

University of Peloponnese
Department of Informatics and Telecommunications

Reconfigurable Intelligent Surfaces for Smart Cities



Ioanna Papailiou
2022202202014

Supervisor: Konstantinos Peppas

A thesis submitted in partial fulfillment of the University's requirements
for the masters degree.

November, 2023

Πανεπιστήμιο Πελοποννήσου
Τμήμα Πληροφορικής και Τηλεπικοινωνιών

Έξυπνες επαναδιομορφώσιμες επιφάνειες στις ευφυείς πόλεις



Ιωάννα Παπαηλίου
2022202202014

Επιβλέπων: Κωνσταντίνος Πέππας

Διπλωματική εργασία

Νοέμβριος, 2023

Copyright © Παπαηλίου Ιωάννα, 2023.

Με επιφύλαξη παντός δικαιώματος . All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τους συγγραφείς. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τους συγγραφείς και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Πανεπιστημίου Πελοποννήσου.

Abstact

This paper refers to Reconfigurable Intelligent Surfaces and the great interest they have attracted due to their ability to enhance the capacity and coverage of wireless networks by intelligently reconfiguring the wireless environment. For this reason, RIS are considered as a promising technology for the sixth generation of communication networks. The heterogeneous network of things and mobile edge computing (MA-MEC) are considered as supporting technologies for building o smart city. To address the conflict between computing capacity and low-cost mobile devices in the IoT, MA-MEC is available to support services and applications with limited resources and high computing demand through computation abstraction and distributed content delivery/storage. However, deploying cloud computing capabilities in the radio access network may face serious security threats, originating not only from existing technologies and networks but also from the MA-MEC based itself. In this work, solutions to address security threats from physical layer perspective are investigated.

Keywords: Reconfigurable Intelligent Surfaces, smart cities, physical layer security, wireless channels, internet of things, multi-access mobile edge computing, MA-MEC-based IoT, heterogeneous internet of things

Περίληψη

Η παρούσα εργασία αναφέρεται στις Ευφυείς Επαναδιαμορφώσιμες Επιφάνειες και στο μεγάλο ενδιαφέρον που έχουν προσελκύσει λόγω της δυνατότητας τους να ενισχύσουν τη χωρητικότητα και την κάλυψη των ασύρματων δικτύων με έξυπνη αναδιαμόρφωση του ασύρματου περιβάλλοντος. Για αυτόν τον λόγο, οι RIS θεωρούνται ως μια ελπιδοφόρα τεχνολογία για την έκτη γενιά των δικτύων επικοινωνίας. Το ετερογενές δίκτυο των πραγμάτων και οι υπολογιστές άκρων για φορητές συσκευές (MA-MEC) θεωρούνται ως υποστηρικτικές τεχνολογίες για την οικοδόμηση μιας έξυπνης πόλης. Για την αντιμετώπιση της σύγκρουσης μεταξύ της ικανότητας υπολογισμού και των κινητών συσκευών χαμηλού κόστους στο IoT, το MA-MEC είναι διαθέσιμο για την υποστήριξη υπηρεσιών και εφαρμογών με περιορισμένους πόρους και υψηλή απαίτηση σε υπολογισμό μέσω της αφαίρεσης υπολογισμού και της κατανεμημένης παράδοσης/αποθήκευσης περιεχομένου. Ωστόσο, η εγκατάσταση δυνατοτήτων υπολογιστικού νέφους στο δίκτυο πρόσβασης ραδιοφώνου μπορεί να αντιμετωπίσει σοβαρές απειλές ασφάλειας, που προέρχονται όχι μόνο από τις υπάρχουσες τεχνολογίες και δίκτυα αλλά και από το ίδιο το IoT που βασίζεται στο MA-MEC. Στην παρούσα εργασία, ερευνούνται λύσεις για την αντιμετώπιση των απειλών ασφάλειας από την οπτική γωνία του φυσικού επιπέδου.

Λέξεις κλειδιά: Επαναδιαμορφώσιμες έξυπνες επιφάνειες, ευφυείς πόλεις, ασφάλεια φυσικού επιπέδου, ασύρματα κανάλια, internet of things, multi-access mobile edge computing, MA-MEC-based IoT, ετερογενές διαδίκτυο των πραγμάτων

Περιεχόμενα

1. Εισαγωγή	9
2. Reconfigurable Intelligent surfaces.....	10
2.1 Πλεονεκτήματα των RIS.....	10
2.2 Εφαρμογές των RIS.....	11
2.3 Από τη φυσική στις ασύρματες επικοινωνίες.....	12
2.4 Διάφορες κατηγορίες των RIS.....	13
2.5 Κατανόηση των μεταεπιφανειών από την οπτική της φυσικής.....	14
2.6 Ανάλυση των RISs: Προοπτική της Οπτικής Ακτίνων έναντι της προοπτικής της κυματικής οπτικής.....	15
2.7 Επίτευξη Ρυθμισιμότητας: Patch Array RIS.....	16
2.8 Αρχές λειτουργίας των RIS.....	17
2.9 Προοπτική των RIS	21
2.10 Ανάλυση απόδοσης συστημάτων πολυκεραιών υποβοηθήμενων RIS....	22
2.10.1 Ανάλυση απόδοσης	24
2.10.2 Συγκριτικές μέθοδοι αναφοράς.....	24
2.10.3 Συμπεράσματα και προοπτικές.....	25
2.11 Διαμόρφωση RIS και κατανομής πόρων	25
2.12 Διαχείριση πόρων σε δίκτυα ενισχυμένα με RIS.....	27
2.13 Μηχανική εκπαίδευση για συστήματα επικοινωνίας ενισχυμένα με RIS.....	30
2.14 Ενσωμάτωση RIS με άλλες τεχνολογίες προς 6G.....	32
2.14.1 NOMA και RIS.....	33
2.14.2 PLS και RIS.....	33
2.14.3 SWIPT και RIS	34
2.14.4 UAV και RIS.....	34
2.14.5 Αυτόνομη οδήγηση/συνδεδεμένα οχήματα και RIS.....	35
2.15 Συμπεράσματα και προκλήσεις	36
3. Έλεγχος αυθεντικότητας φυσικού επιπέδου στις ασύρματες επικοινωνίες.....	37
3.1 Εισαγωγή.....	37
3.2 Αυθεντικοποίηση φυσικού επιπέδου	37
3.3 Σύγκριση μεταξύ του PLA και άλλων τεχνικών ασφαλείας φυσικού επιπέδου	39
3.4 Συνεισφορές.....	41
3.5 Μοντέλο συστήματος του PLA.....	42
4. Ενίσχυση της ασφάλειας πληροφοριών μέσω προσεγγίσεων φυσικού επιπέδου σε ετερογενή IoT με πολλαπλή πρόσβαση Mobile Edge computing σε έξυπνη πόλη....	45
4.1 Εισαγωγή.....	46
4.2 Λύσεις για την ασφάλεια των πληροφοριών στις ασύρματες επικοινωνίες.....	49
4.3 Ασφάλεια φυσικού στρώματος για ασφάλεια IoT βάσει MA-MEC.....	51
5. Συμπεράσματα.....	60
6. Βιβλιογραφία.....	61

Κατάλογος συντομογραφιών

AUV	Autonomous Underwater Vehicle
D2D	Device-to-device
FD	Full-duplex
IoT	Internet of Things
LIS	Large Intelligent Surfaces
LoS	Line-of-sight
QoS	Quality of Service
RIS	Reconfigurable Intelligent Surfaces
SINR	Signal-to-interference plus noise ratio
SWIPT	Simultaneous wireless information and power transfer
UAV	Unmanned Aerial Vehicle

Κατάλογος Σχημάτων

1	RIS σε ασύρματα δίκτυα επικοινωνίας.....	13
2	Αρχή ισοδυναμίας του Love (Για το Region I).....	15
3	Λειτουργίες ανακλαστικών επιφανειών	20
4	Απεικόνιση των γενικευμένων νόμων διάθλασης και ανάκλασης.....	20
5	Συντεταγμένη αναπαράσταση συνθήκης συνφάσεως.....	22
6	Απεικόνιση της διαχείρισης πόρων σε δίκτυα μεγάλης κλίμακας που υποστηρίζονται από RIS.....	29
7	Σχέση μεταξύ διαφορετικών τεχνικών ασφάλειας.....	40
8	Μοντέλο συστήματος του PLA σε ασύρματες επικοινωνίες με τέσσερις κόμβους.....	44
9	Πολλαπλά σενάρια ετερογενούς IoT με βάση MA-MEC σε έξυπνη πόλη	47
10	Η κλασική ιεραρχική δομή της στοίβας πρωτοκόλλου επικοινωνίας και τα παραδείγματα μηχανισμών ασφαλείας που αναπτύσσονται σε κάθε επίπεδο.....	50
11	Η ένθετη δομή ενός κωδικού μυστικότητας.....	52
12	Τα πολυδιάστατα χαρακτηριστικά των πόρων ασύρματου δικτύου.....	55
13	Απεικόνιση ασφαλούς διαμόρφωσης δέσμης σε συστήματα πολλαπλών κεραιών.....	57

1. Εισαγωγή

Τα τελευταία χρόνια το όραμα της οικοδόμησης μιας έξυπνης πόλης είναι σχεδόν πραγματικότητα. Η εξέλιξη του Internet of Things, του cloud computing και άλλων ωθεί την τεχνολογία στη δομή της έξυπνης πόλης. Σε αυτή την διαδικασία, η σύγκλιση διαφοροποιημένων ασύρματων τεχνολογιών είναι απαραίτητη για την υποστήριξη της ομαλής τεχνικής μετάβασης και την παροχή διαφόρων εξατομικευμένων υπηρεσιών. Πολλά ασύρματα δίκτυα με διαφορετικές υποδομές και τεχνολογίες, καθώς και διάφορα ευφυή τερματικά, που συχνά αναφέρονται ως ετερογενή IoT, έχουν εφαρμοστεί ευρέως στην έξυπνη πόλη για την υποστήριξη παρακολούθησης σε πραγματικό χρόνο, απομακρυσμένης ιατρικής και έξυπνων μεταφορών. Για την ανάπτυξη ετερογενούς IoT στην πράξη, ο υπολογισμός κινητής ακμής πολλαπλής πρόσβασης (MA-MEC) που χρησιμοποιεί διάφορες τεχνολογίες ραδιοπρόσβασης με προσαρμοστικό τρόπο έχει προσελκύσει αυξανόμενες ανησυχίες, ιδίως σε σενάρια περιορισμένων πόρων και ευαίσθητων σε υπολογισμούς. Η εφαρμογή του MA-MEC στην έξυπνη πόλη μπορεί να μειώσει σημαντικά τον λανθάνοντα χρόνο επεξεργασίας των εργασιών, να αποφύγει τη συμφόρηση του κεντρικού υπολογιστικού νέφους, να παρατείνει τη διάρκεια ζωής της μπαταρίας των κινητών συσκευών και επομένως θα βελτιώσει την ποιότητα υπηρεσίας και την εμπειρία του χρήστη.

2.Reconfigurable Intelligent Surfaces

Οι έξυπνες επιφάνειες με δυνατότητα επαναδιαμόρφωσης (RIS), γνωστές και ως μεγάλες ευφυείς επιφάνειες (Large Intelligent Surfaces - LISs) έχουν προσελκύσει το επιστημονικό ενδιαφέρον και έχουν λάβει σημαντική προσοχή για την δυνατότητα τους να ενισχύουν τη χωρητικότητα και την κάλυψη των ασύρματων δικτύων με έξυπνη επαναδιαμόρφωση του ασύρματου περιβάλλοντος εξάπλωσης. Για αυτόν το λόγο, οι έξυπνες επιφάνειες με δυνατότητα επαναδιαμόρφωσης θεωρούνται μια πολλά υποσχόμενη τεχνολογία για την 6η γενιά δικτύων επικοινωνίας. Στο πλαίσιο της παρούσας εργασίας, παρέχεται μία εκτενής επισκόπηση των RIS, διερευνάται, επίσης, η αξιολόγηση της απόδοσή τους, μελετώνται οι εφαρμογές της μηχανικής μάθησης στα RIS-enhanced ασύρματα δίκτυα καθώς και η ένταξη των RISs με άλλες αναδυόμενες τεχνολογίες. Οι RIS περιλαμβάνουν μια σειρά από ανακλαστικά στοιχεία για την αναδιαμόρφωση του προσπίπτοντος σήματος.

2.1 Πλεονεκτήματα των RIS

Υπάρχουν αρκετά πλεονεκτήματα για την προτίμηση των RIS. Ορισμένα εκ των οποίων αναφέρονται παρακάτω:

- i. Εύκολη ανάπτυξη: Οι RIS είναι σχεδόν παθητικές συσκευές κατασκευασμένες από ηλεκτρομαγνητικό υλικό. Οι έξυπνες επιφάνειες με δυνατότητα επαναδιαμόρφωσης μπορούν να αναπτυχθούν σε διάφορες συσκευές. Για παράδειγμα προσόψεις κτιρίων, εσωρετικούς τοίχους, εναέριες πλατφόρμες, σταθμών αυτοκινητόδρομων, παράθυρο οχημάτων και λουπά.
- ii. Βελτίωση φασματικής απόδοσης: Οι έξυπνες επιφάνειες με δυνατότητα επαναδιαμόρφωσης έχουν τη δυνατότητα να αναδιαμορφώνουν το περιβάλλον ασύρματης μετάδοσης αντισταθμίζοντας την απώλεια ισχύος σε μεγάλες αποστάσεις. Η ευθεία πορεία που ακολουθεί η οπτική ακτινοβολία κατά τη διάρκεια της μετάδοσης της από τους σταθμούς βάσης στους κινητούς χρήστες μπορούν να δημιουργηθούν μέσω παθητικής ανάκλασης των προσκρούσεων ραδιοφωνικών σημάτων. Η βελτίωση της απόδοσης αποκτά σημασία όταν η παραπάνω σύνδεση μεταξύ σταθμών βάσης και χρηστών μπλοκάρεται από εμπόδια, π.χ. πολυώροφα κτίρια. Δεδομένης της έξυπνης ανάπτυξης και σχεδίασης των RIS, μπορεί να κατασκευαστεί ένα περιβάλλον ασύρματου δικτύου ορισμένο από λογισμικό, το οποίο, με τη σειρά του, παρέχει πιθανές βελτιώσεις του λόγου λαμβανόμενου σήματος προς παρεμβολή συν το λόγο θορύβου (SINR).
- iii. Φιλικά προς το περιβάλλον: Σε αντίθεση με τα συμβατικά συστήματα αναμετάδοσης, οι RIS έχουν την ικανότητα να διαμορφώνουν το εισερχόμενο σήμα ελέγχοντας τη μετατόπιση φάσης κάθε ανακλαστικού στοιχείου αντί να χρησιμοποιούν έναν ενισχυτή ισχύος. Έτσι, λοιπόν, η ανάπτυξη RIS είναι πιο ενεργειακά αποδοτική και φιλική προς το περιβάλλον.
- iv. Συμβατότητα: Οι RIS υποστηρίζουν full duplex (FD) και full band μετάδοση εξαιτίας του γεγονότος ότι αντανακλούν μόνο τα ηλεκτρομαγνητικά κύματα.

Επιπλέον, τα δίκτυα ασύρματης επικοινωνίας με ενισχυμένες αντανάκλασεις είναι συμβατά με τα πρότυπα και το υλικό των υφιστάμενων ασύρματων δικτύων.

Λόγω των προαναφερθέντων ελκυστικών χαρακτηριστικών, οι RIS αναγνωρίζονται ως αποτελεσματική λύση για τον μετριασμό ενός ευρέος φάσματος προκλήσεων σε εμπορικές και μη στρατιωτικές εφαρμογές.

2.2 Εφαρμογές των RIS

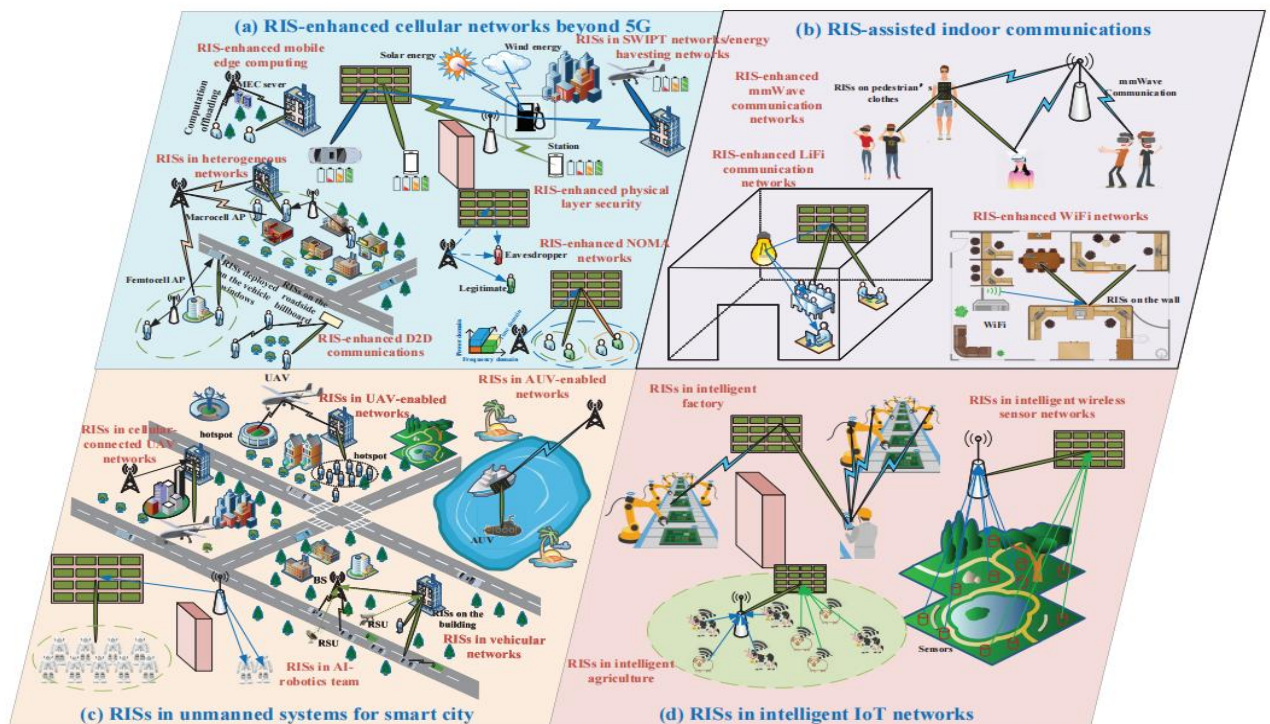
Σε αυτήν την ενότητα, θα αναφερθούν οι εφαρμογές των RIS σε διάφορα ασύρματα δίκτυα επικοινωνίας. Για να επιτευχθεί αυτό, θα χρησιμοποιήσουμε το Σχήμα 1 προκειμένου να γίνει πιο εύκολη η κατανόηση τους. Πιο συγκεκριμένα, στην Εικόνα 1(α) απεικονίζονται κυψελωτά δίκτυα ενισχυμένα με RIS, όπου τα RIS αναπτύσσονται για την παράκαμψη των εμποδίων μεταξύ των σταθμών βάσης και των χρηστών. Έτσι, το QoS σε ετερογενή δίκτυα και η απόδοση του λανθάνοντος χρόνου σε δίκτυα υπολογισμού κινητής άκρης (MEC) βελτιώνονται. Από την άλλη πλευρά, οι RIS μπορούν να λειτουργήσουν ως ένας κόμβος ανάκλασης σήματος για υποστήριξη μαζικής συνδεσιμότητας μέσω μετριασμού παρεμβολών σε δίκτυα επικοινωνίας D2D ή οι RIS μπορούν να ακυρώσουν ανεπιθύμητα σήματα σχεδιάζοντας έξυπνα την παθητική διαμόρφωση δέσμης στο πλαίσιο της ασφάλειας φυσικού επιπέδου. Επιπροσθέτως, τα RIS μπορούν να αναπτυχθούν για να ενισχύσουν την ισχύ του λαμβανόμενου σήματος των χρηστών κινητής τηλεφωνίας και να μετριάσουν τις παρεμβολές από γειτονικές κυψέλες και η απώλεια ισχύος σε μεγάλες αποστάσεις μπορεί να αντισταθμίζεται σε ταυτόχρονα ασύρματα δίκτυα πληροφοριών (SWIPT).

Στην Εικόνα 1(b), απεικονίζονται οι επικοινωνίες εσωτερικών χώρων με τη βοήθεια RIS, όπου οι RIS μπορούν να αναπτυχθούν σε τοίχους για τη βελτίωση του QoS σε ορισμένα σενάρια εσωτερικών χώρων, όπως οι εφαρμογές εικονικής πραγματικότητας. Επιπλέον, για να διασφαλιστεί ότι δεν υπάρχουν τυφλά σημεία στην περιοχή κάλυψης ορισμένων block-sensitive σεναρίων, όπως οι επικοινωνίες ορατού φωτός και τα δίκτυα ασύρματης πιστότητας, μπορεί να δημιουργηθεί μια ενωμένη εικονική σύνδεση LoS με τη βοήθεια RIS μεταξύ των σημείων πρόσβασης και των χρηστών, η οποία υποδεικνύει ότι και οι δυο συνδέσεις μεταξύ των RIS και των χρηστών μπορούν να είναι σε LoS.

Στην Εικόνα 1(c), απεικονίζονται μη επανδρωμένα συστήματα ενισχυμένα με RIS. Σε αυτό το παράδειγμα, οι RIS μπορούν να χρησιμοποιηθούν προκειμένου να βελτιωθεί η απόδοση ασύρματων δικτύων που χρησιμοποιούνται σε αναπτυσσόμενες τεχνολογίες, όπως δίκτυα ασύρματων οχημάτων χωρίς πλήρωμα, δίκτυα UAV που είναι συνδεδεμένα με κινητά δίκτυα, αυτόνομα δίκτυα οχημάτων, αυτόνομα δίκτυα υποβρύχιων οχημάτων AUV και τέλος έξυπνα ρομποτικά δίκτυα. Παραδείγματος χάριν, σε δίκτυα ασύρματων οχημάτων χωρίς πλήρωμα (UAV) με ενισχυμένες επαναδιαμορφούμενες νέες επιφάνειες (RIS) μπορεί κάποιος να προσαρμόσει τις μετατοπίσεις φάσης των RIS αντί να ελέγχει την κίνηση των UAVs, προκειμένου να δημιουργήσει συνενωμένους εικονικούς συνδέσμους ευθείας

ορατότητας (LoS), μεταξύ των UAVs και των χρηστών. Ως εκ τούτου, τα UAVs μπορούν να διατηρούν την κατάσταση αιώρησης μόνο όταν οι συνενωμένοι εικονικοί σύνδεσμοι LoS δεν μπορούν να δημιουργηθούν, ακόμα και με την βοήθεια των RIS, μειώνοντας έτσι τις κινητικές παρεμβάσεις και την κατανάλωση ενέργειας των UAVs.

Στην Εικόνα 1(d), εμφανίζονται δίκτυα Internet of Things (IoT) με ενισχυμένες RIS, όπου οι RIS χρησιμοποιούνται για να βοηθήσουν έξυπνα ασύρματα δίκτυα αισθητήρων.



Σχήμα 1: Το RIS σε ασύρματα δίκτυα επικοινωνίας

2.3 Από τη φυσική στις ασύρματες επικοινωνίες

Μια έξυπνη επαναδιαμορφώσιμη επιφάνεια (RIS) είναι μια δισδιάστατη (2D) δομή υλικού που μπορεί να αλλάξει τις φυσικές ιδιότητες της με προγραμματισμό. Το πιο σημαντικό χαρακτηριστικό μιας RIS είναι η δυνατότητα να αναδιαμορφώνουν την απόκρισή τους στα ηλεκτρομαγνητικά κύματα. Εν αντιθέσει, με τα συμβατικά ασύρματα δίκτυα, όπου τα κανάλια μεταξύ πομπών και δεκτών είναι σταθερά, στα δίκτυα που χρησιμοποιούν RIS, μπορούν να ελέγχονται και να προσαρμόζονται δυναμικά. Αυτός ο δυναμικός έλεγχος των ηλεκτρομαγνητικών κυμάτων επιτρέπει

να ενισχυθεί η ισχύς του επιθυμητού σήματος που λαμβάνεται στις τερματικές συσκευές, βελτιώνοντας την ασύρματη επικοινωνία.

2.4 Διάφορες κατηγορίες RIS

Οι RIS μπορούν να υλοποιηθούν χρησιμοποιώντας τεχνολογίες μετα-υλικά ή βάσει παραγκωνισμένων πινάκων (patch-array). Οι RIS βασισμένες σε μετα-υλικά ονομάζονται “μετα-επιφάνειες”(metasurfaces). Επίσης, οι RIS μπορούν να λειτουργούν ως επιφάνειες ανάκλασης/σύσπασης μεταξύ της βάσης και του χρήστη είτε ως επιφάνειες κυματοθυρίδας που λειτουργούν στη βάση. Με βάση τους μηχανισμούς ρύθμισης, τα RIS μπορούν να αναδιαμορφωθούν ηλεκτρικά, μηχανικά ή θερμικά. Ανάλογα με την κατανάλωση ενέργειας τους, οι RIS μπορούν να κατηγοριοποιηθούν στις εξής κατηγορίες: παθητικές με απώλειες, παθητικές χωρίς απώλειες ή ενεργές. Οι τελικές δυνατότητες απόδοσης των RIS καθορίζονται από την ενεργή ή παθητική τους φύση. Βέβαια, αξίζει να σημειώσουμε ότι οι RIS δεν μπορούν να είναι πλήρως παθητικές λόγω της ενσωματωμένης ιδιότητας τους να είναι προσαρμόσιμες.

Οι RIS μπορούν να λειτουργήσουν ως κυματοθυρίδα, σύσπαση ή ανάκλαση. Με βάση την αρχή της ισοδυναμίας του Love, το ανακλαστικό και το διαθλαστικό ηλεκτρομαγνητικό πεδίο μπορούν να μελετηθούν με την εισαγωγή ισοδύναμων επιφανειακών ηλεκτρικών και μαγνητικών ρευμάτων. Σε αυτές τις λειτουργίες, τα RIS μετατρέπουν και ακτινοβολούν ένα κύμα (είτε προέρχεται από μια περιστρεφόμενη κύματος είτε τροφοδοτείται από μια κυματοθυρίδα) σε ένα επιθυμητό κύμα που διαδίδεται στον ελεύθερο χώρο.

Οι RIS μπορούν να λειτουργήσουν με τρεις διαφορετικούς τρόπους:

1. Waveguide RIS: Στη συγκεκριμένη κατηγορία, οι RIS χρησιμοποιούνται ως κυματοθυρίδες που τροφοδοτούνται με κύματα. Τα στοιχεία της μεταεπιφάνειας λειτουργούν ως μικροκεραίες και προσομοιώνονται ως ανακεφαλιωμένοι μαγνητικοί δίπολοι. Μέσω αυτής της προσαρμογής, οι RIS επιτυγχάνουν το beamforming και μπορούν να μεταδίδουν κύματα προς ευρύτερες γωνίες, καταλαμβάνοντας λιγότερο χώρο σε σύγκριση με τις συμβατικές κεραίες.
2. Refracting RIS: Σε αυτήν την λειτουργία, τα RIS σχεδιάζονται ώστε να διαθλάσουν και να ανακλάσουν τα κύματα με τέλεια απόδοση. Ο σχεδιασμός πραγματοποιείται με τη χρήση μοντέλων ισοδυναμίας που βελτιστοποιούν τις συνιστώσες του πεδίου στις δυο πλευρές τις μεταεπιφάνειας. Επίσης, συζητούνται διάφορες υλοποιήσεις, όπως μεταεπιφάνειες που λειτουργούν με αυτοδιαλείπουσες τηλεμεταφορές ή αποτελούνται αποκλειστικά από απώλειες.
3. Reflecting RIS: Σε αυτή τη λειτουργία, τα RIS σχεδιάζονται ως ανακλαστικές μεταεπιφάνειες που χρησιμοποιούν ηλεκτρονικά στοιχεία για να προσαρμόσουν τη φάση των ανακλασμένων κυμάτων. Μέσω προσχεδιασμένων ψηφιακών επιπέδων τάσης, κάθε στοιχείο μπορεί να επιτύχει διακριτές αλλαγές φάσης και να επιτύχει το beamforming για τα ανακλαστικά κύματα. Στην προκειμένη ενότητα, επικεντρώνεται στις λειτουργικές αρχές των RIS που λειτουργούν ως ανακλαστές.

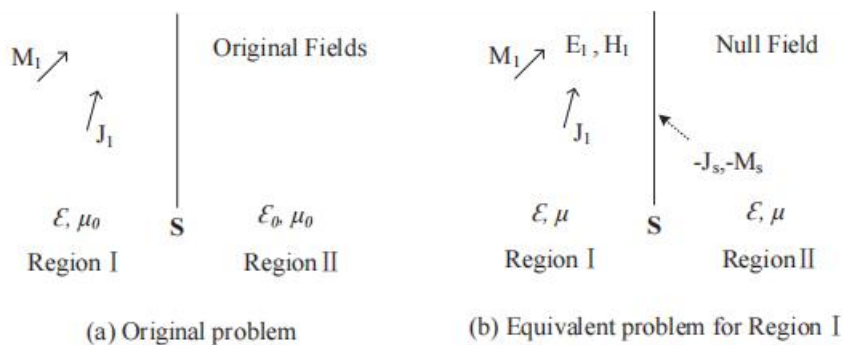
Οι παραπάνω λειτουργίες επιτρέπουν στα RIS να προσαρμόζουν τη συμπεριφορά τους ώστε να εξασφαλίζουν βελτιωμένη ασύρματη επικοινωνία και αποτελεσματική διαχείριση των ηλεκτρομαγνητικών κυμάτων.

2.5 Κατανόηση των μεταεπιφανειών από την οπτική της φυσικής

Σε βασικό επίπεδο, ένα ασύρματο σήμα αποτελεί ηλεκτρομαγνητικό κύμα που εξαπλώνεται στον τρισδιάστατο χώρο. Καθώς το κύμα αλληλεπιδρά με τα αντικείμενα που συναντά, το σήμα μπορεί να υποστεί απόκλιση ή μείωση της ισχύος του. Βάσει των βασικών αρχών του ηλεκτρομαγνητισμού, η ισχύς του σήματος ανά μονάδα επιφάνειας είναι ανάλογη με το τετράγωνο του ηλεκτρικού πεδίου του κύματος σε μια δεδομένη μέση.

Όσον αφορά τις έξυπνες επιφάνειες ανάκλασης και διάθλασης, η κατανόηση του τρόπου που τα ηλεκτρομαγνητικά κύματα αλληλεπιδρούν με τα γύρω αντικείμενα είναι κρίσιμη. Η αρχή της επιφανειακής ισοδυναμίας, γνωστή και ως αρχή του Love, είναι το βασικό εργαλείο για τη μελέτη των μετασχηματισμών των ηλεκτρομαγνητικών κυμάτων. Αυτή η αρχή ισχύει τόσο για προβλήματα εκτός επιφάνειας (περιοχές χωρίς πηγές) όσο και για εσωτερικά προβλήματα. Βασίζεται στο γεγονός ότι το ηλεκτρομαγνητικό πεδίο έξω ή μέσα από ένα κλειστή επιφάνεια μπορεί να καθοριστεί μοναδικά από τις ηλεκτρικές και μαγνητικές ροές που υπάρχουν στην επιφάνεια. Αυτή η αρχή επιτρέπει να αντιμετωπίσουμε τα προβλήματα ανάκλασης και διάθλασης με αντιστοίχιση των ροών σε επιφάνειες που περιγράφουν τη συμπεριφορά των κυμάτων.

Όπως φαίνεται στο Σχήμα 2, το αντίστοιχο πρόβλημα για το Region I μπορεί να αναδιατυπωθεί τοποθετώντας ισοδύναμες ροές στην επιφάνεια S που ικανοποιούν τις συνοριακές συνθήκες για κάθε συγκεκριμένη περίπτωση και γεμίζοντας το Region II με το ίδιο μέσο, χαρακτηριζόμενο από τις σταθερές παραμέτρους ϵ και μ . Έτσι, οι ισοδύναμες ροές ($-J_s, -M_s$), μαζί με τις αρχικές πηγές ροών (J_1, M_1), εκπέμπουν τα σωστά πεδία στην περιοχή I. Το ισοδύναμο πρόβλημα για την περιοχή II μπορεί να διατυπωθεί με παρόμοιο τρόπο.



Σχήμα 2: Αρχή ισοδυναμίας του Love (Για το Region I)

Η αρχή της επιφανειακής ισοδυναμίας του Love αποτελεί τη θεωρητική βάση για την ανάλυση του μοτίβου ακτινοβολίας των RISs. Ωστόσο, η αρχή SEP δεν καθορίζει πως να υπολογιστεί το ηλεκτρομαγνητικό πεδίο που παράγεται από τις επιφανειακές ροές. Για να λάβουμε την ισχύ του σήματος σε ένα αυθαίρετο σημείο του πεδίου, μπορούμε να χρησιμοποιήσουμε την αρχή του Huygens-Fresnel. Η αρχή αυτή αναφέρεται σε μια μέθοδο ανάλυσης προβλημάτων διάδοσης κυμάτων, που δηλώνει ότι κάθε σημείο της προσκεντρικής επιφάνειας είναι καθεαυτό το πηγαίο σημείο σφαιρικών κυμάτων και τα δευτερεύοντα σφαιρικά κύματα που εκπέπονται από διαφορετικά σημεία αλληλεπιδρούν μεταξύ τους. Η συνολική ένωση αυτών των σφαιρικών κυμάτων αποτελεί την προσκεντρική επιφάνεια. Βάσει της αρχής του Huygens-Fresnel, το ηλεκτρομαγνητικό πεδίο που ανακλάται από ένα RIS (σε ανακλαστικές και διαθλαστικές περιπτώσεις) μπορεί να υπολογιστεί αναλυτικά.

Τέλος, όσον αφορά τις RIS που βασίζονται σε κυματοθυρίδες, η αρχή λειτουργίας μπορεί να περιγραφεί ως εξής: ο χειρισμός των ηλεκτρομαγνητικών κυμάτων από την κυματοθυρίδα πραγματοποιεί την σύζευξη μεταξύ των τρισδιάστατων κυμάτων στον ελεύθερο χώρο και των δισδιάστατων επιφανειακών κυμάτων. Ως αποτέλεσμα, η κυματοθυρίδα μπορεί να θεωρηθεί ως ένα ολόγραμμα, το οποίο μεταφέρει επιπλέον πληροφορίες σχετικά με το σήμα που ακτινοβολεί και διαδίδεται στον τρισδιάστατο χώρο.

2.6 Ανάλυση των RISs: Προοπτική της Οπτικής Ακτίνων έναντι της προοπτικής της κυματικής οπτικής

Για να αναλύσουμε την αλληλεπίδραση μεταξύ ενός RIS και των προσπίπτωντων ηλεκτρομαγνητικών κυμάτων, μπορούμε να χρησιμοποιήσουμε δυο διαφορετικές προσεγγίσεις: την προοπτική της οπτικής ακτίνων (Ray Optics) και την προοπτική κυματικής οπτικής (Wave Optics). Αυτές οι δυο προοπτικές χρησιμοποιούνται ευρέως από τους φυσικούς για να μελετήσουν την αλληλεπίδραση του φωτός ή των κυμάτων ραδιοφωνικής συχνότητας με υλικά. Παρόλο που βασίζονται σε κάποιες απλοποιήσεις, αυτές οι δύο μέθοδοι ανάλυσης είναι χρήσιμες για να πάρουμε σημαντικές ερωτήσεις για τη συμπεριφορά των κυμάτων όταν αλληλεπιδρούν με τα υλικά των RIS. Στη βιβλιογραφία για τα RIS, χρησιμοποιούνται συχνά και οι δυο μέθοδοι ανάλυσης, αλλά οι υποθέσεις πίσω από τη χρήση τους και οι φυσικές ερμηνείες τους είναι διαφορετικές. Στην προοπτική της οπτικής ακτίνων, το ηλεκτρομαγνητικό κύμα αναπαρίσταται ως μια συλλογή γεωμετρικών ακτίνων με διαφορετικές φάσεις. Η φάση κάθε ακτίνας αυξάνεται γραμμικά με την οπτική διαδρομή καθώς διασχίζει τον χώρο. Αν το κύμα αλληλεπιδρά με ένα υλικό, το φαινόμενο μελετάται καθορίζοντας τη σχέση μεταξύ της αλλαγής της φάσης και του δείκτη διάθλασης του υλικού.

Πιο συγκεκριμένα, σε σύγκριση με την κυματική οπτική, η προοπτική της οπτικής ακτίνων είναι μια πιο απλοποιημένη αναπαράσταση του πραγματικού συστήματος. Ως αποτέλεσμα, είναι πιο εύκολο να χρησιμοποιηθεί και μπορεί να παράγει γρήγορες προβλέψεις για τον σχεδιασμό του RIS. Ωστόσο, οι μέθοδοι της οπτικής ακτίνων αποτυγχάνουν όταν λαμβάνεται υπόψη η κατανομή της ισχύος στο RIS. Αντίθετα, οι μέθοδοι της κυματικής οπτικής προβλέπουν την κατανομή της

ισχύος χρησιμοποιώντας το διάνυσμα Ruynting, το οποίο μας επιτρέπει να μελετήσουμε την τοπική και συνολική κατανάλωση ισχύος του RIS. Αυτό είναι ένα θέμα υψίστης σημασίας που πρέπει να λαμβάνεται υπόψη κατά τον σχεδιασμό και την κατασκευή των RISs. Για παράδειγμα, υποστήριζεται από ορισμένους συγγραφείς ότι είναι αδύνατο να πραγματοποιηθεί κατεύθυνση πλάνου με απώλειες χρησιμοποιώντας τοπικά παθητικά RISs. Πρέπει να υιοθετηθεί η προοπτική της κυματικής οπτικής για να μελετηθεί η κατανομή της ισχύος του σήματος. Επιπρόσθετα, σύμφωνα με τα αποτελέσματα των προσομοιώσεων τους, μπορούμε να αναμένουμε καλύτερη απόδοση όταν τα RISs σχεδιάζονται βάσει της προσέγγισης της κυματικής οπτικής σε σύγκριση με αυτά που σχεδιάζονται βάσει της προσέγγισης της οπτικής ακτινών.

Εν κατακλείδι, οι δυο προοπτικές έχουν τα πλεονεκτήματα και τους περιορισμούς τους. Βέβαια, η υιοθέτηση της προοπτικής της κυματικής οπτικής είναι η πιο κατάλληλη επιλογή για τις περισσότερες περιπτώσεις.

2.7 Επίτευξη Ρυθμισιμότητας: Patch Array RIS

Οι ιδιότητες των RIS, όπως η αλλαγή φάσης, μπορούν να προσαρμοστούν αλλάζοντας την επιφανειακή αντίσταση μέσω διάφορων μηχανισμών. Εκτός από την ηλεκτρική τάση, μπορούν να χρησιμοποιηθούν κι άλλες μέθοδοι όπως η θερμική διέγερση, η οπτική παροχή ενέργειας και η φυσική επιμήκυνση. Ωστόσο, η ηλεκτρική ρύθμιση είναι η πιο πρακτική επιλογή, καθώς η ηλεκτρική τάση μπορεί να ελεγχθεί εύκολα και να προγραμματιστεί μέσω μικροκυματικών πυλών προγραμματιζόμενης πύλης. Όσον αφορά την επιλογή υλικών για τα RIS, κάποιες επιλογές περιλαμβάνουν ημιαγωγούς και γραφένιο.

Ανεξάρτητα από τους μηχανισμούς ρύθμισης, εστιάζουμε την προσοχή μας στις επιφάνειες μεταφορτωμένων κελυφών (patch-array smart surfaces) στο παρακάτω κείμενο. Η γενική γεωμετρική διάταξη αυτού του είδους των RIS μπορεί να μοντελοποιηθεί ως μια περιοδική (ή ημι-περιοδική στην πιο γενική περίπτωση) συλλογή μονάδων κελυφών που ενσωματώνονται σε ένα υπόστρωμα. Για ευκολία, θεωρούμε ότι οι RIS βασίζονται σε τοπική σχεδίαση, όπου οι μονάδες δεν αλληλεπιδρούν μεταξύ τους. Η τοπική σχεδίαση συνήθως οδηγεί στην σχεδίαση μη βέλτιστων RIS. Για να χαρακτηρίσουμε την ρυθμισιμότητα του RIS, μπορεί να χρησιμοποιηθεί η μέθοδος των ισοδύναμων στοιχείων (equivalent lumped-element circuits). Κάθε μονάδα μπορεί να μοντελοποιηθεί ως ένα ισοδύναμο κύκλωμα με μια ρυθμιζόμενη αντίσταση φορτίου. Η αντίσταση φορτίου μπορεί να ρυθμιστεί αλλάζοντας την τάση πόλωσης της διόδου. Με τη χρήση αυτής της προσέγγισης, μπορούμε να χαρακτηρίσουμε κάθε μονάδα patch-array RIS σε ασύρματα συστήματα επικοινωνίας μέσω ενός ισοδύναμου συντελεστή ανάκλασης. Για παράδειγμα, ο συντελεστής ανάκλασης της i -οστής μονάδας μπορεί να μοντελοποιηθεί ως εξής:

$$r_i = \beta_i * e^{j\phi_i}$$

Όπου β_i και ϕ_i αντιστοιχούν στην απόκριση πλάτους και στην απόκριση φάσης αντίστοιχα. Ο ισοδύναμος συντελεστής ανάκλασης εξαρτάται από την καταλληλότητα πόλωσης του ισοδύναμου κυκλώματος που ελέγχει κάθε μονάδα, καθώς και από τις ιδιοτιμές και τις αμοιβαίες τιμές αντίστασης στις θύρες του RIS. Οι παράμετροι β_i και ϕ_i δεν είναι πλήρως ανεξάρτητες μεταξύ τους, δηλαδή $\beta_i = f(\phi_i)$.

Υπάρχουν ήδη σχεδιασμοί patch-array RISs που εφαρμόζουν διακριτό έλεγχο φάσης και σε ορισμένες περιπτώσεις, έλεγχο πλάτους. Επιστήμονες σχεδίασαν το RFocus, μια δισδιάστατη επιφάνεια με έναν ορθογώνιο πίνακα παθητικών κεραίων. Το μέγεθος κάθε παθητικής μονάδας είναι $\lambda/4 \times \lambda/10$ και τα ηλεκτρομαγνητικά κύματα είτε αντανακλώνται είτε ανακλώνται. Η επιφάνεια RFocus μπορεί να παραχθεί με χαμηλό κόστος καθώς επίσης μπορεί να βελτιώσει τη μέση ισχύ του σήματος κατά 9,5 φορές. Μια άλλη ομάδα επιστημόνων υλοποίησαν το ScatterMIMO, χρησιμοποιώντας μια έξυπνη επιφάνεια για να αυξήσουν τη διάχυση στο περιβάλλον. Στο σχεδιασμό τους, κάθε μονάδα αντανάκλασης χρησιμοποιεί μια κεραία patch συνδεδεμένη με τέσσερις γραμμές μετάδοσης με ανοιχτά άκρα. Οι γραμμές μετάδοσης παρέχουν περιστροφικές αλλαγές φάσης ($0, \pi/2$ ή $3\pi/2$). Με βάση μετρήσεις, το ScatterMIMO αυξάνει τη ροή δεδομένων κατά δυο φορές και το λόγο σήματος προς θόρυβο (SNR) κατά 4,5 dB σε σύγκριση με βασικές τεχνικές. Ενδιαφέρον έχει, επίσης, να αναφερθεί ότι η ρυθμισιμότητα μπορεί να επιτευχθεί με υλοποιήσεις πέρα από τις επιφάνειες μεταμορφωμένων κελυφών. Για παράδειγμα, η PIVOTAL COMMWARE πρότεινε μια νέα τεχνική με την ονομασία Holographic Beam Forming (HBF). Ο προτεινόμενος holographic beamformer έχει χαμηλό κόστος και κατανάλωση ενέργειας συγκριτικά με άλλες τεχνολογίες μετάδοσης, όπως οι massive MIMO.

2.8 Αρχές λειτουργίας των RIS

Σχετικά με την μονόδρομη ανάκλαση, μια RIS που βασίζεται σε πίνακες-παραθύρων μπορεί να ρυθμιστεί να εξυπηρετεί μια τερματική συσκευή τόσο στην περιοχή μακρινού πεδίου (far-field) όσο και στην περιοχή κοντινού πεδίου (near-field). Ανάμεσα στις πολλές λειτουργίες και ρυθμίσεις λειτουργίας των RIS, η ανώμαλη ανάκλαση και η μορφοσύνθεση (beamforming) χρησιμοποιούνται ευρέως στο πλαίσιο των ασύρματων επικοινωνιών. Με την οπτική των κυμάτων, η ανώμαλη ανάκλαση είναι μια μετατροπή της κυματοποίησης από μια επίπεδη κύματος σε μία άλλη επίπεδη κύματος. Εν αντιθέσει, η μορφοσύνθεση είναι μια μετατροπή της κυματοποίησης από μια επίπεδη κύματος σε μία επιθυμητή κυματοποίηση. Από την οπτική των δεσμών (ray-optics), η ανώμαλη ανάκλαση περιλαμβάνει τον σχεδιασμό της RIS έτσι ώστε να ανακλά μια δέσμη προς μια απομακρυσμένη περιοχή, ενώ η μορφοσύνθεση στοχεύει στο να εστιάσει την εισροή του κύματος προς μία επιθυμητή περιοχή, γνωστή ως σημείο εστίασης. Η επιλογή μεταξύ των δυο αυτών οπτικών εξαρτάται από το είδος των εφαρμογών και των απαιτήσεων του συστήματος επικοινωνίας. Κάθε μια από αυτές τις διαμορφώσεις έχει τα πλεονεκτήματα και τους περιορισμούς της και η επιλογή της κατάλληλης μπορεί να επηρεάσει την απόδοση του συστήματος.

- Κοντινό πεδίο (Near Field) vs Μακρινό πεδίο (Far Field): Προκειμένου να διακρίνουμε την περιοχή του κοντινού πεδίου από την περιοχή του μακρινού πεδίου, χρησιμοποιούμε έναν κατάλληλο αδιάστατο αριθμό, ο οποίος θα αντιπροσωπεύει τα χαρακτηριστικά του συστήματος. Έστω ότι L και RF δηλώνουν το μέγεθος του ανοίγματος της κεραίας της RIS και την απόσταση εστίασης, αμτίστοιχα. Υποθέτουμε, επίσης, ότι z είναι η απόσταση ενός συγκεκριμένου σημείου πεδίου από τη RIS. Θεωρητικά, το μακρινό και το κοντινό πεδίο μπορεί να διαχωριστούν ως εξής: Η απόσταση $2L^2/\lambda$ είναι ένα ευρέως χρησιμοποιούμενο κριτήριο για να αποφασίσουμε το όριο μεταξύ του κοντινού και του μακρινού πεδίου. Η θέση που αντιστοιχεί σε $z=2L^2/\lambda$ είναι το όριο μεταξύ του κοντινού και του μακρινού πεδίου. Αυτό προκύπτει από την εξέταση της μεταβολής της πυκνότητας ισχύος με την απόσταση μεταξύ ενός σημείου πεδίου και της RIS. Στο κοντινό πεδίο όπου $z < 2L^2/\lambda$, η πυκνότητα ισχύος δείχνει σημαντικές διακυμάνσεις. Η θέση κορυφής της πυκνότητας ισχύος στο κοντινό πεδίο, δηλαδή R_F , αλλάζει με διαφορετικές διαμορφώσεις της RIS. Χρησιμοποιώντας κατάλληλες συνθήκες συν-φάσης, μπορεί να επιτευχθεί η εστίαση δέσμης εντός του κοντινού πεδίου της RIS. Αξίζει να σημειωθεί ότι, το όριο μεταξύ του κοντινού και του μακρινού πεδίου εξαρτάται από τη συγκεκριμένη διαμόρφωση της RIS.

Γενικά, η κύρια διαφορά μεταξύ της περιοχής του κοντινού πεδίου και της περιοχής του μακρινού πεδίου αφορά τον τρόπο με τον οποίο η πυκνότητα ισχύος αλλάζει. Στην κοντινή περιοχή, η πυκνότητα ισχύος παρουσιάζει σημαντικές μεταβολές, καθώς η απόσταση αυξάνεται. Στο εστιακό σημείο της κεραίας, μπορεί να επιτευχθεί υψηλή εστίαση της δέσμης. Αντίθετα, στην περιοχή του μακρινού πεδίου, η ισχύς διασπάται με την απόσταση και η πυκνότητα ισχύος εμφανίζει πιο ομοιόμορφη κατανομή. Για παράδειγμα, ας θεωρήσουμε ότι η RIS εστιάζει το κύμα εντός μιας περιοχής α . Η συνολική ενέργεια που προσκρούει στην RIS είναι ανάλογη με την γωνία προσκρούσεως, Ω , που σχηματίζεται από την επιφάνεια της RIS σε σχέση με τη θέση του πομπού. Μετά την ανάκλαση, η μεταδιδόμενη ενέργεια διασπάται στην περιοχή α . Έτσι, η πυκνότητα ισχύος γύρω από το εστιακό σημείο είναι ανάλογη με το Ω/α .

Γενικά, η χρήση μιας RIS μπορεί να βελτιώσει την ισχύ του σήματος τόσο στην περιοχή του κοντινού πεδίου όσο και του μακρινού πεδίου. Στο κοντινό πεδίο, ωστόσο, η RIS σχεδιάζεται για να ενισχύσει την ισχύ του σήματος για τους χρήστες που βρίσκονται σε συγκεκριμένες τοποθεσίες σε σχέση με τη RIS ενώ ταυτόχρονα μειώνει το σήμα σε άλλες τοποθεσίες. Στο μακρινό πεδίο, η RIS αναμένεται να ενισχύσει την ισχύ του σήματος για τους χρήστες που βρίσκονται σε συγκεκριμένες γωνίες σε σχέση με την RIS.

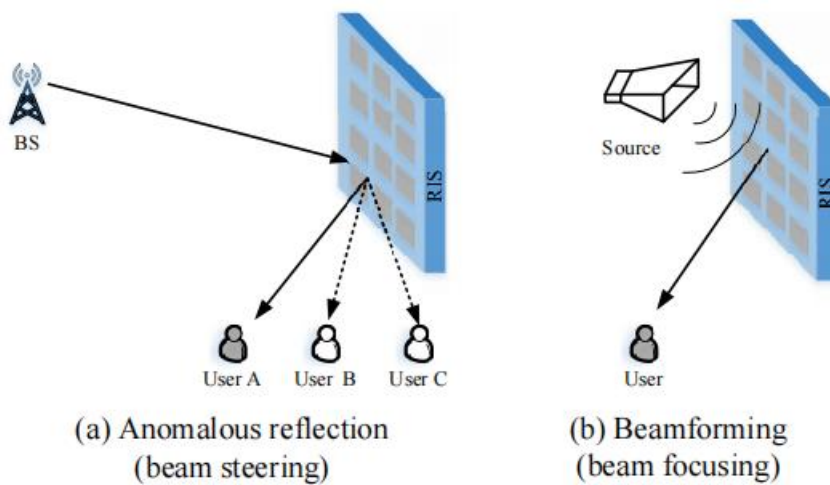
- Γενικευμένοι νόμοι Διάθλασης και Ανάκλασης: Από την οπτική της γεωμετρικής οπτικής, η ανώμαλη ανάκλαση και διάθλαση από μια RIS μπορούν να περιγραφούν χρησιμοποιώντας τους γενικευμένους νόμους διάθλασης και ανάκλασης, που είναι μια φυσική απόρροια της αρχής του Fermat και των συνοριακών συνθηκών στις εξισώσεις Maxwell.

Αρχή 1: Επίτευξη ανώμαλης ανάκλασης (Σχήμα 3α)

Υποθέτουμε ότι η ασυνέχεια της φάσης στο όριο είναι μια συνάρτηση θέσης κατά μήκος της διεύθυνσης x , $\Phi(x)$, όπου x είναι το διανυσματικό πλήθος της θέσης στο όριο. Επιπλέον, υποθέτουμε ότι η παράγωγος της ασυνέχειας της φάσης υπάρχει. Τότε, η γωνία ανάκλασης (θ_1) και η γωνία διάθλασης (θ_2) είναι:

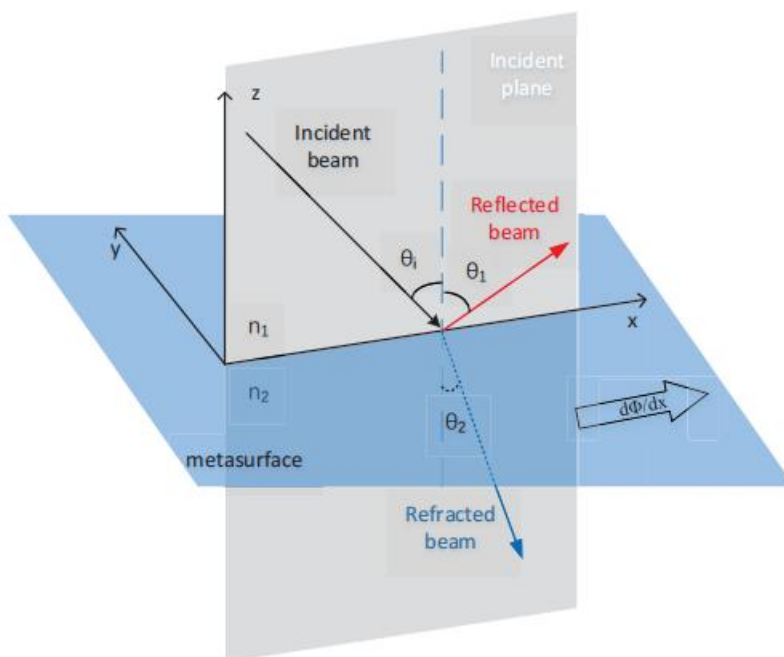
$$\theta_1 = \sin^{-1} \left[\sin\theta_i + \frac{\lambda}{2\pi n_1} \frac{d\Phi}{dx} \right],$$

$$\theta_2 = \sin^{-1} \left[\frac{n_1}{n_2} \sin\theta_i + \frac{\lambda}{2\pi n_2} \frac{d\Phi}{dx} \right],$$



Σχήμα 3. Λειτουργίες ανακλαστικών επιφανειών

Όπου θ_i είναι η γωνία πτώσης, λ είναι το μήκος κύματος του μεταδιδόμενου σήματος στο κενό και n_1, n_2 είναι οι δείκτες διάθλασης, όπως φαίνεται στο Σχήμα 4.



Σχήμα 4: Απεικόνιση των γενικευμένων νόμων Ανάκλασης και Διάθλασης

Υπάρχουν κι άλλα αποτελέσματα που σχετίζονται με τους γενικευμένους νόμους διάθλασης και ανάκλασης, συμπεριλαμβανομένων των κρίσιμων γωνιών για την ολική εσωτερική ανάκλαση ή διάθλαση. Το βασικότερο συμπέρασμα που προκύπτει στην προκειμένη περίπτωση είναι ότι, όταν μια διακοπή φάσης εισάγεται στην επιφάνεια του ορίου, οι γωνίες ανάκλασης και διάθλασης εξαρτώνται όχι μόνο από τη γωνία προσπίπτουσας ακτίνας αλλά και από το μήκος κύματος, τους δείκτες διάθλασης και την ασυνέχεια φάσης. Αυτό δίνει επιπλέον ρυθμιζόμενες παραμέτρους για το χειρισμό των ανακλαστικών και διαθλαστικών κυμάτων ηλεκτρομαγνητικής ακτινοβολίας.

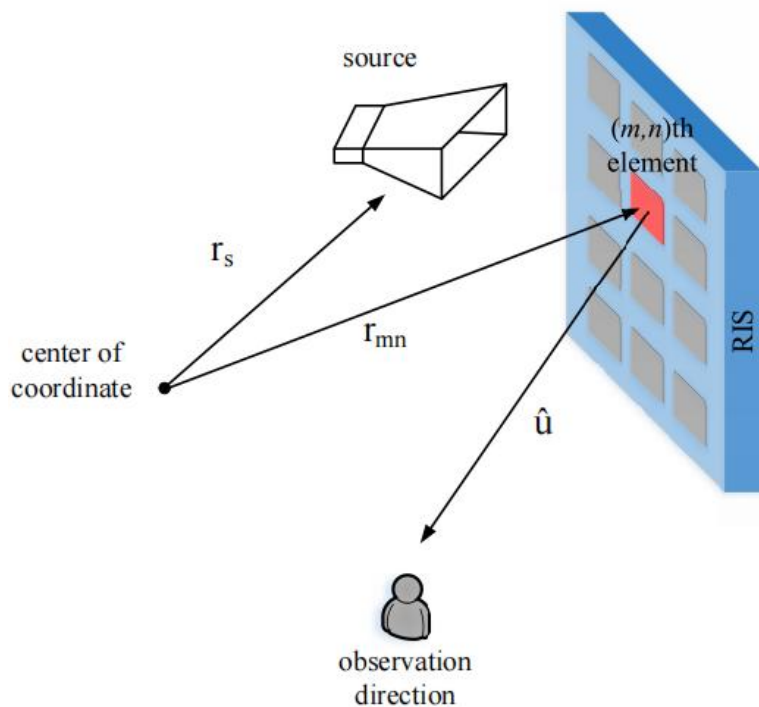
- Η συνθήκη της ομόφασης (co-phase condition) εφαρμόζεται συνήθως όταν η RIS βρίσκεται εντός του κοντινού πεδίου της πηγής ή ο τερματικός είναι κοντά στη RIS. Σε αυτές τις περιπτώσεις, οι καμπυλότητες των εισερχόμενων και ανακλαστικών κυματοστροφών είναι σημαντικές. Η βελτιστοποίηση της επιφάνειας στοχεύει στην παραγωγή μιας μολυβόστυλου με κατεύθυνση προς τον περιορισμένο τερματικό. Όταν οι συνδέσεις μεταξύ της πηγής και της RIS, καθώς και της RIS και του τερματικού είναι σε γραμμή από κοινού, μπορεί να εφαρμοστεί η ακόλουθη συνθήκη όμοφασης.

Αρχή 2: Επίτευξη διαμόρφωσης δέσμης (Σχήμα 3β)

Έστω r_{mn} η θέση του στοιχείου (m,n) της RIS, r_s η θέση της πηγής και u η κατεύθυνση του παρατηρητή έναντι της επιφάνειας. Όπως φαίνεται στο Σχήμα 5, μπορεί να επιλεγεί το ϕ_{mn} ως εξής:

$$-k_0(|\vec{r}_{mn} - \vec{r}_s| - \vec{r}_{mn} \cdot \hat{u}) + \phi_{mn} = 2\pi \cdot t$$

όπου $t=1,2,3\dots$ και $k_0 = 2\pi/\lambda_c$



Σχήμα 5. Συντεταγμένη αναπαράσταση συνθήκης συνφάσεως

Σε πιο περίπλοκα συστήματα ασύρματης επικοινωνίας, ο ρόλος των RIS είναι πιο περίπλοκος και δεν μπορεί να κατηγοριοποιηθεί με βάση της δυο λειτουργίες εργασίες που περιγράφονται στο παραπάνω σχήμα. Σε αυτές τις περιπτώσεις, για να καθοριστεί η διαμόρφωση της RIS πρέπει να διατυπωθεί ένα πρόβλημα βελτιστοποίησης.

2.9 Προοπτική των RIS

Κατά τον σχεδιασμό και τη διαμόρφωση των RIS, υπάρχουν περιορισμοί που προκύπτουν από τις θεωρητικές αναλύσεις και τους περιορισμούς υλοποίησης του υλικού. Οι θεωρητικοί περιορισμοί συνδέονται με τις απλούστερες υποθέσεις και τις απλουστευμένες προσεγγίσεις και την αλληλεπίδραση των RIS με το ηλεκτρομαγνητικό κύμα. Από την άλλη πλευρά, οι περιορισμοί υλοποίησης υλικού προκύπτουν από τους περιορισμούς κατά την κατασκευή και την διαμόρφωση ενός ιδανικά συνεχούς προφίλ RIS. Παρόλο που οι περιορισμοί αυτοί επηρεάζουν την απόδοση, οι θεωρητικοί περιορισμοί μας βοηθούν να κατανοήσουμε τις βασικές αρχές και παράμετρος του RIS, ενώ οι περιορισμοί υλοποίησης υλικού επηρεάζουν την πρακτική εφαρμογή του RIS. Σε αυτή την φάση, πρέπει να επισημανθούν αυτά τα ζητήματα και να αντιμετωπιστούν κατάλληλα κατά την κατασκευή και υλοποίηση των RISs.

1. Περιορισμοί hardware: Σε πρακτικά σενάρια εφαρμογής, πολλοί υλικοί παράμετροι επηρεάζουν σημαντικά την επίδοση που μπορεί να επιτευχθεί από το

σύστημα. Παραδείγματος χάριν, ο αριθμός των επιπέδων κβαντισμού των φάσεων του RIS, ο μέγιστος αριθμός στοιχείων που μπορεί να ολοκληρωθεί στο υπόστρωμα και το ποσοστό του περιβάλλοντος διάχυσης που μπορεί να καλυφθεί από ένα RIS. Οι υπάρχουσες έρευνες μελετούν τους περιορισμούς αναλύοντας την επίδραση τους στην κατανομή του καναλιού, το νόμο κλιμάκωσης ισχύος και τις μετρικές απόδοσης όπως η πιθανότητα αποτυχίας.

2. Απλοποιήσεις σχεδιασμού συστήματος: Οι απλουστεύσεις στον σχεδιασμό των RIS, χρησιμοποιώντας υπεραπλοποιημένα μοντέλα για το υλικό τους ή τα μοντέλα καναλιού, έχουν ως αποτέλεσμα περιορισμούς στον σχεδιασμό του συστήματος. Λόγω της πολύπλοκης φύσης των RIS και της αλληλεπίδρασής τους με το περιβάλλον, οι αρχικές έρευνες χρησιμοποιούν απλά μοντέλα.

3. Περιορισμοί βελτιστοποίησης: Για να εκμεταλλευτούμε τα οφέλη της χρήσης των RISs στα ασύρματα δίκτυα, οι παράμετροι των RISs (π.χ. ο συντελεστής ανάκλασης) και η ανάθεση πόρων του δικτύου (π.χ. διαμόρφωση διάδοσης σήματος και προγραμματισμός χρηστών) πρέπει να βελτιστοποιηθούν συγχρόνως. Ωστόσο, τα προβλήματα αυτής της συγχώνευσης βελτιστοποίησης είναι συνήθως μη-κυρτά και περιλαμβάνουν υψηλά συζευμένες μεταβλητές, κάτι που καθιστά προκλητικό τον εντοπισμό μιας παγκόσμιας βέλτιστης λύσης. Παρόλο που έχουν προταθεί πρόσφατα αποτελεσματικοί αλγόριθμοι για τον υπολογισμό υψηλής ποιότητας υποβέλτιστων λύσεων, τα όρια απόδοσης των RISs παραμένουν άγνωστα.

2.10 Ανάλυση απόδοσης συστημάτων πολυκεραιών υποβοηθήμενων RIS

Παραπάνω συζητήσαμε της θεμελιώδεις φυσικές ιδιότητες των RISs. Ωστόσο, ο τρόπος με τον οποίο τα RIS επηρεάζουν την απόδοση της επικοινωνίας εξακολουθεί να είναι ένα ανοιχτό πρόβλημα. Για να ερευνήσουμε συστηματικά τα υπάρχοντα σχέδια για δίκτυα ενισχυμένα με RIS, θα πρέπει να συζητήσουμε τα ακόλουθα θέματα: (1) μοντέλα καναλιών, (2) ανάλυση απόδοσης και (3) συστήματα αναφοράς.

I. Μοντέλα καναλιού

A. Μοντέλα απώλειας πορείας: Ορισμένες ερευνητικές συνεισφορές για την απώλεια πορείας σε RISs δείχνουν ότι η ισχύς διασκορπίζεται από ένα RIS συνήθως διατυπώνεται σε ένα ολοκλήρωμα που λαμβάνει υπόψη, με τη χρήση της αρχής του Huygens, την επίδραση ολόκληρης της επιφάνειας στο σενάριο του ελεύθερου χώρου, όπου δεν λαμβάνονται υπόψη οι σκιάσεις, η διάχυση και η αντανάκλαση. Βέβαια, η εύρεση ανακλαστικών εκφράσεων του ολοκληρώματος είναι δύσκολη, εκτός από ορισμένες ασυμπτωτικές καταστάσεις, οι οποίες αντιστοιχούν στη θεώρηση του RIS ως ηλεκτρικά μικρού και ηλεκτρικά μεγάλου μεγέθους (σε σχέση προς το μήκος κύματος και τις αποστάσεις). Το μοντέλο απώλειας πορείας εξαρτάται από την ειδική φάση που εφαρμόζεται από το RIS. Οι νόμοι κλιμάκωσης μπορεί να είναι διαφορετικοί εάν το RIS λειτουργεί ως ανακλαστήρας και ως

εστιακός φακός. Στη συνέχεια, θα αναφερθούν δυο νόμοι κλιμάκωσης που λειτουργούν ως ανώμαλοι ανακλαστήρες.

- **Electrical Small RISs:** Στο ασυμπτωτικό καθεστώς των ηλεκτρικά μικρών RIS, υποθέτουμε ότι το RIS είναι σχετικά μικρό σε μέγεθος σε σύγκριση με τις αποστάσεις μετάδοσης. Σε αυτήν την περίπτωση, το RIS μπορεί να προσεγγιστεί ως μικροσκοπικός διασπορέας. Γενικά, ο περίπατος απώλειας κλιμακώνεται με το αντίστροφο του γινομένου της απόστασης του μεταξύ του πομπού και του κέντρου του RIS και του δέκτη. Η ληφθείσα ισχύς συνήθως μεγιστοποιείται στην κατεύθυνση της ανώμαλης αντανάκλασης, όπου ο περίπατος απώλειας μέσω του RIS ακολουθεί τα “μοντέλα γινομένου αποστάσεων”.
- **Electrical Large RISs:** Σε αυτό το ασυμπτωτικό καθεστώς, υποθέτουμε ότι η RIS έχει μεγάλο μέγεθος (ιδανικά άπειρο) συγκριτικά με τις αποστάσεις μετάδοσης και το μήκος κύματος. Σε αυτήν την περίπτωση, η RIS μπορεί να προσεγγιστεί ως μεγάλο επίπεδο καθρέυτη. Ας συμβολίσουμε με x_0 το σημείο του RIS (αν υπάρχει) στο οποίο η πρώτη παράγωγος της συνολικής φάσης του συνδυασμένου εισερχόμενου σήματος, ανάκλητου σήματος και του συντελεστή ανακλαστικότητας του RIS είναι ίση με το μηδέν. Γενικά, ο ασυμπτωτικός λόγος απώλειας ακολουθεί τον αντίστροφο ενός κατάλληλα συνδυασμένου αθροίσματος της απόστασης μεταξύ του πομπού και του x_0 και της απόστασης μεταξύ του x_0 και του δέκτη. Επιπλέον, η ληφθείσα ισχύς δεν εξαρτάται από το μέγεθος του RIS, το οποίο θεωρείται ασυμπτωτικά άπειρο. Αυτό το αποτέλεσμα επιβεβαιώνει το γεγονός ότι ο νόμος κλιμάκωσης του RIS είναι φυσικά σωστός, γιατί δεν αυξάνεται στο άπειρο καθώς το μέγεθος του RIS πλησιάζει το άπειρο. Αυτό συμβαίνει διότι ο νόμος κλιμάκωσης και η συμπεριφορά του RIS διαφέρουν σε σχέση με το καθεστώς ηλεκτρικά μικρού μεγέθους.

II. Μοντέλα χώρου

Τα εργαλεία της στοχαστικής γεωμετρίας είναι ικανά να αντιλαμβάνονται την τυχαιότητα της τοποθέτησης των χρηστών, επιτρέποντας την παραγωγή υπολογίσιμων ή κλειστού τύπου εκφράσεων για τις βασικές μετρικές απόδοσης. Ειδικότερα, υπάρχουν διάφορες χωρικές διαδικασίες που χρησιμοποιούνται για τη μοντελοποίηση των τοποθεσιών των χρηστών σε διάφορα ασύρματα δίκτυα, όπως της ομογενούς διαδικασίας τυχαίων σημείων Poisson (HTTP), της διαδικασίας Poisson Cluster (PCP). Τα στοιχεία του RIS χρησιμοποιούνται σε εμπόδια και υποθέτουμε ότι τυχαία κατανομημένοι χρήστες βρίσκονται στην εξυπηρετούμενη περιοχή των RIS. Τα αντικείμενα μοντελοποιούνται από μια τροποποιημένη τυχαία διαδικασία γραμμών σταθερού μήκους με τυχαίους προσανατολισμούς και τοποθεσίες. Εκεί, ερευνήθηκε η πιθανότητα ότι ένα τυχαία κατανομημένο αντικείμενο που έχει επικαλυφθεί από ένα RIS λειτουργεί ως αντανάκλαστής για ένα συγκεκριμένο ζεύγος πομπού και δέκτη.

III. Μικρής κλίμακας μοντέλα εξασθένισης

Τα συγκεκριμένα μοντέλα αντιπροσωπεύουν την τυχαιότητα των σημαντικών αλλαγών στην ισχύ του σήματος που προκαλούνται από το περιβάλλον. Αυτά τα μοντέλα καθιστούν δυνατή την πρόβλεψη ή περιγραφή της ποικιλίας των συνθηκών καναλιού που παρατηρούνται σε κάθε στιγμή και τοποθεσία. Τα μικρής κλίμακας μοντέλα εξασθένισης περιλαμβάνουν μοντέλα μέσου και περιθώριου καναλιού, όπως το Rayleigh και το Rician, αντίστοιχα. Τα μοντέλα μικρής κλίμακας εξασθένισης είναι ζωτικής σημασίας για την αξιολόγηση της απόδοσης των ασύρματων συστημάτων καθώς επηρεάζουν τη χωρική διαλειτουργικότητα, τη συμπεριφορά του συνδέσμου και την απόδοση του δικτύου γενικά.

2.10.1 Ανάλυση απόδοσης

Η πολύ-κεραία τεχνολογία προσφέρει επιπλέον ποικιλία στον χώρο, και γι' αυτό αποτελεί σημαντική προσέγγιση. Η τεχνολογία πολυ-κεραιών ενισχυμένων με RIS δίκτυα έχει προσελκύσει το ακαδημαϊκό ενδιαφέρον και τη βιομηχανία. Τα πλεονεκτήματα των RIS γίνονται όλο και πιο σαφή, ειδικά όσον αφορά τη βελτίωση της φασματικής αποδοτικότητας και της ενεργειακής αποδοτικότητας. Βέβαια, υπάρχουν διάφορες βασικές προκλήσεις για την ανάλυση της απόδοσης στα δίκτυα με RIS. Υπάρχουν διάφορες βασικές προκλήσεις για την ανάλυση της απόδοσης στα δίκτυα με RIS. Μια από αυτές τις προκλήσεις είναι η αξιολόγηση των ακριβών διανομών των διαδοχικών καναλιών μεταξύ του σταθμού βάσης και των χρηστών μέσω RIS.

2.10.2 Συγκριτικές μέθοδοι αναφοράς

Προκειμένου να αξιολογηθούν τα πλεονεκτήματα και οι περιορισμοί των RIS, λαμβάνονται υπόψη δυο συγκριτικές τεχνολογίες μετάδοσης:

- 1) επιφάνειες με τυχαία μετατόπιση φάσης, και
- 2) δίκτυα αναμετάδοσης (relay networks)

1) **Τυχαία Μετατόπιση Φάσης:** Οι RIS έχουν τη δυνατότητα να μετατοπίσουν τη φάση του εισερχόμενου σήματος, και κατα συνέπεια, πολλά σήματα μπορούν να ενιχυθούν ή να αποκλειστούν στην πλευρά του χρήστη ή στην πλευρά της βάσης. Έτσι, μια καλά αποδεκτή συγκριτική μέθοδος για να ποσοτικοποιηθεί η βελτίωση της απόδοσης από τα στοιχεία RIS παρέχεται από μια επιφάνεια που δεν είναι ρυθμιζόμενη και που μπορεί να προσεγγιστεί ιδανικά από μια επιφάνεια με τυχαία μετατόπιση φάσης.

2) **Δίκτυα αναμετάδοσης:** Τα δίκτυα αυτά μπορούν να κατηγοριοποιηθούν σε δυο ζεύγη κλασικών πρωτοκόλλων αναμετάδοσης:

- α) διπλής κατεύθυνσης και ημιδιπλής κατεύθυνσης, και
- β) δίκτυα μετάδοσης με ακολουθιακή και προς τα εμπρός αναμετάδοση

Υποθέτοντας ότι χρησιμοποιούνται οι βέλτιστες στρατηγικές διαίρεσης ισχύος τόσο για τους αναμεταδότες AF και DF, μπορεί να συγκριθεί η απόδοση μεταξύ δικτύων με ενισχυτές RIS και δικτύων με αναμεταδότες.

2.10.3 Συμπεράσματα και Προοπτικές

Παρά το γεγονός ότι αρκετές έρευνες έχουν αναλύσει την απόδοση των δικτύων RIS, υπάρχουν τρία κύρια ανοιχτά ερευνητικά προβλήματα:

1. Πειράματα μεταβίβασης σήματος για εξωτερικά σενάρια, ειδικά όταν υπάρχουν αντανάκλαστικά και διασκορπισμένα αντικείμενα.
2. Ακριβείς κατανομές, ιδίως ανάλυση της τάξης πολλαπλότητας και της απόδοσης του δικτύου στο Low-SNR
3. Ενοποιημένα σενάρια εφαρμογής: Τα επιθυμητά σήματα και τα σήματα παρεμβολής μπορούν να ενισχυθούν και να μειωθούν ταυτόχρονα, κάτι που αποτελεί μια σημαντική μελλοντική κατεύθυνση.

2.11. Διαμόρφωση RIS και κατανομής πόρων

Όπως αναφέραμε και παραπάνω, η ανάπτυξη των RIS επιτρέπει υψηλές βελτιώσεις απόδοσης στα ασύρματα δίκτυα. Σε αυτήν την ενότητα, θα συζητηθούν τα όρια απόδοσης των RIS από την οπτική της θεωρίας πληροφοριών.

A. Οπτική θεωρίας πληροφοριών

Προκειμένου να ανακαλύψουν τα θεμελιώδη όρια απόδοσης των RIS, ορισμένες έρευνες έχουν αφιερωθεί στην εξέταση της απόδοσης από την οπτική της θεωρίας πληροφοριών.

- Σχεδιασμός για επίτευξη χωρητικότητας: Ορισμένοι επιστήμονες υπολόγισαν τη χωρητικότητα για ένα σύστημα επικοινωνίας βοηθούμενο από RIS μονής εισόδου και πολλαπλών εξόδων (SIMO). Με πεπερασμένες αναπαραστάσεις εισόδου σήματος, αποδείχτηκε ότι είναι απαραίτητο ένα κοινό σχήμα κωδικοποίησης πληροφοριών και για τα δυο μέρη, τόσο για τα μεταδιδόμενα σήματα όσο και για τις διαμορφώσεις του RIS, για την επίτευξη της χωρητικότητας του καναλιού. Με βάση αυτά τα συμπεράσματα, οι συγγραφείς πρότειναν μια τεχνική κωδικοποίησης με στρώματα και αποδοχή με συνεχή ακύρωση.
- Χαρακτηρισμός περιοχής χωρητικότητας: Η περιοχή χωρητικότητας για το ασύρματο κανάλι εκπομπής ενισχυμένο με RIS αποδείχτηκε ότι επιτυγχάνεται με τη χρήση κωδικοποίησης υπερθέσεως στον πομπό και με τη συνεχή ακύρωση παρεμβολών σε πολλαπλούς δέκτες.

B. Κοινός σχεδιασμός εκπομπής και παθητικού σχηματισμού δέσμης.

1. Στόχοι βελτιστοποίησης: Ένα RIS χρησιμοποιείται για να βοηθήσει στη μετάδοση μεταξύ του BS και των χρηστών προσκρούοντας παθητικά τα σήματα. Οι συντελεστές ανάκλασης του RIS μπορούν να προσαρμοστούν από το BS μέσω ενός ελεγκτή RIS.

- Ελαχιστοποίηση ισχύος εκπομπής ή μεγιστοποίηση απόδοσης ενέργειας: Ορισμένοι επιστήμονες ελαχιστοποίησαν την ισχύ εκπομπής για ένα σύστημα MISO ενισχυμένο με RIS τόσο σε περιπτώσεις μονάδας χρήστη όσο και πολλαπλών χρηστών. Αναπτύχθηκαν αλγόριθμοι βάσει εναλλασσόμενης βελτιστοποίησης για να βρεθούν τοπικά βέλτιστες λύσεις. Ανακαλύφθηκε επίσης, ότι ένα RIS μπορεί ταυτόχρονα να ενισχύσει την επιθυμητή ισχύ σήματος και να μειώσει τις παρεμβολές για το σενάριο πολλαπλών χρηστών. Για τη μείωση της υπολογιστικής πολυπλοκότητας, σχεδιάστηκαν ακόμη αποδοτικοί αλγόριθμοι διαδοχικής βελτίωσης.
- Μειστοποίηση SE ή χωρητικότητας: Η προσέγγιση SDR παρέχει μόνο μια προσεγγιστική λύση, προτάθηκαν δυο αποτελεσματικοί αλγόριθμοι με τη χρήση μεθόδου επαναληπτικού σταθερού σημείου και τη μέθοδο βελτιστοποίησης με αλγεβρικούς πολλαπλασιαστές για το σχεδιασμό του παθητικού σχεδιασμού δέσμης. Βάσει αυτών βγήκε το συμπέρασμα ότι οι προτινόμενοι αλγόριθμοι μπορούν να επιτύχουν υψηλότεροι απόδοση και να καταναλώσουν χαμηλότερη πολυπλοκότητα από την προσέγγιση SDR.
- Μειστοποίηση ποσοστού αθροίσματος: Οι επιστήμονες μεγιστοποίησαν το ποσοστό αθροίσματος σε επικοινωνίες MISO πολλαπλών χρηστών ενισχυμένες με RIS στις κατερχόμενες επικοινωνίες. Με τη χρήση της προκωδικοποίησης μηδενισμού των συντελεστών του BS, οι πίνακες ανακλαστικότητας του RIS και η κατανομή ισχύος βελτιστοποιήθηκαν διαδοχικά με τη βοήθεια της προσέγγισης μεγιστοποίησης-ελαχιστοποίησης. Επιπλέον, επιστήμονες ερεύνησαν το πρόβλημα του κληρονομικού συνολικού ρυθμού. Μέσα από το AO πλαίσιο, ο παθητικός σχηματισμός δέσμης εξασφαλίστηκε χρησιμοποιώντας τη μέθοδο κλασματικού προγραμματισμού, και σχεδιάστηκαν τρεις επαναληπτικοί αλγόριθμοι για τη βελτιστοποίηση των συντελεστών ανακλαστικότητας του RIS.
- Δικαιοσύνη των χρηστών: Επιστήμονες μεγιστοποίησαν τον ελάχιστο SNR ενός συστήματος MISO ενισχυμένο με RIS, όπου υποθετόταν ότι ο σύνδεσμος BS-RIS-user είναι ένα κανάλι Line of Sight. Αναπτύχθηκε μια προσέγγιση για την ελάχιστη απόδοση SINR υπό τον βέλτιστο γραμμικό προκωδικοποιητή, με τη χρήση της τυχαίας θεωρίας πινάκων. Ως αποτέλεσμα, οι αλλαγές φάσης του RIS μπορούν να βελτιστοποιηθούν χρησιμοποιώντας τις μεγάλης κλίμακας στατιστικές του καναλιού, κάτι που μπορεί να μειώσει σημαντικά την υπερφόρτωση της ανταλλαγής σημάτων.

2. Προσεγγίσεις για σχεδιασμό παθητικής δέσμης: Ένα παράδειγμα του προβλήματος κοινού σχεδιασμού μεταδόσεων και παθητικών προσανατολισμών μπορεί να διατυπωθεί ως εξής:

$$\begin{aligned} \min / \max_{\mathbf{w}, \boldsymbol{\theta}} f(\mathbf{w}, \boldsymbol{\theta} | \mathcal{H}) \\ \text{s.t. } \mathbf{w} \in \mathcal{T}, \\ \boldsymbol{\theta} \in \mathcal{P}, \end{aligned}$$

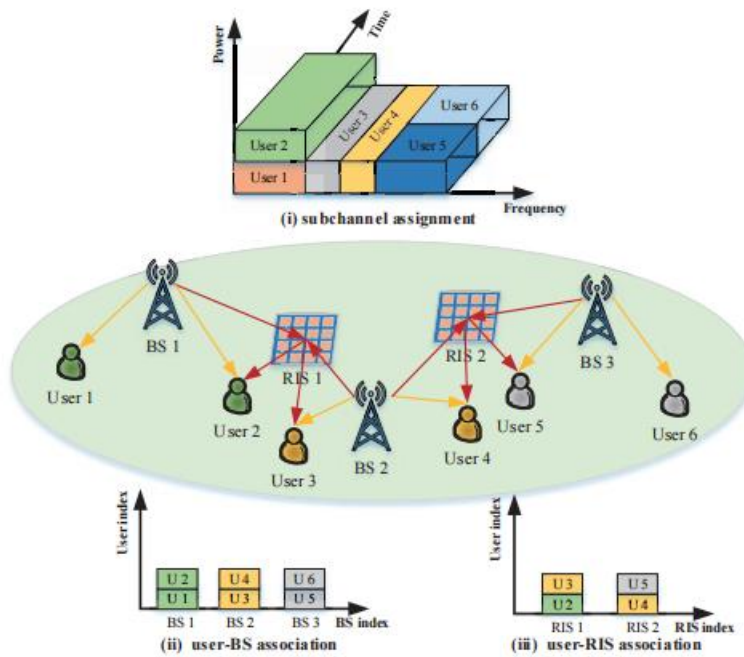
Όπου \mathcal{H} αναπαριστά το σύνολο του δεδομένου CSI, το \mathbf{w} και το $\boldsymbol{\theta}$ δηλώνουν το διάνυσμα διαμόρφωσης δέσμης μετάδοσης και το διάνυσμα παθητικής διαμόρφωσης δέσμης, τα \mathcal{T} και τα \mathcal{P} δηλώνουν το αντίστοιχο εφικτό σύνολο για το \mathbf{w} και το $\boldsymbol{\theta}$.

1. Συνεχής προσαρμογή του πλάτους και της φάσης: Σε αυτήν την περίπτωση, υποθέτουμε ότι το πλάτος και η φάση του κάθε στοιχείου του RIS μπορούν να προσαρμόζονται συνεχώς.
2. Σταθερό πλάτος και συνεχής μετατόπιση φάσης: Σε αυτήν την περίπτωση, υποθέτουμε ότι το πλάτος κάθε στοιχείου του RIS είναι σταθερό, π.χ. $\beta_i = 1$ και μπορεί να προσαρμόζεται συνεχώς η φάση του.
3. Σταθερό πλάτος και διακριτή μετατόπιση φάσης: Σε αυτήν την περίπτωση, υποθέτουμε ότι το πλάτος του κάθε στοιχείου του RIS είναι σταθερό, π.χ., $\beta_i = 1$ και μπορεί να προσαρμοστεί βάσει ενός διακριτού συνόλου τιμών για τη φάση.

Είναι σημαντικό να αναφερθεί ότι τα δυο πρώτα παραδείγματα είναι δύσκολο να υλοποιηθούν στην πράξη. Λόγω περιορισμών στο hardware, είναι πολύ δύσκολο να επιτευχθεί συνεχής έλεγχος του πλάτους κύματος και της φάσης για κάθε στοιχείο του RIS. Όμως, στην πράξη το τρίτο παράδειγμα με σταθερό πλάτος κύματος είναι πιο εφικτό να υπολογιστεί.

2.12. Διαχείριση πόρων σε δίκτυα ενισχυμένα με RIS

1. Προβλήματα κατανομής πόρων: Στο σχήμα 6 βλέπουμε ένα σενάριο μετάδοσης με ενίσχυση από RIS μεγάλης κλίμακας, όπου πολλαπλά BS εξυπηρετούν πολλούς χρήστες με τη βοήθεια πολλαπλών RIS. Στο πλαίσιο αυτό, πρέπει να συζητηθούν αρκετά σοβαρά θέματα.



Σχήμα 6: Απεικόνιση της διαχείρισης πόρων σε δίκτυα μεγάλης κλίμακας που υποστηρίζονται από RIS.

- Ανάθεση υπό-καναλιών: Η απόδοση του εύρους ζώνης μπορεί να βελτιωθεί αν ανατεθούν σωστά οι χρήστες σε διαφορετικά υποκανάλια. Σε περίπτωση που τα στοιχεία του RIS δεν είναι επιλεκτικά στη συχνότητα, χρειάζεται ένας κοινός πίνακας ανάκλασης RIS για κοινή χρήση μεταξύ όλων των υποκαναλιών, γεγονός που καθιστά δύσκολη την επίλυση των προβλημάτων βελτιστοποίησης που προκύπτουν. Για την αντιμετώπιση αυτής της δυσκολίας, οι επιστήμονες προτείνουν ένα δυναμικό σχήμα παθητικής διαμόρφωσης δέσμης, όπου τα μπλοκ πόρων κατανέμονται δυναμικά σε διαφορετικές ομάδες χρηστών με ποικίλες μετατοπίσεις φάσης RIS σε διαφορετικά χρονικά διαστήματα.
- Συσχέτιση χρήστη-RIS: Σε πολυ-συστηματικά δίκτυα όπου πολλαπλά RIS υποστηρίζουν πολλαπλούς χρήστες, η διασύνδεση των χρηστών με διαφορετικά RISs αποτελεί ένα ενδιαφέρον πρόβλημα. Τα σχήματα συσχέτισης χρήστη-RIS καθορίζουν γενικά τη συνολική απόδοση του δικτύου. Σε μια πολυ-συστηματική διάταξη με μαζικό MIMO και πολλαπλά RIS, ισχύει η ιδιότητα αυτόματης ακύρωσης παρεμβολών για RISs με άπειρο μέγεθος. Στη συνέχεια, το μελετώμενο πρόβλημα μέγιστου ελάχιστου SINR μπορεί να μετασχηματιστεί σε ένα πρόβλημα συσχέτισης χρήστη-RIS, το οποίο λύνεται αποδοτικά με τον προτεινόμενο αλγόριθμο greedy search.
- Σύνδεση πολλαπλών RISs με κύτταρα: Σε πολυ-κυψελικά σενάρια, το πρόβλημα βελτιστοποίησης γίνεται πολύπλοκο καθώς πρέπει να ληφθεί υπόψη η συνδυασμένη συσχέτιση χρήστη-BS, η συσχέτιση χρήστη-RIS και η κατανομή των υπο-καναλιών.
- Προσεγγίσεις για προβλήματα διαχείρισης πόρων: Ο προγραμματισμός διαφορετικών χρηστών με διαφορετικά υπο-κανάλια/RIS/BSs είναι ένα πρόβλημα NP-hard. Παρόλο που η βέλτιστη λύση μπορεί να επιτευχθεί με εξαντλητική

αναζήτηση όλων των δυνατών συνδυασμών συσχέτισης, απαιτεί υπερβολικά υψηλή υπολογιστική πολυπλοκότητα, ιδίως για τα μεγάλης κλίμακας δίκτυα στο Σχήμα 6. Άρα, πρέπει να αναπτυχθούν αλγόριθμοι χαμηλής πολυπλοκότητας και αποδοτικοί για να επιτευχθεί μια ισορροπία μεταξύ απόδοσης και πολυπλοκότητας. Παρακάτω γίνεται λόγος σε κάποιες προσεγγίσεις και αναφέρονται τα πλεονεκτήματα και τα μειονεκτήματά τους.

➤ Διαδική χαλάρωση: Μια ιδέα είναι να χαλαρώσουμε τη δυαδική μεταβλητή $\alpha (\alpha \in \{0,1\})$ σε μια συνεχή μεταβλητή $\alpha (\alpha \in [0,1])$, όπου α αντιπροσωπεύει την κατάσταση συσχέτισης του χρήστη. Με αυτόν τον τρόπο, η μη κυρτή ακέραιη περιοριστική συνθήκη χαλαρώνεται σε κυρτή και μπορούν να εφαρμοστούν συμβατικές τεχνικές κυρτού προγραμματισμού για την επίλυση του χαλαρωμένου προβλήματος. Βέβαια, το χαλαρωμένο πρόβλημα μπορεί ακόμα να είναι μη κυρτό, ειδικά όταν οι μεταβλητές βελτιστοποίησης είναι υψηλά συζευμένες. Επίσης, αυτού του είδους η χαλάρωση μπορεί να οδηγήσει σε σημαντική απώλεια απόδοσης μεταξύ του αρχικού ακέραιου προβλήματος και του χαλαρωμένου.

➤ Θεωρία ταιριάσματος: Η θεωρία ταιριάσματος είναι μια ισχυρή μέθοδος που έχει αναπτυχθεί για την επίλυση προβλημάτων συνδυαστικής συσχέτισης χρηστών. Το πρόβλημα συνδυαστικής βελτιστοποίησης συσχετισμού χρηστών σε δίκτυα ενισχυμένα με RIS μπορεί να διαμορφωθεί ως πρόβλημα αντιστοίχισης υποκαναλιών BSs-RISs υψηλών διαστάσεων. Αν και η αντιστοίχιση υψηλών διαστάσεων είναι NP-hard, μπορεί να αποσυντεθεί σε πολλά υποπροβλήματα αντιστοίχισης 2D, τα οποία μπορούν να επιλυθούν αποτελεσματικά. Το μειονέκτημα της θεωρίας ταιριάσματος είναι ότι απαιτεί την καθιέρωση ενός προκαθορισμένου καταλόγου προτίμησης τόσο για τους χρήστες όσο και για τους πόρους.

➤ Ευρετικοί αλγόριθμοι: Για την επίλυση των προβλημάτων που είναι υπολογιστικά πολύπλοκα, μια κοινή μέθοδος είναι η ανάπτυξη ευρετικών αλγορίθμων, όπου μπορούν να ληφθούν προσεγγιστικές λύσεις για το αρχικό πρόβλημα βελτιστοποίησης με αποδέκτη υπολογιστική πολυπλοκότητα. Ωστόσο, η απόδοση των ευρετικών αλγορίθμων είναι ευαίσθητη στις σχεδιασμένες στρατηγικές, που δεν είναι πάντα σταθερή.

Συμπεράσματα που προκύπτουν:

Με την αυξανόμενη έρευνα στις επικοινωνίες με βοήθεια των RIS, έχουμε αναγνωρίσει τα πλεονεκτήματα των RIS όσον αφορά τον υπερδιπλασιασμό της χωρητικότητας, την ενεργειακή απόδοση και τη νομιμότητα των χρηστών. Παρόλο που οι υπάρχουσες μελέτες συνήθως λύνουν το μη κυρτό πρόβλημα της κοινής βελτιστοποίησης της μετάδοσης και της παθητικής διαμόρφωσης των RIS μέσω της μεθόδου AO, υπάρχει ακόμα η ανάγκη για προηγμένες τεχνικές βελτιστοποίησης για να χαρακτηριστεί η βέλτιστη απόδοση που μπορούν να προσφέρουν οι RIS. Επιπλέον, ο σχεδιασμός της τοποθέτησης των RIS είναι ένας σημαντικός παράγοντας για την επίτευξη βέλτιστης απόδοσης. Είναι σημαντικό να σχεδιάσουμε αποτελεσματικούς αλγόριθμους που να λύνουν τα συσχετισμένα προβλήματα των βέλτιστων παθητικών διαμορφώσεων και τοποθετήσεων RIS. Επίσης, η ανάπτυξη

των RIS γίνεται συνήθως για να αποφύγει την αποκοπή του σήματος και να επιτευχθεί ένα κυρίαρχο κανάλι LoS, μειώνοντας την απώλεια δρόμου.

2.13. Μηχανική εκπαίδευση για συστήματα επικοινωνίας ενισχυμένα με RIS

Οι τεχνικές μηχανικής μάθησης έχουν κερδίσει σημαντικό ενδιαφέρον στις ασύρματες επικοινωνίες λόγω της ικανότητας τους να μάθουν και του μεγάλου χώρου αναζήτησης.

A. Κίνητρα και αρχιτεκτονική για την ενσωμάτωση του ML στα Ενισχυμένα Δίκτυα RIS

Προκειμένου να αξιοποιηθούν αποτελεσματικά τα RIS για την βελτιστοποίηση των ασύρματων δικτύων, προηγμένες ερευνητικές συνεισφορές έχουν μελετήσει ορισμένες τεχνικές προκλήσεις, που περιλαμβάνουν την εκτίμηση/μοντελοποίηση των καναλιών, τον κοινό σχεδιασμό της μεταδόσεως και της παθητικής διαμόρφωσης, καθώς και την ανάθεση πόρων από το BS στους χρήστες. Βέβαια υπάρχουν ακόμη κάποιοι περιορισμοί που πρέπει να αντιμετωπίσουν στα συμβατικά δίκτυα RIS:

- Υπόθεση Στατικότητας Χρήστη: Στην πλειοψηφία των υπάρχουσων ερευνών, υποτίθεται ότι οι χρήστες είναι στατικοί, αγνοώντας την κινητικότητα των χρηστών. Όπως, επίσης, παραβλέπεται και η διαφοροποίηση της ζήτησης των χρηστών, οδηγώντας σε υποβέλτιστη ανάθεση πόρων.
- Υπόθεση Άριστης Γνώσης: Οι συμβατικές προσεγγίσεις υποθέτουν άριστη γνώση του περιβάλλοντος επικοινωνίας, συμπεριλαμβανομένων των συνθηκών των καναλιών. Στην πραγματικότητα, το ασύρματο περιβάλλον υπόκειται σε αβεβαιότητες και διακυμάνσεις, καθιστώντας τις συμβατικές μεθόδους βελτιστοποίησης λιγότερο αποτελεσματικές.
- Περιορισμένη ανατροφοδότηση: Η ανατροφοδότηση από τους χρήστες προς τα RIS/BS είναι συχνά περιορισμένη και απαιτεί πολλούς πόρους, καθιστώντας δύσκολη την προσαρμογή σε αλλαγές σε πραγματικό χώρο.

Τέλος, η απόκτηση CSI στα δίκτυα ενισχυμένα από RIS γίνεται πιο προκλητική από αυτήν στα συμβατικά συστήματα αναμετάδοσης λόγω του παθητικού χαρακτήρα των RIS.

B. Deep Learning για συστήματα επικοινωνίας ενισχυμένα με RIS

Το deep learning έχει δείξει μεγάλες δυνατότητες για να επανασχεδιάσει τα συστήματα επικοινωνίας και μπορεί να σχεδιαστεί σε διάφορους τομείς των δικτύων ενισχυμένων από RIS λόγω των ισχυρών δυνατοτήτων μάθησης του.

Η απόκτηση έγκαιρου και ακριβούς CSI διαδραματίζει καθοριστικό ρόλο στα ασύρματα συστήματα, ειδικά στα δίκτυα MIMO. Ωστόσο, η απόκτηση CSI γίνεται πιο δύσκολη λόγω του του μεγάλου αριθμού κεραιών στα συστήματα MIMO. Για να αντιμετωπιστεί αυτή η δυσκολία, πολλές ερευνητικές συνεισφορές έχουν υιοθετήσει τη μέθοδο DL για την εκτίμηση του CSI ειδικά για την εκμετάλλευση δομών CSI πέραν των γραμμικών συσχετίσεων.

Σε αντίθεση με τα συμβατικά δίκτυα αναμετάδοσης με αυτόματη προώθηση (AF), στα δίκτυα ενισχυμένα από RIS, το RIS είναι ένα παθητικό στοιχείο που δεν μπορεί να πραγματοποιεί ενεργή αποστολή/λήψη και επεξεργασία σήματος.

Η προσέγγιση της διάστασης δεδομένων βασιζόμενη στα δεδομένα έχει το πλεονέκτημα της αναπαράστασης χωρίς μοντέλο ή μάθηση συνάρτησης, διότι δεν χρειάζεται ρητά μοντέλα των περιπλοκών ασύρματων καναλιών, με κόστος της απαιτούμενης μεγάλης ποσότητας δεδομένων εκπαίδευσης και αντίστοιχης υπολογιστικής ισχύος. Άρα, η μέθοδος DL μπορεί να χρησιμοποιηθεί για την εκτίμηση του CSI στα δίκτυα ενισχυμένα από RIS.

Εκτός από τις προαναφερθείσες εφαρμογές του DL στα δίκτυα ενισχυμένα από RIS, επιστήμονες εκμεταλλεύτηκαν μια προσέγγιση βαθιάς νευρικής δικτύωσης (DNN) στο περιβάλλον επικοινωνίας εσωτερικών χώρων για την εκτίμηση της αντιστοίχισης μεταξύ της θέσης ενός χρήστη και της διαμόρφωσης του RIS για τη μεγιστοποίηση του λόγου σήματος προς θόρυβο(SNR). Επιπλέον, το DL μπορεί να εφαρμοστεί για την εκμάθηση της βέλτιστης ρύθμισης φάσης του RIS με εκπαίδευση του DL εκτός σύνδεσης.

Γ. Ενισχυτική μάθηση για συστήματα επικοινωνίας ενισχυμένα με RIS

Η ενισχυμένη μάθηση (RL) είναι ένα ισχυρό παράδειγμα τεχνητής νοημοσύνης που μπορεί να εφαρμοστεί για να ενισχύσει τα στοιχεία δικτύων με τον τρόπο που αλληλεπιδρά με το περιβάλλον. Με την εκμετάλλευση της ικανότητας μάθησης (π.χ. μάθηση από το περιβάλλον, μάθηση από την ανατροφοδότηση των χρηστών και μάθηση από τα λάθη του), το μοντέλο RL μπορεί να αντιμετωπίσει τις προκλήσεις που συναντώνται στα συμβατικά ασύρματα δίκτυα με αποτέλεσμα τη βελτίωση της απόδοσης.

Η βασική ιδέα της χρήσης τεχνικών RL στα ενισχυμένα δίκτυα RIS είναι ότι επιτρέπει στους BS/RIS (πράκτορες) να βελτιώσουν την ποιότητα των υπηρεσιών τους μαθαίνοντας από το περιβάλλον, από την ιστορική τους εμπειρία και την ανατροφοδότηση των χρηστών. Συγκεκριμένα, τα μοντέλα RL μπορούν να χρησιμοποιηθούν για να υποστηρίξουν τους BS/RIS στις αλληλεπιδράσεις τους με το περιβάλλον (καταστάσεις), ενώ ταυτόχρονα εντοπίζουν τη βέλτιστη συμπεριφορά (δράσεις) των BS/RIS. Επιπλέον, το μοντέλο RL μπορεί να ενσωματώσει την προοπτική της μακροπρόθεσμης εξέλιξης του συστήματος (μακροπρόθεσμα οφέλη) αντί να επικεντρώνεται μόνο στις τρέχουσες καταστάσεις. Άρα, εφαρμόζεται για την επίλυση δύσκολων προβλημάτων στα ενισχυμένα δίκτυα RIS.

Οι αλγόριθμοι RL μπορούν να χωριστούν σε τρεις κατηγορίες: αλγόριθμους με βάση την αξία, αλγόριθμους με βάση την πολιτική και αλγόριθμους “actor-critic”.

Για να εκμεταλλευτούμε πλήρως τα οφέλη της χρήσης των RIS στα ασύρματα δίκτυα, έχει εξεταστεί ο συνδυασμός του σχεδιασμού μεταδόσεων και παθητικού

beamforming στο ενισχυμένο σύστημα RIS σε συστήματα MISO, συστήματα ασφάλειας ασύρματης επικοινωνίας κλπ. Σε αντίθεση με τη μέθοδο AO, η οποία βελτιστοποιεί εναλλάξ το beamforming μετάδοσης στο BS και το παθητικό beamforming στο RIS, η λύση που βασίζεται σε RL μπορεί να σχεδιαστεί τευτόχρονα.

Δ. Μια νέα αρχιτεκτονική RIS-ενισχυμένα ασύρματα δίκτυα με ενσωματωμένη μάθηση

Χάρη στο μοντέλο με ενσωματωμένη μάθηση, πολλές προκλήσεις στα συμβατικά ασύρματα δίκτυα επικοινωνίας έχουν παρακαμφθεί, οδηγώντας σε βελτιωμένη απόδοση δικτύου, βελτιωμένη αξιοπιστία και ευελιξία προσαρμογής.

Τώρα θα προσπαθήσουμε να περιγράψουμε μια νέα αρχιτεκτονική με ενσωματωμένη μάθηση για τα RIS-ενισχυμένα ασύρματα δίκτυα. Τα RIS είναι εγκατεστημένα στο πρόσωπο ενός κτιρίου για την ενίσχυση της ασύρματης απόδοσης. Το RIS συνδέεται με έναν ελεγκτή, ο οποίος ελέγχει τα αντανακλαστικά στοιχεία για να φιλοξενήσει τη λειτουργικότητα της αλλαγής φάσης και της απορρόφησης της απορρόφησης πλάτους. Στα μέρη συλλογής δεδομένων, επεξεργασίας δεδομένων και εξαγωγής χαρακτηριστικών συλλέγεται, αποθηκεύεται και επεξεργάζεται η σχετιζόμενη πληροφορία των χρηστών (π.χ. τύπος συσκευής, θέση, ζήτηση ρυθμού δεδομένων κλπ). Επομένως, οι συμπεριφορές και οι απαιτήσεις των χρηστών μπορούν να προβλεφθούν για την αποτελεσματική ανάπτυξη και λειτουργία των RIS.

Η έρευνα για τον προσδιορισμό της τοποθεσίας των RIS αποτελεί θεμελιώδες και απαραίτητο ζήτημα. Ωστόσο, δεν υπάρχουν πολλές έρευνες για αυτό το θέμα. Οι τρέχουσες έρευνες εστιάζονται κυρίως στη βελτιστοποίηση της απόδοσης τόσο για μονούς χρήστες όσο και για πολλαπλούς χρήστες.

Σκεπτόμενοι τον προσδιορισμό των RIS βασισμένο στις πληροφορίες κινητικότητας των χρηστών και των συγκεκριμένων απαιτήσεων δεδομένων καταλήγουμε στο συμπέρασμα ότι οι μακροπρόθεσμες πληροφορίες κίνησης και απαιτήσεις τηλεπικοινωνίας των χρηστών μπορούν να προβλεφθούν. Με αυτήν την πρόταση, ο τρόπος ανάπτυξης και έλεγχος των RIS μπορεί να σχεδιαστεί περιοδικά για τη μεγιστοποίηση των μακροπρόθεσμων οφειλών και κατα συνέπεια για τη μείωση του ελέγχου. Με την εξέταση της μακροπρόθεσμης κινητικότητας και απαίτησης των δεδομένων των χρηστών, τα ασύρματα δίκτυα ενισχυμένα με RIS γίνονται υψηλά δυναμικά συστήματα.

Ταυτόχρονα, για να μεγιστοποιήσουν την ποιότητα υπηρεσιών σε ένα άγνωστο περιβάλλον, τα RIS πρέπει να μάθουν αλληλεπιδρώντας με το περιβάλλον και προσαρμόζοντας την πολιτική ελέγχου/ανάπτυξης με βάση τα περιορισμένα σχόλια των χρηστών για να αντιμετωπίσουν την αβεβαιότητα του περιβάλλοντος.

2.14. Ενσωμάτωση RIS με άλλες τεχνολογίες προς 6G

Οι τρέχουσες έρευνες έχουν αποδείξει ότι τα ασύρματα δίκτυα ενισχυμένα με RIS είναι ικανά να αποκτούν καλά ρυθμισμένα κέρδη καναλιού, βελτιωμένη ποιότητα

υπηρεσίας, αυξημένη κάλυψη και μειωμένη κατανάλωση ενέργειας. Αυτές οι σημαντικές βελτιώσεις απόδοσης μπορούν να εφαρμοστούν σε διάφορα ασύρματα δίκτυα επικοινωνίας. Σε αυτήν την ενότητα, αναγνωρίζουμε τα κύρια ζητήματα και τις ευκαιρίες έρευνας προς 6G που σχετίζονται με την ενσωμάτωση των RIS και άλλων αναδυόμενων τεχνολογιών όπως η NOMA, PLS, SWIPT, τα αυτόματα δίκτυα οδήγησης κλπ.

2.14.1 NOMA και RIS

Προκειμένου να βελτιώσουν το SE και τη συνδεσιμότητα των ασύρματων δικτύων που βελτιώνονται από τα RIS, εφαρμόζονται τεχνολογίες NOMA στο πεδίο ισχύος, που η βασική ιδέα είναι να υπερκαλύπτονται τα σήματα δυο χρηστών σε διαφορετικές ισχύς για να αξιοποιήσουν το φάσμα πιο αποτελεσματικά εκμεταλλευόμενοι ευκαιριακά τις διαφορετικές συνθήκες των καναλιών των χρηστών. Η ελάχιστη αποκωσικοποίηση SINR όλων των χρηστών αυξάνεται για τη βελτιστοποίηση της θωράκισης του συστήματος.

2.14.2 PLS και RIS

Είναι φανερό ότι τα RIS είναι ικανά να ενισχύουν τόσο την επιθυμητή ισχύ του σήματος στον προοριζόμενο χρήστη, όσο και να μειώνουν την ισχύ παρεμβολών σε άλλους μη επιθυμητούς χρήστες. Εμπνευσμένοι από αυτό το αποτέλεσμα, αρκετοί επιστήμονες εξερευνούν την πιθανή αύξηση της απόδοσης στο πλαίσιο του PLS εφαρμόζοντας το RIS. Μία ομάδα χρηστών εξετάζει ένα κανάλι ενισχυμένο με RIS πολλαπλών εισόδων μοναδικών εξόδων με μοναδικό κατάσκοπο, όπου ο κατάσκοπος είναι εξοπλισμένος με μια μόνο κεραία. Ο ρυθμός ασφαλείας μεγιστοποιήθηκε με την κοινοτική βελτιστοποίηση του προσανατολισμού της μετάδοσης. Η ασφάλεια μπορεί να βελτιωθεί σημαντικά με την εγκατάσταση των RIS. Μία άλλη ομάδα επιστημόνων επικεντρώθηκαν στην περίπτωση όπου ο κατάσκοπος έχει καλύτερη κατάσταση καναλιού από τον νόμιμο δέκτη και είναι επίσης υψηλά συσχετισμένοι χωρικά, όπου ο ρυθμός ασφάλειας που μπορεί να επιτευχθεί είναι περιορισμένος στις συμβατικές επικοινωνίες. Ωστόσο, φαίνεται ότι τα άμεσα σήματα και τα ανακλώμενα σήματα μπορούν να συνδυαστούν καταστροφικά στον κατάσκοπο με τη βοήθεια των RIS, βελτιώνοντας έτσι σημαντικά τον ρυθμό ασφαλείας.

Το ίδιο πρόβλημα εξετάστηκε περαιτέρω λαμβάνοντας υπόψη έναν κατάσκοπο ή έναν νόμιμο δέκτη με πολλαπλές κεραίες. Μία ομάδα επιστημόνων μελέτησε το πρόβλημα μεγιστοποίησης του ελάχιστου ρυθμού ασφαλείας σε συστήματα ενισχυμένα με RIS πολλαπλών χρηστών, πολλαπλών εισόδων, μοναδικών εξόδων με πολλαπλούς κατασκόπους λαμβάνοντας υπόψη τόσο τις συνεχείς όσο και τις διακριτές φάσεις του RIS. Η εισαγωγή του τεχνητού θορύβου είναι μια αποτελεσματική τεχνική για να βελτιωθεί ο ρυθμός ασφαλείας.

2.14.3 SWIPT και RIS

Το SWIPT είναι μια ελκυστική τεχνική για τα μελλοντικά δίκτυα IoT (Internet of Things). Ωστόσο, το χαμηλό ΕΕ στους δέκτες ενέργειας είναι το κύριο εμπόδιο στα πρακτικά συστήματα SWIPT. Προεκτιμένου να ξεπεραστεί αυτός ο περιορισμός, η εγκατάσταση των RIS αποτελεί μια υποσχόμενη λύση και έχει εξεταστεί η βοήθεια των RIS στο SWIPT σε ορισμένες δημοσιεύσεις. Ορισμένοι επιστήμονες μελέτησαν ένα σύστημα SWIPT ενισχυμένο με RIS, με ατομικές απαιτήσεις SINR για τους δέκτες πληροφοριών. Η συνολική ισχύς που λαμβάνεται από τους δέκτες ενέργειας μετριούνταν και ελαχιστοποιούνταν με την κοινή βελτιστοποίηση του προσανατολισμού μετάδοσης και προσαρμογής με τον προτεινόμενο αλγόριθμο AO. Επιπλέον, μεγιστοποίησαν την ελάχιστη ισχύ που λαμβάνεται από τους δέκτες ενέργειας. Τα αποτελέσματα έδειξαν ότι η εγκατάσταση ενός RIS μπορεί να βελτιώσει την αποδοτικότητα συλλογής ενέργειας.

Σημειώνεται ότι οι παραπάνω ερευνητικές συνεισφορές μελέτησαν το κέρδος από την εγκατάσταση των RIS για το SWIPT κυρίως από την πλευρά της επικοινωνίας και αγνόησαν τα ηλεκτρομαγνητικά χαρακτηριστικά των RIS. Όπως αναφέρθηκε παραπάνω, υπάρχουν σημαντικές διαφορές μεταξύ της περιοχής του κοντινού πεδίου και της περιοχής μακρινού πεδίου των RIS. Επομένως, απαιτούνται εξελιγμένα μοντέλα ασύρματης μεταφοράς ισχύος που βασίζονται στον ηλεκτρομαγνητισμό για να απολαύσουν πλήρως τα οφέλη των RIS.

2.14.4 UAV και RIS

Οι RIS μπορούν να εφαρμοστούν σε δίκτυα ασύρματων μέσων UAV, όπου τα UAV χρησιμοποιούνται για να συμπληρώσουν ή να υποστηρίξουν τα υπάρχοντα γειτονικά κυψελοδίκτυα. Ένα RIS ενισχύει την κάλυψη και την ποιότητα των υπηρεσιών UAV με το να αντισταθμίζει την απώλεια ισχύος σε μεγάλες αποστάσεις, καθώς και με το να δημιουργεί εικονικούς συνδέσμους LoS μεταξύ των UAV και των κινητών χρηστών μέσω παθητικής ανάκλασης των ληφθέντων σημάτων. Μία ομάδα επιστημόνων βελτιστοποίησε συνδυαστικά την πορεία των UAV και τις μετατοπίσεις φάσης του RIS με επαναληπτικό τρόπο οπότε έδειξε οι μέσοι επιτεύξιμοι ρυθμοί των χρηστών βελτιώνονταν σημαντικά με τη βοήθεια των RIS. Με τον συνδυασμό του σχεδιασμού της πορείας UAV και των παραμέτρων ανάκλασης του RIS, διασφαλίστηκε ένας εικονικός σύνδεσμος LoS μεταξύ της BS και των χρηστών. Επομένως, βελτιώθηκε τόσο ο μέσος ρυθμός δεδομένων όσο και η πιθανότητα επίτευξης κάτω από το δέλτα LoS.

Η περιορισμένη διάρκεια πτήσης των UAV (συνήθως κάτω από 30 λεπτά) εμποδίζει την ευρεία εμπορική εφαρμογή των δικτύων που χρησιμοποιούν UAV. Με την ανάπτυξη των RISs, μπορεί κανείς να προσαρμόζει τη φάση του RIS αντί να ελέγχει την κίνηση του UAV για τη δημιουργία εικονικών συνδέσεων LoS μεταξύ του UAV και των χρηστών. Επομένως, το UAV μπορεί να διατηρήσει κατάσταση αιώρησης μόνο όταν οι εικονικοί σύνδεσμοι LoS δεν μπορούν να διαμορφωθούν ακόμα και με την βοήθεια των RISs. Χρησιμοποιώντας το προαναφερθέν πρωτόκολλο, η συνολική κατανάλωση ενέργειας του UAV μειώνεται, κάτι που από τη σειρά, αυξάνει τη διάρκεια πτήσης του UAV. Επιπλέον, τοποθετώντας ένα μικρό

καταμεμημένο δέκτη φόρτωσης (DLC) ή αντάπτορα ασύρματης φόρτισης (WPT) μέσα στα UAV, ενώ ταυτόχρονα τοποθετείται ένας πομπός DLC/WPT στο έδαφος ή στη στέγη κτιρίου, τα UAV μπορούν να φορτίζονται όσο πετούν εντός της εμβέλειας κάλυψης του πομπού DLC/WPT. Ωστόσο, πρέπει να εγγυάται την LoS σύνδεση μεταξύ των UAV και των σταθμών/ οχημάτων φόρτισης, το οποίο είναι δύσκολο σε αστικό σενάριο, όταν η σύνδεση LoS μεταξύ των UAV και των σταθμών/ οχημάτων φόρτισης μπλοκάρεται με μεγάλη πιθανότητα από τα υψηλά κτίρια. Τα RIS μπορούν να διαμορφώσουν ευφυές περιβάλλον ασύρματης διάδοσης δημιουργώντας εικονικούς συνδέσμους LoS μεταξύ των UAV και των σταθμών/οχημάτων φόρτισης μέσω παθητικής ανάκλασης των ληφθέντων σημάτων. Επομένως, η ποιότητα υπηρεσίας φόρτισης βελτιώνεται με την βοήθεια των RIS. Το βελτιωμένο σενάριο επικοινωνίας UAV με RIS είναι φυσικά ένα πολύ δυναμικό, το οποίο ανήκει στο πεδίο της Μηχανικής Μάθησης.

2.14.5 Αυτόνομη οδήγηση/συνδεδεμένα οχήματα και RIS

Τα RIS μπορούν, επίσης, να εγκατασταθούν στα συστήματα αυτόνομης οδήγησης που υποστηρίζονται από vehicle-to-infrastructure (V2I), όπου τα στοιχεία V2I χρησιμοποιούνται για να συμπληρώσουν τις δαπανηρές μονάδες που υπάρχουν στα οχήματα. Τα δίκτυα V2I επιτρέπουν στα αυτόνομα οχήματα ή στα συνδεδεμένα οχήματα να λαμβάνουν αξιόπιστες πληροφορίες κίνησης πραγματικού χρόνου από τους σταθμούς βάσης, οι πληροφορίες συλλέγονται από σταθμούς βάσης παραπλεύρως του δρόμου και μεταδίδονται από τους σταθμούς βάσης στους BSs, που διευκολύνει την αλληλεπίδραση μεταξύ AVs/CVs και των χρηστών του δρόμου, ενισχύοντας έτσι την ασφάλεια και την αποδοτικότητα της κυκλοφορίας.

Δεδομένου ότι η ποιότητα και η αξιοπιστία των συστημάτων AVs/CVs δεν μπορούν να προσβληθούν, το σύστημα AVs/CVs πρέπει να λειτουργεί σε πραγματικό χρόνο, ενώ η μετάδοση πρέπει να είναι απόλυτα αξιόπιστη. Ωστόσο, η ποιότητα των υπηρεσιών των τρέχουσων συστημάτων επικοινωνίας V2I δεν μπορεί να εγγυηθεί λόγω του περίπλοκου τοπίου καναλιού στο αστικό περιβάλλον και της πολυπλοκότητας των οδικών συνθηκών όπως οι κακές καιρικές συνθήκες. Επιστήμονες απέδειξαν ότι η απόδοση των δικτύων των οχημάτων μπορεί να βελτιωθεί σημαντικά με τη βοήθεια των RISs. Αφού τα RISs κατασκευάζονται από ηλεκτρομαγνητικά υλικά, μπορούν να εγκατασταθούν σε κυρίαρχες επιφάνειες όπως τοιχώματα κτιρίων, διαφημιστικές πινακίδες, παράθυρα οχημάτων κλπ. Με τη μαζική ανάπτυξη των RISs, μια εικονική σύνδεση LoS μεταξύ των BSs και των AVs θα εξασφαλιστεί βελτιώνοντας την αξιοπιστία των επικοινωνιών V2I.

Στα συστήματα αυτόνομης οδήγησης που ενισχύονται με RIS, η ασφάλεια οδήγησης των AVs είναι η κύρια προτεραιότητα. Όσον αφορά την ασφάλεια, πρέπει να αποφεύγονται οι συγκρούσεις ενώ πρέπει να τηρούνται οι κανόνες κυκλοφορίας. Επιπλέον, στα συστήματα αυτόνομης οδήγησης που ενισχύονται με RISs και βοηθούνται από V2I, η ποιότητα των ασύρματων υπηρεσιών για τα AVs πρέπει να εγγυάται σε κάθε timeslot.

2.15 Συμπεράσματα και προκλήσεις

Παραπάνω αναφέραμε ορισμένες έρευνες σχετικά με τα ενισχυμένα ασύρματα δίκτυα με χρήση των RIS που προτείνονται για εφαρμογές στα δίκτυα της επόμενης γενιάς. Χρειάζονται περαιτέρω προσπάθειες έρευνας για την ενσωμάτωση των πολύπλοκων φυσικών μοντέλων των διαφορετικών υλοποιήσεων RIS με τα ευρέως χρησιμοποιούμενα μοντέλα επικοινωνίας.

3. Έλεγχος αυθεντικότητας φυσικού επιπέδου στις ασύρματες επικοινωνίες

3.1 Εισαγωγή

Η ταυτοποίηση-αυθεντικότητα είναι ένα σημαντικό θέμα στις ασύρματες επικοινωνίες επειδή η ανοιχτή φύση του ασύρματου μέσου παρέχει περισσότερες ευπάθειες ασφάλειας. Πρόσφατα. Η Ταυτοποίηση Φυσικού Επιπέδου (PLA) έχει προσελκύσει το ενδιαφέρον πολλών ερευνητών επειδή παρέχει ασφάλεια βασισμένη στη θεωρία της πληροφορίας και χαμηλή πολυπλοκότητα. Υπάρχουν δυο κατηγορίες τεχνικών PLA: παθητικές και ενεργές τεχνικές. Στις παθητικές τεχνικές, ένας παραλήπτης ταυτοποιεί τον πομπό βασιζόμενος στα φυσικά χαρακτηριστικά των ληφθέντων σημάτων. Επιπλέον, διαιρούμε τις παθητικές τεχνικές σε δυο υποκατηγορίες τεχνικές βασισμένες σε συσκευές και τεχνικές βασισμένες στο κανάλι. Στις ενεργές τεχνικές, ένας πομπός δημιουργεί μια ετικέτα βασισμένη σε ένα μυστικό κλειδί και την ενσωματώνει σε ένα αρχικό μήνυμα. Συνεπώς, η παρακολούθηση της ετικέτας επιτρέπει στον παραλήπτη να ταυτοποιήσει τον πομπό βασισμένο στην ύπαρξη της ετικέτας στο ληφθέν σήμα. Επιπλέον, διαιρούμε τις ενεργές τεχνικές σε δυο υποκατηγορίες: μη-κρυφές τεχνικές και κρυφές τεχνικές.

Οι υπηρεσίες ασύρματης επικοινωνίας αυξάνονται γρήγορα λόγω της διάδοσης των κινητών συσκευών και του Internet of Things. Η ταυτοποίηση είναι σημαντική στις ασύρματες επικοινωνίες επειδή η ανοιχτή φύση του ασύρματου μέσου παρέχει περισσότερες ευπάθειες ασφάλειας. Οι περισσότεροι μηχανισμοί ταυτοποίησης που υπάρχουν ήδη στις ασύρματες επικοινωνίες επιτυγχάνονται μέσω μηχανισμών ταυτοποίησης στο ανώτερο επίπεδο. Ωστόσο, οι μηχανισμοί αυτοί βασίζονται σε παραδοσιακούς αλγόριθμους κρυπτογραφίας, πράγμα που τους καθιστά ακατάλληλους για νέα ασύρματα συστήματα επικοινωνίας όπως το IoT, το Internet of Vehicles (IoV), τα Smart Grids (SG) και τα Unmanned Aerial Vehicles (UAV). Οι περιορισμοί αυτών των μηχανισμών περιλαμβάνουν το γεγονός ότι η ασφάλεια τους βασίζεται στην υπόθεση της περιορισμένης υπολογιστικής ισχύος, η οποία μπορεί να ανατραπεί καθώς η υπολογιστική ισχύς αυξάνεται και οι αλγόριθμοι κρυπτανάλυσης εξελίσσονται. Αυτό μπορεί να οδηγήσει σε επιθέσεις. Επιπλέον, οι αλγόριθμοι κρυπτογραφίας είναι ευάλωτοι στις επιθέσεις επανάληψης και επιφέρουν υψηλά κόστη επικοινωνίας και πολυπλοκότητα. Οι αλγόριθμοι απαιτούν επίσης διαδικασίες κοινής χρήσης κλειδιών και διαχείρισης, πράγμα που αυξάνει το κόστος και την πολυπλοκότητα, ιδίως σε μεγάλα ασύρματα δίκτυα.

3.2 Αυθεντικοποίηση φυσικού επιπέδου

Η αυθεντικοποίηση στο Φυσικό Επίπεδο (Physical-Layer Authentication - PLA) έχει κερδίσει το ενδιαφέρον της έρευνας λόγω των ακόλουθων πλεονεκτημάτων. Πρώτον, το PLA προσφέρει πληροφοριακή ασφάλεια, καθώς προστατεύει ένα χαρακτηριστικό του φυσικού επιπέδου ή ένα σήμα από τους αντιπάλους με θορυβώδη παρατήρηση μόνο, δηλαδή οι αντίπαλοι δεν γνωρίζουν το ακριβές

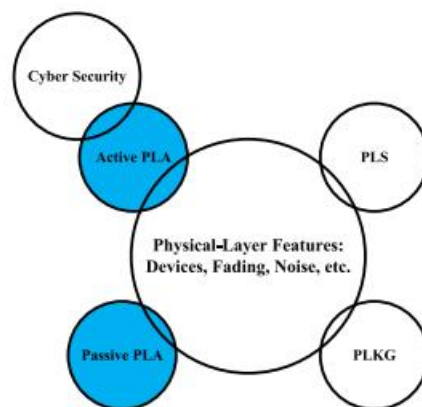
χαρακτηριστικό ή σήμα. Αυτή η αβεβαιότητα των αντιπάλων δεν μπορεί να ανατραπεί από αυξημένη υπολογιστική ικανότητα, καθώς οι αντίπαλοι μαντεύουν το χαρακτηριστικό αυτό bit προς bit. Η θεωρητική βάση των μηχανισμών PLA μπορεί να εξηγηθεί μέσω της ανάλυσης ασφάλειας της πληροφορικής του Shannon. Αν, για παράδειγμα, και ο νόμιμος παραλήπτης παρατηρεί επίσης τη θορυβώδη έκδοση του σήματος, ο νόμιμος παραλήπτης αντιμετωπίζει μόνο το πιο εύκολο πρόβλημα σε σύγκριση με αυτό του αντιπάλου. Συγκεκριμένα, ο νόμιμος παραλήπτης λύνει ένα πρόβλημα ανίχνευσης ενός bit, ενώ ο αντίπαλος πρέπει να λύσει ένα πρόβλημα εκτίμησης πολλών συμβόλων. Ο αντίπαλος πρέπει να εκτιμήσει ακριβώς όλα τα σύμβολα του σήματος πριν προσπαθήσει να εξάγει το μυστικό κλειδί από το εκτιμημένο σήμα. Σε σύγκριση με ένα πρόβλημα ανίχνευσης ενός bit, ένα πρόβλημα εκτίμησης πολλών συμβόλων απαιτεί εξαιρετικά SINR για το ληφθέν σήμα, το οποίο αποτελεί φυσικό πλεονέκτημα του PLA. Δεύτερον, το PLA επιτρέπει στο νόμιμο παραλήπτη να διακρίνει γρήγορα μεταξύ νόμιμου και παράνομου πομπού χωρίς την ανάγκη για πολύπλοκες διαδικασίες στο ανώτερο επίπεδο, εξοικονομώντας υπολογιστική πολυπλοκότητα και χρόνο επεξεργασίας. Τρίτον, το PLA είναι υψηλά συμβατή, καθώς συσκευές που δεν είναι συμβατές μπορούν να ανιχνεύσουν τα φυσικά bit της αλληλεπίδρασης τους, ακόμη κι αν δεν μπορούν να αποκωδικοποιήσουν τα ανώτερα επίπεδα των αλληλεπιδράσεων τους. Τέλος, το PLA δεν αποσκοπεί στο να αντικαταστήσει ένα σύστημα αυθεντικοποίησης στο ανώτερο επίπεδο αλλά να το συμπληρώσει. Αντίθετα, ένα σχέδιο PLA σχεδιάζεται για να αποτελέσει συμπληρωματικό στοιχείο ενός σχεδίου αυθεντικοποίησης στο ανώτερο επίπεδο, το οποίο παρέχει υψηλότερο επίπεδο ασφάλειας. Ο μηχανισμός αυθεντικοποίησης στο ανώτερο επίπεδο χρησιμοποιείται για την αυθεντικοποίηση της ταυτότητας ενός νόμιμου χρήστη, ενώ ο μηχανισμός PLA χρησιμοποιείται για την αυθεντικοποίηση της συσκευής που χρησιμοποιεί ο νόμιμος χρήστης. Για παράδειγμα, ένας νόμιμος χρήστης μπορεί να χρησιμοποιεί διάφορες συσκευές σε διάφορες στιγμές, όπως ένα κινητό τηλέφωνο μια στιγμή και ένα iPad μια άλλη στιγμή. Ένα ακόμα παράδειγμα, ένας νόμιμος χρήστης μπορεί να χρησιμοποιεί διάφορες συσκευές ταυτόχρονα, όπως ένα σύστημα με καταναμημένες κεραίες. Εάν ο παραλήπτης μπορεί να αυθεντικοποιήσει ταυτόχρονα τόσο την ταυτότητα όσο και τη συσκευή του νόμιμου χρήστη, το επίπεδο ασφαλείας του συστήματος διπλής αυθεντικοποίησης θα πρέπει να είναι υψηλότερα από τη χρήση μόνο ενός μηχανισμού αυθεντικοποίησης.

Κατηγοριοποιούμε τα υπάρχοντα σχέδια PLA σε δυο κατηγορίες: παθητικά και ενεργά συστήματα. Στα παθητικά σχέδια, ένας παραλήπτης αυθεντικοποιεί τον πομπό βασιζόμενος στα χαρακτηριστικά του φυσικού στρώματος των ληφθέντων σημάτων όπως τα χαρακτηριστικά των ραδιοσυχνοτήτων (FR) ή τα χαρακτηριστικά του καναλιού. Στα ενεργά σχέδια, ένας πομπός δημιουργεί ένα σήμα βάσει ενός μυστικού κλειδιού και το ενσωματώνει σε ένα πηγαίο μήνυμα. Στη συνέχεια, ένας παραλήπτης αυθεντικοποιεί τον πομπό ελέγχοντας εάν το σήμα υπάρχει στο ληφθέν σήμα. Η βασική διαφορά μεταξύ των δυο κατηγοριών είναι εάν το πηγαίο μήνυμα τροποποιείται σκόπιμα ανάλογα με το σήμα ή όχι. Συγκεκριμένα, ένα παθητικό σχέδιο δεν τροποποιεί καθόλου το πηγαίο μήνυμα, ενώ ένα ενεργό σχέδιο το τροποποιεί για να παρέχει επιπρόσθετα χαρακτηριστικά στο φυσικό επίπεδο. Αξίζει να σημειωθεί ότι το PLA αποτρέπει αποτελεσματικά τις επαναληπτικές επιθέσεις διότι τα χαρακτηριστικά του φυσικού επιπέδου ή τα σήματα συνήθως

μεταβάλλονται με τον χρόνο. Για παράδειγμα, εάν ένας αντίπαλος επαναλάβει ένα παλαιό σήμα στον νόμιμο παραλήπτη, ο νόμιμος παραλήπτης μπορεί να ανιχνεύσει την επαναληπτική επίθεση συγκρίνοντας το τρέχον σήμα με τα προηγούμενα σήματα.

3.3 Σύγκριση μεταξύ του PLA και άλλων τεχνικών ασφαλείας φυσικού επιπέδου

Εκτός από το γεγονός ότι το φυσικό επίπεδο παρέχει έναν υποσχόμενο μηχανισμό αυθεντικοποίησης, παρέχει επίσης άλλες τεχνικές ασφαλείας όπως η Ασφάλεια στο Φυσικό Επίπεδο (Physical Layer Security - PLS) και η Δημιουργία Κλειδιών στο Φυσικό Επίπεδο (Physical Layer Key Generation - PLKG). Στο παρακάτω σχήμα, φαίνεται η σχέση των διάφορων τεχνικών ασφαλείας. Η PLS επιτρέπει την εμπιστευτική μετάδοση χρησιμοποιώντας τα φυσικά χαρακτηριστικά χωρίς την ανάγκη κοινών μυστικών κλειδιών. Στόχος της PLS είναι να χρησιμοποιήσει μια τεχνική μετάδοσης που να παραδίδει τα εμπιστευτικά μηνύματα σε έναν νόμιμο παραλήπτη, αλλά να εξασφαλίζει ότι ο αντίπαλος δεν μπορεί να αποκρυπτογραφήσει τα μεταδιδόμενα εμπιστευτικά μηνύματα. Για παράδειγμα, η ασφάλεια που παρέχει η PLS είναι εφικτή όταν το SINR του νόμιμου παραλήπτη λόγω της ποιότητας του καναλιού, ή καθίσταται χαμηλότερο από το SINR του νόμιμου παραλήπτη λόγω μιας ειδικής τεχνικής όπως η κωδικοποίηση του καναλιού, η προσαρμογή βάσει του καναλιού, η εισαγωγή τεχνητών θορύβων.



Σχήμα 7. Σχέση μεταξύ διαφορετικών τεχνικών ασφαλείας

Το PLKG παρέχει μια συμφωνία μυστικών κλειδιών μεταξύ του νόμιμου πομπού και του παραλήπτη πάνω σε ένα τυχαίο κανάλι εκπομπής, όπου τόσο ο νόμιμος παραλήπτης όσο και ο αντίπαλος έχουν πρόσβαση σε αυτό. Να σημειωθεί ότι ο αντίπαλος έχει πλήρη πρόσβαση με παρατηρήσεις που δεν είναι ταυτόσημες με αυτές του νόμιμου παραλήπτη. Συνεπώς, ο στόχος του PLKG είναι να εξάγει τυχαία κλειδιά από το κανάλι μεταξύ του νόμιμου πομπού και του παραλήπτη αλλά ο αντίπαλος να μην μπορεί να εξάγει τα ίδια κλειδιά. Για παράδειγμα, τα βασικά βήματα του PLKG περιλαμβάνουν τα εξής: ανίχνευση του τυχαίου καναλιού για την

απόκτηση τυχαίων συσχετισμένων μετρήσεων στους ασύρματους μεταδότες, εξαγωγή χαρακτηριστικών του καναλιού, δημιουργία τυχαίων μυστικών κλειδιών με την εκτέλεση κβαντοποίησης του καναλιού, εφαρμογή ιδιωτικής συμφιλίωσης για την αποφυγή της ασυμφωνίας των μυστικών κλειδιών μεταξύ των ασύρματων μεταδοτών και εφαρμογή ιδιωτικής ενίσχυσης για τη βελτίωση της τυχειότητας των μυστικών κλειδιών.

Παρόλο που το PLA, το PLS και το PLKG σχεδιάστηκαν βασισμένα στα χαρακτηριστικά του φυσικού επιπέδου, έχουν διαφορετικούς στόχους και διαφορετικούς περιορισμούς. Για παράδειγμα, το PLS έχει τους ακόλουθους περιορισμούς:

- Ο λόγος του SINR του αντιπάλου πρέπει να είναι μικρότερος από αυτόν του νόμιμου παραλήπτη
- Η φθορά του σήματος του αντιπάλου πρέπει να είναι πιο έντονη από αυτήν του νόμιμου παραλήπτη
- Η ικανότητα μυστικότητας (secrecy capacity) επιτυγχάνεται εις βάρος της εφικτής μείωσης της χωρητικότητας
- Είναι ευαίσθητο στα σφάλματα εκτίμησης του καναλιού
- Είναι ευαίσθητο στις παρατηρήσεις από πολλούς συνεργαζόμενους αντιπάλους

Το PLKG έχει τους ακόλουθους περιορισμούς:

- Οι διάφοροι δέκτες θα πρέπει να έχουν χωρική αποσυσχέτιση καναλιών
- Οι νόμιμοι πομποδέκτες να έχουν αμοιβαιότητα καναλιού
- Η διακύμανση του καναλιού πρέπει να υπάρχει σε χρονικούς, φασματικούς ή χωρικούς τομείς
- Ο αντίπαλος θα πρέπει να έχει περιορισμένους υπολογιστικούς πόρους
- Είναι ευαίσθητο σε σφάλματα εκτίμησης καναλιών και σφάλματα αναντιστοιχίας αμοιβαιότητας
- Ευαίσθητο στην ικανότητα του αντιπάλου να εκτιμήσει το νόμιμο κανάλι

Ο στόχος του PLA είναι να επαληθεύει την προέλευση του ληφθέντος σήματος βασιζόμενο στα χαρακτηριστικά του φυσικού επιπέδου. Για παράδειγμα, το παθητικό PLA επιτυγχάνει την επαλήθευση συγκρίνοντας τα χαρακτηριστικά του φυσικού επιπέδου ενός άγνωστου πομπού με αυτά του νόμιμου πομπού. Το ενεργό PLA χρησιμοποιεί την κυβερνοασφάλεια για τη δημιουργία μιας κοινόχρηστης ετικέτας μεταξύ νόμιμων πομπών και επιτυγχάνει την επαλήθευση ελέγχοντας εάν η ετικέτα υπάρχει στο ληφθέν σήμα, όπου η τυχειότητα των χαρακτηριστικών του φυσικού επιπέδου προστατεύει την ετικέτα από την παρακολούθηση από τον αντίπαλο.

Από την άποψη της ασφάλειας του συστήματος, το PLA είναι πιο σημαντικό από άλλες τεχνικές ασφάλειας του φυσικού επιπέδου, επειδή ένας παραλήπτης πρέπει πρώτα να επαληθεύσει την προέλευση του ληφθέντος σήματος. Στη συνέχεια, εάν το τεστ επαλήθευσης είναι επιτυχημένο, ο παραλήπτης μπορεί να αποκωδικοποιήσει αξιόπιστα εμπιστευτικά μηνύματα. Επιπλέον, το PLA μπορεί να αμυνθεί αποτελεσματικά ενάντια σε ενεργές επιθέσεις, όπως η παρακολούθηση. Ωστόσο, τόσο τα υπάρχοντα PLS όσο και τα PLKG μπορούν να αμυνθούν μόνο ενάντια σε παθητικές επιθέσεις και όχι ενάντια σε ενεργές επιθέσεις.

3.4 Συνεισφορές

Σε αυτήν την ενότητα, παρουσιάζουμε μια σφαιρική ταξινόμηση για το PLA. Συγκεκριμένα, διαιρούμε τα παθητικά σχήματα σε τρεις υποκατηγορίες: χαρακτηριστικά βασισμένα στη συσκευή, χαρακτηριστικά βασισμένα στο κανάλι και επεκτεινόμενα παθητικά σχήματα, τα οποία μπορούν να περιγραφούν ως εξής:

1. Τα χαρακτηριστικά βασισμένα στη συσκευή αντικατροπτίζουν την υλική ατέλεια της συσκευής που είναι ο πομπός, όπως η Απόκλιση Συχνότητας Φέροντος (CFO), η ανισοροπία I/Q και η απόκλιση του ρολογιού (clock skew). Τα χαρακτηριστικά βασισμένα στη συσκευή είναι συγκεκριμένα στο υλικό και μοναδικά, ακόμα κι όταν οι πομποί παράγονται από τον ίδιο κατασκευαστή.
2. Τα χαρακτηριστικά βασισμένα στο κανάλι αντικατροπτίζουν τις πληροφορίες του καναλιού μεταξύ του νόμιμου πομπού και του παραλήπτη, όπως η Ισχύς Λήψης Σήματος (RSS) και η Πληροφορία Κατάστασης Καναλιού (CSI). Τα χαρακτηριστικά βασισμένα στο κανάλι των διάφορων πομπών πρέπει να έχουν ισχυρή χωρική αποκόσμηση. Συγκεκριμένα, σε ένα περιβάλλον με πλούσια διασπορά, αν η απόσταση μεταξύ δυο πομπών είναι μεγαλύτερη από το μισό του μήκους κύματος, τα χαρακτηριστικά βασισμένα στο κανάλι από διάφορους πομπούς προς τον ίδιο παραλήπτη μπορούν να θεωρηθούν ως εντελώς μη συσχετισμένα. Αντίθετα, εάν το κανάλι δεν έχει πλούσια διασπορά και ένας αντίπαλος βρίσκεται σε κοντινή απόσταση από τον νόμιμο πομπό, τα παθητικά σχήματα με χαρακτηριστικά βασισμένα στο κανάλι μπορεί να αποτύχουν, επειδή τα χαρακτηριστικά βασισμένα στο κανάλι των διαφορετικών πομπών μπορεί να γίνουν παρόμοια.
3. Το επεκτεινόμενο παθητικό σχήμα περιλαμβάνει τρεις τύπους βελτιωμένων παθητικών σχημάτων. Πρώτον, το υβριδικό σχήμα χρησιμοποιεί και τα χαρακτηριστικά βασισμένα στη συσκευή και τα χαρακτηριστικά βασισμένα στο κανάλι για να βελτιώσει περαιτέρω την ακρίβεια της επαλήθευσης. Δεύτερον, χρησιμοποιήθηκε η μη εποπτευόμενη Μηχανική Μάθηση (UML) για την ταξινόμηση των ληφθέντων χαρακτηριστικών χωρίς το στάδιο εκπαίδευσης. Τρίτον, ο τεχνητός θόρυβος (AN) χρησιμοποιείται για να βελτιώσει περαιτέρω την ασφάλεια.

Ένα καλά σχεδιασμένο σύστημα PLA θα πρέπει να λαμβάνει υπόψη τρεις ιδιότητες: ανθεκτικότητα, ασφάλεια και μυστικότητα. Για τη διασφάλιση της αυθεντικότητας, είναι υψηλά επιθυμητό ένα σύστημα PLA να αντιστέκεται στις επιδράσεις της φθοράς του καναλιού και του θορύβου, καθώς οι ασύρματες μεταδόσεις λαμβάνουν χώρα σε τυχαία περιβάλλοντα φθοράς. Για τη διασφάλιση της ασφάλειας, ένα σύστημα PLA πρέπει να αποτρέπει τη δυνατότητα του αντιπάλου να πραγματοποιεί επιτυχημένες επιθέσεις. Για τη διασφάλιση της μυστικότητας, ένα σύστημα PLA δεν μπορεί να θυσιάσει εμφανώς τη δυνατότητα αποκωδικοποίησης του αρχικού μηνύματος. Δεδομένου ότι τα παθητικά σχήματα δεν ενσωματώνουν καμία ετικέτα στο αρχικό μήνυμα, λαμβάνουν υπόψη τόσο την ανθεκτικότητα όσο και την ασφάλεια, αφληνοντας έξω την μυστικότητα. Αντιθέτως, τα ενεργά

συστήματα πρέπει να λάβουν υπόψη ταυτόχρονα την αυθεντικότητα, την ασφάλεια και την μυστικότητα. Επομένως, διαιρούμε τα ενεργά σχήματα σε δυο υποκατηγορίες:

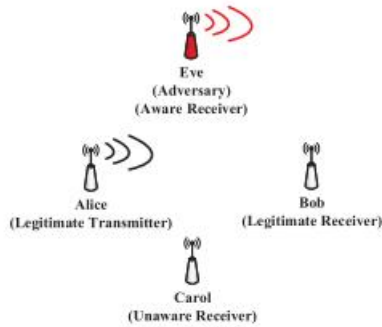
1. Στα μη-κρυφά σχήματα, δεδομένου ότι η μυστικότητα δεν λαμβάνεται υπόψη στον σχεδιασμό ενός ενεργού σχήματος, ένα τέτοιο ενεργό σχήμα μπορεί να χρησιμοποιηθεί μόνο από έναν παραλήπτη που είναι ενήμερος για την ύπαρξη του, και όχι από έναν παραλήπτη που δεν είναι ενήμερος, πράγμα που περιορίζει την ευρεία εφαρμογή του.
2. Στα κρυφά σχήματα, δεδομένου ότι η μυστικότητα λαμβάνεται υπόψη στον σχεδιασμό ενός ενεργού σχήματος, ο αρνητικός αντίκτυπος της ενσωμάτωσης μιας ετικέτας στο αρχικό μήνυμα μπορεί να ελεγχθεί μέσω της προσαρμογής των παραμέτρων του ενεργού σχήματος.

3.5 Μοντέλο συστήματος του PLA

Σε αυτήν την ενότητα, εξετάζουμε ένα τυπικό σενάριο χρήσης του PLA στις ασύρματες επικοινωνίες με τέσσερα σημεία και εξηγούμε το μοντέλο του συστήματος ως εξής:

- Η Alice είναι ο νόμιμος πομπός που θέλει να επικοινωνήσει με τον Bob.
- Ο Bob είναι ο νόμιμος παραλήπτης που λαμβάνει το μεταδιδόμενο σήμα και επαληθεύει την προέλευση του με συγκεκριμένο σχήμα PLA για την προστασία από ενεργές επιθέσεις, όπως οι επιθέσεις Sybil.
- Η Eve είναι ο αντίπαλος που παρακολουθεί όλες τις ασύρματες μεταδόσεις μεταξύ της Alice και του Bob, ή αποστέλλει ένα πλαστό σήμα στον Bob προσποιούμενη την Alice. Επειδή η Eve δρα ως ενήμερος παραλήπτης, υποθέτουμε ότι η Eve γνωρίζει τα πάντα για το σχήμα PLA εκτός από τις πληροφορίες απορρήτου μεταξύ της Alice και του Bob. Κάτω από παθητικές επιθέσεις, η Eve προσπαθεί να εξάγει τις πληροφορίες απορρήτου από τις παρατηρήσεις της.
- Η Carol είναι ο ανενήμερος παραλήπτης που λαμβάνει το μεταδιδόμενο σήμα, αλλά επαληθεύει την προέλευση του ληφθέντος σήματος μέσω μηχανισμών αυθεντικοποίησης σε ανώτερα επίπεδα. Ο ρόλος της απόδοσης λήψης της Carol είναι να αξιολογεί το επίπεδο μυστικότητας του σχήματος PLA.

Αυτό το παράδειγμα φαίνεται αναλυτικότερα και στο παρακάτω σχήμα.



Σχήμα 8. Μοντέλο συστήματος του PLA σε ασύρματες επικοινωνίες με τέσσερις κόμβους

Κατηγοριοποιούμε τα συστήματα PLA σε δυο κατηγορίες: παθητικά και ενεργά σχήματα.

- Στα παθητικά σχήματα, ο Bob ελέγχει τον πομπό βασιζόμενο στα χαρακτηριστικά του φυσικού επιπέδου των ληφθέντων σημάτων.
- Στα ενεργά σχήματα, η Alice πρώτα δημιουργεί μια ετικέτα βασισμένη σε ένα μυστικό κλειδί που μοιράζεται με τον Bob. Στη συνέχεια, η Alice ενσωματώνει την ετικέτα σε ένα αρχικό μήνυμα για να δημιουργήσει ένα ετικεταρισμένο σήμα. Τέλος, η Alice στέλνει το ετικεταρισμένο μήνυμα στον Bob μέσω ασύρματου καναλιού. Ο Bob ελέγχει τον πομπό ελέγχοντας εάν η ετικέτα υπάρχει στο ληφθέν σήμα. Σημειώστε ότι τα παθητικά σχήματα χρησιμοποιούν φυσικά χαρακτηριστικά για τον έλεγχο του πομπού, ενώ τα ενεργά σχήματα χρησιμοποιούν ένα τεχνητό χαρακτηριστικό, δηλαδή την ετικέτα για να επιτύχουν τον ίδιο σκοπό. Συνεπώς, οι πληροφορίες απορρήτου στα παθητικά σχήματα είναι τα φυσικά χαρακτηριστικά ενώ στα ενεργά σχήματα είναι το μυστικό κλειδί. Δεδομένα ότι τα παθητικά σχήματα δεν ενσωματώνουν καμία ετικέτα στο αρχικό μήνυμα, λαμβάνουν υπόψη τόσο την αυθεντικότητα όσο και την ασφάλεια, εξαιρώντας την μυστικότητα. Αντίθετα, τα ενεργά σχήματα πρέπει να λάβουν υπόψη ταυτόχρονα την αυθεντικότητα, την ασφάλεια και την μυστικότητα.

Για λόγους ευκολίας στην παρουσίαση, η απόφαση αυθεντικοποίησης στον Bob μοντελοποιείται ως ένα κατωφλικό τεστ με βάση της ακόλουθες υποθέσεις:

H_0 : Νόμιμο σήμα (Πραγματικό σήμα)

H_1 : Πλαστό σήμα (Ψεύτικο σήμα)

Ο κύριος ρόλος του PLA είναι να διασφαλίσει ότι ο Bob αξιόπιστα διακρίνει την υπόθεση H_0 με την υπόθεση H_1 .

B. Ανασκόπηση του PLA

1. Παθητικά σχήματα: Τα παθητικά σχήματα αποτελούνται γενικά από δυο στάδια. Ένα στάδιο εκπαίδευσης και ένα στάδιο μετάδοσης μηνυμάτων. Υπάρχουν δυο υποθέσεις στα παθητικά σχήματα.

Η πρώτη υπόθεση είναι ότι η ασφάλεια του σταδίου εκπαίδευσης επιτυγχάνεται μέσω μηχανισμών ασφάλειας στα ανώτερα επίπεδα, π.χ. αλγορίθμων κρυπτογράφησης. Η πρώτη εξασφαλίζει ότι όλα τα χαρακτηριστικά στη λίστα είναι νόμιμα.

Η δεύτερη υπόθεση είναι ότι το χρονικό διάστημα μεταξύ δυο σταδίων πρέπει να είναι αρκούντως μικρό π.χ. $t_2 - t_1 \leq \tau$, όπου το τ αντιπροσωπεύει το χρόνο συνεκτικότητας ενός ασύρματου καναλιού. Η δεύτερη υπόθεση εξασφαλίζει ότι τα νόμιμα χαρακτηριστικά στο στάδιο εκπαίδευσης είναι ισχυρά συσχετισμένα με αυτά στο στάδιο μετάδοσης μηνυμάτων. Αντίθετα, εάν το χρονικό διάστημα υπερβαίνει το χρόνο συνεκτικότητας ενός ασύρματου καναλιού π.χ. σε ένα γρήγορα μεταβαλλόμενο κανάλι, τα παθητικά σχήματα με χαρακτηριστικά βασισμένα στο κανάλι ενδέχεται να αποτύχουν, διότι τα χαρακτηριστικά βασισμένα στο κανάλι ενδέχεται να αποτύχουν, διότι τα χαρακτηριστικά βασισμένα στο κανάλι από την ίδια συσκευή πομπού γίνονται ασυσχέτιστα.

Επιπλέον, τα χαρακτηριστικά στη λευκή λίστα πρέπει να πληρούν δυο απαιτήσεις για την εξασφάλιση μιας αξιόπιστης απόφασης αυθεντικοποίησης

- Πρώτον, αυτά τα χαρακτηριστικά πρέπει να έχουν υψηλή αυθεντικότητα κατά τη διάρκεια ολόκληρης της διαδικασίας αυθεντικοποίησης, ανεξάρτητα από αλλαγές στο περιβάλλον επικοινωνίας, την κινητικότητα του χρήστη ή και τους δυο παράγοντες.
- Δεύτερον, αυτά τα χαρακτηριστικά πρέπει να έχουν υψηλή ασφάλεια για την προστασία από την ψευδοποίηση των αντιπάλων.

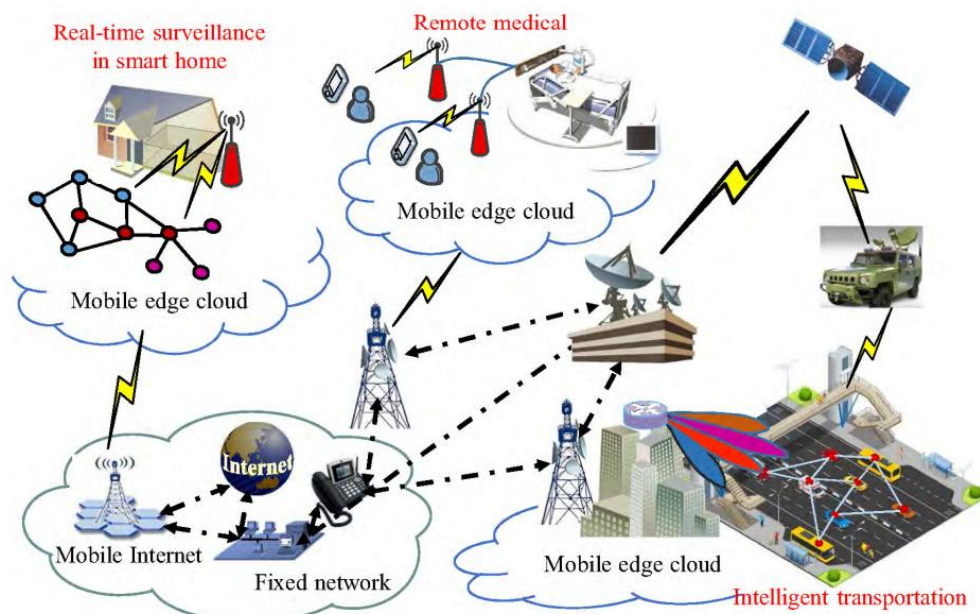
4. Ενίσχυση της ασφάλειας πληροφοριών μέσω προσεγγίσεων φυσικού επιπέδου σε ετερογενή IoT με πολλαπλή πρόσβαση Mobile Edge computing σε έξυπνη πόλη

Οι ποικίλες τεχνολογίες του Διαδικτύου των πραγμάτων (IoT) και οι υπολογιστές άκρων για φορητές συσκευές πολλαπλής πρόσβασης (multi-access mobile edge computing - MA-MEC) θεωρούνται ως υποστηρικτικές τεχνολογίες για την οικοδόμηση μιας έξυπνης πόλης. Η πρόοδος και η άνθηση του IoT διευκολύνουν την είσοδο της ανθρώπινης κοινωνίας στην εποχή του Διαδικτύου των Πάντων, που θέτει τα θεμέλια της έξυπνης πόλης. Για να αντιμετωπιστεί ο συγκριτικά περίπλοκος ρόλος μεταξύ της ικανότητας υπολογισμού και των φορητών συσκευών χαμηλού κόστους στο IoT, η MA-MEC είναι διαθέσιμη για την υποστήριξη υπηρεσιών και εφαρμογών με περιορισμένους πόρους και ευαίσθητων σε υπολογισμούς και εφαρμογές με υπολογιστική εκφόρτωση και διανομή περιεχομένου/κρυφής αποθήκευσης.

Ωστόσο, η ανάπτυξη της ικανότητας υπολογισμού του νέφους εντός του δικτύου ραδιοπρόσβασης μπορεί να αντιμετωπίσει σοβαρές απειλές για την ασφάλεια, οι οποίες πηγάζουν όχι μόνο από τις υπάρχουσες τεχνολογίες και δίκτυα, αλλά και από το ίδιο το IoT βασισμένο στο MA-MEC. Έτσι, σε αυτήν την εργασία εξετάζονται λύσεις για την αντιμετώπιση των απειλών ασφαλείας από την οπτική γωνία του φυσικού επιπέδου. Οι τεχνολογίες ασφαλείας του φυσικού επιπέδου έχουν τα πλεονεκτήματα της επίτευξης της απόλυτης μυστικότητας, της χαμηλής υπολογιστικής πολυπλοκότητας, της κατανάλωσης των πόρων καθώς και της καλής προσαρμογής στις αλλαγές του καναλιού. Πιο συγκεκριμένα, εξετάζουμε την ασφαλή κωδικοποίηση για ανίχνευση παρακολούθησης, την εκχώρηση πόρων, την επεξεργασία σημάτων και τη συνεργασία πολλαπλών κόμβων μαζί με τη δημιουργία και την αυθεντικοποίηση κλειδιών στο φυσικό επίπεδο για την αντιμετώπιση των αναδυόμενων προκλήσεων ασφαλείας.

4.1 Εισαγωγή

Μετά την ραγδαία ανάπτυξη των τεχνολογιών πληροφορικής και επικοινωνιών, καθώς και της επιστήμης υπολογιστών, το όραμα μιας έξυπνης πόλης είναι πιο κοντά στην πραγματικότητα από ποτέ πριν. Η εξέλιξη του IoT, του Cloud Computing, της κοινωνικής δικτύωσης και άλλων ωθεί την τεχνολογία στη δομή της έξυπνης πόλης. Στην προκειμένη διαδικασία, η σύγκλιση διάφορων ασύρματων τεχνολογιών είναι αναπόφευκτη για την υποστήριξη ομαλής τεχνικής μετάβασης και την παροχή διάφορων εξατομικευμένων υπηρεσιών.



Σχήμα 9: Πολλαπλά σενάρια ετερογενούς IoT με βάση MA-MEC σε έξυπνη πόλη

Στο παραπάνω σχήμα, φαίνεται ότι πολλά ασύρματα δίκτυα με διάφορες υποδομές και τεχνολογίες, καθώς και διάφορες έξυπνες τερματικές συσκευές συχνά αναφέρονται ως ετερογενής IoT, έχουν εφαρμοστεί ευρέως στην έξυπνη πόλη για την υποστήριξη απομακρυσμένης ιατρικής, έξυπνων μεταφορών κ.λπ. Για την ανάπτυξη του ετερογενούς IoT στην πράξη, το MA-MEC χρησιμοποιεί διάφορες τεχνολογίες πρόσβασης στο ραδιοκύμα εκ περιτροπής, έχει τραβήξει το ενδιαφέρον ιδίως σε σενάρια με περιορισμένους πόρους και ευαισθησία στον υπολογισμό. Το MA-MEC, το οποίο αναπτύσσει τη δυνατότητα υπολογισμού στο νέφος εντός του δικτύου πρόσβασης στο ραδιοκύμα, παρέχει μια νέα οπτική για την αντιμετώπιση των βαριών υπολογιστικών εργασιών των κινητών τερματικών μέσω της εκκαθάρισης του υπολογισμού. Η εφαρμογή του MA-MEC έχει πολλά θετικά αποτελέσματα στην Έξυπνη Πόλη. Για παράδειγμα, μπορεί να μειώσει σημαντικά το χρόνο επεξεργασίας των εργασιών, να αποφύγει τη συμφόρηση του κεντρικού υπολογισμού στο νέφος, να αυξήσει τη διάρκεια ζωής της μπαταρίας των κινητών συσκευών και, κατά συνέπεια, να βελτιώσει την ποιότητα της υπηρεσίας και την εμπειρία του χρήστη.

Προκειμένου να διασφαλίσουμε την ασφάλεια και το απόρρητο των δεδομένων, των υπηρεσιών και των εφαρμογών στην Έξυπνη Πόλη, εκτός από τους

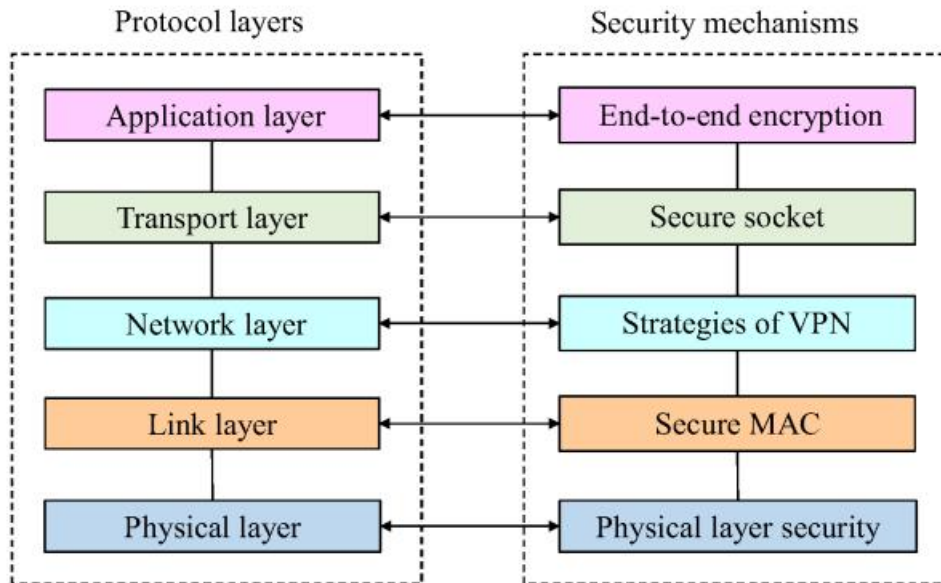
φυσικούς κινδύνους ασφαλείας που προκύπτουν από τις υπάρχουσες τεχνολογίες και δίκτυα, πρέπει να αντιμετωπίσουμε και τους νέους κινδύνους ασφαλείας που προκύπτουν από τις εφαρμογές του ετερογενούς IoT και του MA-MEC. Η ανάπτυξη των τεχνολογιών επικοινωνίας έχει, επίσης, επεκτείνει τους τρόπους με τους οποίους μπορούν να πραγματοποιηθούν επιθέσεις. Όλα τα στάδια της μετάδοσης πληροφοριών μπορούν να δέχονται επιθέσεις μέσω διάφορων τρόπων, όπως παρακολούθηση, ανάλυση κίνησης, τροποποίηση μηνυμάτων κ.λπ. Η πραγματικού χρόνου σύνδεση μεταξύ του κινητού υπολογισμού στο χέρι και των έξυπνων συσκευών, καθώς και η εμπιστευτικότητα, η ακεραιότητα, η ορθότητα και η διαθεσιμότητα των εμπιστευτικών δεδομένων μπορούν να κινδυνεύσουν. Έχει αναφερθεί σε έρευνα που διενεργήθηκε από μια συμβουλευτική εταιρεία στρατηγικού σχεδιασμού ότι έως και το 48% των εταιρειών στις Ηνωμένες Πολιτείες που χρησιμοποιούν ένα δίκτυο IoT έχουν πέσει θύματα πρόσφατων παραβιάσεων ασφαλείας. Επομένως, συνειδητοποιούμε ότι υπάρχει επείγουσα ανάγκη να αναπτυχθούν νέες τεχνολογίες ασφάλειας για τη δημιουργία της Έξυπνης Πόλης.

Οι λύσεις για την ασφάλεια των πληροφοριών μπορούν να χωριστούν σε δυο κατηγορίες. Πιο συγκεκριμένα, η πρώτη κατηγορία βασίζεται στην παραδοσιακή κρυπτογράφηση, η οποία έχει αποδείξει την αποτελεσματικότητα της σε πολλές ασφαλείς εφαρμογές. Αυτές οι τεχνολογίες ασφαλείας χρησιμοποιούνται συνήθως στα ανώτερα επίπεδα πρωτοκόλλων πάνω από το φυσικό. Ωστόσο, έχουν υψηλή πολυπλοκότητα αλγορίθμου και κατανάλωση πόρων λόγω της δύσκολης δημιουργίας και διαχείρισης κλειδιών. Η δεύτερη κατηγορία περιλαμβάνει τεχνολογίες ασφαλείας στο φυσικό επίπεδο, οι οποίες θεωρούνται αποτελεσματικές προσθήκες στις κρυπτογραφικές τεχνολογίες ασφαλείας για την ενίσχυση της ασφάλειας των ασύρματων δικτύων από το φυσικό επίπεδο. Σε σύγκριση με τις κρυπτογραφικές τεχνολογίες ασφαλείας, οι τεχνολογίες στο φυσικό επίπεδο έχουν τα ακόλουθα καθοριστικά πλεονεκτήματα.

- Επίτευξη απόλυτου απορρήτου: Οι τεχνολογίες ασφάλειας στο φυσικό επίπεδο μπορούν να εξασφαλίσουν απόλυτο απόρρητο (perfect secrecy) ακόμη κι αν οι κακόβουλοι χρήστες έχουν υψηλή υπολογιστική ισχύ. Αυτό διαφέρει από τις μεθόδους κρυπτογράφησης που μπορούν να αποκρυπτογραφηθούν με ακατάπαυστους υπολογιστικούς υπολογισμούς.
- Χαμηλή υπολογιστική πολυπλοκότητα και κατανάλωση πόρων: Επειδή δεν απαιτείται υπολογισμός και διαχείριση κλειδιών, η ασφάλεια στο φυσικό επίπεδο δεν εξαρτάται από την υπολογιστική ικανότητα του υλικού και είναι ελαφριά όσον αφορά την υπολογιστική πολυπλοκότητα και τις απαιτήσεις σε πόρους.
- Καλή προσαρμοστικότητα στις αλλαγές του φυσικού επιπέδου: Με την αξιοποίηση των φυσικών ιδιοτήτων, αυτές οι τεχνολογίες ασφαλείας μπορούν να προσαρμοστούν στις αλλαγές του ασύρματου καναλιού, βελτιστοποιώντας τις ρυθμίσεις του συστήματος και τα σχήματα μετάδοσης.

4.2 Λύσεις για την ασφάλεια των πληροφοριών στις ασύρματες επικοινωνίες

Οι συνηθισμένες λύσεις για να διασφαλίσουμε την πληροφοριακή ασφάλεια στις ασύρματες επικοινωνίες βασίζονται στην κρυπτογράφηση και έχουν κεντρική θέση. Για να απλοποιηθούν οι σχεδιασμοί των δικτύων και να διευκολυνθεί η μηχανική υλοποίηση, τα ασύρματα δίκτυα συνήθως χρησιμοποιούν την κλασική αρχιτεκτονική πρωτοκόλλου διασύνδεσης ανοιχτού συστήματος, όπως φαίνεται στο παραάτω σχήμα. Με την υιοθέτηση της ιεραρχικής δομής των πρωτοκόλλων, διάφοροι μηχανισμοί ασφάλειας μπορούν να εφαρμοστούν σε κάθε επίπεδο για να επιτύχουν τις απαιτήσεις ασφάλειας όπως η αυθεντικότητα, η ακεραιότητα και η διαθεσιμότητα. Για παράδειγμα, στο επίπεδο σύνδεσης, μπορεί να χρησιμοποιηθεί ένα ασφαλές πρωτόκολλο ελέγχου πρόσβασης στο μέσο (MAC) για να αποτρέψει την μη εξουσιοδοτημένη πρόσβαση ανεξουσίαστων χρηστών. Στο επίπεδο δικτύου, μπορούν να χρησιμοποιηθούν πλαίσια και ασφαλείς στρατηγικές εικονικών ιδιωτικών δικτύων (VPN) για να παρέχουν υπηρεσίες κρυπτογραφημένης ασφάλειας. Η ασφαλής σύνδεση είναι κατάλληλη για εφαρμογή στο επίπεδο μεταφοράς για να πιστοποιήσει τη νομιμότητα ενός χρήστη. Οι μέθοδοι κρυπτογράφησης από άκρο σε άκρο, όπως ασφαλή πρωτόκολλα μεταφοράς υπερκειμένου, μπορούν να εφαρμοστούν στο επίπεδο εφαρμογής για την κρυπτογράφηση των εμπιστευτικών πληροφοριών των χρηστών. Αυτές οι τεχνολογίες ασφαλείας εφαρμόζονται στα ανώτερα επίπεδα της στοίβας πρωτοκόλλου και βασίζονται σε θεωρίες κρυπτογραφίας. Όλες χρησιμοποιούν αλγορίθμους κρυπτογράφησης ή ασφαλή λογικά πρωτόκολλα για την υλοποίηση της αυθεντικότητας, της διανομής κλειδιών και της ασφαλούς μετάδοσης πληροφοριών. Λόγω του υψηλού φόρτου εργασίας και του αυξημένου κόστους πόρων, οι τεχνολογίες ασφάλειας βασισμένες στην κρυπτογράφηση είναι περιορισμένες σε κάποια ειδικά σενάρια, όπως στα ασύρματα δίκτυα όπου τα εξοπλιστικά μέσα επικοινωνίας είναι φθηνά και έχουν μικρή αυτονομία μπαταρίας και επομένως έχουν περιορισμένη υπολογιστική ικανότητα.



Σχήμα 10. Η κλασική ιεραρχική δομή της στοίβας πρωτοκόλλου επικοινωνίας και τα παραδείγματα μηχανισμών ασφαλείας που αναπτύσσονται σε κάθε επίπεδο

Η κεντρική ιδέα της ασφάλειας στο φυσικό επίπεδο είναι η υλοποίηση της εχεμύθειας των δεδομένων στο φυσικό επίπεδο, εκμεταλλευόμενο τη διαφορά μεταξύ των νόμιμων καναλιών και των καναλιών υποκλοπής που μπορούν να παραχθούν από την ενσωματωμένη τυχαιότητα των ασύρματων μέσων (όπως η δειγματοληψία του καναλιού και οι θόρυβοι) ή από το σχεδιασμό των στρατηγικών μετάδοσης. Αυτό διαφέρει από τις τεχνολογίες ασφαλείας βασισμένες στην κρυπτογράφηση, καθώς το φυσικό στρώμα ασφαλείας μειώνει την υπολογιστική πολυπλοκότητα και την κατανάλωση πόρων, αφού αυτή η τεχνολογία δεν εξαρτάται άμεσα από την υπολογιστική ικανότητα των κινητών συσκευών. Αυτά τα πλεονεκτήματα καθιστούν δυνατή την εφαρμογή αυτής της τεχνολογίας σε ορισμένα δίκτυα με περιορισμένους πόρους. Επίσης, με την πλήρη χρήση των χαρακτηριστικών του ασύρματου καναλιού, το φυσικό επίπεδο ασφαλείας μπορεί να προσαρμόσει ευέλικτα τις στρατηγικές μετάδοσης για να ταιριάζουν με τις αλλαγές του καναλιού μέσω της άμεσης βελτιστοποίησης και του σχεδιασμού ασφαλών στρατηγικών μετάδοσης.

Στο IoT που βασίζεται στο MA-MEC, πολλά σενάρια εφαρμογής έχουν τα εξής χαρακτηριστικά: απουσία υποδομής, αυτοοργανωμένα δίκτυα, περιορισμένη υπολογιστική ικανότητα, περιορισμένους πόρους και άλλα, τα οποία περιορίζουν σημαντικά την εφαρμογή των τεχνολογιών ασφαλείας βασισμένων στην κρυπτογράφηση. Η ασφάλεια στο φυσικό επίπεδο έχει τα πλεονεκτήματα της επίτευξης της απόλυτης εχεμύθειας, της χαμηλής απαίτησης σε υπολογιστική ικανότητα, της καλής προσαρμογής στις αλλαγές του καναλιού και της εξοικονόμησης των πόρων. Επομένως, μπορεί να χρησιμοποιηθεί ενεργά για την ενίσχυση της ασφάλειας των πληροφοριών στις πρακτικές εφαρμογές.

Για την ασφαλή ανταλλαγή πληροφοριών κατά την υπολογιστική εκφόρτωση, μπορούμε να χρησιμοποιήσουμε ασφαλή κωδικοποίηση για να προστατεύσουμε τις εμπιστευτικές πληροφορίες από παρακολούθηση και επιθέσεις. Σε αυτό το σχέδιο κωδικοποίησης, συνδυάζουμε τις συμβατικές διαδικασίες κρυπτογράφησης και

κωδικοποίησης σε έναν σχεδιασμό ασφαλούς κωδικοποίησης που εξασφαλίζει τόσο την αξιοπιστία όσο και την ασφάλεια των μεταδόσεων πληροφοριών και εξαλείφει τα προβλήματα δημιουργίας και διαχείρισης κλειδιών.

Επιπλέον, η αυξημένη κατανάλωση ενέργειας στα ασύρματα δίκτυα δημιουργεί μεγάλη ζήτηση για τον “πράσινο” υπολογισμό. Οι τεχνολογίες ασφάλειας στο φυσικό επίπεδο, όπως η ασφαλής διάθεση πόρων και η δέσμευση/προσκόλυψη, είναι χρήσιμες για τον συνδυασμό πράσινων και ασφαλών στρατηγικών για την αντιμετώπιση της διπλής πρόκλησης της κατανάλωσης ενέργειας και των απειλών ασφάλειας.

Οι χρήστες του MA-MEC στο πολυσύνδεσμο IoT, όπως η αποκοπή υπολογισμού και η κατανεμημένη παράδοση/αποθήκευση περιεχομένου, μπορεί να προκαλέσουν σοβαρή παρεμβολή και κίνδυνο ασφάλειας, ιδίως σε υπερπυκνά δίκτυα. Προκειμένου να αντιμετωπίσουν αυτό το ζήτημα, οι τεχνολογίες ασφαλούς επεξεργασίας σήματος που είναι γνωστές ως δέσμευση και προσκόλυψη μπορούν να χρησιμοποιηθούν για να ενισχύσουν ή να ασθενούν τα σήματα σε συγκεκριμένες κατευθύνσεις προκειμένου να επιτευχθούν βελτιώσεις στην εχεμύθεια και τη διαχείριση της παρεμβολής. Επιπλέον, για την υλοποίηση του MA-MEC μπορούμε να χρησιμοποιήσουμε οποιεσδήποτε δικτυακές συσκευές με δυνατότητες υπολογισμού, αποθήκευσης και δικτύωσης. Έτσι, χρησιμοποιώντας πολλούς κινητούς κόμβους ακμής, μπορούμε να δημιουργήσουμε ένα εικονικό πολλαπλών κεραίων σύστημα για τη διανεμημένη επεξεργασία σήματος. Επίσης, οι κινητοί κόμβοι ακμής μπορούν να χρησιμοποιηθούν συνεργατικά όχι μόνο για υπολογισμό και αποθήκευση αλλά και για την προώθηση εμπιστευτικών πληροφοριών για τη βελτίωση της ποιότητας της μετάδοσης και τη δημιουργία τεχνητής παρεμβολής για να μπερδέψουν τους επιτιθέμενους. Επιπλέον, στο MA-MEC βασισμένο στο IoT, απαιτούνται ελαφριές προσεγγίσεις για τη δημιουργία κλειδιών υβριδικών λύσεων ασφάλειας για να μειώσουν το υπολογιστικό φορτίο των χαμηλού κόστους συσκευών.

4.3 Ασφάλεια φυσικού στρώματος για ασφάλεια IoT βάσει MA-MEC

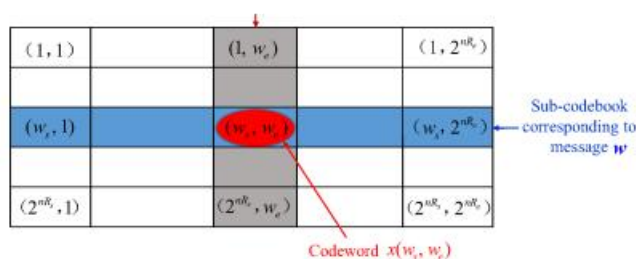
Λόγω του γεγονότος ότι το MA-MEC βασισμένο στο IoT είναι ανοιχτό και κοινόχρηστο και η ασύρματη μετάδοση είναι διαδεδομένη, η ασφάλεια των πληροφοριών είναι εξαιρετικά ευάλωτη σε κακόβουλες επιθέσεις, όπως η παρακολούθηση και παρεμβολή, απειλές κατά της κατάκτησης κόμβων, επαναληπτικές επιθέσεις, ψευδείς αναπαραστάσεις, κακόβουλες εισαγωγές κώδικα, επιθέσεις στο πλευρικό κανάλι κ.λπ. Ως εκ τούτου, οι ασφαλείς προσεγγίσεις που επικεντρώνονται στα χαρακτηριστικά του φυσικού επιπέδου προσελκύουν αυξανόμενο ενδιαφέρον. Αυτές οι προσεγγίσεις συνήθως περιλαμβάνουν ασφαλή κωδικοποίηση, κατανομή πόρων, επεξεργασία σήματος, συνεργασία πολλαπλών κόμβων, παραγωγή κλειδιών στο φυσικό επίπεδο και αυθεντικοποίηση στο φυσικό επίπεδο για να αντιμετωπιστούν αυτές οι απειλές.

A. Ασφαλής κωδικοποίηση παρακολούθησης

Έχει αποδειχθεί ότι οι ατέλειες στα ασύρματα κανάλια, όπως ο θόρυβος, η απόσβεση και οι παρεμβολές δεν αποτελούν πλέον εμπόδιο για την ασφάλεια των επικοινωνιών στο φυσικό επίπεδο. Εν αντιθέση, με κατάλληλο σχεδιασμό ασφαλούς κωδικοποίησης, μπορούμε να χρησιμοποιήσουμε αυτές τις ατέλειες για να προστατεύσουμε τις επικοινωνίες μας από επιθέσεις. Η ασφαλής κωδικοποίηση παρακολούθησης είναι μια σημαντική στρατηγική ασφάλειας στο MA-MEC βασισμένο στο IoT και περιλαμβάνει συνήθως τεχνικές όπως στοχαστική κωδικοποίηση, κωδικοποίηση για τον έλεγχο σφαλμάτων και κωδικοποίηση δικτύου.

I. Στοχαστική κωδικοποίηση

Η στοχαστική κωδικοποίηση είναι ένας τρόπος ασφαλούς κωδικοποίησης στον τομέα της ασφαλούς επικοινωνίας στο φυσικό επίπεδο, στην οποία ένας κωδικός ασφάλειας πρέπει να εμφανίζει μια δομή ενσωματωμένου κώδικα. Όπως φαίνεται στο Σχήμα 9, δημιουργείται ένας μητρικός κατάλογος κωδικών με $2^{n(R_s+R_e)}$ κωδικούς λέξεις μέσω της πιθανότητας διανομής των εισόδων x_n , ενώ ο μητρικός κατάλογος ευρετηριάζεται από (w_s, w_e) με $w_s \in \{1, \dots, 2^{nR_s}\}$ και $w_e \in \{1, \dots, 2^{nR_e}\}$. Εδώ, ο ρυθμός κώδικα χωρίζεται στον ρυθμό R_s των πραγματικών μυστικών μηνυμάτων και το R_e των μηνυμάτων προστασίας χωρίς περιεχόμενο πληροφοριών. Για κάθε μήνυμα w που πρέπει να μεταδοθεί με ασφάλεια, συσχετίζεται ένας υποκατάλογος ευρετηριασμένος από το w_s του μητρικού καταλόγου με το συγκεκριμένο μήνυμα και η μεταδιδόμενη κωδική λέξη επιλέγεται τυχαία μέσα στον υποκατάλογο επιλέγοντας το w_e τυχαία από το $1, \dots, 2^{nR_e}$. Συνεπώς, η κωδική λέξη (w_s, w_e) θα αποσταλεί. Με αυτόν τον στοχαστικό σχεδιασμό κωδικοποίησης, η αξιοπιστία και η ασφάλεια των εμπιστευτικών μηνυμάτων εξασφαλίζονται ταυτόχρονα, καθώς ο επαρκής πλεονασμός του μητρικού καταλόγου περιέχει την προστασία για την αξιόπιστη αποκωδικοποίηση των νόμιμων παραληπτών και η επαρκής τυχαιότητα του υποκαταλόγου αυξάνει την ανεξαρτησία του αντίπαλου σχετικά με το μεταδιδόμενο μήνυμα.



Σχήμα 11. Η ένθετη δομή ενός κωδικού μυστικότητας

II. Κωδικοποίηση ελέγχου σφάλματος

Εκτός από το σχήμα της στοχαστικής κωδικοποίησης, ορισμένα δημοφιλή σχήματα κωδικοποίησης καναλιού μπορούν να εξεταστούν και να χρησιμοποιηθούν για εφαρμογές ασφάλειας στο MA-MEC βασισμένο στο IoT. Στην οικογένεια της κωδικοποίησης ελέγχου σφάλματος, οι κώδικες LDPC (Low-Density Parity-Check) και οι πολικοί κώδικες διαδραματίζουν πολύ σημαντικό ρόλο στην κωδικοποίηση για την ασφάλεια. Οι κώδικες LDPC αποτελούν μια οικογένεια κωδικών μπλοκ βασισμένων σε γράφους, οι οποίοι μπορούν να πλησιάσουν τα θεμελιώδη όρια της κωδικοποίησης του καναλιού όταν το μήκος του μπλοκ είναι αρκετά μεγάλο. Οι κώδικες LDPC μπορούν να παράγονται με έναν αραιό πίνακα ελέγχου παραγόντων που περιγράφεται ευρέως από έναν διμερή γράφο που ονομάζεται γράφος Tanner. Με τη σύσταση ενός γράφου Tanner και του αραιού πίνακα ελέγχου παραγόντων του, μπορούμε εύκολα να καθορίσουμε τους κώδικες LDPC για την ασφάλεια. Σε πρακτικές εφαρμογές, προκειμένου να κατασκευαστεί μια δομή ενσωματωμένου κώδικα για την κωδικοποίηση ασφαλείας, μπορούν να χρησιμοποιηθούν ορισμένοι προσαρμοσμένοι κώδικες LDPC, όπως οι κώδικες LDPC δυο ακμών, οι διακοπούμενοι κώδικες LDPC και οι κώδικες coset με το διπλό των κωδικών LDPC.

Οι πολικοί κώδικες, ως μια οικογένεια γραμμικών κωδικών μπλοκ χαμηλής πολυπλοκότητας, βασίζονται στο φαινόμενο της πόλωσης του καναλιού. Η πόλωση του καναλιού, περιλαμβανομένης της συνδυασμένης και της αποσύνθεσης της πόλωσης, μπορεί να χωρίσει τα κανάλια σε υπό-κανάλια χωρίς θόρυβο και υπο-κανάλια με καθαρό θόρυβο. Χρησιμοποιώντας τα πολωμένα κανάλια, τα κομμάτια πληροφορίας μπορούν να μεταδοθούν στους επιθυμητούς κόμβους και τους ανταγωνιστές μέσω των υπο-καναλιών χωρίς θόρυβο και των υπο-καναλιών με καθαρό θόρυβο αντίστοιχα. Συνεπώς, οι επιθυμητοί κόμβοι μπορούν να αποκωδικοποιήσουν με ασφάλεια και αξιόπιστα τα μυστικά κομμάτια λόγω σχεδόν αθόρυβων μεταδόσεων, ενώ οι ανταγωνιστές δεν μπορούν να αποκτήσουν καμία μυστική πληροφορία λόγω μεταδόσεων με καθαρό θόρυβο. Συνεπώς, η ασφάλεια της πληροφορίας μπορεί να εξασφαλιστεί με αυτόν τον τρόπο κωδικοποίησης. Επιπλέον, μπορούν να χρησιμοποιηθούν κι άλλα σχήματα κωδικοποίησης για τη βελτίωση της ασφάλειας, όπως σχήματα κωδικοποίησης βασισμένα σε turbo κώδικες και σχήματα κωδικοποίησης καταλόγου.

III. Δικτυακή κωδικοποίηση

Η δικτυακή κωδικοποίηση, η οποία χρησιμοποιείται εκτενώς στα συνεργατικά δίκτυα, μπορεί να φέρει σημαντικά οφέλη όσον αφορά τη ροή δεδομένων, την αξιοπιστία και την ασφάλεια. Η βασική ιδέα της δικτυακής κωδικοποίησης είναι ότι η στρατηγική κωδικοποίησης επιτρέπει στους ενδιάμεσους κόμβους σε ένα συνεργατικό δίκτυο να ανακατεύουν διάφορες ροές δεδομένων μέσω αλγεβρικών συνδυασμών. Όπως φαίνεται και στο Σχήμα 10, έστω ότι έχουμε δυο κόμβους που ανταλλάσσουν δεδομένα με έναν ενδιάμεσο κόμβο. Η δικτυακή κωδικοποίηση μπορεί να εκτελεστεί στον ενδιάμεσο κόμβο μέσω απλών λειτουργιών ή με τα δυο

ληφθέντα μηνύματα και ένα συνδυασμένο μήνυμα αποστέλλεται σε μία μόνο εκπομπή. Ως εκ τούτου, μπορούν να επιτευχθούν εξοικονόμηση ενέργειας και μείωση των καθυστερήσεων λόγω της μείωσης των μεταδόσεων και των χρονοθυρίδων, ενώ η ασφάλεια μπορεί να αξασφαλιστεί μέσω των αλγεβρικών συνδυασμών πολλαπλών datagrams που βελτιώνουν την ασφάλεια των μεταδιδόμενων μηνυμάτων. Για την επίτευξη υψηλών απαιτήσεων απόδοσης, μπορούν να σχεδιαστούν περίπλοκοι σχεδιασμοί δικτυακής κωδικοποίησης για τον μετασχηματισμό των πακέτων δεδομένων σε μια συλλογή συμβόλων από ένα συγκεκριμένο πεπερασμένο σύνολο, και στη συνέχεια μια γραμμική συνδυασμένη αποστολή αυτών των συμβόλων επανατροφοδοτείται στο δίκτυο.

B. Ασφαλής ανάθεση πόρων

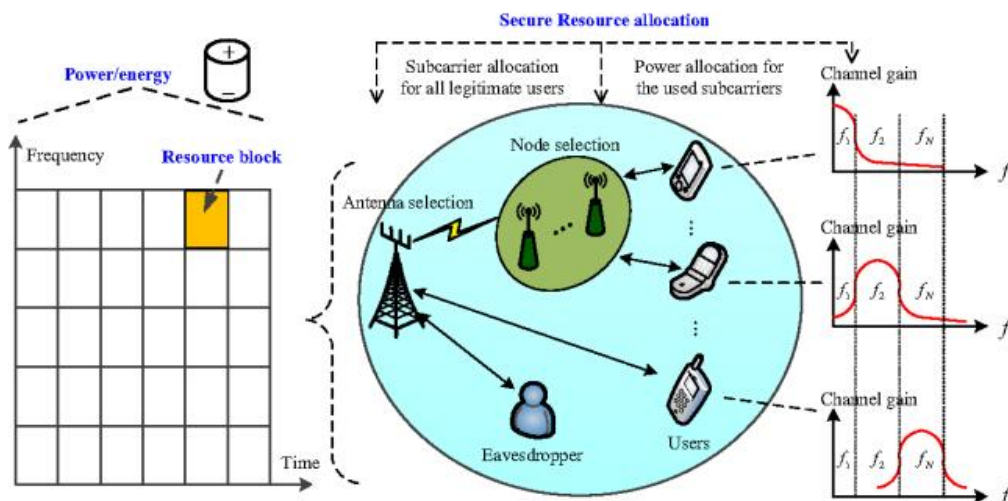
Έχει διεξαχθεί εκτενής έρευνα σχετικά με το ότι οι πόροι του ασύρματου δικτύου έχουν μεγάλες δυνατότητες για τη βελτίωση της ασφάλειας στο φυσικό επίπεδο. Με την εκμετάλλευση των πολυδιάστατων πόρων των ασύρματων δικτύων, είναι δυνατό να επεκταθεί εσκεμμένα η διαφορά μεταξύ των νόμιμων καναλιών και των καναλιών παρακολούθησης, ώστε να επιτευχθεί υψηλότερο ποσοστό για την κωδικοποίηση του απορρήτου και να βελτιώσει το επίπεδο της ασφάλειας. Συνεπώς, η ασφαλής ανάθεση πόρων αποτελεί διαθέσιμο μέτρο κατά των επιθέσεων ασφαλείας στο MA-MEC βασισμένο στο IoT, το οποίο μπορεί να πραγματοποιηθεί μεταξύ των τελικών συσκευών και του κινητού ακριανού νέφους ή να εφαρμοστεί ανάμεσα σε συνεργατικούς ακριανούς κόμβους.

Όπως φαίνεται στο Σχήμα 10, οι πολυδιάστατοι ασύρματοι πόροι του δικτύου περιλαμβάνουν συνήθως τη συχνότητα, τη χρονική υποδιαίρεση (timeslot) και την ισχύ στα δίκτυα πολλαπλής πρόσβασης με ορθογώνια διαίρεση συχνότητας (Orthogonal frequency division multiple access - OFDMA). Σε πολυκεραία και πολυκόμβια ασύρματα δίκτυα, οι πόροι αναφέρονται γενικά στις χωρικές ελευθερίες για την ασφαλή διαχείριση των πόρων στη χωρική διάσταση. Σε τέτοια πολυκεραία και πολυκόμβια σενάρια, η ασφαλής διαχείριση πόρων σημαίνει την επιλογή κατάλληλου συνόλου κεραιών ή κόμβων για τις τερματικές συσκευές και τους κόμβους της mobile-edge με πολλαπλούς στόχους όπως ασφάλεια, αξιοπιστία και εξοικονόμηση ενέργειας.

Όταν χρησιμοποιείται η τεχνολογία OFDMA στο MA-MEC, μπορούν να εφαρμοστούν λεπτομερείς τεχνικές για την ασφαλή διαχείριση των χρονικών και συχνοτικών πόρων και του επιπέδου ισχύος για τη μεταφορά πληροφοριών βάσει μετρήσεων που αφορούν την ασφάλεια. Συγκεκριμένα, η ασφαλής διαχείριση πόρων σημαίνει την επιλογή των καλύτερων χρονο-συχνοτικών πόρων (με βάση μετρήσεις όπως ο ασφαλής ρυθμός ή άλλες μετρικές ασφαλείας) για τα νόμιμα ζευγάρια χρηστών και την προσαρμογή της ισχύος στους επιλεγμένους πόρους με βάση τις αλλαγές στο κανάλι. Για την επίτευξη αυτών των στόχων, πραγματοποιείται η γενική βελτιστοποίηση της επιλογής των διαθέσιμων υποφορέων και της διανομής της ισχύος πάνω σε όλους τους διαθέσιμους πόρους, λαμβάνοντας υπόψη την άμεση πληροφορία κατάστασης του καναλιού.

Σε περιοχές του ετερόγενου Διαδικτύου των Πραγμάτων (IoT), όπου χρησιμοποιούνται πολλαπλές κεραιές και πολλαπλοί κόμβοι επικοινωνίας, μπορεί να μην είναι προς όφελος της ασφάλειας να χρησιμοποιούνται όλες οι κεραιές για τη μετάδοση πληροφοριών. Αυτό συμβαίνει επειδή, όταν όλες οι κεραιές χρησιμοποιούνται ταυτόχρονα τόσο ο νόμιμος χρήστης όσο και ο ακροατής μπορεί να λαμβάνουν ισχυρότερο σήματα, μειώνοντας τη διαφορά μεταξύ τους. Σε αυτές τις περιπτώσεις, μπορούμε να εφαρμόσουμε ασφαλή διαχείριση πόρων για να επιλέξουμε τις κατάλληλες κεραιές που θα χρησιμοποιηθούν για τη μετάδοση πληροφοριών μεταξύ των νόμιμων χρηστών. Αυτό θα αυξήσει τη διαφορά μεταξύ των καναλιών που χρησιμοποιούνται από τους νόμιμους χρήστες και των καναλιών που χρησιμοποιούνται από τους ακροατές, ενώ θα εξοικονομήσει ενέργεια ταυτόχρονα.

Στα συνεργατικά δίκτυα, μπορούν να χρησιμοποιηθούν τεχνολογίες αναμετάδοσης για τη δημιουργία συνδέσεων δικτύου προστατεύοντας ταυτόχρονα από την παρακολούθηση. Στη συνέχεια, η ασφαλής διαχείριση πόρων θα διευρυνθεί περαιτέρω στους συνεργατικούς κόμβους άκρης, περιλαμβάνοντας την βέλτιστη επιλογή των κόμβων αναμετάδοσης σε συνδυασμό με την ανάθεση υποκαναλιών και ισχύος. Σχεδιάζοντας την βέλτιστη στρατηγική ασφάλειας για την κοινή διαχείριση κόμβων και πόρων, μπορούν να επιτευχθούν ταυτόχρονα βελτιώσεις στην ασφάλεια και την αποδοτικότητα ενέργειας για την υποστήριξη του MA-MEC.



Σχήμα 12. Τα πολυδιάστατα χαρακτηριστικά των πόρων ασύρματου δικτύου

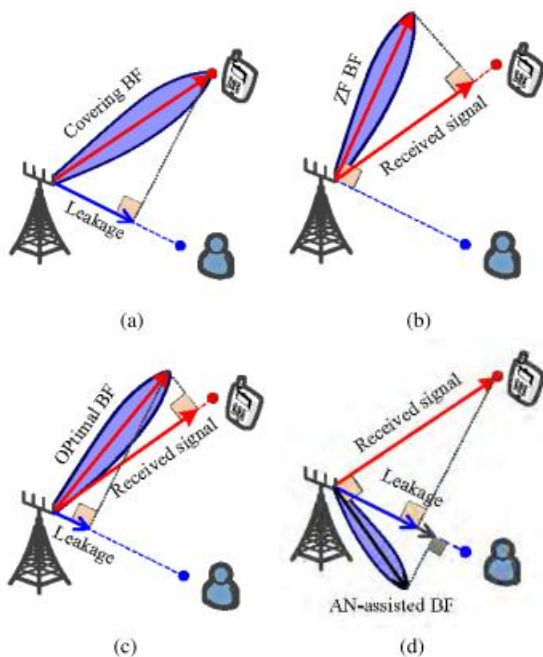
Γ. Ασφαλής επεξεργασία σήματος

Οι εγκαταστάσεις πολλαπλών κεραιών και κόμβων στο MA-MEC βασισμένο στο IoT είναι επωφελής για την ασφαλή επεξεργασία σήματος, η οποία συνήθως αναφέρεται σε διαμόρφωση δέσμης και προκωδικοποίηση. Με την ασφαλή διαμόρφωση δέσμης, πραγματοποιείται μετάδοση μονό-κατηγορίας για την

μετάδοση μονού μυστικού ροής δεδομένων μέσω πολλών κεραιών ή κόμβων. Γενικά, η διαμόρφωση δέσμης λειτουργεί ως ειδική περίπτωση της προκωδικοποίησης. Και οι δυο τεχνικές επεξεργασίας σήματος σχεδιάστηκαν για την αξιοποίηση των κεραιών ή των κόμβων για την επίτευξη χώρου ποικιλίας ή πολλαπλασιαστικών κερδών, έτσι ώστε να επιτευχθεί ένα υψηλό επίπεδο ασφάλειας, ενώ παράλληλα επιτυγχάνεται υψηλή αποδοτικότητα μετάδοσης και αξιοπιστία.

Η ασφαλής διαμόρφωση δέσμης/προκωδικοποίηση μπορεί να κατηγοριοποιηθεί περίπου σε τέσσερις κατηγορίες, που είναι η διαμόρφωση κάλυψης (covering beamforming), η μηδενική εξαναγκαστική διαμόρφωση (zero-forcing beamforming), η βέλτιστη διαμόρφωση (optimal beamforming) και η διαμόρφωση με τη χρήση τεχνητού θορύβου (artificial noise assisted beamforming) < όπως φαίνεται και στο Σχήμα 11. Η διαμόρφωση κάλυψης, όπως η διαμόρφωση μέγιστου λόγου μετάδοσης, ελέγχει τη δέσμη προς τους επιθυμητούς κόμβους για να επιτύχει ακριβή κάλυψη ενώ ταυτόχρονα ενισχύει τα σήματα των επιθυμητών κόμβων. Ωστόσο, η δέσμη στρέφεται προς τον αντίπαλο, όπως φαίνεται στο Σχήμα 11(α). Η διαμόρφωση μηδενικής εξαναγκαστικής διαμόρφωσης έχει ιδιαίτερο ενδιαφέρον στην πράξη λόγω της χαμηλής πολυπλοκότητας της που μπορεί να εφαρμοστεί εύκολα βρίσκοντας τον μηδενικό χώρο των καναλιών αποκλεισμού. Συνεπώς, το προφανές χαρακτηριστικό της διαμόρφωσης μηδενικής εξαναγκαστικής διαμόρφωσης είναι ότι η δέσμη είναι ορθογώνια προς το διάνυσμα του καναλιού του αντιπάλου. Ωστόσο, η διαμόρφωση μηδενικής εξαναγκαστικής διαμόρφωσης δεν είναι ιδανική για την κάλυψη του επιθυμητού κόμβου. Για να επιτευχθούν οι απαιτήσεις βέλτιστης απόδοσης του φυσικού επιπέδου σε ασφάλεια, η βέλτιστη διαμόρφωση σχεδιάζεται λαμβάνοντας υπόψη στόχους ασφάλειας και περιορισμούς πόρων, όπως φαίνεται στο Σχήμα 11(γ).

Εκτός από τις παραπάνω τεχνικές διαμόρφωσης δέσμης, η διαμόρφωση με χρήση τεχνητού θορύβου είναι επίσης ελκυστική στην ασφάλεια στο φυσικό επίπεδο. Η βασική ιδέα της διαμόρφωσης με χρήση τεχνητού θορύβου είναι ότι το μεταδιδόμενο σήμα υπερκαλύπτεται με τον τεχνητό θόρυβο, με το οποίο μπορούμε να διακόψουμε τη λήψη από τον αντίπαλο. Ένα απλό αλλά όχι βέλτιστο σύστημα διαμόρφωσης με χρήση τεχνητού θορύβου αφήνει τον τεχνητό θόρυβο να βρίσκεται στον μηδενικό χώρο των νόμιμων καναλιών, ώστε ο επιθυμητός κόμβος να μπορεί πλήρως να αποφεύγει τις ανεπιθύμητες επιδράσεις που προκαλούνται από τον τεχνητό θόρυβο, όπως φαίνεται στο Σχήμα 11(δ). Για να διασφαλιστεί η παγκόσμια βέλτιστη απόδοση σε ασφάλεια, η διαμόρφωση με χρήση τεχνητού θορύβου συνήθως σχεδιάζεται προσεκτικά ενώ η υπολογιστική πολυπλοκότητα και οι διαρροές τεχνητού θορύβου στον επιθυμητό κόμβο μπορεί να είναι αναπόφευκτες. Η χρήση του τεχνητού θορύβου μπορεί να καταναλώσει επιπλέον ενέργεια έτσι ώστε η ενέργεια που εκχωρείται για τη μετάδοση των μυστικών μηνυμάτων μειώνεται.



Σχήμα 13. Απεικόνιση ασφαλούς διαμόρφωσης δέσμης σε συστήματα πολλαπλών κεραιών

Δ. Ασφαλής συνεργασία πολλαπλών κόμβων

Η συνεργασία πολλών κόμβων έχει αποδειχθεί ότι έχει μεγάλες δυνατότητες για την ασφάλεια των ασύρματων μεταδόσεων από το πλαίσιο της πληροφοριακής θεωρητικής ασφάλειας, η οποία είναι επίσης χρήσιμη στο MA-MEC με βάση το IoT. Σε αυτό το πλαίσιο, η συνεργατική αρχιτεκτονική παρέχει ευκαιρίες για την ασφαλή μετάδοση χρησιμοποιώντας την συνεργασία πολλών κόμβων. Υπάρχουν πρωτόκολλα συνεργατικής αναμετάδοσης, όπως το “decode-and-forward” (DF), “amplify-and-forward”(AF), “noise-forward”(NF) κ.λπ.

Τα πρωτόκολλα DF και AF επικεντρώνονται στο να βελτιώσουν τα σήματα που λαμβάνονται από τους περιορισμένους κόμβους για να αυξήσουν την ασφάλεια. Το πρωτόκολλο NF επιτρέπει στους κόμβους αναμετάδοσης να προωθούν πληροφορίες και να εκπέμπουν “τεχνητό θόρυβο” ταυτόχρονα, προστατεύοντας έτσι τα μεταδιδόμενα σήματα από κατασκοπεία. Το πρωτόκολλο CF είναι παρόμοιο με το NF, αλλά ο κόμβος αναμετάδοσης προωθεί μια ποσοτικοποιημένη έκδοση των θορυβώδων παρατηρήσεων του για να βοηθήσει τον προορισμό να αποκωδικοποιήσει το μήνυμα και να μπερδέψει τους κατασκόπους με το AN.

Αξίζει να σημειωθεί ότι αυτή η συνεργατική αναμετάδοση μπορεί να χρησιμοποιηθεί ακόμα και με μη αξιόπιστους κόμβους για να επιτευχθεί υψηλότερο επίπεδο ασφαλείας ενώ προστατεύονται τα εμπιστευτικά δεδομένα από αυτούς.

Μια άλλη ενδιαφέρουσα στρατηγική είναι η συνεργατική παρέμβαση, η οποία επιτρέπει στους ενδιάμεσους κόμβους να εκπέμπουν παρεμβατικά σήματα

για την υποβάθμιση των καναλιών κατάκλειψης. Συγκεκριμένα, σε πλήρη διπλή μετάδοση, όχι μόνο οι ενδιάμεσοι κόμβοι αλλά και ο πηγαίος κόμβος και ο επιθυμητός κόμβος μπορούν να χρησιμοποιηθούν για την εκπομπή παρεμβατικών σημάτων. Η συνεργατική παρέμβαση στον χώρο μηδενικού υπόχωρου είναι ένας απλός και αποτελεσματικός τρόπος χωρίς καμία βλάβη στους νόμιμους κόμβους, καθώς αυτή η στρατηγική εκπέμπει παρεμβατικά σήματα στον χώρο μηδενικού υπόχωρου των νόμιμων καναλιών. Μπορεί να εφαρμοστεί εύκολα για απλή αναμετάδοση ή παρέμβαση.

Ε. Δημιουργία κλειδιού φυσικού στρώματος

Οι ασύρματες μεταδόσεις πληροφοριών στο IoT βασισμένες σε MA-MEC παρέχουν αρκετή τυχαιότητα για τη δημιουργία κρυπτοκλειδιών στο φυσικό επίπεδο, χωρίς να απαιτούν υπολογιστική ισχύ ή βοήθεια από άλλους χρήστες. Αυτοί οι μηχανισμοί βασίζονται στην τυχαιότητα των καναλιών επικοινωνίας, που περιλαμβάνει το CSI (πληροφορίες κατάστασης του καναλιού), την ισχύ του ληφθέντος σήματος (RSS) και τη φάση του σήματος (PI).

Αυτό σημαίνει ότι οι ιδιότητες του καναλιού, όπως η χρονική μεταβολή, ο χωρικός αποσυσχετισμός και η αμοιβαιότητα του καναλιού, χρησιμοποιούνται για τη δημιουργία των κλειδιών. Αυτές οι ιδιότητες περιλαμβάνουν:

- Η χρονική μεταβολή, που προκαλείται από τις απρόβλεπτες κινήσεις των ασύρματων συσκευών ή άλλων αντικειμένων στο περιβάλλον εξάπλωσης. Αυτή η τυχαιότητα μπορεί να χρησιμοποιηθεί για τη δημιουργία κλειδιών.
- Ο χωρικός αποσυσχετισμός, που υποδηλώνει ανεξαρτησία της μεταβολής του καναλιού σε διάφορα σημεία του χώρου. Αυτό μπορεί να χρησιμοποιηθεί ως πηγή τυχαιότητας για τη δημιουργία κλειδιών.

Η διαδικασία δημιουργίας κλειδιών στο φυσικό επίπεδο περιλαμβάνει διάφορες υπο-διαδικασίες, όπως τον χαρακτηρισμό του καναλιού, την εξαγωγή τυχαιότητας, την κβαντοποίηση, τον συντονισμό πληροφοριών και την ενίσχυση του απορρήτου.

Βασικά, υπάρχουν τέσσερις τρόποι για να δημιουργήσουμε κρυπτοκλειδιά στο φυσικό επίπεδο, ανάλογα με τις επιλογές παραμέτρων του καναλιού.

- Η πρώτη προσέγγιση βασίζεται στις πληροφορίες κατάστασης του καναλιού (CSI) και χρησιμοποιεί σήματα πιλότων και εκτιμήσεις του καναλιού για να αποκτήσει CSI και να εξάγει τυχαιότητα στο κανάλι.
- Η δεύτερη προσέγγιση βασίζεται στις μετρήσεις της ισχύος που μεταφέρεται από τα ληφθέντα σήματα (RSS). Αυτή η προσέγγιση χρησιμοποιεί συνήθως πιλοτικά σήματα και εκτιμήσεις του καναλιού για να αποκτήσει το RSS, μπορεί να ενισχυθεί με τη χρήση πολλαπλών κεραιών και φορέων για να αυξήσει το ρυθμό δημιουργίας κλειδιών.
- Η τρίτη προσέγγιση βασίζεται στη φάση του ληφθέντος σήματος (PI). Αυτή η προσέγγιση χρησιμοποιεί τυχαιότητα που εξάγεται από την PI των ληφθέντων σημάτων και μπορεί να επιτύχει υψηλότερο ρυθμό δημιουργίας κλειδιών και αποτελεσματική δημιουργία ομαδικών κλειδιών.

- Η τέταρτη προσέγγιση χρησιμοποιεί κωδικοποιήσεις ασφαλείας για να μεταδώσει εμπιστευτικά δεδομένα μέσω ασύρματων καναλιών και να δημιουργήσει κλειδιά bits. Αυτή η προσέγγιση μπορεί να χρησιμοποιηθεί επίσης για τον συντονισμό πληροφοριών και την ενίσχυση του απορρήτου.

ΣΤ. Αυθεντικότητα φυσικού στρώματος

Στον τομέα αυθεντικοποίησης του φυσικού επιπέδου, ο σκοπός είναι να αναγνωρίσουμε την ταυτότητα των οντοτήτων που επικοινωνούν, προκειμένου να διαπιστώσουμε εάν η επικοινωνία συμβαίνει μεταξύ εξουσιοδοτημένων χρηστών και εάν τα δεδομένα που λαμβάνονται έχουν τροποποιηθεί. Συνήθως, η ταυτοποίηση βασισμένη σε μυστικά κλειδιά εφαρμόζεται στα ανώτερα επίπεδα του πρωτοκόλλου, όπως το MAC, το επίπεδο δικτύου και το επίπεδο μεταφοράς. Εν αντιθέσει, η ταυτοποίηση του φυσικού επιπέδου πραγματοποιείται στο φυσικό επίπεδο, χρησιμοποιώντας τις φυσικές ιδιότητες των ασύρματων καναλιών και των συσκευών. Αυτή η τεχνική ασφαλείας είναι εξαιρετικά σημαντική, ιδίως για το IoT βασισμένο στο MA-MEC. Συγκεκριμένα, μπορεί να αποδειχθεί αποτελεσματική στην αντιμετώπιση επιθέσεων όπως η υποκλοπή ταυτότητας καθώς οι φυσικές ιδιότητες σχετίζονται άμεσα με το περιβάλλον εξάπλωσης και τις υλικοτεχνικές συσκευές, οι οποίες είναι δύσκολο να παραπλανηθούν. Ένας κοινός τρόπος αυθεντικοποίησης είναι η ταυτοποίηση βασισμένη στο κανάλι, που χρησιμοποιεί τη μοναδικότητα των ασύρματων καναλιών μεταξύ των νόμιμων κόμβων για τον εντοπισμό εισβολέων.

5. Συμπεράσματα

Στην παρούσα εργασία, αναφέρονται πρόσφατες έρευνες σχετικά με τα δίκτυα ασύρματων επικοινωνιών ενισχυμένα με έξυπνες επαναδιαμορφώσιμες επιφάνειες που προτείνονται για εφαρμογές σε δίκτυα επόμενης γενιάς. Επιπλέον, τονίζονται τα πλεονεκτήματα και οι περιορισμοί της χρήσης των RIS σε εφαρμογές επικοινωνίας, οι λειτουργικές αρχές των RIS, η αξιολόγηση της απόδοσης των συστημάτων RIS που βασίζονται σε πολλαπλές κεραίες. Επιπρόσθετα, δίνεται έμφαση στα οφέλη της ενσωμάτωσης των RIS με την NOMA, τα δίκτυα UAV, τον συντονισμόδιακομιστών ενέργειας, την ασύρματη μεταφορά ενέργειαςμέσω κύματος και τα αυτόνομα οχήματα. Ταυτόχρονα, για να υλοποιηθούν πόλεις που είναι συνδεδεμένες με αισθητήρες και νέους τρόπους νοημοσύνης, διάφορες ασύρματες τεχνολογίες και νέους τρόπους νοημοσύνης, διάφορες ασύρματες τεχνολογίες και δίκτυα συγκλίνουν αναπόφευκτα για να υποστηρίξουν διάφορες εξοικονομημένες υπηρεσίες με υψηλή αξιοπιστία και ασφάλεια. Το ομογενές IoT και το MA-MEC θεωρούνται ως οι τεχνολογίες που υποστηρίζουν την έξυπνη πόλη και, συνεπώς, προσελκύουν αυξανόμενο ενδιαφέρον. Βέβαια, αυτές οι τεχνολογίες για την κατασκευή έξυπνων πόλεων μπορεί να επιφέρουν κάποια προβλήματα ασφάλειας. Για αυτόν τον λόγο, συγκρίνουμε την ασφάλεια που βασίζεται στην κρυπτογράφηση με την ασφάλεια στο φυσικό επίπεδο. Μέσω αυτής της σύγκρισης γίνεται η πρόταση για την αντιμετώπιση των προκλήσεων ασφαλείας στο MA-MEC βασισμένο στο IoT μέσω φυσικών προσεγγίσεων που περιλαμβάνουν ασφαλή κρυφή κωδικοποίηση, κατανομή πόρων, επεξεργασία σήματος και πολυκόμβια συνεργασία μαζί με τη δημιουργία και πιστοποίηση φυσικών κλειδιών στο συστικό επίπεδο. Αυτές οι προσεγγίσεις είναι κατάλληλες για ασφαλή σενάρια εφαρμογής με συσκευές χαμηλού κόστους και περιορισμένης ενέργειας, χάρη στη χαμηλή πολυπλοκότητα και κατανάλωση πόρων.

6. Βιβλιογραφία

[1] Yuanwei Liu, Senior Member, IEEE, Xiao Liu, Xidong Mu, Tianwei Hou, Jiaqi Xu, Marco Di Renzo, Fellow, IEEE, and Naofal Al-Dhahir Fellow, IEEE. Reconfigurable Intelligent Surfaces: Principles and Opportunities. <https://ieeexplore.ieee.org/document/9424177>.

[2] Pablo Angueira, Inaki Val, Jon Montalban, Oscar Seijo, Eneko Iradier, Pablo Sanz Fontaneda, Lorenzo Fanari, Aitor Arriola. A survey of Physical Layer Techniques for Secure Wireless Communications in Industry. <https://ieeexplore.ieee.org/document/9702524/authors#authors>.

[3] Ning Xie, Zhuoyuan Li, Haijun Tan. A survey of Physical-Layer Authentication in Wireless Communications. <https://ieeexplore.ieee.org/document/9279294>.

[4] Dong Wang, Bo Bai, Kai Lei, Wenbo Zhao, Yanping Yang, Zhu Han. Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT with Multiple Access Mobile Edge Computing in Smart Cities. <https://ieeexplore.ieee.org/document/8703710>.

[5] Qingqing Wu, Shuowen Zhang, Beixiong Zheng, Changsheng You, Rui Zhang. Intelligent Reflecting Surfaces-Aided Wireless Communications: A tutorial. <https://ieeexplore.ieee.org/document/9326394>.

[6] Steven Kisseleff, Wallace A. Martins, Hayder Al-Hraishawi, Symeon Chatzinotas, Bjorn Ottersten. Reconfigurable Intelligent Surfaces for Smart Cities: Research Challenges and Opportunities. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9253607>.