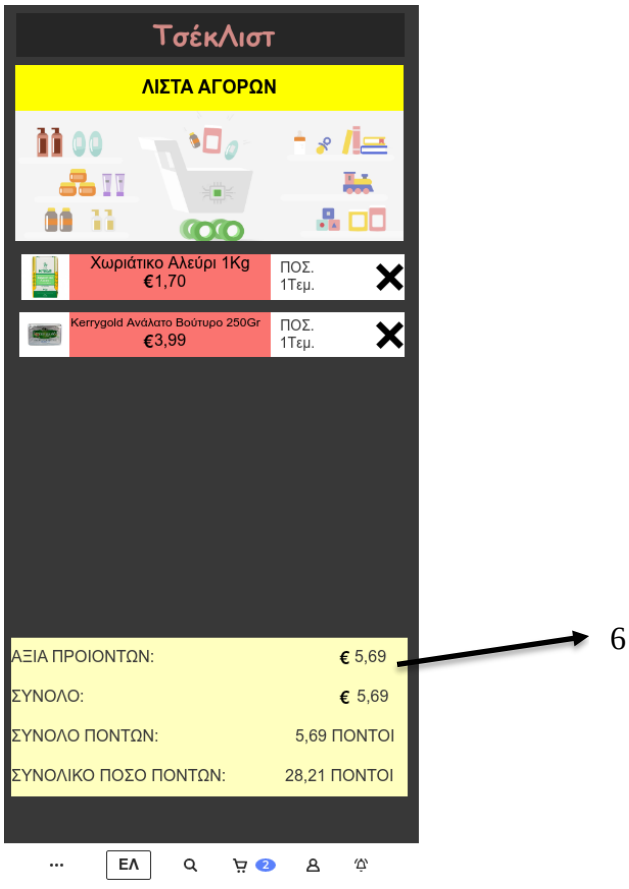
Μπορεί ο καταναλωτής να συνδεθεί με τον λογαριασμό του στο Facebook να επιλέξει κατηγορία αγαθών και στην συνέχεια προϊόντα του καταστήματος, και αφού ενημερωθεί για το που είναι τοποθετημένα , για την τιμή και για την θρεπτική τους αξία μπορεί να τα προσθέσει στην τελική του λίστα ψωνίσματος , που θα φαίνεται η συνολική αξία των αγορών που θέλει να κάνει και οι πόντοι που κερδίζει από την συγκεκριμένη περίπτωση. Με την εφαρμογή αυτή δεν είναι δυνατή η αγορά αγαθών .





Εικόνα 23

Εικόνα 24



Εικόνα 25

Εικόνα 26

Λειτουργικότητα:

1. Σύνδεση μέσω Facebook και προώθηση στο μενού με τις κατηγορίες αγαθών
2. Επιλογή ειδών κουζίνας και ζαχαροπλαστικής
3. Επιλογή χωριάτικο αλεύρι «Μιτσίδης»
4. Επιλογή ανάλατου βουτύρου «Kerrygold»
5. Μετάβαση στην τελική λίστα αγορών
6. Λίστα πιθανών αγορών από το κατάστημα με ενδείξεις πιθανής συνολικής τιμής και πιθανών πόντων που θα κερδηθούν από την πιθανή αγορά

7.4. Ανάπτυξη εφαρμογής σε συστήματα IOS

Σύμφωνα με το **Apple's developer website**, το iOS 11 έφερε μαζί του μια νέα δυνατότητα με το όνομα **«Core NFC»**, που θα είναι συμβατό με τα άλλα συστήματα που κυκλοφορούν, παρέχοντας έτσι ένα τεράστιο αριθμό δυνατοτήτων συνδεσιμότητας με τον «έξω κόσμο». Η εφαρμογή σας θα μπορεί να διαβάζει ετικέτες και να δίνει πληροφορίες στους χρήστες για τα αντικείμενα του φυσικού κόσμου. Για παράδειγμα, η εφαρμογή σας θα μπορεί να διαβάζει τις ετικέτες των τροφίμων σε ένα μπακάλικο ή τις ετικέτες των εκθεμάτων σε ένα μουσείο.

Σε μια από τις άπειρες εφαρμογές της, μπορεί να χρησιμεύσει για τον υπολογισμό των θερμίδων των τροφών, όπως είχε περιγραφεί στην αντίστοιχη πατέντα της Apple, όπου οι εταιρίες συσκευασίας τροφίμων θα μπορούν να προσθέτουν ετικέτες με πληροφορίες των συστατικών των επί μέρους τροφών ενός έτοιμου γεύματος και έτσι να υπολογίζεται από την αντίστοιχη εφαρμογή, η θρεπτική και διατροφική του αξία. Αν και το μέλλον του iPhone με την ενσωμάτωση αυτής της τεχνολογίας δε θα μπορούσε να είναι καλύτερο ίσως, υπάρχει ωστόσο ένα εμπόδιο: η συγκεκριμένη τεχνολογία είναι συμβατή μόνο με iPhone 7 και 7 Plus και νεότερες συσκευές. Δηλαδή, παρόλο που υπάρχει η δυνατότητα σε συσκευές iPhone και iPad από την εποχή του iPhone 6, θα παραμείνει κλειδωμένη σε αυτά.

8. «ICU» PROJECT ΣΕ ΜΕΛΛΟΝΤΙΚΗ ΒΑΣΗ

Η παρούσα διατριβή ερευνά επίσης το πως άτομα που έχουν προβλήματα όρασης λειτουργούν στο σύστημα αγορών. Το κομμάτι της μεθοδολογίας, χωρίζεται σε δύο μέρη.

Στο πρώτο μέρος θα ερωτηθούν πελάτες από την υπεραγορά για να ανάκτηση βασικών πληροφοριών και απόψεων για το πώς θα έπρεπε να είναι φτιαγμένο ένα σύστημα στις υπεραγορές για τους ανθρώπους με προβλήματα όρασης. Το δεύτερο μέρος βασίζεται στο προϊόν, ότι δηλαδή η υπεραγορά θα έχει ενσωματώσει το σύστημα RFID στο μέλλον και οι άνθρωποι με προβλήματα όρασης έχουν συγκεκριμένα ρολόγια με ενσωματωμένο RFID τα οποία θα τους βοηθούν στην πλοήγησή τους μέσα στην υπεραγορά και να βρίσκουν τα προϊόντα που θέλουν αλλά και πληροφορίες για αυτά. Το σύστημα αυτό θέλει επίσης να καταλάβει τις συγκεκριμένες δυσκολίες και προβλήματα που οι άνθρωποι με προβλήματα όρασης μπορεί να συναντήσουν και τι χρειάζονται όταν πηγαίνουν στην υπεραγορά.

Το παρόν κεφάλαιο θα εξηγήσει το σύστημα που θα μπορούσε να χρησιμοποιηθεί στις υπεραγορές και θα αναλυθούν τα αποτελέσματα της έρευνας που έγιναν στην υπεραγορά με τις απόψεις των ανθρώπων με τα προβλήματα όρασης όσον αφορά την εφαρμογή του συστήματος RFID. Επιπλέον, θα αναλυθεί το κόστος της εφαρμογής αυτού του συστήματος.

8.1.Το πρόβλημα

Ο εικοστός-πρώτος αιώνας, είναι γνωστός και σαν ο τεχνολογικός αιώνας. Η επιτυχία μιας τεχνολογικής προόδου ή όχι παίζει αποφασιστικό ρόλο σε μια εθνική ή τοπική ανταγωνιστική δύναμη, τώρα πολλές χώρες προτίθενται ήδη να ξεκινήσουν. Οι ίδιες οι υψηλές τεχνολογίες μπορούν να δημιουργήσουν ανεξαρτησία σε βιομηχανία. Το επιστημονικό πάρκο Hsinchu της Ταϊβάν και η Silicon Valley των ΗΠΑ, είναι η ανεξάρτητη επιβίωση της βιομηχανίας υψηλής τεχνολογίας, που οδηγεί οικονομική ανάπτυξη και στην επιτυχία. Από την άλλη πλευρά, η υψηλή τεχνολογία μπορεί επίσης να βοηθήσει το κάθε επάγγελμα να αναβαθμιστεί τεχνικά και να ενισχύσει τις παραγωγικές δυνάμεις, αυξάνοντας την αποδοτικότητα εργασίας.

Όλα γύρω μας γίνονται ψηφιακά και υψηλής ποιότητας. Θα πίστευε κανείς ότι όλοι οι άνθρωποι μπορούν να επωφεληθούν από αυτό. Αυτό που δεν αντιλαμβανόμαστε είναι ότι υπάρχουν κάποιες

ομάδες ανθρώπων στην κοινωνία, που δεν μπορούν να απολαύσουν την ζωή τόσο άνετα. Μια από τις ομάδες αυτές είναι και οι άνθρωποι με προβλήματα όρασης που ζουν και που συναντούν δυσκολίες ακόμη και στο να επισκεφθούν την υπεραγορά. Αυτό κάνει τη ζωή τους πολύ δύσκολη και έτσι η τεχνολογία θα μπορούσε να διευκολύνει τη ζωή τους πάρα πολύ.

Ο Παγκόσμιος Οργανισμός Υγείας ανακοίνωσε πως περίπου 45,000,000 άνθρωποι παγκοσμίως έχουν προβλήματα όρασης. Το 90% των ανθρώπων αυτών βρίσκεται στις ανεπτυγμένες χώρες του κόσμου. Οι περισσότεροι άνθρωποι με προβλήματα όρασης, αντιμετωπίζουν προβλήματα στην καθημερινότητα τους όπως για παράδειγμα το να επιλέξουν ένα προϊόν από το ράφι και να πληρώσουν στο ταμείο. Υπάρχουν πολλοί και διάφοροι τρόποι που θα μπορούσαν να εφαρμοστούν για την διευκόλυνση των ατόμων αυτών στη καθημερινότητα τους. Για παράδειγμα, θα μπορούσε να υπάρχει ένας χάρτης με ανάγλυφα γράμματα και μαγνητοφωνημένες οδηγίες που να τους βοηθά στην πλοήγηση μέσα στην υπεραγορά. Δυστυχώς όμως δεν υπάρχουν αυτά τα εφόδια στις υπεραγορές. Θα μπορούσαν όμως να φτιαχτούν για να μπορούν να χρησιμοποιηθούν από αυτά τα άτομα, κάνοντας τα να νιώθουν πιο άνετοι και με περισσότερη αυτοπεποίθηση όταν ψωνίζουν.

Το σύστημα που θα βοηθήσει τα άτομα με προβλήματα όρασης, θα έχει ως βάση ένα ρολόι με ενσωματωμένο σύστημα RFID και ακουστικά για την καθοδήγηση των ατόμων προς το τι προϊόν έχει μπροστά του και σε τι τιμές κυμαίνεται. Στον εικοστό-δεύτερο αιώνα, οι άνθρωποι θα χρησιμοποιούν ολοκληρωτικά την υψηλή τεχνολογία για να διευκολύνουν τη ζωή τους, πόσο μάλλον τα άτομα με προβλήματα όρασης. Είναι αναμενόμενο από τις υπεραγορές να εφαρμόσουν τέτοιου είδους, χρήσιμες τεχνολογίες στο μέλλον.

8.2. Στόχος

Στόχος είναι η μελέτη της ψηλής τεχνολογίας εύρεση τρόπων εφαρμογής της στις υπεραγορές, προς όφελος των ατόμων με προβλήματα όρασης. Τα άτομα αυτά μπορούν να φορέσουν το ρολόι με το ενσωματωμένο σύστημα RFID και τα ακουστικά που θα τους διευκολύνουν να ψάξουν το προϊόν που θέλουν σκανάρωντας το bar code του προϊόντος και ακούγοντας την επεξήγηση από τα ακουστικά. Τα άτομα με προβλήματα όρασης αποτελούν μια πολύ ευάλωτη ομάδα του πληθυσμού μας, έτσι θα πρέπει να τους δίνεται περισσότερη προσοχή και βοήθεια διευκολύνοντας

τη ζωή τους και κάνοντας τους πιο ανεξάρτητους. Για τους ανθρώπους αυτούς, το πιο δύσκολο κομμάτι επιβίωσης είναι αυτό του να κυκλοφορούν και να προμηθεύονται τα πρώτης ανάγκης αγαθά με ασφάλεια.

Στο σουπερμάρκετ, είναι γνωστό ότι τα άτομα με προβλήματα όρασης αντιμετωπίζουν δυσκολίες ως προς το πού πρέπει να πάνε, αλλά και για τις πληροφορίες του προϊόντος. Πάντα ζητούν βοήθεια, κάτι το οποίο κάνει την επίσκεψη τους στην υπεραγορά χρονοβόρα και δύσκολη.

Άτομα με προβλήματα όρασης, κάνουν τα πάντα για να αποκτήσουν ανεξαρτησία στη ζωή τους. Ορισμένα θέματα, τα οποία αντιμετωπίζουν στην καθημερινή ζωή είναι ότι, ζουν σε έναν σκοτεινό κόσμο, περπατούν και δεν βρίσκουν τη συγκεκριμένη θέση και είναι δύσκολο να ανακαλύψουν τα πράγματα που θέλουν. Γι 'αυτό και προσφέρεται το σύστημα για το σουπερμάρκετ.

Για την επίτευξη των στόχων, η μελέτη επικεντρώθηκε στη σχέση μεταξύ του συστήματος αγορών και του συστήματος κωδικοποίησης που παρέχει το σουπερμάρκετ. Ακολουθούν ορισμένες υποθέσεις .

1. Τα περισσότερα άτομα με προβλήματα όρασης δεν είναι εύκολο να ψωνίσουν στο σούπερ-μάρκετ.
2. Τα περισσότερα άτομα με προβλήματα όρασης χρειάζονται το σύστημα αγορών.
3. Το σύστημα αγορών για άτομα με προβλήματα όρασης λειτουργεί και αποκτά κέρδος.
4. Παρέχετε το υψηλής ποιότητας συσκευή συστήματος αγορών διεπαφής χρήστη

8.3. Περιγραφή του συστήματος «ICU»

Στο σύστημα, περιλαμβάνονται τέσσερα κύρια προϊόντα – χάρτης αφής, διακομιστής, σύστημα RFID και το ρολόι για χρήση από άτομα με προβλήματα όρασης. Ο πρώτος χάρτης αφής διάταξης σουπερμάρκετ, είναι εγκατεστημένος στην κύρια είσοδο. Αυτό μπορεί να κάνει εύκολο στον χρήστη να τον ανακαλύψει. Ο χάρτης αφής είναι σημαντικό εργαλείο για την εύρεση βοήθειας για άτομα με προβλήματα όρασης. Για να χρησιμοποιηθεί ένας χάρτη πιο αποτελεσματικά, είναι σημαντικό να είναι γνωστή η θέση κάποιου προϊόντος στον χάρτη. Για ένα άτομο με προβλήματα όρασης, αυτό συνήθως σημαίνει τον προσδιορισμό μιας τοποθεσίας διακριτικών ορόσημων στο

περιβάλλον του σουπερμάρκετ, που επί της ουσίας θα παρέχει στις βασικές πληροφορίες για τη θέση του προϊόντος σε σχέση με τη δική του θέση.

Επιπλέον, ο χάρτης θα παρέχει την ημερομηνία, ακόμη και τελευταίες προσφορές και επιλογή άφιξης νέου προϊόντος. Μπορούν να αναζητήσουν με βάση τον τύπο ή την επωνυμία του προϊόντος, το οποίο θα παρέχετε στις γλώσσες, Ελληνικά ή Αγγλικά ή και τις δύο γλώσσες για να επιλέξει ο χρήστης και να γίνει πιο αποτελεσματικό. Ίσως να μην ξέρουν πώς να χρησιμοποιούν τον χάρτη, οπότε ο χάρτης θα παρέχει επίσης μια λειτουργία «ΒΟΗΘΕΙΑ» στην οποία θα ανταποκρίνεται αμέσως το προσωπικό για να λύσει το πρόβλημά. Το σύστημα θα παρέχει επίσης την ακουστική συσκευή που επιτρέπει τη λειτουργία ομιλίας που θα είναι σαν ένα κινητό τηλέφωνο.

Κάθε σουπερμάρκετ θα έχει το δικό του σύστημα για να παρέχει το κόστος και τις πληροφορίες του προϊόντος, το σουπερμάρκετ θα χρησιμοποιήσει το RFID εφαρμόζοντάς το ή ενσωματώνοντας το στα προϊόντα με σκοπό την αναγνώριση και την παρακολούθηση τους με χρήση ραδιοκυμάτων. Ορισμένες ετικέτες μπορούν να διαβαστούν από αρκετά μέτρα μακριά και πέρα από την οπτική γωνία του αποδέκτη, όπως έχει ήδη αναφερθεί σε πιο πάνω κεφάλαια

Θα υπάρχει ένας διακομιστής για να αποθηκεύσει την ημερομηνία για την τιμή και τις πληροφορίες του προϊόντος, χωρίς να χρειάζεται η συσκευή αποθήκευσης, ένας απλός υπολογιστής μπορεί να το κάνει. η ημερομηνία θα αποστέλλεται στον χάρτη αφής του σουπερμάρκετ για την παροχή ημερομηνίας του προϊόντος.

Τα άτομα με προβλήματα όρασης θα χρησιμοποιούν και το ρολόι. Μέσα στο ρολόι έχουν τον αναγνώστη RFID για να λαμβάνουν τις πληροφορίες που χρειάζονται, για παράδειγμα, μπορούν να ακούσουν την τιμή, την ημερομηνία λήξης, τις διατροφικές πληροφορίες και την επωνυμία του προϊόντος με το ακουστικό τους.

9. ΤΕΛΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα τελευταία χρόνια έχει γίνει κοινή αντίληψη για σχεδόν ολόκληρο τον επιχειρηματικό κόσμο ότι η αποτελεσματική διαχείριση και χρήση της τεχνολογίας αποτελεί το σημαντικότερο στοιχείο για την επιτυχία και την βελτίωση της απόδοσης μιας επιχείρησης προσδίδοντας σε αυτήν ανταγωνιστικό πλεονέκτημα. Το ενδιαφέρον για τη χρήση της τεχνολογίας RFID ως βελτιστοποίηση των διαδικασιών ιχνηλάτησης , αναζήτησης και βοήθειας μεγαλώνει ραγδαία, αφού όλο και περισσότερες επιχειρήσεις την εφαρμόζουν και επιζητούν την από κοινού χρήση της με τους πελάτες ή/και τους προμηθευτές τους.

Η καινοτόμα αυτή τεχνολογία δίνει την δυνατότητα αυτόματης αναγνώρισης μεμονωμένων προϊόντων ή ολόκληρων κιβωτίων χωρίς να χρειάζεται η οπτική επαφή μετασχηματίζοντας ολοκληρωτικά όλες τις παρούσες διαδικασίες της καταναλωτικής αλυσίδας. Το σημαντικότερο σημείο που διακρίνει την συγκεκριμένη τεχνολογία έγκειται στο γεγονός ότι δίνει την δυνατότητα να χαρακτηριστεί μοναδικά κάθε προϊόν ενώ τα δεδομένα που περικλείονται στην ετικέτα του μπορεί να μεταβάλλονται. Με αυτόν τον τρόπο μπορεί να παρακολουθείται ο κύκλος ζωής του προϊόντος από την στιγμή που θα παραχθεί μέχρι την τελική του κατανάλωση. Η δημιουργία βάσεων δεδομένων για μεμονωμένα προϊόντα φάνταζε πριν από κάποια χρόνια ανέφικτο. Μέσω των συστημάτων RFID κάθε επιχείρηση μπορεί να μοιραστεί πλήθος σημαντικών πληροφοριών με τους πελάτες της, να ολοκληρώσει τις ενέργειες της καταναλωτικής αλυσίδας και να αποκομίσει τα οφέλη από την δημιουργία συνεργασίας μεταξύ των επιχειρήσεων που μοιράζονται την εν λόγω τεχνολογία.

Όπως συμβαίνει με κάθε νέα τεχνολογία, έτσι και στην περίπτωση της εφαρμογής του RFID υπάρχουν πολλά οφέλη και κίνδυνοι. Πολλές είναι οι αντιδράσεις και οι ανυσηχίες των καταναλωτών που προκύπτουν από την εφαρμογή αυτής της τεχνολογίας, λόγω των παραβίασης του ιδιωτικού απορρήτου. Η αντίθεση για τη χρήση του RFID οφείλεται στη δυνατότητα αυτόματης χρησιμοποίησης των συσσωρευμένων πληροφοριών που αφορούν καταναλωτές από τις επιχειρήσεις χωρίς ενημέρωση τους και στην , χωρίς εμπόδιο, συλλογή δεδομένων που πραγματοποιείται δημιουργώντας της αίσθηση του « Big Brother» να βρίσκεται σε κάθε κίνηση του καταναλωτή. Οι οργανώσεις και οι πολιτικοί φορείς μπορούν να αναπτύξουν και να θέσουν αυστηρά μέτρα προστασίας σε ότι αφορά τον τρόπο με τον οποίο τα συστήματα RFID

εφαρμόζονται και χρησιμοποιούνται έτσι ώστε να μην παραβιάζουν σε κανένα σημείο την ιδιωτικότητα κανενός .

Χρειάζεται λοιπόν δημόσια ευαισθητοποίηση για να καθοριστούν τα όρια χρήσης της εν λόγω τεχνολογίας και ρυθμιστικό νομοθετικό πλαίσιο που θα ακολουθηθούν για τον χειρισμό και τον περιορισμό της - χωρίς κρίση - χρήσης της . Από την άλλη πλευρά, τα μέλη της βιομηχανίας του RFID πρέπει να ανταποκριθούν στις ανησυχίες και αντιδράσεις των καταναλωτών για την παραβίαση του ιδιωτικού απορρήτου. Το σίγουρο είναι ότι η αποδοχή του RFID από τους καταναλωτές θα αυξηθεί κατά μεγάλο ποσοστό εάν και εφόσον ενισχυθεί η εμπιστοσύνη των καταναλωτών. Ωστόσο, άλλοι παράγοντες που σχετίζονται με την αποδοχή ή μη της τεχνολογίας από τους καταναλωτές όπως ηλικία, μορφωτικό επίπεδο, φύλο, κ.α.

Όσον αφορά την Κυπριακή επιχειρηματική οντότητα, θα πρέπει να δοθεί ιδιαίτερο βάρος στην σφαιρική συλλογή επιτυχημένων πρακτικών από επιχειρήσεις από το διεθνή χώρο που θα οδηγήσουν στην ομαλή υιοθέτηση της τεχνολογίας RFID αρχικά από τις μεγάλες κυπριακές επιχειρήσεις και στην συνέχεια στην σταδιακή εξάπλωσή της και στις υπόλοιπες επιχειρήσεις

Εν κατακλείδι να αναφέρω ότι η ευρεία διάδοση του RFID, ειδικά στην Κύπρο, αποτελεί έναν τομέα πάνω στον οποίο στηρίζονται πολλά projects. Επίσης εξυπηρετεί πολύ τις καθημερινές λειτουργίες ενός χρήστη με τις αμέτρητες δυνατότητες που παρέχει, όπως προαναφέρθηκε, με τα RFID Tags, είτε για πραγματική ευκολία, είτε για απλή διασκέδαση.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] J. Landt. The history of RFID. Potentials, IEEE, 24(4):8–11, 2005.

[2] Adam Laurie. Practical attacks against RFID. Network Security, 2007(9):4 – 7, 2007.

[3] Simson Garfinkel and Beth Rosenberg. RFID: Applications, Security, and Privacy. Addison-Wesley Professional, July 2005.

[4] Bill Glover and Himanshu Bhatt. RFID essentials. 2006.

[5] EPCTM radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz 960 MHz version 1.2.0," October 2008.

[6] RFID in healthcare - a panacea for the regulations and issues affecting the industry?. http://www.ups-scs.com/solutions/white_papers/wp_RFID_in_Healthcare.pdf.

[7] Medicarte uses RFID and biometrics to reduce counterfeiting. http://www. rfidjournal.com/article/view/9065.

[8] Rishab Nithyanand. The Evolution of Cryptographic Protocols in Electronic Passports. Cryptology ePrint Archive, Report 2009/200, 2009.

[9] Martin Hlavác. Known—Plaintext—Only Attack on RSA—CRT with Montgomery Multiplication. In Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, CHES ’09, pages 128–140, Berlin, Heidelberg, 2009. Springer-Verlag.

[10] Carlo Blundo, Giuseppe Persiano, Ahmad-Reza Sadeghi, and Ivan Visconti. Improved security notions and protocols for non-transferable identification. In Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security, ESORICS ’08, pages 364–378, Berlin, Heidelberg, 2008. Springer-Verlag.

[11] Mary Catherine O'Connor. Mccarran airport RFID system takes off. RFID Journal, Oct 2005. http://www.rfidjournal.com/article/view/1949.

[12] Mark Palmer. The main challenges of RFID, Oct 2011. http://www.ebizq.net/topics/scm/features/3916.html

[13] Aikaterini Mitrokotsa, Melanie R. Rieback, and Andrew S. Tanenbaum. Classification of RFID attacks. In IWRT, pages 73–86, 2008.

[14] Aikaterini Mitrokotsa, Melanie R. Rieback, and Andrew S. Tanenbaum. Classifying RFID attacks and defenses. Information Systems Frontiers, 12(5):491–505, 2010.

[15] Xiaolan Zhang and Brian King. Modeling RFID security. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, Information Security and Cryptology, volume 3822 of Lecture Notes in Computer Science, pages 75–90. Springer Berlin / Heidelberg, 2005. 10.1007/11599548_7.

[16] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Dieter Hutter, Günter Müller, Werner Stephan, and Markus Ullmann, editors, International Conference on Security in Pervasive Computing – SPC 2003, volume 2802 of Lecture Notes in Computer Science, pages 454–469, Boppard, Germany, March 2003. Springer.

[17] Hung-Yu Chien. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. IEEE Transactions on Dependable and Secure Computing, 4(4):337–340, December 2007.

[18] Gildas Avoine. Adversary Model for Radio Frequency Identification. Technical Report LASEC-REPORT-2005-001, Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC), Lausanne, Switzerland, September 2005

[19] Ching Yu Ng, Willy Susilo, Yi Mu, and Rei Safavi-Naini. RFID privacy models revisited. In Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security, ESORICS '08, pages 251–266, Berlin, Heidelberg, 2008. Springer-Verlag.

[20] Gerhard Hancke and Markus Kuhn. An RFID Distance Bounding Protocol. In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005, pages 67–73, Athens, Greece, September 2005. IEEE, IEEE Computer Society.

[21] Gerhard Hancke. A practical relay attack on ISO 14443 proximity cards. Technical report, 2005.

[22] Stefan Brands and David Chaum. Distance-bounding protocols. In EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology, pages 344–359, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.

[23] Yvo Desmedt, Claude Goutier, and Samy Bengio. Special uses and abuses of the Fiat-Shamir passport protocol. In CRYPTO, pages 21–39, 1987.

[24] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical NFC peer-to-peer relay attack using mobile phones. In Proceedings of the 6th international conference on Radio frequency identification: security and privacy issues, RFIDSec'10, pages 35–49, Berlin, Heidelberg, 2010. Springer- Verlag.

[25] Gildas Avoine, Muhammed Ali Bingöl, Süleyman Kardas, Cédric Lauradoux, and Benjamin Martin. A Framework for Analyzing RFID Distance Bounding Protocols. Journal of Computer Security – Special Issue on RFID System Security, 19(2):289–317, March 2011.

[26] Gildas Avoine and Aslan Tchamkerten. An efficient distance bounding RFID authentication protocol: balancing false-acceptance rate and memory requirement. In Information Security Conference – ISC'09, volume 5735 of Lecture Notes in Computer Science, Pisa, Italy, September 2009.

[27] Laurent Bussard and Walid Bagga. Distance-bounding proof of knowledge to avoid real-time attacks. In Ryoichi Sasaki, Sihan Qing, Eiji Okamoto, and Hiroshi Yoshiura, editors, Security and Privacy in the Age of Ubiquitous Computing, volume 181 of IFIP Advances in Information and Communication Technology, pages 223–238. Springer Boston, 2005. 10.1007/0-387-25660-1_15.

[28] Gildas Avoine and Aslan Tchamkerten. An efficient distance bounding RFID authentication protocol: balancing false-acceptance rate and memory requirement. In Information Security Conference – ISC'09, volume 5735 of Lecture Notes in Computer Science, Pisa, Italy, September 2009.

[29] Latanya Sweeney. k-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzz., 10(5):557–570, 2002.

[30] Benjamin Fung, Ke Wang, Rui Chen, and Philip S. Yu. Privacy-preserving data publishing: a survey on recent developments. ACM Comput. Surv., 42(4):to appear, 2010

[31] Emre Kaplan, Thomas Brochmann Pedersen, Erkay Savas, and Yücel Saygin. Discovering private trajectories using background information. Data Knowl. Eng., 69(7):723–736, 2010.

[32] Chong Hee Kim and Gildas Avoine. RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks. In 8th International Conference on Cryptology And Network Security – CANS'09, Kanazawa, Ishikawa, Japan, December 2009. Springer.

[33] Chong Hee Kim and Gildas Avoine. RFID distance bounding protocols with mixed challenges. IEEE Transactions on Wireless Communications, 10(5):1618-1626, May 2011.

[34] Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer, and Muthuramakrishnan Venkitasubram

[35] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. t-closeness: privacy beyond k-anonymity and `-diversity. In Proceedings of the 23rd International Conference on Data Engineering, ICDE 2007, Istanbul, Turkey, 15-20 April 2007, pages 106–115. IEEE, 2007.

[36] Ninghui Li, Wahbeh H. Qardaji, and Dong Su. Provably private data anonymization: Or, k-anonymity meets differential privacy. CoRR, abs/1101.2604, 2011.

[37] Pierangela Samarati and Latanya Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical Report SRI-CSL-98-04, SRI Computer Science Laboratory, 1998.

[38] Qing Zhang, Nick Koudas, Divesh Srivastava, and Ting Yu. Aggregate query answering on anonymized tables. In In ICDE, pages 116–125, 2007.

[39] Josep Domingo-Ferrer and Vicenç Torra. Ordinal, continuous and heterogenerous k-anonymity through microaggregation. Data Min. Knowl. Disc., 11(2):195–212, 2005.

[40] Josep Domingo-Ferrer and Josep Maria Mateo-Sanz. Practical data-oriented microaggregation for statistical disclosure control. IEEE Trans. Knowl. Data Eng., 14(1):189–201, 2002.

[41] Osman Abul, Francesco Bonchi, and Mirco Nanni. Never walk alone: uncertainty for anonymity in moving objects databases. In Proceedings of the 24th International Conference on Data Engineering, ICDE 2008, Cancun, Mexico, 7-12 April 2008, pages 376–385. IEEE, 2008.

[42] Osman Abul, Francesco Bonchi, and Mirco Nanni. Anonymization of moving objects databases by clustering and perturbation. Inf. Syst., 35(8):884–910, 2010.

[43] Charu C. Aggarwal and Philip S. Yu. A condensation approach to privacy preserving data mining. In Proceedings of the 9th International Conference on Extending Database Technology,

EDBT 2004, Heraklion, Crete, Greece, 14-18 March 2004, volume 2992 of Lecture Notes in Computer Science, pages 183–199. Springer, 2004.

[44] Marco Gruteser and Dirk Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In Proceedings of the 1st International Conference on Mobile Systems, Applications, and Services, MobiSys 2003, San Francisco, California, USA, 5-8 May 2003. USENIX, 2003.

[44] Baik Hoh, Marco Gruteser, Hui Xiong, and Ansaf Alrabady. Preserving privacy in GPS traces via uncertainty-aware path cloaking. In Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, 28-31 October 2007, pages 161–171. ACM, 2007.

[45] Baik Hoh, Marco Gruteser, Hui Xiong, and Ansaf Alrabady. Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking. IEEE Trans. Mob. Comput., 9(8):1089–1107, 2010.

[46] Manolis Terrovitis and Nikos Mamoulis. Privacy preservation in the publication of trajectories. In IEEE International Conference on Mobile Data Management, pages 65–72, Los Alamitos, CA, USA, 2008. IEEE Computer Society.

[47] Adam Meyerson and Ryan Williams. On the complexity of optimal k-anonymity. In Proceedings of the twenty-third ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems, PODS ’04, pages 223–228, New York, NY, USA, 2004. ACM.

[48] Lei Chen, M. Tamer Özsu, and Vincent Oria. Robust and fast similarity search for moving object trajectories. In Proceedings of 2005 ACM SIGMOD International Conference on Management of Data, Baltimore, Maryland, USA, 14-16 June 2005, pages 491–502. ACM, 2005.

[49] Haibo Hu, Jianliang Xu, Sai Tung On, Jing Du, and Joseph Kee-Yin Ng. Privacyaware location data publishing. ACM Trans. Database Syst., 35:18:1–18:42, July 2010.

[50] Anna Monreale, Gennady Andrienko, Natalia Andrienko, Fosca Giannotti, Dino Pedreschi, Salvatore Rinzivillo, and Stefan Wrobel. Movement data anonymity through generalization. Trans. Data Privacy, 3(2):91–121, 2010.

[51] Ιωσήφ Σηφάκης, (Ιούλιος 2011), «Συνέντευξη και προοπτικές της Πληροφορικής και των Επικοινωνιών», Διαθέσημο online στο: http://www.adslgr.com/forum/archive/index.php/t-529204.html, Τελευταία πρόσβαση: Δεκέμβριος 2011

[52] Πρωτονοτάριος Δ., (2004), «Τεχνολογίες Αυτόματης Αναγνώρισης Προϊόντων με Χρήση Ραδιοκυμάτων για την Ολοκλήρωση της Εφοδιαστικής Αλυσίδας», Μεταπτυχιακή Διπλωματική εργασία Τμήμα Μηχανικών Παραγωγής και Διοίκησης, Πανεπιστήμιο Κρήτης, Διαθέσιμο Online στο: http://www.logistics.tuc.gr/Contents/Diatrives/Protonotarios.pdf, Τελευταία Πρόσβαση: Ιανουάριος 2012

[53] Weis, S.,(2003), «Security and Privacy in Radio-Frequency Identification Devices»

[54] The Boston Consulting Group, (2003), «Customer Acceptance of FSI Applications», Metro Group, Διαθέσιμο Online στο: http://www- 05.ibm.com/cz/download/metro.pdf, Τελευταία Πρόσβαση: Σεπτέμβριος 2011

[55] Αγγελίδου Ζ., (2010), «Προστασία της Ιδιωτικότητας και των Προσωπικών Δεδομένων στο χώρο της Εκπαίδευσης», Μεταπτυχιακή Διπλωματική εργασία Πανεπιστημίου Μακεδονίας, Διαθέσιμο Online: http://dspace.lib.uom.gr/bitstream/2159/13751/1/Aggelidou_Msc2010.pdf,

[56] Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία, Μαυρίδης Ιωάννης, (2009), «Η προστασία των προσωπικών δεδομένων ενόψει της εφαρμογής της νέας τεχνολογίας της ταυτοποίησης με ραδιοσυχνότητες (R.F.I.D): Νομική και τεχνολογική προσέγγιση» Διαθέσιμο Online στο: http://openarchives.gr/view/305151 Τελευταία Πρόσβαση: Ιανουάριος 2012

[57] Η Νέα Βιομηχανική Πολιτική της Κύπρου 2019-2030 [Σχέδιο Δράσης για την περίοδο 2019-2022]

[58] https://www.epixeiro.gr/article/148764 Η τεχνολογική ωριμότητα των επιχειρήσεων στην Ελλάδα παραμένει σε χαμηλά επίπεδα

[59] https://www.philenews.com/oikonomia/kypros/article/820621 Εκ βάθρων αναδιάρθρωση για προώθηση της Digital Cyprus

Angeles R., (2007) *«RFID Technologies: Supply-Chain Applications and Implementation Issues»*, IEEE Engineering Management Review, Vol.35, No 2

Metro Group, (2008), *«Future Store Initiative»*, Διαθέσιμο σε: http://www.future- store.org, Τελευταία πρόσβαση στις 15/10/2008

Miller J., (2007) *«Criteria for Evaluating RFID Solutions for Records and Information»*, IEEE Engineering Management Review, Vol.35, No 2

O'Connor C.M., (2006), «*At McDonald's, ExpressPay Fits the Bill*», RFID Journal, Jan. 23

Sensap,(2008), *«Η STAFF JEANS εισάγει την τεχνολογία RFID στην εφοδιαστική της αλυσίδα»*,Διαθέσιμο σε : http://www.sensap.eu,Τελευταία πρόσβαση στις 15/10/2008

RFID Journal, (2003), *«Wal-Mart spells out RFID vision»*,Διαθέσιμο σε : http://www.rfidjournal.com/article/articleview/463/1/3/,(June16,2003), Τελευταία πρόσβαση στις 10/10/2008

Chuang M., Shaw W., (2007), *«RFID: Integration Stages in Supply Chain Management»*, IEEE Engineering Management Review, Vol.35, No 2

Smith, R., (2004), *«RFID: A Brief Technology Analysis»*. Ανακτήθηκε στις 21-11-2012, από: http://rdiego.diatel.upm.es/r%26d/chen%20xi/RFIDA%20Brief%20Technology%20Analysis.pdf

Roberts, C. M., (2006), "Radio frequency identification (RFID)", *Computers & Security*, **25**, pp. 18-26.

Angeles, R., (2005), "RFID Technologies: Supply-chain applications and implementation issues",*Information Systems Management*, **22** (1), pp. 51-65.

ΠΑΡΑΡΤΗΜΑ

Στο παρόν παράρτημα παρατίθεται το ερωτηματολόγιο στην μορφή την οποία και έγινε. Η έρευνα διεξάχθηκε σε μορφή συνέντευξης και συμπληρωνόταν από τον υποφαινόμενο.