ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Επιθέσεις Άρνησης Υπηρεσιών σε Παθητικά RFID Δίκτυα με Χρήση Θεωρίας Παιγνίων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Ηλία Η. Μπίμπα

Επιβλέπων: Συμεών Παπαβασιλείου
Καθηγητής

Αθήνα, Οκτώβριος 2018

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

Επιθέσεις Άρνησης Υπηρεσιών σε Παθητικά RFID Δίκτυα με Χρήση Θεωρίας Παιγνίων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Ηλία Η. Μπίμπα

Επιβλέπων: Συμεών Παπαβασιλείου
Καθηγητής

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την $8^{η}$ Οκτωβρίου 2018.

.....	.....	.....
Συμεών Παπαβασιλείου	Θεοδώρα Βαρβαρίγου	Ιωάννα Ρουσσάκη
Καθηγητής Ε.Μ.Π.	Καθηγήτρια Ε.Μ.Π.	Επίκουρη Καθηγήτρια Ε.Μ.Π.

Αθήνα, Οκτώβριος 2018.

.....
Ηλίας Μπίμπας
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών

Περίληψη

Η τεχνολογία RFID (Radio Frequency Identification, ταυτοποίηση μέσω ραδιοσυχνοτήτων) χρησιμοποιεί ηλεκτρομαγνητική ακτινοβολία για να προσφέρει ασύρματη ταυτοποίηση και δυνατότητες απομακρυσμένου ελέγχου. Λόγω των χαρακτηριστικών της, απαντάται σε ποικιλία εφαρμογών, όπως για παράδειγμα ο αυτοματοποιημένος έλεγχος πρόσβασης σε εγκαταστάσεις, ο εντοπισμός εμπορικών αγαθών κατά την μεταφορά ή αποθήκευση τους, καθώς και η παρακολούθηση της πορείας του ασθενούς σε σύγχρονα συστήματα υγείας. Ανάλογα με την διαχείριση ισχύος και την απαιτούμενη αξιοπιστία σε μια εφαρμογή τα συστήματα RFID ποικίλουν. Επικεντρωνόμαστε στα παθητικά δίκτυα RFID, τα οποία έχουν αναδειχθεί ως λύση χαμηλού κόστους, λόγω της ενεργειακής τους απόδοσης σε σύγκριση με συστήματα των οποίων η αρχιτεκτονική βασίζεται στην απρόσκοπτη παροχή ισχύος. Ωστόσο, λόγω του σχεδιασμού τους και των περιορισμένων δυνατοτήτων τους, τα παθητικά δίκτυα RFID είναι ευάλωτα σε επιθέσεις. Προτείνουμε μια ανάλυση επιθέσεων άρνησης υπηρεσιών από εισβολείς, βασισμένη στην θεωρία παιγνίων, η οποία περιγράφει την συμπεριφορά των παθητικών ετικετών (passive tags) βασισμένη σε μια συνάρτηση χρησιμότητας (utility function). Η συνάρτηση αυτή εκφράζει για τις κανονικές ετικέτες τον στόχο τους να εκπέμπουν σήμα το οποίο θα μπορεί να αποδιαμορφωθεί από την συσκευή ανάγνωσης (reader), ενώ για τους εισβολείς την προσπάθειά τους να παρεμποδίζουν την λειτουργία του δικτύου. Στη συνάρτηση χρησιμότητας περιλαμβάνεται και ένας όρος ο οποίος περιγράφει το ρίσκο που έχουν οι ετικέτες ανάλογα με την συμπεριφορά τους στο δίκτυο. Το δυναμικό αυτό σύστημα μοντελοποιείται ως ένα μη συνεργατικό παίγνιο, στο οποίο προσδιορίζεται το σημείο ισορροπίας Nash για την κάθε ετικέτα. Ακόμα, προτείνεται ένας κατανεμημένος, επαναληπτικός αλγόριθμος για τον προσδιορισμό αυτών των σημείων ισορροπίας, καθώς και μια ενδεικτική υλοποίησή του, που δείχνει την σύγκλιση του συστήματος.

Λέξεις κλειδιά: Ασύρματα Δίκτυα, Ταυτοποίηση Μέσω Ραδιοσυχνοτήτων, Παθητικές Ετικέτες RFID, Θεωρία Παιγνίων, Επιθέσεις Άρνησης Υπηρεσιών

Abstract

Radio-Frequency Identification (RFID) is a technology that utilizes electromagnetic waves to provide wireless identification and remote control capabilities. Due to its characteristics, it is used in a wide range of applications; automated access control, tracking of commercial goods, and health monitoring systems, among others. Depending on the power management and the required reliability of the components involved, RFID systems can vary. We focus on the operation of RFID networks with passive tags, which have emerged as a low cost, energy-efficient alternative to systems that require a more power-oriented architecture. However, due to their design and limited capabilities they can be susceptible to several intrusive actions. We propose a game-theoretic analysis of denial of service attacks by intruders on such networks, that describes the behaviour of the passive tags based on a utility function. For the normal tags, this function reflects their goal to have their signal properly demodulated by the reader, and for the intruder tags it describes their attempt to disrupt the network's operation. The utility function also contains a term that reflects the penalty imposed to each tag, depending on its behaviour within the network. The dynamic system is formulated as a non-cooperative game for which the Nash equilibrium of each tag is determined. A distributed, iterative algorithm to locate the Nash equilibrium point is proposed, as well as an indicative implementation of this algorithm that demonstrates the convergence of the system.

Keywords: Wireless Networks, RFID, Passive RFID Tags, Game Theory, Denial of Service Attacks

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κύριο Συμεών Παπαβασιλείου και την κυρία Ειρήνη Ελένη Τσιροπούλου για την άριστη συνεργασία που είχαμε και την καθοδήγηση που μου προσέφεραν κατά την διάρκεια εκπόνησης αυτής της διπλωματικής εργασίας. Ακόμα, οφείλω να ευχαριστήσω θερμά τον πατέρα μου, την μητέρα μου, και τον αδελφό μου, οι οποίοι με στήριξαν και με βοήθησαν ανιδιοτελώς κατά την διάρκεια της φοίτησής μου.

Ηλίας Η. Μπίμπας
Αθήνα, Οκτώβριος 2018

Περιεχόμενα

1 Εισαγωγή 15
1.1 Πρόλογος 15
1.2 Αντικείμενο της εργασίας 17
1.3 Δομή της εργασίας 18
2 Τεχνολογίες RFID 19
2.1 Ορολογία και Αρχές Λειτουργίας 19
2.2 Πλεονεκτήματα και εφαρμογές 23
2.3 Περιορισμοί 26
3 Επιθέσεις σε δίκτυα RFID 28
3.1 Περί ασφάλειας ασύρματων δικτύων 28
3.2 Κατηγορίες επιθέσεων 30
3.3 Επιθέσεις άρνησης υπηρεσιών 33
4 Μοντελοποίηση του προβλήματος ως μη συνεργατικό παίγνιο 35
4.1 Εισαγωγή 35
4.2 Περιγραφή του δικτύου 37
4.3 Παίγνιο μετριασμού παρεμβολών 39
4.4 Προσδιορισμός σημείου ισορροπίας Nash 43
5 Ο Αλγόριθμος για το παίγνιο IM 47
5.1 Η ιδέα του αλγορίθμου 47
5.2 Παρουσίαση του αλγορίθμου 48
6 Προσομοίωση της λειτουργίας του δικτύου 49
6.1 Παραμετροποίηση του αλγορίθμου 49
6.2 Συνοπτική παρουσίαση της υλοποίησης 51
6.3 Ενδεικτικά αποτελέσματα 53
7 Επίλογος 56
7.1 Σύνοψη 56
7.2 Μελλοντική εργασία 58
8 Βιβλιογραφία 59

Κατάλογος Σχημάτων

1	Σχηματικό παράδειγμα επικοινωνίας ενός παθητικού πομποδέκτη RFID με την συσκευή ανάγνωσης.	19
2	Το κύκλωμα μιας παθητικής ετικέτας.	20
3	Παθητική ετικέτα μιας χρήσης από αγώνες ταχύτητας.	20
4	Σχηματικό παράδειγμα επικοινωνίας παθητικής ετικέτας, παρουσία κακόβουλου ενδιάμεσου κόμβου.	31
5	Σχηματικό παράδειγμα δικτύου RFID που περιέχει εισβολέα, με σκοπό να εκπέμψει σήμα οπισθοσκέδασης υψηλής ισχύος και να μειώσει το SINR των κανονικών ετικετών.	36
6	Η μορφή της συνάρτησης απόδοσης.	40
7	Η μορφή των συναρτήσεων χρησιμότητας πέντε κανονικών ετικετών.	53
8	Η ισχύς που επιλέγουν οι κανονικές ετικέτες.	54
9	Η ισχύς οπισθοσκέδασης των κανονικών ετικετών παρουσία εισβολέα.	55
10	Η ισχύς οπισθοσκέδασης του εισβολέα.	55

1 Εισαγωγή

1.1 Πρόλογος

Η ιδέα για την ανάπτυξη τεχνολογιών που θα χρησιμοποιούνταν για την ασύρματη ταυτοποίηση αντικειμένων ήταν κάτι το οποίο υπήρχε από τις πρώτες δεκαετίες του περασμένου αιώνα. Με την εφεύρεση και την διαδεδομένη χρήση του radar άνοιξε ο δρόμος προς την βαθύτερη κατανόηση και εκμετάλλευση των ιδιοτήτων των ηλεκτρομαγνητικών κυμάτων ώστε να επιτυγχάνονται ακριβείς μετρήσεις από απόσταση. Κατά την διάρκεια του Β΄ Παγκοσμίου Πολέμου, η ανάγκη αναγνώρισης φίλιων αεροσκαφών οδήγησε τους Βρετανούς στην ανάπτυξη των συστημάτων IFF (Identification, friend or foe). Το σύστημα αυτό χρησίμευε στην θετική αναγνώριση συμμαχικών αεροσκαφών χρησιμοποιώντας αναμετάδοση ραδιοκυμάτων και θεωρείται από πολλούς η πρώτη χρήση της τεχνολογίας RFID [1], [2]. Στις δεκαετίες που ακολούθησαν, η τεχνολογία συνέχισε να βελτιώνεται αυξάνοντας τις δυνατότητες των ετικετών και μειώνοντας το μέγεθος τους. Έτσι, στην δεκαετία του 70΄ και την δεκαετία του 80΄, ερευνητές, εταιρίες και κρατικές υπηρεσίες εργάζονταν για την ανάπτυξη των συστημάτων RFID με σκοπό την χρήση τους σε ένα μεγάλος εύρος εφαρμογών, όπως η παρακολούθηση οχημάτων και η αυτοματοποίηση στις γραμμές παραγωγής [1].

Στην συνέχεια, η εξέλιξη των RFID δικτύων υπήρξε αλματώδης, και η τεχνολογία τους αναμένεται να παίξει καθοριστικό ρόλο στην ανάπτυξη του Internet of Things και την αυτοματοποίηση διαδικασιών τόσο στο εμπόριο και την παραγωγή, όσο και στην καθημερινή ζωή. Το χαμηλό κόστος παραγωγής των ετικετών, η σχετική ενεργειακή αυτονομία τους και η περιορισμένη ανάγκη συντήρησης βοήθησαν να ξεπεραστούν οι δυσκολίες που προέκυπταν στην προσπάθεια εξάπλωσης έξυπνων συσκευών [1], [3]. Η ανάγκη για ανθρώπινη παρέμβαση σε εργασίες καταμέτρησης και παρακολούθησης αγαθών μειώθηκε, ενώ λύθηκαν προβλήματα που προέκυπταν με την χρήση τεχνολογιών όπως το barcode, σχετικά με την ανάγκη ύπαρξης οπτικής επαφής μεταξύ της συσκευής ανάγνωσης και της ετικέτας που περιείχε την ωφέλιμη πληροφορία [4].

Παρά τα πολλαπλά οφέλη που προσφέρουν, τα RFID δίκτυα μειονεκτούν σε ορισμένους τομείς, ενώ η διαδεδομένη χρήση τους έχει εγείρει ανησυχία τόσο στην κοινή γνώμη, όσο και στην επιστημονική κοινότητα. Η διασφάλιση των προσωπικών δεδομένων των χρηστών, η ανθεκτικότητα τους σε επιθέσεις και παρεμβολές, καθώς και η ανάγκη για υψηλή αξιοπιστία συχνά αποτελούν εμπόδια στην ευρύτερη υιοθέτηση τους [5]. Για να αντιμετωπιστούν αυτά τα προβλήματα, έχουν γίνει διαχρονικά προσπάθειες τυποποίησης των συσκευών ανάγνωσης και των ετικετών, έτσι ώστε οι κατασκευα-

στές να συμμορφώνονται σε πρότυπα που θα διασφαλίζουν την εφαρμογή των RFID τεχνολογιών. Ένα παράδειγμα τέτοιου προτύπου αποτελεί το EPC Gen2 το οποίο στοχεύει στην τυποποίηση RFID παθητικών πομποδεκτών υπερυψηλής συχνότητας, οι οποίοι είναι πλέον διαδεδομένοι στις αλυσίδες εφοδιασμού [6].

1.2 Αντικείμενο της εργασίας

Στόχος αυτής της διπλωματικής εργασίας είναι η παρουσίαση ενός μοντέλου που περιγράφει μια επίθεση άρνησης υπηρεσιών σε ένα δίκτυο RFID παθητικών ετικετών, με όρους θεωρίας παιγνίων.

Αναλυτικότερα, παρουσιάζονται οι αρχές λειτουργίας, οι ιδιότητες και οι περιορισμοί τέτοιων δικτύων, ενώ γίνεται αναφορά του ρόλου τους στην εξάπλωση του Internet of Things. Στην συνέχεια, ορίζονται χρήσιμες έννοιες σχετικά με τις επιθέσεις άρνησης υπηρεσιών σε ασύρματα δίκτυα RFID, και πιο συγκεκριμένα σε επιθέσεις που βασίζονται σε ασύρματες παρεμβολές από εισβολείς.

Ως απαραίτητη για την περαιτέρω ανάλυση, γίνεται μια σύντομη εισαγωγή στην θεωρία παιγνίων και ειδικότερα στα μη συνεργατικά παίγνια. Με βάση αυτήν την θεωρία επιχειρείται η μοντελοποίηση της συμπεριφοράς ενός δικτύου RFID που αποτελείται από μια συσκευή ανάγνωσης (reader), παθητικές ετικέτες κόμβους, και κόμβους εισβολείς οι οποίοι εισάγουν στο δίκτυο παρεμβολές με σκοπό την παρεμπόδιση της λειτουργίας των ωφέλιμων κόμβων. Κάθε κόμβος-ετικέτα που συμμετέχει στο δίκτυο συσχετίζεται με μια καλώς ορισμένη συνάρτηση χρησιμότητας (utility function) η οποία εξυπηρετεί δύο σκοπούς. Για τις κανονικές ετικέτες (normal tags), φανερώνει τον στόχο τους να εκπέμπουν με την απαιτούμενη ισχύ ώστε το σήμα τους να μπορεί να αποδιαμορφωθεί επιτυχώς από την συσκευή ανάγνωσης, ενώ παράλληλα εκφράζει και την ποινή που επιβάλλεται σε αυτές όταν η συμπεριφορά τους δεν είναι κοινωνική, δηλαδή όταν στην προσπάθεια τους να εκπέμψουν με την επιθυμητή ισχύ προκαλούν υψηλές παρεμβολές στο δίκτυο. Αντίστοιχα, η συνάρτηση χρησιμότητας για τις ετικέτες εισβολείς (intruder tags) εκφράζει τον στόχο τους να εισάγουν υψηλές παρεμβολές στο σύστημα, καθώς και την ποινή που τους επιβάλλεται για αυτή την συμπεριφορά τους.

Με βάση τα παραπάνω ορίζεται το πρόβλημα μετριασμού των παρεμβολών στο δίκτυο, το οποίο λαμβάνει υπ΄όψιν το ρίσκο - ποινή για τις παθητικές ετικέτες RFID (interference mitigation problem, IM). Στόχος αυτού του προβλήματος είναι η μεγιστοποίηση της τιμής της συνάρτησης χρησιμότητας για την κάθε παθητική ετικέτα. Λόγω της φύσης του προβλήματος, αυτό αναλύεται ως ένα μη συνεργατικό παίγνιο μεταξύ των ετικετών του δικτύου, και στην συνέχεια προσδιορίζεται το σημείο ισορροπίας Nash για το σύστημα. Τέλος, προτείνεται ένας κατανεμημένος, επαναληπτικός αλγόριθμος χαμηλής πολυπλοκότητας για τον προσδιορισμό αυτού του σημείου ισορροπίας, καθώς και μια ενδεικτική υλοποίηση του που δείχνει την σύγκλιση του συστήματος και παράγει αριθμητικά αποτελέσματα.

1.3 Δομή της εργασίας

Στο Κεφάλαιο 1 γίνεται μια σύντομη εισαγωγή στις ανάγκες που οδήγησαν στην ανάπτυξη της τεχνολογίας RFID και παρουσιάζονται συνοπτικά οι λύσεις που αυτή προσέφερε. Το πρώτο μέρος καταλήγει με την περιγραφή της διάρθρωσης της εργασίας.

Στο Κεφάλαιο 2 αναλύονται οι αρχές λειτουργίας και η σημασία της συγκεκριμένης τεχνολογίας και παρουσιάζονται τα τεχνικά χαρακτηριστικά της. Αναφέρονται πλεονεκτήματα και παραδείγματα εφαρμογών καθώς και οι περιορισμοί που προκύπτουν κατά την χρήση της. Σκοπός αυτού του κεφαλαίου είναι η εξοικείωση του αναγνώστη με την βασική ορολογία και τις έννοιες που απαντώνται στα δίκτυα RFID.

Στο Κεφάλαιο 3 παρουσιάζονται εν συντομία βασικές αρχές για την διασφάλιση ασύρματων δικτύων, και κατά επέκταση δικτύων RFID. Δίνονται ως παραδείγματα κατηγορίες επιθέσεων και αναλύεται ο τρόπος με τον οποίο παρεμποδίζουν την ομαλή λειτουργία ενός συστήματος, καθώς και η έκταση της επιβάρυνσης που συχνά προκαλείται. Στο τέλος του κεφαλαίου, επικεντρωνόμαστε στις επιθέσεις άρνησης υπηρεσιών.

Στο Κεφάλαιο 4 εισάγονται βασικές έννοιες από την θεωρία μη συνεργατικών παιγνίων που θα χρειαστούν στην συνέχεια. Έπειτα, παρουσιάζεται το υπό μελέτη δίκτυο RFID και τα τεχνικά χαρακτηριστικά του. Αφού οριστούν οι συναρτήσεις χρησιμότητας των ετικετών, η συμπεριφορά του συστήματος μοντελοποιείται ως ένα παίγνιο μετριασμού παρεμβολών.

Στο Κεφάλαιο 5, παρουσιάζεται ο αλγόριθμος IM με τον οποίο περιγράφεται η συμπεριφορά των παθητικών ετικετών σε ένα δίκτυο που συνυπάρχουν τόσο κανονικές ετικέτες, όσο και ετικέτες εισβολείς. Παρουσιάζεται η ιδέα πίσω από την ανάπτυξη αυτού του αλγορίθμου, και παρατίθεται ψευδοκώδικας ο οποίος σκιαγραφεί την υλοποίηση του.

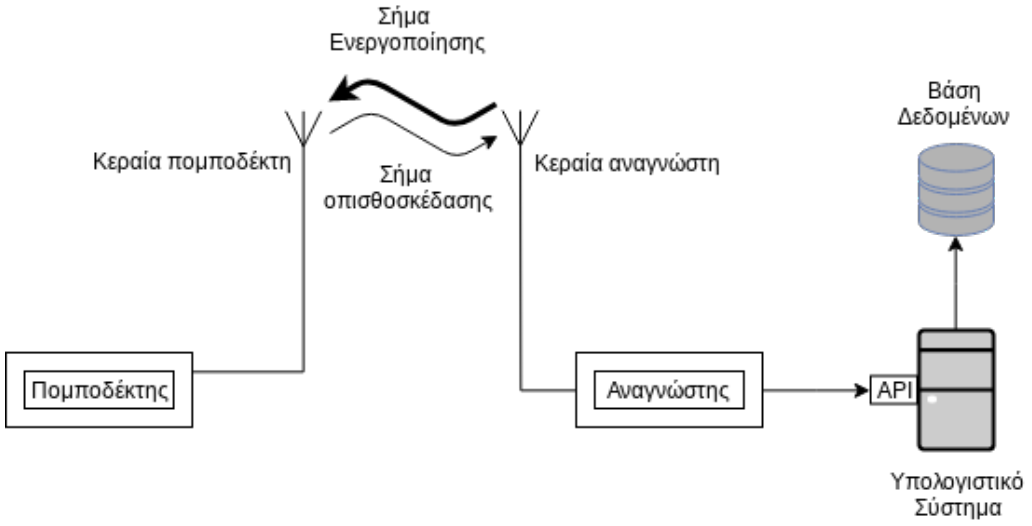
Στο Κεφάλαιο 6, γίνεται αναφορά στην παραμετροποίηση των μεγεθών που εμπλέκονται στον αλγόριθμο και παρουσιάζεται συνοπτικά η εκτέλεση του. Βάσει αυτής, παρατίθενται ενδεικτικές γραφικές παραστάσεις, που περιγράφουν την συμπεριφορά των ετικετών.

Στο τελευταίο κεφάλαιο, το οποίο αποτελεί τον επίλογο, βρίσκεται μια σύνοψη της εργασίας και αναφέρονται οι δυσκολίες που προέκυψαν κατά την εκπόνηση της. Τέλος, θίγονται εναλλακτικές της λογικής που ακολουθήθηκε και εντοπίζονται νέα πιθανά αντικείμενα για μελλοντική εργασία.

2 Τεχνολογίες RFID

2.1 Ορολογία και Αρχές Λειτουργίας

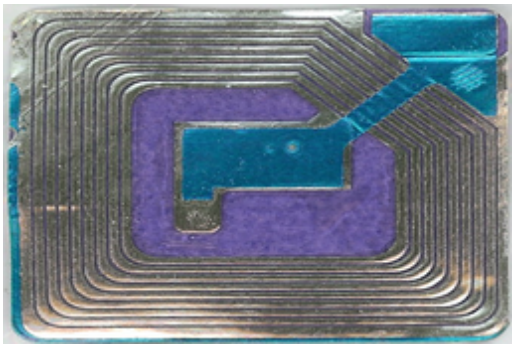
Με τον όρο RFID (Radio Frequency Identification, ταυτοποίηση μέσω ραδιοσυχνοτήτων) αναφερόμαστε σε ένα σύνολο τεχνολογιών που εκμεταλλεύονται την μετάδοση ηλεκτρομαγνητικής ακτινοβολίας για να επιτύχουν αυτοματοποιημένη αναγνώριση και παρακολούθηση αντικειμένων, χρησιμοποιώντας ειδικές συσκευές που ονομάζονται *πομποδέκτες* ή πιο απλά *ετικέτες* (στα αγγλικά συνήθως χρησιμοποιούνται οι όροι *transponders* ή *tags* αντίστοιχα). Ένα τυπικό δίκτυο RFID αποτελείται από τις ετικέτες και από μία ή περισσότερες συσκευές που ονομάζονται *αναγνώστες* (*readers*) [3], [6]. Οι ετικέτες RFID είναι υπεύθυνες για την αποθήκευση πληροφοριών και την ταυτοποίηση των αντικειμένων. Καθεμία από αυτές χαρακτηρίζεται από ένα μοναδικό αναγνωριστικό, το οποίο, μαζί με όσες άλλες πληροφορίες έχει αποθηκευμένες, μπορεί να μεταδώσει στον αναγνώστη. Ο αναγνώστης είναι υπεύθυνος για την συγκέντρωση αυτών των πληροφοριών από τις ετικέτες, την προσωρινή επεξεργασία τους, και συχνά την μετάδοση τους σε κάποιο κέντρο συλλογής δεδομένων, όπως ένα κεντρικό υπολογιστικό σύστημα [6].



Σχήμα 1: Σχηματικό παράδειγμα επικοινωνίας ενός παθητικού πομποδέκτη RFID με την συσκευή ανάγνωσης.

Ανάλογα με τον τρόπο λειτουργίας της, κάθε συσκευή που συμμετέχει στο δίκτυο RFID χαρακτηρίζεται ως *ενεργή* (*active*) ή *παθητική* (*passive*). Ενεργές ονομάζονται οι συσκευές οι οποίες είναι εξοπλισμένες με σύστημα παροχής ισχύος (παραδείγματος χάριν μπαταρία, συνεχή παροχή ρεύματος) και είναι ικανές να εκπέμπουν σήμα όποτε το απαιτούν οι ανάγκες λειτουργίας τους. Αντίθετα, οι παθητικές συσκευές δεν διαθέτουν τέτοιο σύστημα και η εκπομπή του σήματός τους εξαρτάται από την ενέργεια που τους μεταφέρεται σε μορφή ηλεκτρομαγνητικής ακτινοβολίας από κάποια άλλη συσκευή στο δίκτυο (Σχήμα 1). Ασφαλώς, αυτή η κατηγοριοποίηση δεν είναι απόλυτη. Σε ορισμένες εφαρμογές γίνεται χρήση *ημι-παθητικών ετικετών* (*semi-passive* ή *battery-assisted tags*). Οι ετικέτες αυτές, ενώ εκπέμπουν την ωφέλιμη πληροφορία όπως οι αντίστοιχες παθητικές ετικέτες, διαθέτουν και μια μπαταρία η οποία συχνά τροφοδοτεί κάποιον αισθητήρα στην συσκευή ή είναι υπεύθυνη για την παροχή ρεύματος στο κύκλωμα της ετικέτας. Η παρουσία αυτής της μπαταρίας δίνει την δυνατότητα στις ημι-παθητικές ετικέτες να εκπέμπουν σήμα υψηλότερης ισχύος, με αποτέλεσμα να λειτουργούν σε μεγαλύτερη εμβέλεια σε σχέση με τις παθητικές και να είναι, έστω και περιορισμένα, ενεργειακά αυτόνομες [2], [3].

Παρακάτω φαίνονται δύο παραδείγματα παθητικών ετικετών.



Σχήμα 2: Το κύκλωμα μιας παθητικής ετικέτας.

Σχήμα 3: Παθητική ετικέτα μιας χρήσης από αγώνες ταχύτητας.

Με βάση τον παραπάνω διαχωρισμό, τα δίκτυα RFID ταξινομούνται σε τρεις βασικές κατηγορίες [7]:

- Δίκτυα Ενεργού Αναγνώστη και Ενεργών Ετικετών (*Active Reader Active Tag Networks*)
- Δίκτυα Ενεργού Αναγνώστη και Παθητικών Ετικετών (*Active Reader Passive Tag Networks*)
- Δίκτυα Παθητικού Αναγνώστη και Ενεργών Ετικετών (*Passive Reader Active Tag Networks*)

Πέρα από τις διαφορές που παρουσιάζουν τα δίκτυα RFID με βάση την παροχή ισχύος του αναγνώστη και των ετικετών, σημαντικό κριτήριο για την επιλογή του κατάλληλου εξοπλισμού αποτελεί το μέγεθος της πληροφορίας που μπορούν να αποθηκεύσουν οι ετικέτες. Λόγω του ευρέος φάσματος εφαρμογών στις οποίες μπορούν να χρησιμοποιηθούν τα δίκτυα RFID, αλλά και λόγω της εξειδίκευσης στην λειτουργία τους που συχνά απαιτείται, η αποθηκευτική ικανότητα και ο τρόπος με τον οποίο οργανώνονται τα δεδομένα στις ετικέτες ποικίλει.

Το πλήθος των δεδομένων που μπορεί να αποθηκευτεί σε μια ετικέτα κυμαίνεται από ορισμένα bytes μέχρι αρκετά kilobytes. Εξαίρεση στο παραπάνω αποτελούν οι λεγόμενες *1-bit ετικέτες*. Οι συγκεκριμένες ετικέτες δεν διαθέτουν εσωτερική μνήμη, και η λειτουργία τους περιορίζεται στην αναγνώριση της παρουσίας τους ή της απουσίας τους από την συσκευή ανάγνωσης. Επειδή δεν διαθέτουν εσωτερικό τσιπ το κόστος κατασκευής τους είναι πολύ χαμηλό, και για αυτό χρησιμοποιούνται σε μεγάλες ποσότητες σε αντικλεπτικά συστήματα, όπως αυτά που διαθέτουν πολλά καταστήματα λιανικής (για παράδειγμα με την τοποθέτηση ετικετών σε ρούχα) [6].

Η οργάνωση της μνήμης σε μια ετικέτα, καθώς και το αν κάποια τμήματα αυτής είναι επανεγγράψιμα, εξαρτάται από τις απαιτήσεις της εκάστοτε εφαρμογής ή του κατασκευαστικού προτύπου που ακολουθείται. Για παράδειγμα, το πρότυπο EPC Class1 Gen2 (EPC Gen2) ορίζει μεταξύ άλλων τα παρακάτω τμήματα μη πτητικής μνήμης για παθητικές ετικέτες [8]:

- Τμήμα δεσμευμένης μνήμης το οποίο περιέχει δύο συνθηματικά. Το πρώτο ονομάζεται *kill password* και χρησιμοποιείται για την μόνιμη απενεργοποίηση της ετικέτας. Το δεύτερο αποτελεί το συνθηματικό πρόσβασης (*access passsword*) της ετικέτας.

- Τμήμα *EPC (Electronic Product Code)*, το οποίο περιέχει μεταξύ άλλων έναν κωδικό που χρησιμοποιείται για την ταυτοποίηση ενός συγκεκριμένου αγαθού. Το τμήμα αυτό είναι εγγράψιμο.

- Τμήμα *TID (Tag Identifier)*, το οποίο γράφεται από τον κατασκευαστή της ετικέτας, δεν μπορεί να μεταβληθεί και χρησιμεύει στην ταυτοποίηση της ετικέτας από τον αναγνώστη.

- Τμήμα επανεγγράψιμης μνήμης, το οποίο είναι στην διάθεση του χρήστη για την αποθήκευση λοιπών χρήσιμων πληροφοριών.

Με βάση τα παραπάνω, είναι φανερό ότι για τις ανάγκες αποθήκευσης και επεξεργασίας δεδομένων στις RFID ετικέτες, μπορούν να χρησιμοποιηθούν μνήμες διαφόρων τεχνολογιών. Στις απλές ετικέτες που δεν απαιτείται επανεγγραφή, συχνά χρησιμοποιείται μη πτητική μνήμη ROM (Read only Memory) η οποία προγραμματίζεται μόνο κατά την κατασκευή της ετικέτας και περιέχει τα αναγνωριστικά της

συσκευής. Σε παθητικές ετικέτες που υπάρχει η ανάγκη επανεγγραφής, η πιο διαδεδομένη μνήμη είναι η EEPROM (Electrically Erasable Programmable Read-Only Memory). Αυτού του είδους η μνήμη μπορεί να επανεγγραφεί προγραμματιστικά και, όπως η ROM, διατηρεί τα δεδομένα της ακόμα και όταν δεν υπάρχει τροφοδότηση με ρεύμα. Πρόσφατα, ως εναλλακτική των EEPROM, έχουν χρησιμοποιηθεί μνήμες FRAM (Ferromagnetic Random Access Memory) οι οποίες προσφέρουν υψηλότερη ταχύτητα εγγραφής, όμως λόγω του κόστους και προβλημάτων στην παραγωγή τους δε έχουν υιοθετηθεί ευρέως. Τέλος, σε ετικέτες μικροκυμάτων που διαθέτουν μπαταρία, χρησιμοποιούνται και μνήμες SRAM (Static Random Access Memory) οι οποίες προσφέρουν υψηλότερη ταχύτητα, όμως τα δεδομένα τους χάνονται όταν πάψει η τροφοδοσία τους [6].

Ένα ακόμα σημαντικό χαρακτηριστικό των δικτύων RFID είναι η *συχνότητα λειτουργίας* τους. Με αυτόν τον όρο, περιγράφουμε την συχνότητα με την οποία εκπέμπει ο αναγνώστης και σχετίζεται στενά με την εμβέλεια του σήματος. Η συχνότητα λειτουργίας ενός δικτύου ποικίλει και κυμαίνεται από ~30 kHz, έως περισσότερα από 5 GHz. Όσον αφορά την συχνότητα εκπομπής των ετικετών, στις περισσότερες περιπτώσεις είναι ίδια με αυτή του αναγνώστη, όμως η ισχύς του σήματός τους είναι συχνά αρκετές τάξεις μεγέθους χαμηλότερη [6].

Με βάση την συχνότητα λειτουργίας τους, μπορούμε να ταξινομήσουμε αδρομερώς τα περισσότερα δίκτυα RFID σε τέσσερις κατηγορίες [2], [5], [6]:

- *Δίκτυα Χαμηλής Συχνότητας* (*Low Frequency Networks, LF*). Η συχνότητά τους κυμαίνεται από 30 έως 300 kHz, αν και συνήθως τα δίκτυα που βρίσκονται σε αυτή την κατηγορία λειτουργούν στα 125 ή 134 kHz.

- *Δίκτυα Υψηλής Συχνότητας* (*High Frequency Networks, HF*). Η συχνότητά τους κυμαίνεται από 3 έως 30 MHz. Η πλειοψηφία των δικτύων αυτής της κατηγορίας λειτουργούν στα 13.56 MHz.

- *Δίκτυα Υπερυψηλής Συχνότητας* (*Ultra High Frequency Networks, UHF*). Αποτελούν τα πιο δημοφιλή συστήματα RFID και πολλά από αυτά ακολουθούν το πρότυπο EPC Gen2. Ανάλογα με την περιοχή που χρησιμοποιούνται λειτουργούν σε συγκεκριμένες συχνότητες. Για παράδειγμα, στην Ευρώπη η συχνότητα λειτουργία τους είναι συνήθως 865-868 MHz, ενώ στην Αμερική είναι 902-928 MHz.

- *Δίκτυα Μικροκυμάτων* (*Microwave Networks*). Η συνηθέστερες συχνότητες λειτουργίας αυτών των δικτύων είναι τα 2.45 ή 5.8 GHz.

2.2 Πλεονεκτήματα και εφαρμογές

Η χρήση τεχνολογιών RFID είναι ήδη ευρέως διαδεδομένη στην βιομηχανία και στην καθημερινή ζωή, και τα πλεονεκτήματά της αποτελούν παράγοντα προόδου για νέες εφαρμογές. Αυτή η τάση επιβεβαιώνεται τόσο από τις προοπτικές τους στις αγορές, όσο και από τον ρόλο τους στην ανάπτυξη του Internet of Things [9].

Οι λόγοι για την επιτυχία των δικτύων RFID είναι πολλοί. Σημαντικός παράγοντας στην διάδοση της χρήσης τους αποτελούν τα χαρακτηριστικά των συσκευών ανάγνωσης και των πομποδεκτών-ετικετών. Επειδή η επικοινωνία τους βασίζεται στην ανταλλαγή δεδομένων με την χρήση διαμορφωμένων ηλεκτρομαγνητικών κυμάτων, η σωστή λειτουργία του δικτύου δεν βασίζεται στην ύπαρξη οπτικής επαφής μεταξύ του αναγνώστη και των ετικετών. Αυτή η ιδιότητα καθιστά τις τεχνολογίες RFID πιο ευέλικτες σε σύγκριση με εναλλακτικές, όπως το barcode, καθώς επιτρέπει την τοποθέτησή τους στο εσωτερικό συσκευασιών ή άλλων αντικειμένων που πρέπει να αναγνωριστούν, χωρίς να επηρεάζεται η λειτουργία τους [7].

Σε αντίθεση με άλλα συστήματα ταυτοποίησης οι ετικέτες RFID έχουν συχνά την δυνατότητα να αποθηκεύουν, πέρα από το μοναδικό αναγνωριστικό, και άλλη ωφέλιμη πληροφορία. Αυτή η δυνατότητα κατανεμημένης αποθήκευσης δεδομένων, αυξάνει την συνολική ανοχή σφαλμάτων του συστήματος. Ακόμα, οι ετικέτες με ικανότητα επανεγγραφής, δίνουν την επιλογή στον χρήστη να τροποποιεί δυναμικά τα δεδομένα που βρίσκονται σε αυτές, χωρίς να υπάρχει η ανάγκη αντικατάστασής τους [10].

Δύο ακόμα σημαντικά πλεονεκτήματα της χρήσης των δικτύων RFID είναι η υψηλή αξιοπιστία τους, καθώς και το γεγονός ότι το κόστος του εξοπλισμού που απαιτείται είναι τα τελευταία χρόνια μειούμενο [11]. Παρά το γεγονός ότι το κόστος που απαιτείται για την αγορά και την αρχική εγκατάσταση ενός συστήματος RFID μπορεί να παραμένει σχετικά υψηλό, η συγκεκριμένη τεχνολογία προσφέρει έμμεσα οικονομικά οφέλη. Η αυτοματοποίηση που προσφέρει στην βιομηχανία λόγω της ταυτόχρονης ανάγνωσης πολλών ετικετών, μειώνει τον χρόνο που απαιτείται για την καταμέτρηση και τον έλεγχο αγαθών, ενώ ταυτόχρονα ελαττώνεται σημαντικά ο κίνδυνος ανθρώπινου σφάλματος [10].

Παρακάτω παρουσιάζονται συνοπτικά ορισμένες από τις εφαρμογές των δικτύων RFID:

- Αλυσίδες εφοδιασμού και αποθήκευση εμπορικών αγαθών. Οι συσκευασίες των προϊόντων και οι παλέτες μεταφοράς διαθέτουν ετικέτες οι οποίες, με την βοήθεια συσκευών ανάγνωσης επιτρέπουν την παρακολούθηση του φορτίου κατά την μεταφορά. Τα πλεονεκτήματα αυτής της εφαρμογής είναι η αυτοματοποίη-

ση της αποθήκευσης και της διανομής των προϊόντων, η μείωση των απωλειών λόγω καλύτερης παρακολούθησης, η ανίχνευση απομιμήσεων, καθώς και η πιο αποτελεσματική διαχείριση των αποθεμάτων, με παρακολούθηση πραγματικού χρόνου [5], [10].

- Έλεγχος πρόσβασης. Εδώ και καιρό οι ετικέτες RFID χρησιμοποιούνται ως ηλεκτρονικά κλειδιά σε χώρους εργασίας. Αν και παλαιότερα χρησιμοποιούνταν ετικέτες που λειτουργούσαν σε χαμηλές συχνότητες, πρόσφατα έχουν εισαχθεί ετικέτες στα 13.56 MHz, που προσφέρουν μεγαλύτερη εμβέλεια. Τα πλεονεκτήματα αυτής της χρήσης είναι η άνεση του εργαζομένου, και η μείωση της φθοράς των συστημάτων ασφαλείας. Όσο η συγκεκριμένη τεχνολογία αναπτύσσεται, αναμένεται να εφαρμοστεί για την λύση περισσότερων προβλημάτων στον χώρο εργασίας [10].

- Ανέπαφες πληρωμές. Ένα χαρακτηριστικό και διαδεδομένο παράδειγμα είναι οι σταθμοί των διοδίων που επιτρέπουν την γρηγορότερη διέλευση των διερχόμενων οχημάτων χωρίς οι οδηγοί να χρειάζεται να σταματήσουν. Αυτά τα συστήματα έχουν ήδη βρει εφαρμογή σε πολλές χώρες, και γίνεται πειραματική χρήση των ίδιων ενεργών ετικετών RFID σε καταστήματα εστίασης τύπου drive-through [10].

- Ηλεκτρονικό διαβατήριο. Μετά την εισαγωγή τους από το κράτος της Μαλαισίας το 1998 [5], πολλά από τα νεότερα διαβατήρια ενσωματώνουν ετικέτες RFID με βιομετρικές τεχνολογίες για την αποθήκευση δεδομένων του κατόχου. Η υιοθέτηση τους στις Ηνωμένες Πολιτείες, στην Ευρώπη και σε χώρες της Ανατολής είναι ήδη διαδεδομένη. Στόχος των ηλεκτρονικών διαβατηρίων είναι μεταξύ άλλων οι ταχύτερη εξυπηρέτηση των ταξιδιωτών, η αύξηση της ασφάλειας, καθώς και η μείωση περιπτώσεων πλαστοπροσωπίας [12].

- Μικροτσίπ για ζώα. Η ταυτοποίηση ζώων με την χρήση ετικετών RFID είναι σημαντική για την διαχείρισή τους σε κτηνοτροφικές μονάδες, καθώς και για τον περιορισμό εξάπλωσης ασθενειών ζώων. Για αυτές τις εφαρμογές συνήθως χρησιμοποιούνται ετικέτες που λειτουργούν σε χαμηλές (LF) ή υψηλές (HF) συχνότητες [5].

- Εισιτήρια μέσων μαζικής μεταφοράς. Σε ορισμένες χώρες παρατηρείται αντικατάσταση των χάρτινων εισιτηρίων με αντίστοιχα πλαστικά, τα οποία περιέχουν ετικέτες RFID που αλληλεπιδρούν με αναγνώστες στα μέσα μαζικής μεταφοράς. Αυτά μπορούν να χρησιμεύσουν στην αυτοματοποιημένη παρακολούθηση της κίνησης του επιβατικού κοινού και να συνεισφέρουν στην βελτίωση της οργάνωσης των δρομολογίων [13], [14].

- Νοσοκομεία και υγειονομική περίθαλψη. Συστήματα RFID χρησιμοποιούνται σε νοσοκομεία και χώρους περίθαλψης για την παρακολούθηση προμηθειών, τον έλεγχο πλαστών σκευασμάτων και την πραγματοποίηση ασφαλών συστημάτων που χρησιμεύουν στην φύλαξη του ιστορικού των ασθενών [5], [14].

- Ενσωμάτωση σε συστήματα με αισθητήρες. Οι ετικέτες RFID οι οποίες έχουν ενσωματωμένους αισθητήρες ανοίγουν τον δρόμο για ένα πλήθος νέων εφαρμογών, όπως η παρακολούθηση θερμοκρασίας και η παροχή φροντίδας σε ηλικιωμένους. Η τροφοδοσία αυτών των αισθητήρων μπορεί να βασίζεται στην ενέργεια που απορροφούν οι ετικέτες από το σήμα της συσκευής ανάγνωσης [5], ή, στην περίπτωση ημι-παθητικών ετικετών, από την συνυπάρχουσα μπαταρία [11].

- Αυτοματοποιημένες βιβλιοθήκες. Οι παθητικές ετικέτες RFID είναι χρήσιμες στην αποδοτικότερη λειτουργία των βιβλιοθηκών και την επίσπευση των καθημερινών εργασιών που απαιτούνται. Η χρήση τους αυτοματοποιεί τις διαδικασίες δανεισμού και της επιστροφής βιβλίων, ενώ επιτρέπει την απογραφή τους σε πραγματικό χρόνο, χωρίς την ανάγκη απομάκρυνσής τους από τα ράφια [5], [15].

2.3 Περιορισμοί

Παρά τα πλεονεκτήματα που προσφέρουν τα δίκτυα RFID, υπόκεινται, όπως και κάθε τεχνολογία σε περιορισμούς. Σε αυτή την ενότητα θα αναφέρουμε μερικούς από αυτούς, καθώς και τρόπους με τους οποίους ορισμένοι μπορούν να ξεπεραστούν.

Αν και η επιλογή του κατάλληλου είδους ετικέτας εξαρτάται από το περιβάλλον και τα χαρακτηριστικά της εφαρμογής, η έλλειψη κοινώς αποδεκτών προτύπων για την κατασκευή τους, επιτρέπει στις εταιρίες να χρησιμοποιούν ένα μεγάλο εύρος από πρωτόκολλα επικοινωνίας, και να αποθηκεύουν δεδομένα σε μορφές που τις εξυπηρετούν. Αυτό εμποδίζει την συνεργασία μεταξύ πολλών πλευρών, καθώς πρέπει να συμφωνηθούν παράμετροι όπως ο τύπος διαμόρφωσης της πληροφορίας και ο ρυθμός μετάδοσης δεδομένων [10]. Το συγκεκριμένο πρόβλημα παρουσιάζεται ακόμα και στις διαφορετικές συχνότητες λειτουργίας δικτύων που ανήκουν στην ίδια κατηγορία, ανάλογα με την χώρα χρήσης τους. Για αυτόν το λόγο, έχουν ήδη προταθεί και σχεδιαστεί αναγνώστες οι οποίοι είναι ικανοί να λειτουργούν σε ένα ευρύτερο φάσμα συχνοτήτων [16], [17].

Ένας ακόμα περιορισμός των RFID δικτύων, είναι η μέγιστη δυνατή απόσταση μεταξύ των ετικετών και του αναγνώστη, στην οποία μπορεί να πραγματοποιηθεί επιτυχής ανάγνωση της μεταδιδόμενης πληροφορίας. Αν και σε πολλές περιπτώσεις αυτή εξαρτάται από τα χαρακτηριστικά των πομποδεκτών και του αναγνώστη, σημαντικός περιοριστικός παράγοντας είναι και το περιβάλλον μετάδοσης του σήματος [18]. Μάλιστα, το σήμα των συσκευών RFID που λειτουργούν σε δίκτυα υπερυψηλών συχνοτήτων και μικροκυμάτων, εμποδίζεται από την παρουσία μετάλλων ή νερού, θέτοντας περιορισμούς στα αντικείμενα στα οποία μπορούν να τοποθετηθούν. Αυτό, μπορεί να αποτελέσει εμπόδιο στην υιοθέτηση τους σε εφαρμογές όπως η γεωργία και η παρακολούθηση αγροτικών προϊόντων. [16].

Σημαντική πρόκληση σε δίκτυα στα οποία συνυπάρχουν πολλαπλοί πομποδέκτες είναι η αντιμετώπιση συγκρούσεων που προκαλείται από την ταυτόχρονη προσπάθεια ανάγνωσης του σήματος από διαφορετικές ετικέτες. Αυτό συχνά οδηγεί σε απώλεια δεδομένων και μείωση της αξιοπιστίας του συστήματος. Για την αποφυγή τέτοιων φαινομένων, έχουν αναπτυχθεί αλγόριθμοι επίλυσης συγκρούσεων οι οποίοι όμως αυξάνουν το συνολικό οικονομικό κόστος της εφαρμογής. Η ανάπτυξη αυτών των αλγορίθμων αποσκοπεί στην μείωση του συνολικού χρόνου ανάγνωσης, και την αύξηση του αριθμού των ετικετών που μπορούν να διαβαστούν από τον κάθε αναγνώστη [10].

Όπως και άλλα πληροφοριακά συστήματα, έτσι και τα συστήματα RFID είναι ευάλωτα σε επιθέσεις και είναι δυνατόν να παραβιαστούν σε διάφορα στάδια της χρήσης τους. Παρακάτω αναφέρουμε επιγραμματικά ορισμένα από τα είδη αυτών των επιθέσε-

ων και αδυναμιών, καθώς και τους όρους με τον οποίους απαντώνται στην διεθνή βιβλιογραφία [19], [20]. Πολλές από αυτές θα αναπτυχθούν περαιτέρω στο επόμενο κεφάλαιο:

- Επιθέσεις ανάλυσης ισχύος (Power analysis)
- Επιθέσεις υποκλοπής (Eavesdropping)
- Επιθέσεις ενδιάμεσου (Man in the middle attacks)
- Επιθέσεις άρνησης υπηρεσιών (Denial of service attacks)
- Επιθέσεις πλαστογραφίας (Spoofing)
- Επιθέσεις κλωνοποίησης (Cloning)
- Επιθέσεις επανάληψης μηνύματος (Replay attack)

Τέλος, σημαντικός κίνδυνος είναι και η πιθανότητα παρακολούθησης, και η διαρροή προσωπικών δεδομένων. Σε αντίθεση με τα προηγούμενα, η παρακολούθηση αποτελεί απειλή για το ίδιο το άτομο. Το ενδεχόμενο όλο και περισσότερα οικιακά αντικείμενα να διαθέτουν τεχνολογίες RFID έχει εγείρει ανησυχίες σχετικά με την διασφάλιση των προσωπικών δεδομένων των χρηστών [21], [22]. Οι πληροφορίες που θα συγκεντρώνονται από αυτά τα δίκτυα θα μπορούσαν να χρησιμοποιηθούν για την παρακολούθηση των κινήσεων, καθώς και των καταναλωτικών συνηθειών τους. Μια λύση για αυτό το πρόβλημα είναι η ύπαρξη κωδικού ο οποίος απενεργοποιεί μόνιμα την λειτουργία του κάθε πομποδέκτη [19], [23].

3 Επιθέσεις σε δίκτυα RFID

3.1 Περί ασφάλειας ασύρματων δικτύων

Όπως αναφέρθηκε, η εξάπλωση του Internet of Things έχει πολλαπλά οφέλη. Ανάμεσα τους, προβλέπεται η δημιουργία νέων τεχνολογιών και εφαρμογών σε υπηρεσίες που βασίζονται σε πληροφορίες σχετικά με την ταυτοποίηση αντικειμένων, την κατάσταση και την θέση κόμβων του δικτύου, καθώς και η συμβολή τους σε κοινωνικές υπηρεσίες που θα βελτιώσουν την ποιότητα ζωής. Εξέχουσα θέση, ανάμεσα σε άλλες τεχνολογίες που καθιστούν το Internet of Things εφικτό (για παράδειγμα το Σύστημα Γεωγραφικών Πληροφοριών, GIS, και το Παγκόσμιο Σύστημα Στιγματοθέτησης, GPS), έχουν και οι τεχνολογίες RFID [24], [25].

Αυτή ακριβώς η σημασία τους, καθιστά την ανάγκη εύρεσης λύσεων στα προβλήματα ασφάλειας επιτακτική. Οι δυσκολίες που παρουσιάζονται στην διασφάλιση των δικτύων RFID συχνά προέρχονται από τα εγγενή χαρακτηριστικά τους. Για παράδειγμα, οι ετικέτες που συμμετέχουν στο δίκτυο έχουν πολύ περιορισμένους πόρους και χαμηλή υπολογιστική ισχύ. Αυτός είναι επιβαρυντικός παράγοντας για την υλοποίηση συμβατικών μηχανισμών προστασίας, η εφαρμογή των οποίων περιορίζεται στις συσκευές ανάγνωσης και στα υπολογιστικά συστήματα με τα οποία επικοινωνούν [26]. Επιπλέον, πρέπει να ληφθεί υπ'όψιν η ασύρματη και κατανεμημένη φύση αυτών των συστημάτων. Σε αντίθεση με τα ενσύρματα δίκτυα, τα στοιχεία των οποίων προστατεύονται τόσο από κεντρικούς όσο και από ατομικούς μηχανισμούς (για παράδειγμα firewalls), στα δίκτυα RFID οι ετικέτες και οι συσκευές ανάγνωσης λειτουργούν σε ένα συχνά ασταθές και δυνητικά θορυβώδες (όσον αφορά τις πιθανές παρεμβολές) περιβάλλον. Αυτή η ιδιαιτερότητα επιτρέπει σε πολλές περιπτώσεις την εξαπόλυση κατανεμημένων επιθέσεων προς τις συσκευές του ασύρματου δικτύου. Επειδή η ταχεία εξέλιξη της τεχνολογίας RFID συνοδεύεται από την εμφάνιση νέων απειλών, υπάρχει η ανάγκη για την μοντελοποίησή τους [27].

Για την ασφαλή και αποτελεσματική λειτουργία τους, τα ασύρματα δίκτυα, και κατά επέκταση τα δίκτυα RFID, πρέπει να πληρούν ορισμένες προδιαγραφές για την αντιμετώπιση πιθανών επιθέσεων σε όλα τα επίπεδα (ή στρώματα) που τα διέπουν. Εδώ με τον όρο ''επίπεδο'' εννοούμε τον λογικό διαχωρισμό των τεχνολογιών και των μέσων που χρησιμοποιούνται για την υλοποίησή τους (για παράδειγμα, το φυσικό στρώμα, το επίπεδο μεταφοράς, το επίπεδο δικτύου, το επίπεδο εφαρμογής και ούτω καθεξής) [27]. Στην συνέχεια αναφέρονται τέσσερα από τα χαρακτηριστικά ασφαλείας αυτών των δικτύων:

- *Αυθεντικοποίηση (Authentication).* Με τον όρο αυθεντικοποίηση (ή αυθεντικότητα) δηλώνουμε την επαλήθευση της πραγματικής ταυτότητας ενός κόμβου του δικτύου, έτσι ώστε να είναι δυνατός ο διαχωρισμός του από μη εξουσιοδοτημένα στοιχεία μέσα στο σύστημα [28]. Πιο συγκεκριμένα για τα δίκτυα RFID, η παρουσία ενός μη εξουσιοδοτημένου πομποδέκτη μπορεί να προκαλέσει διαταραχή στην ομαλή λειτουργία του συστήματος, ενώ η παρουσία μιας μη εξουσιοδοτημένης συσκευής ανάγνωσης μπορεί να οδηγήσει σε υποκλοπή πληροφοριών και πιθανή κακόβουλη χρήση τους [29]. Σημαντικό παράγοντα στην αυθεντικοποίηση αποτελεί και η εξακρίβωση της προέλευσης των δεδομένων που φτάνουν σε έναν κόμβο του δικτύου [30].

- *Εμπιστευτικότητα (Confidentiality).* Με τον όρο εμπιστευτικότητα αναφερόμαστε στον περιορισμό της πρόσβασης των δεδομένων που μεταδίδονται στο δίκτυο μεταξύ των στοιχείων του, έτσι ώστε να μην συμμετέχουν μη εξουσιοδοτημένοι κόμβοι στην επικοινωνία [28]. Στα δίκτυα RFID αποτελεί παράγοντα κινδύνου καθώς η επικοινωνία αυτή, μεταξύ του αναγνώστη και των ετικετών πραγματοποιείται μέσω ενός ασύρματου, μη ασφαλούς καναλιού [29].

- *Ακεραιότητα δεδομένων (Data Integrity).* Με τον όρο ακεραιότητα δηλώνουμε την αποθήκευση και την μεταφορά των δεδομένων μεταξύ κόμβων του συστήματος, χωρίς να υπάρξει καμία τροποποίηση της πληροφορίας που περιέχουν. Αυτή η τροποποίηση μπορεί να συνίσταται στην μεταβολή της ωφέλιμης πληροφορίας ή και στην καταστροφή της. Ένα παράδειγμα απώλειας της ακεραιότητας δεδομένων σε δίκτυα RFID είναι η τροποποίηση της πληροφορίας που βρίσκεται αποθηκευμένη στις ετικέτες, και στην συνέχεια η μετάδοση της στην συσκευή ανάγνωσης [28], [29], [30].

- *Διαθεσιμότητα (Availability).* Με τον όρο διαθεσιμότητα αναφερόμαστε στην ικανότητα του δικτύου να είναι λειτουργικό ανά πάσα στιγμή για τους εξουσιοδοτημένους χρήστες [30]. Οι επιθέσεις οι οποίες έχουν ως σκοπό την (μόνιμη ή προσωρινή) παρεμπόδιση της ομαλής λειτουργίας του δικτύου ονομάζονται επιθέσεις άρνησης υπηρεσιών [28]. Δύο παραδείγματα τέτοιων ενεργειών εναντίων δικτύων RFID αποτελούν οι επιθέσεις με την χρήση σημάτων παρεμβολής από ισχυρούς πομπούς, καθώς και η εκτέλεση εντολών απενεργοποίησης σε ετικέτες που διαθέτουν αυτή την δυνατότητα [29].

3.2 Κατηγορίες επιθέσεων

Ο σχηματισμός συνολικής εικόνας του προβλήματος διασφάλισης των δικτύων RFID και η κατηγοριοποίηση των απειλών που αντιμετωπίζουν, αποτελούν ένα πρόβλημα η δυσκολία του οποίου συνεχώς αυξάνεται λόγω της γρήγορης εξέλιξής τους. Ασφαλώς, η ταξινόμηση που επιχειρείται ποικίλει ανάλογα με τις ανάγκες της εκάστοτε ανάλυσης. Για παράδειγμα, στο [27] η ταξινόμηση αυτή γίνεται με βάση το επίπεδο του συστήματος RFID που βάλλεται και των ευπαθειών που εκμεταλλεύονται οι επιτιθέμενοι. Στα [31], [32], [33], οι συγγραφείς επικεντρώνονται στις απειλές κατά της διαφύλαξης των προσωπικών δεδομένων και την προστασία της ιδιωτικότητας, ενώ στο [34] προτείνεται μια λεπτομερής ταξινόμηση των δικτύων επιχειρηματικών διαδικασιών, και των πληροφοριακών ρίσκων [27]. Σε αυτή την ενότητα θα περιγράψουμε κατηγορίες επιθέσεων σε δίκτυα RFID, προτείνοντας τρόπους αντιμετώπισης, και μέσα για τον μετριασμό των επιπτώσεών τους.

Σημαντικό εργαλείο για την διευκόλυνση εξαπόλυσης επιθέσεων και εύρεσης του ακριβούς τρόπου λειτουργίας ενός συστήματος RFID είναι η *ανάστροφη μηχανική ανάλυση* του (*reverse engineering*). Για παράδειγμα, αναλογιζόμενοι τα ζητήματα διασφάλισης προσωπικών δεδομένων στα ηλεκτρονικά διαβατήρια, ένας επιτιθέμενος μπορεί να αποκτήσει πρόσβαση στο κύκλωμα και να προσπελάσει την μνήμη του με σκοπό την εύρεση του κωδικού ασφαλείας του και την ανακάλυψη βιομετρικών και προσωπικών δεδομένων. Η τεχνική ικανότητα και ο εξοπλισμός που απαιτείται για την διάπραξη τέτοιων επιθέσεων ποικίλει από εργαλεία χαμηλού κόστους που είναι εύκολα διαθέσιμα, μέχρι δυσεύρετο εξοπλισμό που χρησιμοποιείται από τεχνικά ικανές ομάδες ατόμων. Δυστυχώς, οι μέθοδοι για τις επιθέσεις ανάλυσης σε ολοκληρωμένα συστήματα εφαρμογών είναι γνωστές και η πρόσβαση σε αυτές είναι εύκολη [35]. Ένα παράδειγμα για την αντιμετώπιση τέτοιων φαινομένων παραβίασης είναι η εγκατάσταση μηχανισμού στους πομποδέκτες που θα ανιχνεύει εγκαίρως την απόπειρα παραβίασής του [19].

Η κατηγορία των επιθέσεων που εκμεταλλεύονται τις αυξομοιώσεις στην κατανάλωση ισχύος των συσκευών του δικτύου ονομάζονται *επιθέσεις ανάλυσης ισχύος* (*power analysis attacks*). Καθώς το μοτίβο εκπομπής των συσκευών είναι διαφορετικό όταν γίνεται ανάγνωση λανθασμένων bits από πληροφορίες ασφαλείας, οι επιθέσεις αυτές έχουν αποδειχθεί εξαιρετικά αποτελεσματικές, οδηγώντας ακόμα και σε πλήρη ανάκτηση κρυπτογραφικών κλειδιών [36], [37]. Οι συνηθέστεροι τρόποι αντιμετώπισης αυτών των επιθέσεων είναι το φιλτράρισμα των σημάτων ισχύος και η τυχαιοποιημένη καθυστέρηση των απαιτούμενων υπολογισμών. Στον σχεδιασμό ορισμένων έξυπνων καρτών μια ακόμα μέθοδος αντιμετώπισης είναι η προσθήκη ενός στοιχείου που καταναλώνει τυχαίες ποσότητες ισχύος. Μια τέτοια προσέγγιση, αν και δυνητικά αποτελεσματική, ενέχει κινδύνους για τα συστήματα RFID, καθώς η ελαχιστοποίηση

της κατανάλωσης ισχύος αποτελεί προτεραιότητα [19].

Στην συνέχεια αναφερόμαστε στις *επιθέσεις υποκλοπής* (*eavesdropping*) και τις *επιθέσεις ενδιάμεσου* (*man-in-the-middle attacks*). Επειδή η επικοινωνία μεταξύ των πομποδεκτών και του αναγνώστη γίνεται ασύρματα, υπάρχει το ρίσκο η πληροφορία που ανταλλάσσεται να υποκλαπεί από κάποιον που ''κρυφακούει'' [38]. Μάλιστα, σε αυτές τις παθητικές επιθέσεις υποκλοπής, ο επιτιθέμενος πέρα από την ωφέλιμη πληροφορία που μεταδίδεται, μπορεί να συγκεντρώσει μεταδεδομένα σχετικά με την επικοινωνία και τα πρωτόκολλα που χρησιμοποιούνται [39]. Αξίζει να σημειωθεί ότι επειδή οι παθητικοί πομποδέκτες RFID έχουν συνήθως περιορισμένη εμβέλεια εκπομπής, σε σύγκριση με τους ενεργούς, είναι ανθεκτικότεροι σε τέτοιους είδους επιθέσεις υποκλοπής [19], [40]. Πιθανές λύσεις για αυτά τα προβλήματα είναι η εγκατάσταση ασφαλούς διαύλου επικοινωνίας μεταξύ των στοιχείων του δικτύου, καθώς και η κρυπτογράφηση της πληροφορίας που μεταδίδεται [19].

Αντίστοιχα στις επιθέσεις ενδιάμεσου, ανάλογα και με την τοπολογία του δικτύου, ένα κακόβουλο στοιχείο μπορεί να παρεμβληθεί ανάμεσα σε δύο εξουσιοδοτημένους κόμβους, και να αλλοιώσει σε πραγματικό χρόνο την μεταδιδόμενη πληροφορία, χωρίς αυτό να γίνεται αντιληπτό. Ακόμα και αν δεχτεί μη έγκυρα δεδομένα, ο παραλήπτης δεν είναι πάντα σε θέση να αναγνωρίσει την επίθεση, και έτσι θα θεωρήσει ότι η αποτυχημένη επικοινωνία είναι προσωρινή και οφείλεται σε σφάλματα δικτύου. Τα συστήματα RFID είναι ιδιαιτέρως ευάλωτα σε αυτές τις επιθέσεις, καθώς οι πομποδέκτες είναι μικροί σε μέγεθος και φθηνοί σε κόστος, κάτι το οποίο συνήθως σημαίνει ότι δεν διαθέτουν εκλεπτυσμένα κυκλώματα προστασίας [19], [38].

Σχήμα 4: Σχηματικό παράδειγμα επικοινωνίας παθητικής ετικέτας, παρουσία κακόβουλου ενδιάμεσου κόμβου.

Ένα ακόμα είδος επιθέσεων οι οποίες είναι δυνατές απέναντι σε δίκτυα RFID είναι οι *επιθέσεις επανάληψης μηνύματος* (*replay attacks*), οι οποίες ουσιαστικά στοχεύουν στην λανθασμένη αυθεντικοποίηση ενός μη εξουσιοδοτημένου στοιχείου του συστήματος και βάλλουν κατά τις ακεραιότητας των δεδομένων του. Για την πραγματοποίηση αυτών των επιθέσεων, ένας εισβολέας αρχικά υποκλέπτει το μήνυμα που στέλνεται

μεταξύ εξουσιοδοτημένων στοιχείων του δικτύου. Σε μετέπειτα στιγμή, αποστέλλει αυτό το μήνυμα ξανά με αποτέλεσμα ο παραλήπτης να θεωρεί ότι επικοινωνεί με ένα εξουσιοδοτημένο κόμβο του δικτύου. Ένα απλό παράδειγμα μιας τέτοιας επίθεσης είναι η επανάληψη αποστολής μηνύματος που είχε υποκλαπεί σε κάποιο σύστημα πρόσβασης ή σύστημα ταυτοποίησης RFID. Αυτό θα είχε ως αποτέλεσμα την έγκριση πρόσβασης ή την λανθασμένη ταυτοποίηση της ετικέτας εισβολέα. Για την επιτυχή αντιμετώπιση τέτοιων φαινομένων είναι αναγκαία η πρόβλεψη για την συμπερίληψη κρυπτογραφικά ψευδοτυχαίων δεδομένων στα μηνύματα που ανταλλάσσονται μεταξύ των κόμβων του δικτύου [36], [41].

Πέρα από τις επιθέσεις επανάληψης μηνύματος, σημαντική απειλή για τα δίκτυα RFID αποτελούν και οι *επιθέσεις κλωνοποίησης* (*cloning attacks*). Για να είναι επιτυχής μια τέτοια επίθεση, ο επιτιθέμενος πρέπει να αντιγράψει την πληροφορία που περιέχεται σε μια ετικέτα του δικτύου, να εγκαταστήσει αυτή την πληροφορία σε μια νέα, δική του ετικέτα, και στην συνέχεια να την εισάγει στο δίκτυο. Αυτή η αντιγραφή μπορεί να αποδειχτεί εύκολη, καθώς δεν έχει υψηλό κόστος, ούτε απαιτεί εξειδίκευση από τον επιτιθέμενο λόγω της μεγάλης διαθεσιμότητας εγγράψιμων και επαναπρογραμματιζόμενων ετικετών. Στην περίπτωση που οι ετικέτες δεν διαθέτουν μηχανισμούς ασφαλείας, τότε η επιτυχημένη κλωνοποίηση έγκειται απλά στην αντιγραφή του κωδικού ταυτοποίησης και λοιπών δεδομένων που περιέχει μια εξουσιοδοτημένη ετικέτα. Ασφαλώς, η προσπάθεια που πρέπει να καταβληθεί για δημιουργία της ετικέτας κλώνου είναι ανάλογη της πολυπλοκότητας των μέτρων ασφαλείας που έχουν χρησιμοποιηθεί για την προστασία των πομποδεκτών του δικτύου [27], [38], [41].

Μια παρεμφερής, με την κλωνοποίηση, κατηγορία επιθέσεων είναι οι *επιθέσεις πλαστογραφίας* (*spoofing*). Η βασική διαφορά τους είναι ότι στις επιθέσεις πλαστογραφίας δεν πραγματοποιείται αντιγραφή δεδομένων σε μια νέα φυσική RFID ετικέτα. Αντιθέτως, ορίζεται απλά ως η επαναπροώθηση ενός έγκυρου μηνύματος από ένα μη εξουσιοδοτημένο στοιχείο του δικτύου. Επιπλέον, αυτές οι επιθέσεις δεν περιορίζονται μόνο σε ετικέτες, αλλά επεκτείνονται και στην πλαστογραφία σήματος από συσκευές ανάγνωσης. Η επιτυχία αυτών των επιθέσεων απαιτεί ειδικό εξοπλισμό για την αναπαραγωγή του σήματος, και ο επιτιθέμενος πρέπει να έχει πλήρη πρόσβαση στους υφιστάμενους διαύλους επικοινωνίας των στοιχείων του συστήματος, καθώς και γνώση τυχόν πρωτοκόλλων ή μυστικών που χρησιμοποιούνται κατά την διαδικασία αυθεντικοποίησης [22], [27], [41].

3.3 Επιθέσεις άρνησης υπηρεσιών

Οι επιθέσεις που ανήκουν στις κατηγορίες που περιγράφηκαν μέχρι στιγμής, έχουν ως κοινό στοιχείο το στόχο τους να βλάψουν ένα ασύρματο δίκτυο RFID με έναν ή περισσότερους από τους παρακάτω τρόπους:

- Να πλήξουν την ακεραιότητα των δεδομένων που μεταφέρονται από τα εξουσιοδοτημένα στοιχεία του δικτύου.
- Να παραβιάσουν την εμπιστευτικότητα στην επικοινωνία των κόμβων του συστήματος.
- Να διαταράξουν τις διαδικασίες αυθεντικοποίησης του δικτύου και να αποκρύψουν την παρουσία κακόβουλων στοιχείων σε αυτό.

Πέραν αυτών τα δίκτυα RFID οφείλουν να προστατεύονται και από επιθέσεις άρνησης υπηρεσιών, που βάλλουν κατά της διαθεσιμότητάς τους, εξασφαλίζοντας την απρόσκοπτη επικοινωνία μεταξύ των συσκευών ανάγνωσης και των πομποδεκτών. Η πρόληψη και αναγνώριση τέτοιων επιθέσεων αποτελεί γνωστό πρόβλημα και δεν μπορεί να επιλυθεί με την χρήση κρυπτογραφίας [42].

Ένα απλός, αλλά αποτελεσματικός τρόπος για την διακοπή της λειτουργικότητας του δικτύου είναι η υλική καταστροφή ή η αφαίρεση των ετικετών και του αναγνώστη. Η συχνή απουσία επιτήρησης των ετικετών διευκολύνει την χρήση μηχανικών (για παράδειγμα σπάσιμο, ή αφαίρεση της κεραίας τους) και χημικών μέσων για την εξουδετέρωση τους. Ειδικά οι παθητικές ετικέτες που χρησιμοποιούνται σε εφοδιαστικές αλυσίδες, αντιμετωπίζονται ως αναλώσιμα αντικείμενα καθώς ενδέχεται να καταστραφούν κατά την μεταχείριση των αγαθών που συνοδεύουν. Παρότι η καταπόνησή τους λόγω περιβαλλοντικών συνθηκών έχει προβλεφθεί κατά την κατασκευή τους, οι λειτουργία των ετικετών μπορεί να υποβαθμιστεί και από παράγοντες όπως η θερμοκρασία και η υγρασία [34].

Μια ακόμη ευπάθεια που παρουσιάζουν οι ετικέτες RFID είναι η ευαισθησία τους στον στατικό ηλεκτρισμό. Η ζημιά που προκαλείται στο εσωτερικό κύκλωμα της ετικέτας είναι ακαριαία, και συχνά μπορεί να οφείλεται σε ακούσια εκφόρτιση από το περιβάλλον λειτουργίας της (για παράδειγμα από την παρουσία της πάνω σε ιμάντες μεταφοράς αποσκευών). Αυτό το μειονέκτημα εκμεταλλεύονται επιτιθέμενοι, χρησιμοποιώντας συσκευές (RFID Zappers) ικανές να παράγουν ισχυρό ηλεκτρομαγνητικό πεδίο με εσωτερικά πηνία που διαθέτουν. Μάλιστα, η χρήση τέτοιων συσκευών εναντίων παθητικών ετικετών μπορεί να τις απενεργοποιήσει μόνιμα [27].

Στα πλαίσια των χαρακτηριστικών ασφαλείας τους, πολλές ετικέτες διαθέτουν εγκατεστημένους μηχανισμούς που επιτρέπουν στους χρήστες να τις καταστήσουν μη

λειτουργικές. Διαδεδομένο παράδειγμα αποτελούν οι ετικέτες που παράγονται σύμφωνα με το πρότυπο EPC Gen2, οι οποίες διαθέτουν στην εσωτερική τους μνήμη κωδικό για την μόνιμη ή προσωρινή απενεργοποίηση τους. Διάφορα άλλα πρότυπα χρησιμοποιούν παρόμοιους μηχανισμούς (lock commands) ώστε να είναι σε θέση να εμποδίζουν τον επαναπρογραμματισμό ετικετών. Αν οι κωδικοί που χρησιμοποιούνται για την υλοποίηση αυτής της λειτουργικότητας είναι χαμηλής πολυπλοκότητας, τότε μπορούν να παραβιαστούν ακόμα και με επιθέσεις ωμής βίας, δηλαδή ανακαλύπτοντας τον κωδικό με αλλεπάλληλες δοκιμές. [41].

Τέλος, πέρα από τις παθητικές παρεμβολές που υφίστανται τα ασύρματα δίκτυα RFID και οφείλονται στο περιβάλλον στο οποίο λειτουργούν, οι επιτιθέμενοι μπορούν ενεργά να παράξουν ισχυρά σήματα παρεμβολών για την παρεμπόδιση της επικοινωνίας των πομποδεκτών με τις συσκευές ανάγνωσης (jamming). Οι επιθέσεις αυτές δρουν στο φυσικό στρώμα επικοινωνίας του συστήματος, και το σήμα που χρησιμοποιείται έχει την συχνότητα λειτουργίας του δικτύου [27]. Οι συσκευές-εισβολείς μπορούν να παράγουν αυτό το σήμα ως συνεχή θόρυβο, ή να παραμένουν αδρανείς μέχρι να ανιχνεύσουν την παρουσία ωφέλιμου σήματος [30]. Σε πολλές περιπτώσεις, εξαπολύονται σε συνδυασμό με άλλες επιθέσεις με σκοπό την δυσχέρανση της αντιμετώπισής τους [34]. Μεταξύ άλλων, για την πρόληψη επιθέσεων άρνησης υπηρεσιών που βασίζονται σε ασύρματες παρεμβολές, μπορούν να χρησιμοποιηθούν τεχνικές παρακολούθησης του διαύλου επικοινωνίας, ώστε να εντοπίζονται συσκευές που παράγουν σήματα με ισχύ υψηλότερη ενός ανεκτού ορίου [19].

4 Μοντελοποίηση του προβλήματος ως μη συνεργατικό παίγνιο

4.1 Εισαγωγή

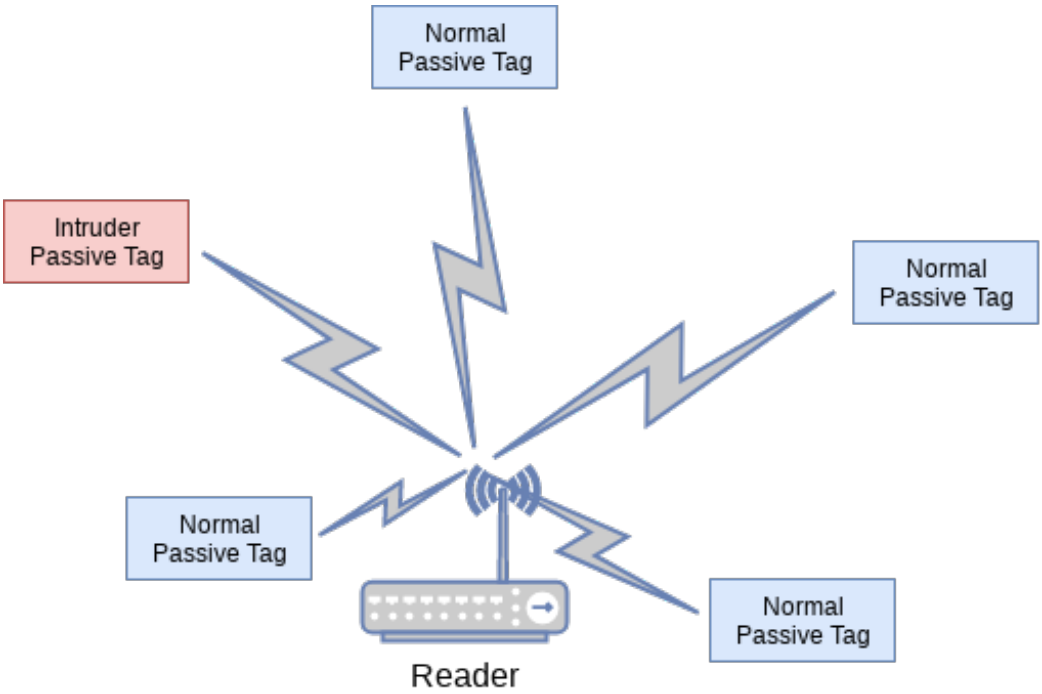
Η θεωρία παιγνίων αποτελεί ένα σύνολο από αναλυτικά εργαλεία, για την κατανόηση φαινομένων στα οποία αλληλεπιδρούν οντότητες ικανές να αποφασίζουν. Βασική προϋπόθεση αυτής της θεωρίας είναι ότι οι αποφάσεις λαμβάνονται ορθολογικά (δηλαδή οι οντότητες προσπαθούν να επιτύχουν καλά ορισμένους στόχους) και στρατηγικά (λαμβάνουν δηλαδή υπ΄όψιν τους την γνώση ή την προσδοκία που έχουν σχετικά με τις αποφάσεις των υπολοίπων).

Σε όλα τα μοντέλα στα οποία χρησιμοποιείται η θεωρία παιγνίων, κεντρική οντότητα είναι ο παίκτης - δράστης. Ως παίκτης μπορεί να ερμηνευτεί η κάθε μοναδική οντότητα του συστήματος, ή ένα σύνολο από οντότητες που λαμβάνουν αποφάσεις. Έχοντας καθορίσει το σύνολο των παικτών, μπορούμε να διακρίνουμε δύο περιπτώσεις μοντέλων: αυτά για τα οποία μελετάμε τις δράσεις και τις αποφάσεις που λαμβάνουν μεμονωμένοι παίκτες, και αυτά στα οποία μελετάμε τις από κοινού πράξεις και τις αποφάσεις ενός συνόλου παικτών. Στην πρώτη περίπτωση αναφερόμαστε σε *μη συνεργατικά (non-cooperative)* παίγνια, ενώ στην δεύτερη σε *συνεργατικά (cooperative)* [43].

Χρησιμοποιώντας το θεωρητικό πλαίσιο των μη συνεργατικών παιγνίων, θα μοντελοποιήσουμε την συμπεριφορά ενός δικτύου ενεργού αναγνώστη και παθητικών ετικετών το οποίο βρίσκεται υπό επίθεση άρνησης υπηρεσιών. Για τον σκοπό αυτό διαχωρίζουμε τους παθητικούς πομποδέκτες που βρίσκονται στο δίκτυο σε δύο κατηγορίες:

- *Κανονικές ετικέτες (normal tags).* Πρόκειται για τις ετικέτες που αναμένονται να είναι στο συγκεκριμένο RFID δίκτυο ώστε να παράγουν ωφέλιμο έργο. Στόχος τους είναι η μεγιστοποίηση της διεκπεραιωτικής ικανότητάς τους (throughput) και η επιτυχής αποκωδικοποίηση του σήματός τους από την συσκευή ανάγνωσης.
- *Ετικέτες εισβολείς (intruder tags).* Πρόκειται για τις ετικέτες που βρίσκονται στο δίκτυο για να πραγματοποιήσουν την επίθεση άρνησης υπηρεσιών. Στόχος τους είναι η παρεμπόδιση της ομαλής λειτουργίας του δικτύου με την εισαγωγή υψηλών επιπέδων παρεμβολών.

Για την μελέτη της συμπεριφοράς των παθητικών ετικετών του δικτύου (είτε κανονικών, είτε εισβολέων) σε ένα κοινό πλαίσιο βελτιστοποίησης, εισάγουμε την έννοια της *συνάρτησης χρησιμότητας (utility function)*. Αυτή η συνάρτηση χαρακτηρίζει την συμπεριφορά των ετικετών, και επειδή εκφράζει τους στόχους τους, θα είναι διαφορετική για τις κανονικές και τις παθητικές ετικέτες.



Σχήμα 5: Σχηματικό παράδειγμα δικτύου RFID που περιέχει εισβολέα, με σκοπό να εκπέμψει σήμα οπισθοσκέδασης υψηλής ισχύος και να μειώσει το SINR των κανονικών ετικετών.

4.2 Περιγραφή του δικτύου

Υποθέτουμε ένα δίκτυο το οποίο αποτελείται από μια συσκευή ανάγνωσης και από παθητικές ετικέτες RFID οι οποίες μπορούν να είναι είτε κανονικές, είτε ετικέτες εισβολείς, με βάση την διαφοροποίηση που παρουσιάσαμε στην προηγούμενη ενότητα. Συμβολίζουμε με N_n το σύνολο των κανονικών ετικετών, και με N_{in} το σύνολο των εισβολέων, ενώ το πλήθος τους συμβολίζεται με $|N_n|$ και $|N_{in}|$ αντίστοιχα. Υποθέτουμε ότι η συσκευή ανάγνωσης αλληλεπιδρά με $|N| = |N_n| + |N_{in}|$ παθητικές ετικέτες, όπου $N = N_n \cup N_{in}$ το σύνολο όλων των παθητικών ετικετών στο δίκτυο. Αυτές οι ετικέτες αναμεταδίδουν το σήμα τους στο αναγνώστη, μέσω οπισθοσκέδασης, ώστε αυτό να αποδιαμορφωθεί.

Όσον αφορά την συσκευή ανάγνωσης, υποθέτουμε ότι έχει σταθερή ισχύ εκπομπής P_R, η οποία εξαρτάται από τα τεχνικά χαρακτηριστικά και την κατασκευή της. Συμβολίζουμε με $P_i,\ i = 1, 2, 3, ...N$ την ισχύ εκπομπής της i-οστής παθητικής ετικέτας, όπου $i \in N = N_n \cup N_{in}$, και $P_i \in A_i,\ A_i = [P_i^{Min}, P_i^{Max}]$. Η μέγιστη δυνατή ισχύς P_i^{Max} με την οποία μπορεί να εκπέμψει η κάθε παθητική ετικέτα εξαρτάται από δύο παράγοντες:

- Τα χαρακτηριστικά της τοπολογίας του συστήματος, δηλαδή της απόστασης d_i της κάθε παθητικής ετικέτας από τον αναγνώστη.
- Τα κατασκευαστικά χαρακτηριστικά των ετικετών. Καθώς είναι παθητικές, η ισχύς της εκπομπής του σήματος τους είναι ανάλογη της ισχύος του σήματος ενεργοποίησης του αναγνώστη.

Υποθέτοντας ότι η επικοινωνία του αναγνώστη και των ετικετών γίνεται σε ένα βήμα, το άνω όριο ισχύος του ανακλώμενου σήματος για την κάθε ετικέτα δίνεται από τον τύπο:

$$P_i^{Max} = P_R \cdot G_R \cdot G_i \cdot K_i \cdot \left(\frac{\lambda}{4\pi d_i}\right)^2 \tag{1}$$

όπου:
- P_R, η ισχύς εκπομπής του αναγνώστη στην απευθείας επικοινωνία του με την παθητική ετικέτα.
- G_R, G_i, οι απολαβές κεραίας (antenna gain) του αναγνώστη και της παθητικής ετικέτας αντίστοιχα.
- K_i, η απολαβή οπισθοσκέδασης (backscatter gain) της παθητικής ετικέτας.
- $\left(\frac{\lambda}{4\pi d_i}\right)^2$, όρος που εκφράζει την απώλεια διαδρομής ελευθέρου χώρου.

Στο επικοινωνιακό σύστημα οπισθοσκέδασης που περιγράφεται, για να αποδιαμορφωθεί το σήμα των ετικετών επιτυχώς από την συσκευή ανάγνωσης, πρέπει ο λόγος του σήματος προς τις παρεμβολές και τον θόρυβο (*signal to interference plus noise ratio, SINR*) να είναι μεγαλύτερος από μια ελάχιστη τιμή. Ο λόγος αυτός στην συσκευή ανάγνωσης, για κάθε ετικέτα $i \in N = N_n \cup N_{in}$ συμβολίζεται με γ_i και η αντίστοιχη ελάχιστη τιμή του με γ_i^{Min}. Το SINR σε αυτή την περίπτωση δίνεται από το παρακάτω τύπο [44]:

$$\gamma_i = \frac{h_i P_i}{\sum\limits_{j \neq i} h_j P_j + n} \tag{2}$$

όπου:
- h_i, οι απώλειες του διαύλου επικοινωνίας (channel loss) από την i-οστή παθητική ετικέτα προς τον αναγνώστη.
- n, ο θόρυβος του περιβάλλοντος (background noise).
- ο όρος $\sum\limits_{j \neq i} h_j P_j$, που εμφανίζεται στον παρανομαστή, εκφράζει τις παρεμβολές που αντιλαμβάνεται η συσκευή ανάγνωσης, όταν επιχειρεί να λάβει δεδομένα από την i-οστή παθητική ετικέτα.

Το παραπάνω προτεινόμενο πλαίσιο θα μπορούσε να επεκταθεί άμεσα και σε δίκτυα με παραπάνω από έναν αναγνώστες, στα οποία κάθε παθητική ετικέτα θα συσχετιζόταν με τον πλησιέστερο σε αυτήν αναγνώστη.

4.3 Παίγνιο μετριασμού παρεμβολών

Έχοντας περιγράψει το δίκτυο RFID, συνεχίζουμε με τον ορισμό των *συναρτήσεων χρησιμότητας (utility, payoff functions)*, οι οποίες είναι απαραίτητες για την μοντελοποίηση της συμπεριφοράς των παθητικών ετικετών σε ένα κοινό πλαίσιο βελτιστοποίησης.

Όπως αναφέρθηκε ο στόχος των κανονικών RFID ετικετών του δικτύου είναι η μεγιστοποίηση της διεκπεραιωτικής τους ικανότητας, πρέπει όμως να λάβουμε υπ΄όψιν και το αντίκτυπο που έχει η παρουσία τους στο σύστημα. Έτσι, η συνάρτηση χρησιμότητάς τους θα αποτελείται από δύο μέρη: (α) την *καθαρή συνάρτηση χρησιμότητας (pure utility function)* και (β) την *συνάρτηση ρίσκου (risk function)*. Η καθαρή συνάρτηση χρησιμότητας που ανατίθεται στην i-οστή κανονική ετικέτα έχει την μορφή:

$$U_i^{Pure}(\boldsymbol{P}) = R_{fix}^n \, f_i(\gamma_i), \quad i \in N_n \tag{3}$$

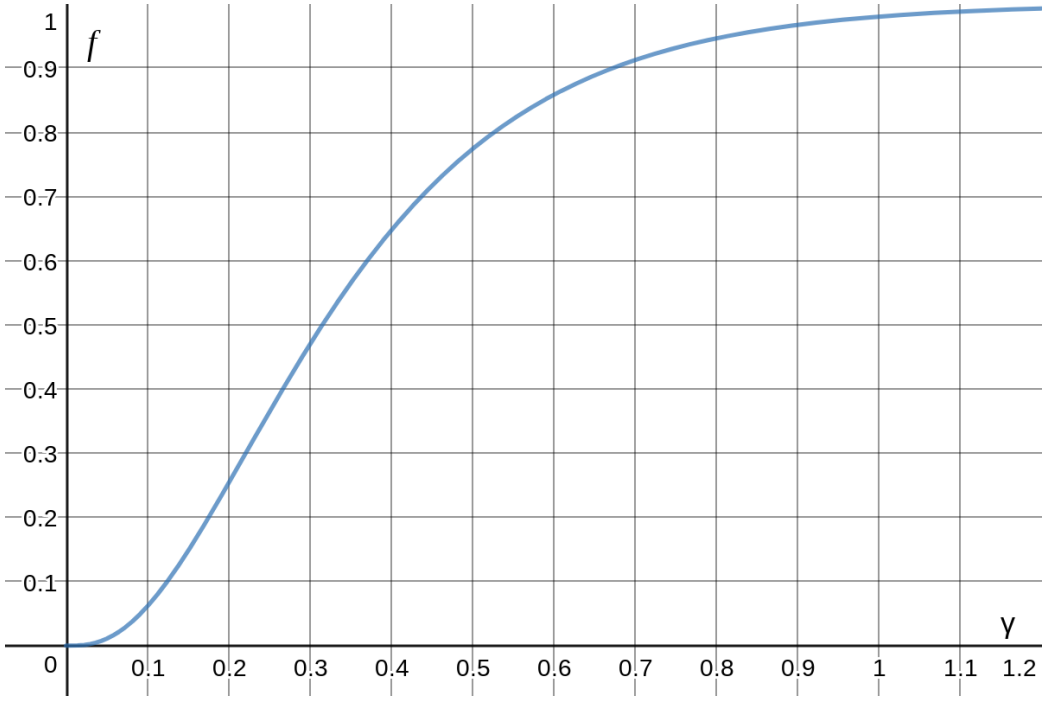
Η συνάρτηση αυτή εκφράζει τον ρυθμό μετάδοσης που επιτυγχάνει η i-οστή κανονική παθητική ετικέτα. Ο όρος R_{fix}^n δηλώνει τον σταθερό ρυθμό μετάδοσής της, ενώ ο όρος $f_i(\gamma_i)$ αποτελεί την συνάρτηση απόδοσης, και εκφράζει την πιθανότητα η μετάδοση της πληροφορίας από την συγκεκριμένη ετικέτα να ολοκληρωθεί με επιτυχία. Με $\boldsymbol{P}$ συμβολίζουμε το διάνυσμα που περιγράφει την ισχύ εκπομπής όλων των ετικετών του δικτύου.

Η συνάρτηση απόδοσης $f_i(\gamma_i)$ είναι μια συνεχής, διαφορίσιμη, και αύξουσα συνάρτηση του γ_i. Ακόμα, είναι σιγμοειδής, δηλαδή υπάρχει τιμή γ_i^{Min} κάτω από την οποία η $f_i(\gamma_i)$ είναι κυρτή, και πάνω από την οποία κοίλη. Στο μοντέλο μας η συνάρτηση αυτή έχει την μορφή [45]:

$$f_i(\gamma_i) = (1 - e^{-A\gamma_i})^M, \quad i \in N_n \tag{4}$$

όπου A, M πραγματικές σταθερές που ελέγχουν την κλίση της. Ο περιορισμός στο SINR για τις κανονικές ετικέτες είναι $\Gamma_i = [\gamma_i^{Min}, \ \gamma_i^{Max}], \ i \in N_n$, και εκφράζει την απαιτούμενη ποιότητα εξυπηρέτησής τους.

Στο παρακάτω σχήμα φαίνεται ενδεικτικά η μορφή της συνάρτησης απόδοσης για $A = 5, \ M = 3$.



Σχήμα 6: Η μορφή της συνάρτησης απόδοσης.

Παρόμοια με την σχέση (3) ορίζουμε και την καθαρή συνάρτηση των εισβολέων που θα εκφράζει την ικανότητα τους να εμποδίζουν την επιτυχή επικοινωνία των κανονικών ετικετών στο δίκτυο ως εξής:

$$U_i^{Pure}(\boldsymbol{P}) = R_{fix}^{in} \sum_{j \in N_n} (1 - f_j(\gamma_j)), \quad i \in N_{in} \tag{5}$$

Για τον ολοκληρωμένο ορισμό των συναρτήσεων χρησιμότητας, εισάγουμε και την συνάρτηση ρίσκου, η οποία έχει ως στόχο την περιγραφή των αρνητικών επιπτώσεων που μπορεί να έχει η παρουσία της κάθε παθητικής ετικέτας στο δίκτυο. Αξίζει να σημειωθεί ότι δυνητικά κάθε ετικέτα θα μπορούσε να θεωρηθεί εισβολέας αν η λειτουργία της εισήγαγε υψηλά επίπεδα παρεμβολών στο δίκτυο, και θα πρέπει να της επιβάλλεται ποινή για την ‘‘μη κοινωνική’’ συμπεριφορά της, καθώς θα μπορούσε να οδηγήσει και στην αύξηση της ισχύος εκπομπής από τις άλλες ετικέτες του συστήματος. Δεδομένου ότι το P_i^{Max} είναι περιορισμένο (σχέση (1)), είναι πιθανό οι παθητικές ετικέτες να μην μπορέσουν να πετύχουν το επιθυμητό SINR, και ο αναγνώστης να αποτύχει στην αποδιαμόρφωση του σήματός τους. Έτσι, η συνάρτηση ρίσκου προσφέρει την δυνατότητα επιβολής μιας αποδεκτής συμπεριφοράς από τις παθητικές ετικέτες, με σκοπό τον περιορισμό των επιπτώσεων από την παρουσία κάποιου εισβολέα στο δίκτυο. Η συνάρτηση αυτή εξαρτάται από τα κατασκευαστικά χαρακτηριστικά της κάθε ετικέτας

(απολαβή κεραίας G_i, απολαβή οπισθσκέδασης K_i), και από την ισχύ του ανακλώμενου σήματος:

$$R_i(G_i, K_i, P_i) = G_i \cdot K_i \cdot P_i, \quad i \in N = N_i \cup N_{in} \tag{6}$$

Με βάση την παραπάνω ανάλυση καταλήγουμε ότι η συνάρτηση χρησιμότητας για τις παθητικές ετικέτες του δικτύου SINR έχει την παρακάτω μορφή:

$$\begin{aligned} U_i(\boldsymbol{P}) &= U_i^{Pure}(\boldsymbol{P}) - R_i(G_i, K_i, P_i) \\ &= \begin{cases} R_{fix}^n f_i(\gamma_i) - G_i \cdot K_i \cdot P_i, & i \in N_n \\ R_{fix}^{in} \sum\limits_{j \in N_n} (1 - f_j(\gamma_j)) - G_i \cdot K_i \cdot P_i, & i \in N_{in} \end{cases} \end{aligned} \tag{7}$$

Συνοψίζοντας, βλέπουμε ότι με βάση την συνάρτηση χρησιμότητας οι παθητικές ετικέτες του δικτύου θα έχουν τους εξής στόχους:

- Κανονικές ετικέτες. Μεγιστοποίηση του ρυθμού μετάδοσης $R_{fix}^n f_i(\gamma_i)$, χωρίς να αυξήσουν υπερβολικά την ισχύ του σήματος τους. Οι κανονικές ετικέτες είναι πρόθυμες να ελέγξουν την ισχύ εκπομπής τους, ώστε να συνυπάρχουν σε ένα δίκτυο με μετριασμένες παρεμβολές.
- Ετικέτες εισβολείς. Μεγιστοποίηση της ζημιάς $\sum\limits_{j \in N_n} (1 - f_j(\gamma_j))$ που προκαλούν στο δίκτυο, εκμεταλλευόμενοι το άνω όριο της ισχύος ανάκλασης P_i^{Max} για τις παθητικές ετικέτες, χωρίς να εντοπιστούν για τα υψηλά επίπεδα παρεμβολών που εισάγουν στο σύστημα.

Μετά τον ορισμό των συναρτήσεων χρησιμότητας για τις παθητικές ετικέτες του δικτύου, είμαστε σε θέση να ορίσουμε το παίγνιο που περιγράφει την αλληλεπίδραση τους στο σύστημα. Έστω $G_{IM} = [N, \{A_i\}, U_i(\cdot)]$, όπου $N = N_n \cup N_{in}$ και $i \in N$, το μη συνεργατικό παίγνιο μετριασμού παρεμβολών. Στον παραπάνω ορισμό, N είναι το σύνολο των δεικτών όλων των παθητικών RFID ετικετών του δικτύου, $A_i = [P_i^{Min}, P_i^{Max}] \subseteq \mathbb{R}^{|N|}$ το σύνολο στρατηγικής της i-οστής ετικέτας, και $U_i(\cdot)$ η συνάρτηση χρησιμότητας, όπως ορίστηκε για τις κανονικές ετικέτες και τους εισβολείς στην σχέση (7). Επειδή η κάθε παθητική ετικέτα προσπαθεί να μεγιστοποιήσει την συνάρτηση χρησιμότητάς της (μέσω του P_i) μη συνεργατικά, το παίγνιο μετριασμού παρεμβολών (Interference Mitigation, IM game) μπορεί να εκφραστεί ως ένα μη συνεργατικό πρόβλημα βελτιστοποίησης:

$$\begin{aligned} &\max_{P_i \in A_i} U_i(\boldsymbol{P}), \quad \forall i \in N \\ &\text{τ.ω. } P_i^{Min} \leq P_i \leq P_i^{Max} \end{aligned} \tag{8}$$

συνυπολογίζοντας και τον περιορισμό γ_i^{Min} για τις κανονικές παθητικές ετικέτες, όπως

παρουσιάζεται στην συνάρτηση χρησιμότητάς τους.

Ακόμα, έχουμε ότι οι λύσεις στο σημείο ισορροπίας Nash για αυτό το μη συνεργατικό παίγνιο, τις οποίες συμβολίζουμε με $P_i^* \in A_i,\ \forall i \in N = N_n \cup N_{in}$, θα πρέπει να ικανοποιούν την σχέση:

$$U_i(\boldsymbol{P}^*) \geq U_i(P_i, \boldsymbol{P}_{-i}^*), \quad \forall P_i \in A_i \tag{9}$$

όπου με $\boldsymbol{P}_{-i}$ συμβολίζουμε το διάνυσμα των ισχύων εκπομπής όλων των ετικετών πλην της i-οστής. Καμία ετικέτα δεν μπορεί μονομερώς να βελτιώσει την επίδοση της στο σύστημα πέρα από αυτό το σημείο ισορροπίας Nash.

4.4 Προσδιορισμός σημείου ισορροπίας Nash

Σε αυτή την ενότητα μελετάμε αναλυτικά την συμπεριφορά του δικτύου για τρεις περιπτώσεις, ανάλογα με τα στοιχεία που το απαρτίζουν, καταλήγοντας για καθεμία από αυτές στην εύρεση του σημείου ισορροπίας του παιγνίου:

(A) *Δύο κανονικές ετικέτες.*

Υποθέτουμε την ύπαρξη δύο κανονικών παθητικών ετικετών, $i = A, B$ στο δίκτυο RFID, και την απουσία στοιχείου εισβολέα. Οι δύο ετικέτες, με βάση την σχέση (7), υιοθετούν την συνάρτηση χρησιμότητας

$$U_i(P_A, P_B) = R_{fix}^n \, f_i(\gamma_i) - G_i \cdot K_i \cdot P_i \tag{10}$$

με πεδίο ορισμού $P_i \in A_i = [P_i^{Min}, P_i^{Min}]$. Σκοπός και των δύο είναι η μεγιστοποίηση της συνάρτησης χρησιμότητας για την επίτευξη των στόχων ποιότητας εξυπηρέτησης.

Θεώρημα 1. *Το παίγνιο μετριασμού παρεμβολών για τις δύο κανονικές παθητικές ετικέτες $i = A, B$, έχει μοναδικό σημείο ισορροπίας Nash:*

$$P_i^* = max\left(min\left(f_i^{'}(\gamma_i^*)\frac{\gamma_i^* R_{fix}^n}{G_i K_i}, P_i^{Max}\right), P_i^{Min}\right) \tag{11}$$

όπου, $\gamma_i^* = max\left(min\left(\hat{\gamma}_i, \gamma_i^{Max}\right), \gamma_i^{Min}\right)$ *και* $\hat{\gamma}_i = \frac{h_i P_i^*}{h_j P_j^* + n}, \; j \neq i.$

Απόδειξη. Για τον καθορισμό του σημείου ισορροπίας Nash εξετάζουμε την συνθήκη $\frac{\partial U_i(P_A, P_B)}{\partial P_i} = 0$. Παραγωγίζοντας μερικώς την συνάρτηση χρησιμότητας ως προς τις μεταβλητές ισχύος για τις δύο κανονικές ετικέτες, και λαμβάνοντας υπ'όψιν ότι $\frac{\partial \gamma_i}{\partial P_i} = \frac{\gamma_i}{P_i}$ καταλήγουμε στην σχέση $f_i^{'}(\gamma_i)\gamma_i = \frac{G_i K_i}{R_{fix}^n} P_i, \; i = A, B$, από την οποία έχουμε ότι η μοναδική λύση για την βέλτιστη τιμή ισχύος του σήματος οπισθοσκέδασης είναι:

$$\hat{P}_i = f_i^{'}(\gamma_i^*)\frac{\gamma_i^* R_{fix}^n}{G_i K_i} \tag{12}$$

όπου, $\gamma_i^* = max\left(min\left(\hat{\gamma}_i, \gamma_i^{Max}\right), \gamma_i^{Min}\right)$ και $\hat{\gamma}_i = \frac{h_i P_i^*}{h_j P_j^* + n}, \; j \neq i.$

■

(B) *Μια κανονική ετικέτα και μια ετικέτα εισβολέας.*

Υποθέτουμε μια απλοποιημένη τοπολογία του δικτύου RFID στο οποίο, πέρα της συσκευής ανάγνωσης, βρίσκεται μια κανονική ετικέτα (A), και ένας εισβολέας (B). Με βάση την σχέση (7), οι συμπεριφορά των δύο ετικετών περιγράφεται από τις συναρτήσεις χρησιμότητας:

$$U_i(P_A, P_B) = \begin{cases} R^n_{fix}\, f_A(\gamma_A) - G_A \cdot K_A \cdot P_A, & A : \text{Κανονική ετικέτα} \\ R^{in}_{fix}\,(1 - f_A(\gamma_A)) - G_B \cdot K_B \cdot P_B, & B : \text{Ετικέτα εισβολέας} \end{cases} \tag{13}$$

όπου, $\gamma_A = \frac{h_A P_A}{h_B P_B + n}$ το SINR της κανονικής ετικέτας.

Η επίθεση άρνησης υπηρεσιών μοντελοποιείται ως ένα μη συνεργατικά παίγνιο μεταξύ των δύο ετικετών, με βάση την ισχύ του σήματος οπισθοσκέδασής τους. Συμβολίζουμε το παίγνιο αυτό ως $G = [\{A, B\}, \{A_A, A_B\}, \{U_A, U_B\}]$, όπου $A_A = [P_A^{Min}, P_A^{Max}]$ και $A_B = [P_B^{Min}, P_B^{Max}]$ τα σύνολα στρατηγικής των δύο ετικετών και $U_A,\ U_B$ οι αντίστοιχες συναρτήσεις χρησιμότητας. Με βάση τα παραπάνω και την σχέση (8), το πρόβλημα βελτιστοποίησης για την συγκεκριμένη τοπολογία διατυπώνεται ως:

$$\begin{aligned} &\max_{P_i \in A_i} U_i(P_A, P_B), \quad i = A, B \\ &\text{τ.ω. } P_i^{Min} \le P_i \le P_i^{Max} \end{aligned} \tag{14}$$

Το διάνυσμα ισχύος $\boldsymbol{P}^* = (P_A^*, P_B^*) \in A_A \times A_B$ αποτελεί, βάσει της σχέσης (9), σημείο ισορροπίας Nash εάν $U_i(\boldsymbol{P}^*) \ge U_i(P_i, \boldsymbol{P}^*_{-i}),\ i = A, B$.

Για την μεγιστοποίηση της συνάρτησης χρησιμότητας $U_A(P_A, P_B)$ της κανονικής ετικέτας ως προς το P_A εξετάζουμε την συνθήκη $\frac{\partial U_A(P_A, P_B)}{\partial P_A} = 0$. Παραγωγίζοντας μερικώς την συνάρτηση χρησιμότητας της και λαμβάνοντας υπ'όψιν ότι $\frac{\partial \gamma_A}{\partial P_A} = \frac{\gamma_A}{P_A}$ καταλήγουμε στην σχέση:

$$\frac{\partial f(\gamma_A)}{\partial \gamma_A}\gamma_A = \frac{G_A K_A}{R^n_{fix}} P_A \tag{15}$$

Ομοίως, για την μεγιστοποίηση της συνάρτηση χρησιμότητας $U_B(P_A, P_B)$ του εισβολέα ως προς το P_B εξετάζουμε την συνθήκη $\frac{\partial U_B(P_A, P_B)}{\partial P_B} = 0$. Παραγωγίζοντας μερικώς την συνάρτηση χρησιμότητας του, και λαμβάνοντας υπ'όψιν ότι ο λόγος $\frac{\partial \gamma_A}{\partial P_B} = -\frac{h_A P_A h_B}{(h_B P_B + n)^2} = -\gamma_A \frac{h_B}{h_B P_B + n}$ καταλήγουμε στην σχέση:

$$\frac{\partial f(\gamma_A)}{\partial \gamma_A}\gamma_A = \frac{G_B K_B}{R_{fix}^{in} h_B}(h_B P_B + n) \tag{16}$$

Συνδυάζοντας τις σχέσεις (15) και (16) και με βάση τον ορισμό του γ_A για την συγκεκριμένη τοπολογία λαμβάνουμε την μοναδική τιμή SINR:

$$\hat{\gamma_A} = \frac{G_B K_B h_A R_{fix}^n}{G_A K_A h_B R_{fix}^{in}} \tag{17}$$

συνεπώς η βέλτιστη τιμή στο σημείο ισορροπίας είναι, $\gamma_A^* = max\left(min\left(\hat{\gamma_A}, \gamma_A^{Max}\right), \gamma_A^{Min}\right)$.

Με βάση την παραπάνω ανάλυση (σχέσεις (15), (16), (17)) και την ένα προς ένα αντιστοιχία μεταξύ της τιμής της ισχύος οπισθοσκέδασαης και του SINR καταλήγουμε στο ακόλουθο θεώρημα.

Θεώρημα 2. *Το παίγνιο μετριασμού παρεμβολών για το δίκτυο μια κανονικής ετικέτας (A) και μιας ετικέτας εισβολέα (B), έχει μοναδικό σημείο ισορροπίας Nash:*

$$P_A^* = max\left(min\left(\frac{f_A^{'}(\gamma_A^*)\gamma_A^* R_{fix}^n}{G_A K_A}, P_A^{Max}\right), P_A^{Min}\right) \tag{18}$$

$$P_B^* = max\left(min\left(\frac{f_A^{'}(\gamma_A^*)\gamma_A^* R_{fix}^{in}}{G_B K_B} - \frac{n}{h_B}, P_B^{Max}\right), P_B^{Min}\right) \tag{19}$$

όπου, $\gamma_A^* = max\left(min\left(\hat{\gamma_A}, \gamma_A^{Max}\right), \gamma_i^{Min}\right)$ *και* $\hat{\gamma_A} = \frac{G_B K_B h_A R_{fix}^n}{G_A K_A h_B R_{fix}^{in}}$.

(C) *Αυθαίρετος αριθμός ετικετών.*

Επεκτείνοντας την παραπάνω ανάλυση, θα μελετήσουμε ένα δίκτυο με αυθαίρετο αριθμό κανονικών παθητικών ετικετών $|N_n|$ και εισβολέων $|N_{in}|$. Καθεμία από τις ετικέτες υιοθετεί την συνάρτηση χρησιμότητας που παρουσιάζονται στην σχέση (7) ανάλογα με το είδος της. Για την εύρεση του σημείου ισορροπίας Nash εξετάζουμε την μερική παράγωγο της συνάρτησης χρησιμότητας $\frac{\partial U(\boldsymbol{P})}{\partial P_i} = 0$, τόσο για τις κανονικές, όσο και για τις παθητικές ετικέτες.

Για τις κανονικές ετικέτες, η παραπάνω συνθήκη είναι ισοδύναμη με:

$$R_{fix}^n f_i^{'}(\gamma_i)\gamma_i - G_i K_i P_i = 0, \quad i \in N_n \tag{20}$$

Όμοια, για τις ετικέτες εισβολέων, η συνθήκη ισοδυναμεί με:

$$R_{fix}^{in} \sum_{j \in N_n} \left(\frac{f_j^{'}(\gamma_j) \gamma_j^2 h_i}{h_j P_j} \right) - G_i K_i = 0, \quad i \in N_{in} \tag{21}$$

χρησιμοποιώντας το γεγονός ότι $\frac{\partial \gamma_j}{\partial P_i} = -\frac{\gamma_j^2 h_i}{h_j P_j}$ για κάθε κανονική ετικέτα j, και ετικέτα εισβολέα i.

Με βάση τις σχέσεις (20) και (21) καταλήγουμε στην ακόλουθη πρόταση:

Θεώρημα 3. *Το σημείο ισορροπίας Nash για αυθαίρετο αριθμό κανονικών ετικετών και εισβολέων δίνεται από την σχέση:*

$$P_i^* = max \left(min \left(\hat{P}_i, P_i^{Max} \right), P_i^{Min} \right) \tag{22}$$

όπου για τις κανονικές παθητικές ετικέτες:

$$\hat{P}_i = \frac{R_{fix}^n}{G_i K_i} f_i^{'}(\gamma_i^*) \gamma_i^*, \quad i \in N_n \tag{23}$$

με $\gamma_i^* = max \left(min \left(\hat{\gamma}_i, \gamma_i^{Max} \right), \gamma_i^{Min} \right)$ *και* $\hat{\gamma}_i = \frac{h_i P_i^*}{\sum_{j \neq i} h_j P_j^* + n}$, $j \neq i$,
και για τις ετικέτες εισβολείς:

$$\hat{P}_i = \frac{R_{fix}^{in} h_j P_j^*}{R_{fix}^n h_i \gamma_j^*} - \frac{1}{h_i} \left(\sum_{\substack{k \neq i \\ k \neq j}} h_k P_k^* + n \right), \quad i \in N_{in}, \forall j \in N_n \tag{24}$$

με το γ_j^* *να ικανοποιεί την σχέση* $\sum_{j \in N_n} \frac{G_j K_j}{h_j} \gamma_j^* = \frac{G_i K_i}{h_i}$, $i \in N_{in}$.

Σύμφωνα με την παραπάνω πρόταση, η βέλτιστη στρατηγική για την κάθε παθητική ετικέτα του δικτύου προσδιορίζεται με βάση την βέλτιστη ισχύ οπισθοσκέδασής της. Ακολουθώντας την συμπεριφορά που περιγράφουν αυτές οι σχέσεις, οι κανονικές ετικέτες επιτυγχάνουν την προαπαιτούμενη ποιότητα εξυπηρέτησής τους, λαμβάνοντας υπ΄όψιν τους κατασκευαστικούς περιορισμούς τους. Αντίστοιχα, οι ετικέτες εισβολείς μεγιστοποιούν την ζημιά που προκαλούν στην λειτουργία των κανονικών ετικετών, εμποδίζοντας την επιτυχή μετάδοση της πληροφορίας τους.

5 Ο Αλγόριθμος για το παίγνιο IM

5.1 Η ιδέα του αλγορίθμου

Τα δίκτυα παθητικών RFID ετικετών, ως μέρος του Internet of Things, χαρακτηρίζονται από την κατανεμημένη φύση τους. Πράγματι, στην πλειοψηφία των εφαρμογών που αναφέραμε στο κεφάλαιο 2.2, οι οποίες χρησιμοποιούν παθητικές ετικέτες, υπάρχει η ανάγκη δημιουργίας ενός πλέγματος από πομποδέκτες, ο καθένας από τους οποίους τοποθετείται σε ένα συγκεκριμένο αντικείμενο του εκάστοτε συστήματος, χωρίς να υπάρχει μεταξύ τους επικοινωνία. Σημαντικό χαρακτηριστικό τέτοιων δικτύων, είναι η πλήρης απουσία κάποιου κεντρικού και λογικού μηχανισμού ο οποίος είναι υπεύθυνος για την λήψη αποφάσεων εκ μέρους των ετικετών, σε αντίθεση με το υπολογιστικό σύστημα το οποίο μπορεί να ελέγχει την λειτουργία της συσκευής ανάγνωσης. Για αυτόν τον λόγο, κάθε παθητική ετικέτα του δικτύου (όταν ενεργοποιηθεί από την παρουσία του αναγνώστη), πρέπει να προσδιορίζει μόνη της την ισχύ του ανακλώμενου σήματος στο σημείο ισορροπίας, με σκοπό την τελική μεγιστοποίηση της διεκπεραιωτικής της ικανότητας.

Για τον προσδιορισμό αυτής της βέλτιστης τιμής ισχύος οι παθητικές RFID ετικέτες χρειάζεται να έχουν στην διάθεση τους ορισμένες πληροφορίες. Πέρα από τα κατασκευαστικά χαρακτηριστικά της και την απώλεια του διαύλου επικοινωνίας, τα οποία είναι διαθέσιμα στην εκάστοτε παθητική ετικέτα, υπάρχει η ανάγκη να γνωρίζουν και το συνολικό μέγεθος των παρεμβολών στο δίκτυο. Αυτό, μπορεί να γίνει με την τακτική αναμετάδοση αυτής της τιμής από την συσκευή ανάγνωσης. Στηριζόμενοι στο παραπάνω σκεπτικό, προτείνουμε έναν κατανεμημένο, επαναληπτικό αλγόριθμο χαμηλής υπολογιστικής πολυπλοκότητας, με σκοπό τον προσδιορισμό του σημείου ισορροπίας Nash για το παίγνιο μετριασμού παρεμβολών (IM game), όπως αυτό ορίστηκε στην σχέση (8). Ο αλγόριθμος αυτός εκτελείται κάθε φορά που μια παθητική ετικέτα (κανονική ή εισβολέας) ενεργοποιείται από την συσκευή ανάγνωσης, με σκοπό την μετάδοση της πληροφορίας της. Όπως φαίνεται και από την μορφή των συναρτήσεων χρησιμότητας της σχέσης (7), οι οποίες εκφράζουν τους στόχους των ετικετών, λαμβάνουμε υπ΄όψιν και το ρίσκο που επιβαρύνει κάθε ετικέτα για την συμμετοχή της στο δίκτυο (risk aware algorithm).

5.2 Παρουσίαση του αλγορίθμου

Παρακάτω παρουσιάζεται συνοπτικά ο αλγόριθμος:

Βήμα 1 Κάθε παθητική ετικέτα στο δίκτυο εκπέμπει με τυχαία ισχύ $P_i^{(ite=0)}$, $\forall i \in N = N_n \cup N_{in}$, όπου $P_i^{Min} \leq P_i^{(ite=0)} \leq P_i^{Max}$.
Η μεταβλητή ite δηλώνει τον αριθμό της επανάληψης στην εκτέλεση του αλγορίθμου και αρχικά τίθεται ίση με 0.

Βήμα 2 Η συσκευή ανάγνωσης, για να ενημερώσει τις παθητικές ετικέτες, εκπέμπει στο δίκτυο την τιμή της συνολικής παρεμβολής που αντιλαμβάνεται: $\sum_{i \in N} h_i P_i$ (network interference).
Χρησιμοποιώντας αυτή την τιμή, η κάθε ετικέτα υπολογίζει την παρεμβολή, όπως αυτή την αντιλαμβάνεται: $\sum_{j \neq i} h_j P_j$ (sensed interference).
Στην συνέχεια η κάθε ετικέτα αποφασίζει την βέλτιστη στρατηγική της, όσον αφορά την ισχύ εκπομπής της, με βάση την συνάρτηση χρησιμότητάς της ως εξής: $P_i^{(ite)} = \underset{P_i \in A_i}{\operatorname{argmax}} U_i(P_i, \boldsymbol{P}_{-i}^{(ite-1)})$.

Βήμα 3 Για κάθε ετικέτα i, ορίζεται η συνθήκη σύγκλισης $\left| P_i^{(ite)} - P_i^{(ite-1)} \right| < \epsilon$, όπου ϵ μια μικρή θετική σταθερά. Στην περίπτωση που οι ισχύες εκπομπής όλων των παθητικών ετικετών συγκλίνουν, με βάση την παραπάνω σχέση, τότε συμπεραίνουμε ότι η συσκευή ανάγνωσης κατάφερε να διαβάσει επιτυχώς την πληροφορία από όλες της ετικέτες και ο αλγόριθμος τερματίζει.
Σε αντίθετη περίπτωση, θέτουμε ite = ite + 1, η συσκευή ανάγνωσης εκπέμπει εκ νέου και επιστρέφουμε στην βήμα 2.

Όπως φαίνεται από τα παραπάνω, σε κάθε επανάληψη του αλγορίθμου, οι ετικέτες για να καταλήξουν στην βέλτιστη ισχύ εκπομπής, λαμβάνουν υπ΄όψιν μόνο πληροφορίες από την προηγούμενη επανάληψη (στην μορφή των παρεμβολών του δικτύου που εκπέμπει η συσκευή ανάγνωσης). Αυτό, σε συνδυασμό με το γεγονός ότι κάθε ετικέτα αποφασίζει την στρατηγική της ανεξάρτητα από τις άλλες, επιτρέπει την παράλληλη εκτέλεση του αλγορίθμου, επιτυγχάνοντας ταχύτερα τον τερματισμό του και την εύρεση του σημείου ισορροπίας.

6 Προσομοίωση της λειτουργίας του δικτύου

6.1 Παραμετροποίηση του αλγορίθμου

Για την προγραμματιστική προσομοίωση της συμπεριφοράς του δικτύου RFID με βάση τον αλγόριθμο που περιγράφηκε, δοκιμάζονται διαφορετικές διατάξεις των στοιχείων που συμμετέχουν. Σε αυτή την ενότητα αναφέρεται η επιλογή των τιμών των παραμέτρων που αφορούν τα χαρακτηριστικά κατασκευής της συσκευής ανάγνωσης, των ετικετών (οι οποίες διαχωρίζονται σε κανονικές και εισβολείς), καθώς και των σταθερών που διέπουν την λειτουργία του συστήματος.

- **Συσκευή Ανάγνωσης**.
  Επιλέγεται ενεργός αναγνώστης με σταθερή ισχύ εκπομπής σήματος $P_R = 2\text{W}$, ο οποίος είναι υπεύθυνος για την ενεργοποίηση των ετικετών και την συλλογή των δεδομένων τους. Η απολαβή της κεραίας του (antenna gain) θεωρείται ότι είναι $G_R = 6\text{dBi}$. Για την επιτυχή αποδιαμόρφωση του σήματος οπισθοσκέδασης που λαμβάνει η συσκευή ανάγνωσης από την εκάστοτε ετικέτα, πρέπει η ισχύς του να είναι υψηλότερη της τιμής $P_{TH} = -15\text{dBm}$. Η τιμή αυτή καθορίζει το κατώτατο όριο γ_i^{Min} των ετικετών για την διασφάλιση της ποιότητας εξυπηρέτησής τους.

- **Ετικέτες**.
  Επιλέγονται αποκλειστικά παθητικές ετικέτες, με μοναδική τροφοδοσία ισχύος το σήμα ενεργοποίησης της συσκευής ανάγνωσης. Ο διαχωρισμός μεταξύ κανονικών και παθητικών ετικετών έγκειται στα κατασκευαστικά χαρακτηριστικά τους. Για τις κανονικές παθητικές ετικέτες η απολαβή οπισθοσκέδασης (backscatter gain) είναι $K_{i,n} = 60\%$, ενώ η απολαβή της κεραίας τους είναι $G_{i,n} = 12\text{dBi}$. Αντίθετα, οι παθητικές ετικέτες εισβολείς λαμβάνεται να έχουν απολαβή οπισθοσκέδασης $K_{i,in} = 90\%$, και απολαβή κεραίας $G_{i,in} = 16\text{dBi}$. Αυτή η διαφοροποίηση είναι υπεύθυνη για τα υψηλότερα επίπεδα παρεμβολών που εισάγουν οι εισβολής στο δίκτυο. Οι αντίστοιχες σταθερές R_{fix}^{n} και R_{fix}^{in} θεωρούνται 64 και 300 Kbps.

- **Χαρακτηριστικά δικτύου**.
  Θεωρούμε δίκτυο υπερυψηλών συχνοτήτων (UHF) με συχνότητα λειτουργίας $f = 915\text{MHz}$. Η επικοινωνία μεταξύ αναγνώστη και παθητικών ετικετών γίνεται σε ένα βήμα, και για τον υπολογισμό των απωλειών του διαύλου επικοινωνίας h_i, για την εκάστοτε ετικέτα, υιοθετούμε το απλό μοντέλο απώλειας μονοπατιού. Έτσι, έχουμε ότι $h_i = \frac{c_i}{d_i^{\alpha}}$, όπου d_i η απόσταση της i-οστής ετικέτας

από τον αναγνώστη, και $\alpha = 2$ ο εκθέτης απωλειών διάδοσης. Η σταθερά c_i επιλέγεται να είναι κοινή για όλες τις παθητικές ετικέτες και ίση με 0.097. Τέλος, καθώς το ασύρματο δίκτυο επηρεάζεται και από την παρουσία άλλων πηγών παρεμβολών, θεωρούμε ότι εισάγεται στο σύστημα ηλεκτρομαγνητικός θόρυβος από το περιβάλλον $n = 5 \cdot 10^{-16}$W.

6.2 Συνοπτική παρουσίαση της υλοποίησης

Η υλοποίηση του προγράμματος προσομοίωσης έγινε στην γλώσσα προγραμματισμού Python 3.5.3. Οι οντότητες του δικτύου (αναγνώστης, κανονικές παθητικές ετικέτες, και ετικέτες εισβολείς) ορίζονται σε κλάσεις Python, οι οποίες διαθέτουν μεταβλητές για τις τιμές των παραμέτρων τους. Σε καθεμία από αυτές τις κλάσεις ορίζονται μέθοδοι για τον υπολογισμό δυναμικών μεγεθών που απαιτούνται κατά την εκτέλεση του προγράμματος προσομοίωσης. Παραδείγματος χάριν, η κλάση που περιγράφει την συσκευή ανάγνωσης διαθέτει μέθοδο που υπολογίζει τις συνολικές παρεμβολές στο δίκτυο, δεδομένων των ισχύων και των απωλειών διαύλου της κάθε ετικέτας. Αντίστοιχα, οι κλάσεις για τις παθητικές ετικέτες ορίζουν μεθόδους για τον υπολογισμό των παρεμβολών όπως αυτές τις αντιλαμβάνονται σε κάθε επανάληψη του αλγορίθμου, καθώς και μεθόδους για τον υπολογισμό τυχαίων μεγεθών που χρειάζονται (π.χ. αρχική τιμή ισχύος οπισθοσκέδασης, απόσταση από τον αναγνώστη κ.α.). Για την τήρηση της ακρίβειας κατά τους υπολογισμούς χρησιμοποιείται η βιβλιοθήκη decimal που περιέχεται στον πυρήνα της Python. Τέλος, οι τιμές που αφορούν τα σταθερά χαρακτηριστικά του δικτύου (για παράδειγμα η συχνότητα λειτουργίας του) ορίζονται ως global μεταβλητές και είναι διαθέσιμες καθολικά.

Στην κύρια μέθοδο του προγράμματος, αρχικοποιούνται τα αντικείμενα που αντιπροσωπεύουν τα στοιχεία του δικτύου, και στην συνέχεια ακολουθεί ο βρόχος που υλοποιεί τον αλγόριθμο που περιγράφηκε στο κεφάλαιο 5.2. Αναλυτικότερα, στην αρχή της κάθε επανάληψης αποθηκεύεται ο αύξων αριθμός της και αρχικοποιείται μια μεταβλητή-φρουρός που είναι υπεύθυνη για τον τερματισμό του βρόχου.

Κάθε ετικέτα (κανονική ή εισβολέας) αποθηκεύει σε έναν προσωρινό πίνακα την τρέχουσα τιμή ισχύος οπισθοσκέδασης και την τιμή της απώλειας διαύλου επικοινωνίας. Υπενθυμίζουμε ότι στην πρώτη επανάληψη του βρόχου οι παθητικές ετικέτες έχουν επιλέξει τυχαία τιμή για την ισχύ τους, εντός των επιτρεπτών ορίων. Βάσει αυτών των δεδομένων, η συσκευή ανάγνωσης υπολογίζει την τιμή των συνολικών παρεμβολών στο δίκτυο και στην συνέχεια την ανακοινώνει, ώστε να είναι διαθέσιμη σε όλες τις ετικέτες. Χρησιμοποιώντας αυτή την τιμή, η κάθε ετικέτα υπολογίζει τις παρεμβολές που αυτή αντιλαμβάνεται στην επικοινωνία της με τον αναγνώστη, αφαιρώντας από τις συνολικές παρεμβολές αυτές που οφείλονται στο δικό της σήμα.

Έχοντας ορίσει, με βάση τις σχέσεις (2), (4) και (7), τις μεθόδους που υλοποιούν τις συναρτήσεις χρησιμότητας, η κάθε παθητική ετικέτα είναι πλέον σε θέση να υπολογίσει ανεξάρτητα από τις άλλες το σημείο μεγιστοποίησης της συνάρτησης μεταφοράς της χρησιμοποιώντας πληροφορίες που διαθέτει από την προηγούμενη επανάληψη του βρόχου. Για την επίλυση του προβλήματος βελτιστοποίησης χρησιμοποιούνται τα πακέτα SciPy (v1.0.1) και NumPy (v1.14.3) της Python, που προσφέρουν μεθόδους

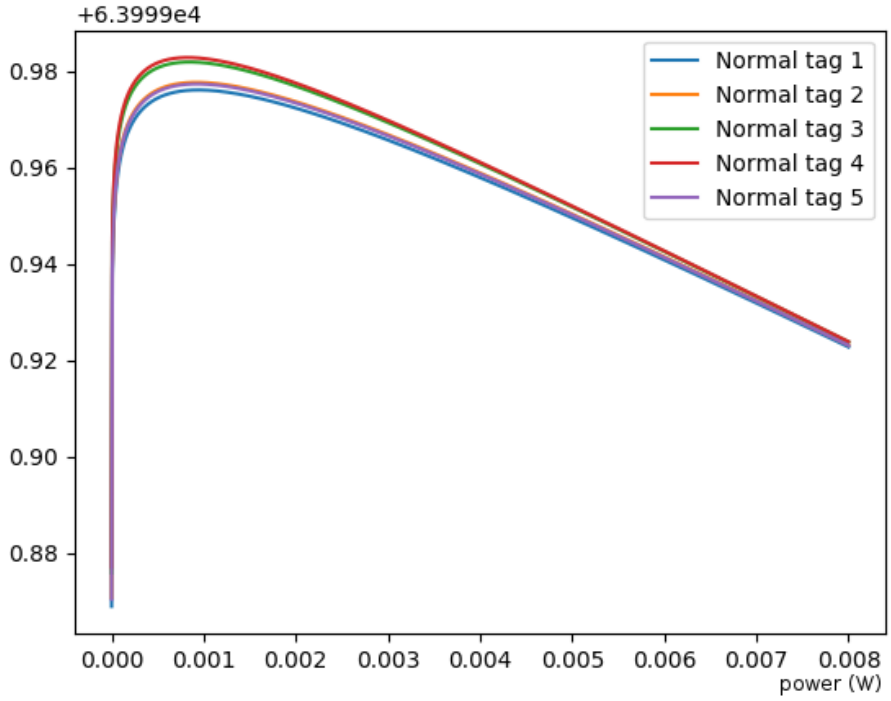
για την εύρεση ακροτάτων σε δοθέντα φραγμένα διαστήματα.

Όταν ολοκληρωθεί ο υπολογισμός της ισχύος οπισθοσκέδασης για την οποία μεγιστοποιείται η συνάρτηση μεταφοράς της, στην τρέχουσα επανάληψη, η κάθε παθητική ετικέτα αποθηκεύει την τιμή και στην συνέχεια την συγκρίνει με την αντίστοιχη που είχε προκύψει από την αμέσως προηγούμενη επανάληψη. Στα πλαίσια της προσομοίωσης, για την ικανοποίηση της συνθήκης σύγκλισης που ορίστηκε στο κεφάλαιο 5.2, επιλέγουμε $\epsilon = 10^{-8}$. Στην περίπτωση που συγκλίνουν όλες οι παθητικές ετικέτες, ενημερώνεται η μεταβλητή-φρουρός και η εκτέλεση του επαναληπτικού βρόχου τερματίζει επιτυχώς. Εναλλακτικά, ξεκινάει από την αρχή με την διαδικασία υπολογισμού και ενημέρωσης των ετικετών σχετικά με την νέα τιμή των συνολικών παρεμβολών στο δίκτυο.

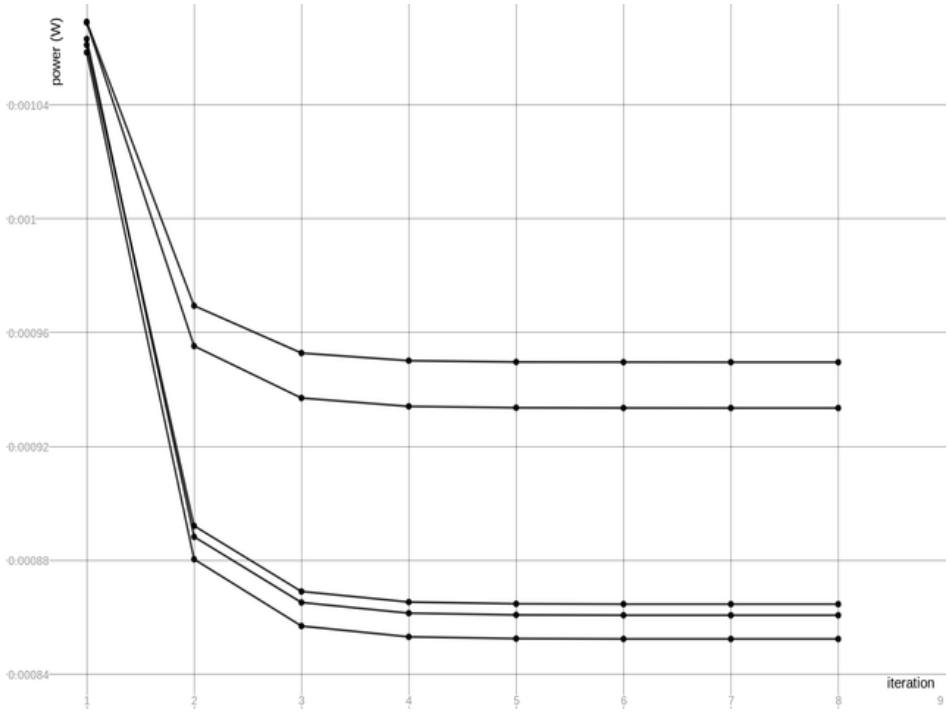
Για λόγους πληρότητας, αναφέρουμε ότι η εκτέλεση του προγράμματος προσομοίωσης πραγματοποιείται σε φορητό υπολογιστή με τετραπύρηνο επεξεργαστή (8 νημάτων), αρχιτεκτονικής 64-bit Intel® Core™ i7-6700HQ CPU, ονομαστικής συχνότητας λειτουργίας 2.60GHz και μέγιστης διαθέσιμης μνήμη RAM 7.60GB. Το λειτουργικό σύστημα είναι Debian GNU / Linux 9 (stretch).

6.3 Ενδεικτικά αποτελέσματα

Εκτελώντας το πρόγραμμα προσομοίωσης με την παρουσία μόνο κανονικών παθητικών ετικετών στο δίκτυο λαμβάνουμε τις δύο παρακάτω γραφικές παραστάσεις. Η πρώτη παρουσιάζει την μορφή των συναρτήσεων χρησιμότητας πέντε κανονικών παθητικών ετικετών στο τέλος της προσομοίωσης. Η δεύτερη δείχνει την ισχύ οπισθοσκέδασης που επιλέγει καθεμία από τις κανονικές παθητικές ετικέτες σε κάθε επανάληψη του αλγορίθμου. Οι ετικέτες τοποθετούνται σε τυχαία απόσταση μεταξύ 1.2 και 1.8 μέτρων από την συσκευή ανάγνωσης. Η σταθερά A λαμβάνεται 1.45, ενώ η σταθερά M λαμβάνεται 0.00000016.



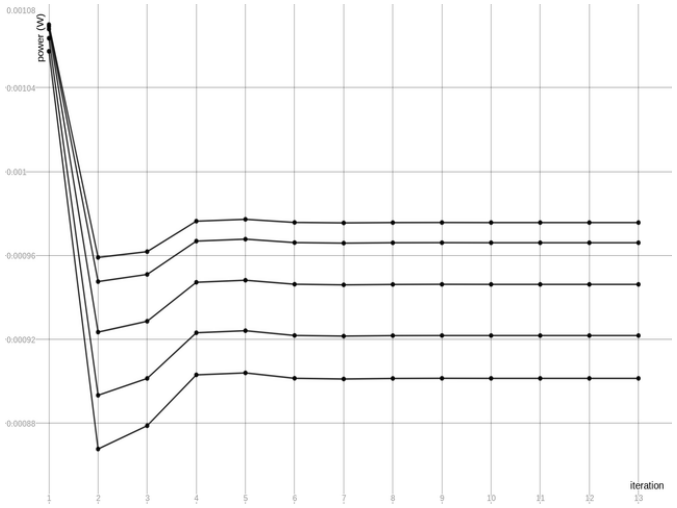
Σχήμα 7: Η μορφή των συναρτήσεων χρησιμότητας πέντε κανονικών ετικετών.



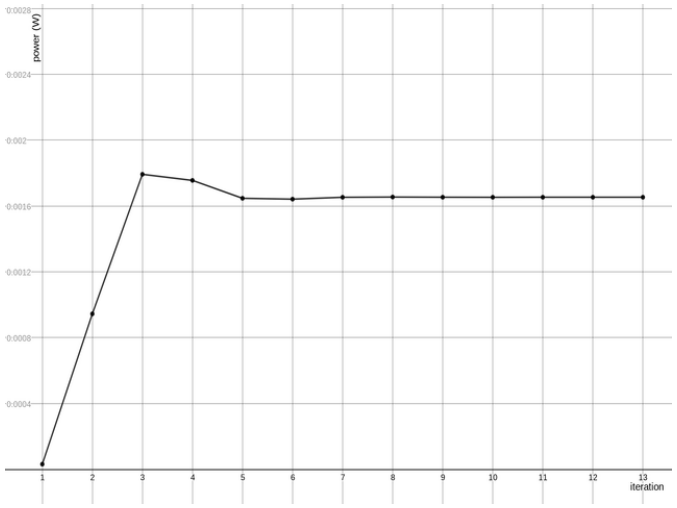
Σχήμα 8: Η ισχύς που επιλέγουν οι κανονικές ετικέτες.

Όπως φαίνεται στο παραπάνω σχήμα καθεμία από τις κανονικές παθητικές ετικέτες συγκλίνει σε μια τελική τιμή ισχύος οπισθοσκέδασης η οποία κυμαίνεται περίπου από $8.5 * 10^{-4}$ έως $9.5 * 10^{-4}$ Watt. Στο παραπάνω σχήμα δεν εμφανίζονται οι τυχαίες τιμές ισχύος που είχαν ανατεθεί στις ετικέτες κατά την αρχικοποίηση του αλγορίθμου.

Στην συνέχεια προστίθεται στο δίκτυο μια ετικέτα εισβολέα με τις τεχνικές προδιαγραφές που αναφέρθηκαν στο κεφάλαιο 6.1. Η απόσταση του εισβολέα από την συσκευή ανάγνωσης ορίζεται στα 1.5 μέτρα. Στην επόμενη σελίδα παρουσιάζεται η τιμή της ισχύος του μέχρι το σημείο σύγκλισης όπου και περιορίζεται λίγο πάνω από τα $16 * 10^{-4}$ Watt. Οι αντίστοιχες τιμές ισχύος για τις κανονικές ετικέτες αυξάνονται ελαφρώς και κυμαίνονται περίπου από $9 * 10^{-4}$ έως $9.75 * 10^{-4}$ Watt. Όπως και παραπάνω δεν εμφανίζονται οι τυχαίες τιμές ισχύος που είχαν ανατεθεί στις ετικέτες κατά την αρχικοποίηση του αλγορίθμου.



Σχήμα 9: Η ισχύς οπισθοσκέδασης των κανονικών ετικετών παρουσία εισβολέα.



Σχήμα 10: Η ισχύς οπισθοσκέδασης του εισβολέα.

7 Επίλογος

7.1 Σύνοψη

Με την παρούσα διπλωματική εργασία επιχειρείται η περιγραφή της λειτουργίας ενός ασύρματου δικτύου από παθητικές RFID ετικέτες, το οποίο βρίσκεται υπό επίθεση άρνησης υπηρεσιών από ετικέτες εισβολείς. Για την μοντελοποίηση της συμπεριφοράς του σε ένα γενικότερο πλαίσιο βελτιστοποίησης χρησιμοποιείται η θεωρία των μη συνεργατικών παιγνίων.

Για τον σκοπό αυτό γίνεται μια σύντομη αναφορά στις αρχές λειτουργίας των ετικετών και συσκευών ανάγνωσης RFID δίνοντας έμφαση στα χαρακτηριστικά των παθητικών ετικετών. Επιπλέον, αναφέρονται παραδείγματα εφαρμογής της συγκεκριμένης τεχνολογίας τόσο στην καθημερινή ζωή όσο και στις βιομηχανίες, παρουσιάζοντας τον ρόλο που έχει στην διάδοση του Internet of Things. Αναφέρονται τα πλεονεκτήματα της τεχνολογίας RFID, ενώ παρουσιάζονται και τα μειονεκτήματα που μπορεί να εμφανιστούν στην χρήση τέτοιων δικτύων. Για την εισαγωγή του αναγνώστη στις επιθέσεις έναντι ασύρματων δικτύων παρουσιάζονται συνοπτικά ορισμένες από τις κατηγορίες επιθέσεων και η μέθοδοι που ακολουθούνται για την περάτωσή τους, αναλύοντας περαιτέρω τις επιθέσεις άρνησης υπηρεσιών.

Στην συνέχεια, γίνεται αναλυτική περιγραφή του υπό επίθεση δικτύου (προσδιορίζοντας τα τεχνικά χαρακτηριστικά των ετικετών) το οποίο μοντελοποιείται ως ένα μη συνεργατικό παίγνιο μεταξύ των ετικετών που συμμετέχουν σε αυτό. Για να καταστεί αυτό δυνατό, ορίζονται οι συναρτήσεις χρησιμότητας που περιγράφουν την συμπεριφορά τόσο των κανονικών ετικετών όσο και των εισβολέων, λαμβάνοντας υπό όψιν τους στόχους της κάθε ετικέτας. Για τις κανονικές ετικέτες αυτό σημαίνει την μεγιστοποίηση της διεκπεραιωτικής ικανότητάς τους, ενώ για τους εισβολείς σημαίνει την παρεμπόδιση της αποκωδικοποίησης του ωφέλιμου σήματος που στέλνουν οι κανονικές ετικέτες στην συσκευή ανάγνωσης, εισάγοντας υψηλά επίπεδα παρεμβολών στο σύστημα. Αυτές οι συναρτήσεις χρησιμότητας περιέχουν και έναν όρο ο οποίος εκφράζει το ρίσκο για την συμμετοχή της στο δίκτυο, και έχει ως σκοπό την συμμόρφωση των ετικετών σε μια πιο ‘‘κοινωνική’’ συμπεριφορά. Με βάση αυτές τις συναρτήσεις και το σημείο μεγιστοποίησής τους προσδιορίζεται το σημείο ισορροπίας στο οποίο φτάνουν οι ετικέτες όσον αφορά την ισχύ οπισθοσκέδασής.

Για την εύρεση αυτών των τελικών τιμών ισχύος που φτάνουν οι ετικέτες προτείνεται ένας κατανεμημένος επαναληπτικός αλγόριθμος, ο οποίος τερματίζει όταν οι

ετικέτες συγκλίνουν στο σημείο ισορροπίας. Βασικά πλεονεκτήματα αυτού του αλγορίθμου είναι η χαμηλή πολυπλοκότητά του, καθώς και το γεγονός ότι μπορεί να εκτελεστεί ανεξάρτητα σε κάθε ετικέτα, χωρίς να απαιτείται μεταξύ τους επικοινωνία (δεδομένων πληροφοριών σχετικά με τις παρεμβολές του δικτύου που η συσκευή ανάγνωσης γνωστοποιεί στις ετικέτες). Αυτό επιτρέπει την παραλληλοποίηση του προβλήματος κάτι που έχει ως συνέπεια την ταχύτερη εύρεση του σημείου ισορροπίας.

Τέλος, με την χρήση προγράμματος που υλοποιεί τον επαναληπτικό αλγόριθμο, γίνεται ενδεικτική προσομοίωση της λειτουργίας ενός δικτύου στο οποίο συμμετέχουν πέντε κανονικές ετικέτες, και στην συνέχεια εισάγεται μια ετικέτας εισβολέας. Με βάση τα αποτελέσματά του παρατίθενται γραφικές παραστάσεις που περιγράφουν την συμπεριφορά των ετικετών και τον περιορισμό στον θόρυβο που εισάγει ο εισβολέας στο σύστημα.

7.2 Μελλοντική εργασία

Παρότι στην συγκεκριμένη εργασία επικεντρώσαμε το ενδιαφέρον μας στην θεωρητική προστασία και την μελέτη της διεκπεραιωτικής ικανότητας των ετικετών με βάση τις συναρτήσεις χρησιμότητας που περιγράφουν την συμπεριφορά τους στο δίκτυο, υπάρχουν και άλλες μετρικές που θα μπορούσαν να μελετηθούν. Ένα παράδειγμα είναι η ενεργειακή απόδοση των κανονικών ετικετών στο δίκτυο και το πως αυτή μεταβάλλεται με την παρουσία κάποιου εισβολέα. Για την μελέτη αυτής της μετρικής οι συναρτήσεις χρησιμότητας θα έπρεπε να λαμβάνουν υπό όψιν την διεκπεραιωτική ικανότητα των κανονικών ετικετών ως προς την ισχύ του σήματος τους.

Όσον αφορά τις συναρτήσεις χρησιμότητας που μελετήθηκαν στην παρούσα εργασία, κατά τον ορισμό του προβλήματος μεγιστοποίησης, θα μπορούσαν να μεταβληθούν (διαφορετική μορφή της καθαρής συνάρτησης χρησιμότητας ή και της συνάρτησης ρίσκου, κανονικοποίηση κτλπ) έτσι ώστε να περιγράφουν με μεγαλύτερη ακρίβεια την συμπεριφορά ενός τέτοιου δικτύου, συνεχίζοντας ωστόσο να εκφράζουν τους στόχους της κάθε ετικέτας ανάλογα με το είδος της. Τέτοιες μετατροπές θα βοηθούσαν στο να είναι οι συναρτήσεις λιγότερο ευαίσθητες στην παραμετροποίηση, καθώς και να μπορούν να εφαρμοστούν σε μεγαλύτερο εύρος διαφορετικών τοπολογιών και μορφών (για παράδειγμα περισσότερες ετικέτες, διαφορετικές αποστάσεις από την συσκευή ανάγνωσης) ενός παθητικού δικτύου RFID. Η παραμετροποίηση και η σύγκλιση των ετικετών σε ακραίες τιμές ισχύος οπισθοσκέδασης ανάλογα με την μορφή του δικτύου προσομοίωσης, υπήρξε μια από τις σημαντικότερες δυσκολίες κατά την εκπόνηση αυτής της εργασίας.

Με την χρήση κατάλληλων συναρτήσεων χρησιμότητας, που θα εκφράζουν συγκεκριμένες μετρικές για τις παθητικές ετικέτες, θα μπορούσε να δοκιμαστεί η αποτελεσματικότητα του πλαισίου που παρουσιάστηκε στην παρούσα εργασία είτε σε ένα πραγματικό και ελεγχόμενο δίκτυο παθητικών ετικετών (όπως για παράδειγμα μια βιβλιοθήκη ή έναν χώρο αποθήκευσης), είτε στα πλαίσια πειραματικών υποδομών του Internet of Things. Τέλος, λόγω της κατανεμημένης φύσης συστημάτων που αναδεικνύεται κατά την ανάπτυξη του Internet of Things, θα μπορούσαν να μελετηθούν και διαφορετικά είδη επιθέσεων, όπως για παράδειγμα επιθέσεις στις οποίες οι εισβολείς τοποθετούνται στρατηγικά σε συγκεκριμένες θέσεις με στόχο την μεγιστοποίηση της ζημιάς που προκαλούν, ή επιθέσεις που στοχεύουν σε ένα συγκεκριμένο υποσύνολο των κανονικών RFID του δικτύου [3].

8 Βιβλιογραφία

[1] J. Landt, "The history of RFID", *IEEE potentials*, vol. 24, no. 4, pp. 8–11, 2005.

[2] K. Domdouzis, B. Kumar, and C. Anumba, "Radio-Frequency Identification (RFID) applications: A brief introduction", *Advanced Engineering Informatics*, vol. 21, no. 4, pp. 350–355, 2007.

[3] E. E. Tsiropoulou, J. S. Baras, S. Papavassiliou, and G. Qu, "On the Mitigation of Interference Imposed by Intruders in Passive RFID Networks", in *International Conference on Decision and Game Theory for Security*, Springer, 2016, pp. 62–80.

[4] M. Bolic, D. Simplot-Ryl, and I. Stojmenovic, *RFID systems: research trends and challenges*. John Wiley & Sons, 2010.

[5] V. Chawla and D. S. Ha, "An overview of passive RFID", *IEEE Communications Magazine*, vol. 45, no. 9, 2007.

[6] K. Finkenzeller, *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John Wiley & Sons, 2010.

[7] V. K. Bachu, S. Saram, and N. V. S. Shravan kumar Sharma, "A Review of RFID Technology", *International Journal of Engineering Sciences & Research Technology*, vol. 2, pp. 2760–2762, Oct. 2013.

[8] M. Burmester and B. De Medeiros, "The security of EPC Gen2 compliant RFID protocols", in *International Conference on Applied Cryptography and Network Security*, Springer, 2008, pp. 490–506.

[9] Y. Duroc and S. Tedjini, "RFID: A key technology for Humanity", *Comptes Rendus Physique*, vol. 19, no. 1, pp. 64–71, 2018.

[10] M. Kaur, M. Sandhu, N. Mohan, and P. S. Sandhu, "RFID technology principles, advantages, limitations & its applications", *International Journal of Computer and Electrical Engineering*, vol. 3, no. 1, p. 151, 2011.

[11] I. Antic and T. I. Tokic, "RFID: Past, present, future", *Scientific Publications of the State University of NOVI PAZAR SER.*, vol. 4, no. 1, pp. 39–52, 2012.

[12] A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in E-passports", in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, IEEE, 2005, pp. 74–88.

[13] C. Oberli, M. Torres-Torriti, and D. Landau, "Performance evaluation of UHF RFID technologies for real-time passenger recognition in intelligent public transportation systems", *IEEE transactions on intelligent transportation systems*, vol. 11, no. 3, pp. 748–753, 2010.

[14] T. Borgohain and S. Sanyal, "Technical Analysis of Security Infrastructure in RFID Technology", *arXiv preprint arXiv:1505.00172*, 2015.

[15] A. Narayanan, S. Singh, and M. Somasekharan, "Implementing RFID in Library: Methodologies, advantages and disadvantages", *Recent Advances in Information Technology*, vol. 271, 2005.

[16] L. Ruiz-Garcia and L. Lunadei, "The role of RFID in agriculture: Applications, limitations and challenges", *Computers and Electronics in Agriculture*, vol. 79, no. 1, pp. 42–50, 2011.

[17] Z. N. Chen, X. Qing, and H. L. Chung, "A universal UHF RFID reader antenna", *IEEE Transactions on Microwave Theory and Techniques*, vol. 57, no. 5, pp. 1275–1282, 2009.

[18] P. V. Nikitin and K. Rao, "Performance limitations of passive UHF RFID systems", in *Antennas and Propagation Society International Symposium 2006, IEEE*, IEEE, 2006, pp. 1011–1014.

[19] Q. Xiao, T. Gibbons, and H. Lebrun, "RFID Technology, Security Vulnerabilities, and Countermeasures", in *Supply Chain the Way to Flat Organisation*, InTech, Jan. 2009, pp. 357–382. DOI: 10.5772/6668.

[20] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "RFID systems: A survey on security threats and proposed solutions", in *IFIP international conference on personal wireless communications*, Springer, 2006, pp. 159–170.

[21] A. Juels and S. A. Weis, "Defining strong privacy for RFID", *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 1, p. 7, 2009.

[22] A. Grover and H. Berghel, "A survey of RFID deployment and security issues", *Journal of information processing systems*, vol. 7, no. 4, pp. 561–580, 2011.

[23] Q. Z. Sheng, X. Li, and S. Zeadally, "Enabling next-generation RFID applications: Solutions and challenges", *Computer*, vol. 41, no. 9, 2008.

[24] L. Tan and N. Wang, "Future internet: The Internet of Things", in *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, vol. 5, Aug. 2010, pp. V5–376–V5–380. DOI: 10.1109/ICACTE.2010.5579543.

[25] B. Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy", in *Internet of Things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing*, IEEE, 2011, pp. 709–712.

[26] K. Singh, "Security in RFID Networks and Protocols", *International Journal of Information and Computation Technology.*, pp. 425–432, ISSN: 0974-2239.

[27] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses", *Information Systems Frontiers*, vol. 12, no. 5, pp. 491–505, Nov. 2010, ISSN: 1572-9419. DOI: 10.1007/s10796-009-9210-z. [Online]. Available: https://doi.org/10.1007/s10796-009-9210-z.

[28] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends", *Proceedings of the IEEE*, pp. 1–39, 2016.

[29] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis, "Security threats on EPC based RFID systems", in *Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on*, IEEE, 2008, pp. 1242–1244.

[30] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial", *IEEE wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[31] S. L. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions", *IEEE Security & Privacy*, vol. 3, no. 3, pp. 34–43, 2005.

[32] J. Ayoade, "Roadmap to solving security and privacy concerns in RFID systems", *Computer Law & Security Review*, vol. 23, no. 6, pp. 555–561, 2007.

[33] G. Avoine and P. Oechslin, "RFID Traceability: A Multilayer Problem", in *Financial Cryptography and Data Security*, A. S. Patrick and M. Yung, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 125–140, ISBN: 978-3-540-31680-0.

[34] A. Karygiannis, T. Phillips, and A. Tsibertzopoulos, "RFID Security: A Taxonomy of Risk", in *2006 First International Conference on Communications and Networking in China*, IEEE, Oct. 2006, pp. 1–8. DOI: 10.1109/CHINACOM.2006.344722.

[35] S. Blythe, B. Fraboni, S. Lall, H. Ahmed, and U. de Riu, "Layout reconstruction of complex silicon chips", *IEEE journal of solid-state circuits*, vol. 28, no. 2, pp. 138–145, 1993, ISSN: 0018-9200.

[36] M. Burmester and B. De Medeiros, "RFID Security: Attacks, Countermeasures and Challenges", in *The 5th RFID Academic Convocation, The RFID Journal Conference*, 2007.

[37] Y. Oren and A. Shamir, "Power analysis of RFID tags", *Rump session of Advances in Cryptology, CRYPTO*, vol. 2006, 2006.

[38] G. Kulkarni, R. Shelke, R. Sutar, and S. Mohite, ""RFID security issues & challenges"", in *2014 International Conference on Electronics and Communication Systems (ICECS)*, Feb. 2014, pp. 1–4. DOI: 10.1109/ECS.2014.6892730.

[39] D. Welch and S. Lathrop, "Wireless security threat taxonomy", in *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, IEEE, 2003, pp. 76–83.

[40] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, "Guidelines for securing radio frequency identification (RFID) systems", *NIST Special publication 800-98*, vol. 80, pp. 1–154, 2007.

[41] A. Mitrokotsa, M. Beye, and P. Peris-Lopez, "Classification of RFID Threats based on Security Principles", 2010.

[42] H. Knospe and K. Lemke-Rust, "Towards Secure and Privacy-Enhanced RFID Systems", *RFID SYSTEMS: RESEARCH TRENDS AND CHALLENGES*, p. 417, 2010.

[43] M. J. Osborne and A. Rubinstein, *A course in game theory*. MIT press, 1994.

[44] E. E. Tsiropoulou, T. Kastrinogiannis, and S. Papavassiliou, "Uplink power control in qos-aware multi-service cdma wireless networks", *Journal of Communications*, vol. 4, no. 9, pp. 654–668, 2009.

[45] E. E. Tsiropoulou, T. Kastrinogiannis, and S. Papavassiliou, "A utility-based power allocation non-cooperative game for the uplink in multi-service CDMA wireless networks", in *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, ACM, 2009, pp. 365–370.