ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
Σχολη Θετικων Επιστημων
Τμήμα Επιστήμης και Τεχνολογίας Υπολογιστών

Διπλωματική Εργασία

Cognitive Radio Security

Ντρούλια Μαρία, Α.Μ.–200920
pst0920@uop.gr

Επιβλέπων Καθηγητής

Νικόλαος Κολοκοτρώνης, *Επίκουρος Καθηγητής*

Φεβρουάριος 2013

Πίνακας Περιεχομένων

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κατάλογος Συντομογραφιών

FCC	Federal Communications Commission
GSM	Global System for Mobile Communications
CR	Cognitive Radio
SR	Software Radio
SDR	Software-Defined Radio
ADC	Analog-to-Digital Converter
A/D	Analog-to-Digital
DSP	Digital Signal Processors
JTRS	Joint Tactical Radio System
SCA	Software Communications Architecture
DR	Digital Radio
DDC	Digital Down Converter
DUC	Digital Up Converter
IF	Intermediate Frequency
PDR	Programmable Digital Radio
PaC	Parameter-Controlled
RF	Radio Frequency
SRA	Sampling Rate Adaptation
NPRM	Notices of Proposed Rulemaking
PU	Primary Users
LOS	Line-of-sight
NLOS	Non-Line-of-sight
WRAN	Wireless Regional Area Network
BS	Base Station
CPE	Consumer Premise Equipments
PMP	Point-to-Multipoint
EIRP	Equivalent Isotropically Radiated Power
UGS	Unsolicited Grant Service
rtPS	real-time Polling Service
nrtPS	non-real -time Polling Service
ertPS	extended-real-time Polling Service
BE	Best Effort
VoIP	Voice over IP

DFS	Dynamic Frequency Selection
TPC	Transmit Power Control
PDA	Personal Digital Assistants
IEEE	Institute of Electrical and Electronics Engineers
OPRS	Open Procedural Reasoning System
CN	Cognitive Network
RXML	Radio XML
API	Application Programming Interface
ISO	International Organization for Standardization
OSI	Open System Interconnection
HTTP	HyperText Transfer Protocol
MIMO	Multiple-input Multiple-output
IDP	Incumbent Profile Detection
MAC	Medium Access Control
CAP	Service Access Points
CRN	Cognitive Relay Nodes
ISM	Industrial Scientific and Medical Radio Bands
DSA	Dynamic Spectrum Access
OFDMA	Orthogonal Frequency Division Multiple Access
TDD	Time Division Duplex
FDD	Frequency Division Duplex
OFDM	Orthogonal Frequency Division Multiplexing
DC	Direct Current
FFT	Fast Fourier Transformations
SNR	Signal to Noise Ratio
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
TTG	Transmission Time Gap
FCH	Frame Control Header
FEC	Forward Error Correction
SCD	Spectral Correlation Density
ODSC	On-demand Spectrum Contention
ERP	Effective Radiated Power
MIC	Message Integrity Check
DoS	Denial-of-Service
CCMP	Counter mode encryption with CBC-MAC Protocol
AES	

AES	Advanced Encryption Standard
IMEI	International Mobile Equipment Identifier
CA	Certificate Authority
PUEA	Primary User Emulation Attacks
OFA	Objective Function Attacks
CCDA	Common Control Data Attacks
UHF	Ultra High Frequency
TCP	Transmission Control Protocol
RTO	Retransmission Timer
RTT	Round Trip Timer
IDS	Intrusion Detection System
LV	Location Verifiers
RSS	Received Signal Strength
ZWP	Zero Window Probe
GKM	Group Key Management
PKC	Public Key Cryptography
SKE	Symmetric Key Encryption
RFF	Radio Frequency Fingerprinting
CIA	Confidentiality, Integrity and Availability
AI	Artificial Intelligence
SS	Spread Spectrum

1 Εισαγωγή

Με τη ραγδαία αύξηση των ασύρματων εφαρμογών, το ραδιοφάσμα καθίσταται ένας σπάνιος πόρος, όπως όλες οι συχνότητες κάτω των 3GHz που έχουν κατανεμηθεί σε συγκεκριμένους χρήστες. Οι ρυθμιστικοί οργανισμοί όπως η Ομοσπονδιακή Επιτροπή Επικοινωνιών (FCC) εκχωρεί φάσμα για συγκεκριμένους τύπους υπηρεσιών που είναι κατόπιν αδειοδοτημένοι πλειοδότες έναντι αμοιβής. Οι συγκεκριμένες αδειοδοτήσεις έχουν στατικό χαρακτήρα, κάτι που έχει οδηγήσει σε σημαντικά αναποτελεσματική χρήση του φάσματος δημιουργώντας συνωστισμό χρηστών σε πολλές φασματικές περιοχές. Οι πραγματικές μετρήσεις δείχνουν ότι το μεγαλύτερο μέρος του φάσματος που διατίθενται χρησιμοποιείται ανεπαρκώς σε οποιοδήποτε χρόνο και χώρο.

Μια συμβατική, βασισμένη στο υλικό ασύρματη συσκευή μπορεί να έχει πρόσβαση μόνο σε μια περιοχή του φάσματος των ραδιοσυχνοτήτων, αλλά μια έξυπνη γνωστική ράδιο-συσκευή (cognitive radio - CR) μπορεί να αισθανθεί και να εντοπίσει φασματικές οπές, ή αλλιώς κενές περιοχές, οι οποίες μπορούν να χρησιμοποιηθούν για τις επικοινωνίες. Οι εν λόγω συσκευές επιτρέπουν στους έξυπνους αναπροσαρμόσιμους πομποδέκτες να κάνουν βέλτιστη χρήση του φάσματος με την αναζήτηση κενών φασματικών ζωνών και σε συντονισμό με το λογισμικό να μπορούν να προσαρμόσουν σε ένα ευρύ φάσμα από διαφορετικές συχνότητες και συστήματα διαμόρφωσης. Με άλλα λόγια, τα CRs έχουν προταθεί ως τρόπος για την επαναχρησιμοποίηση του φάσματος και η ευελιξία τους θεωρείται ως μια πιθανή λύση για το πρόβλημα του συνωστισμού του ραδιοφάσματος (spectral congestion problem). Το γεγονός αυτό δίνει την ευκαιρία σε συσκευές χωρίς άδεια χρήσης του φάσματος να είναι δευτερεύοντες χρήστες και να χρησιμοποιούν τις ζώνες συχνοτήτων μόνο εάν ο νόμιμος ή κύριος χρήστης του φάσματος δεν τις χρησιμοποιεί. Δυστυχώς, υπάρχουν επίσης μοναδικές νέες ευκαιρίες που παρουσιάζονται για τους κακόβουλους εισβολείς. Έτσι τα γνωστικά ράδιο-δίκτυα (CRNs) εισάγουν μια ολόκληρη νέα σειρά από απειλές που δεν μπορούν εύκολα να μετριαστούν.

Στο δεύτερο κεφάλαιο αυτής της εργασίας θα μιλήσουμε για την πρόσφατη πρόοδο στην τεχνολογία των ασύρματων ραδιοεπικοινωνιών που οδήγησε σε αυξημένες απαιτήσεις σε φάσμα και επομένως στην ανάπτυξη του CR. Προπομπός του cognitive radio θεωρείται το software radio, μια έννοια που χρησιμοποιήθηκε για πρώτη φορά από τον Joseph Mitola, το 1991. Ένα Software Radio είναι ένα σύστημα ραδιοεπικοινωνίας στο οποίο τα συστατικά του, τα οποία βρίσκονται σε μορφή υλικού (hardware), όπως ο μετατροπέας αναλογικού σε ψηφιακού σήματος (ADC), ο μετατροπέας ψηφιακού σε αναλογικού σήματος (DAC), τα φίλτρα κτλ., υλοποιούνται με λογισμικό. Με βάση τον παραπάνω ορισμό, σε ένα ιδανικό software radio, όλα τα βήματα με τα οποία γίνεται η ραδιοεπικοινωνία, επιτυγχάνονται με τη βοήθεια ενός προγραμματίσημου (programmable) hardware που ελέγχεται από το λογισμικό.

Στο τρίτο κεφάλαιο θα κάνουμε μια ιστορική αναδρομή στο CR, θα δώσουμε τον ορισμό του αλλά θα μιλήσουμε και για τα χαρακτηριστικά του. Το CR στηρίζεται στην τεχνολογία SDR. Αντιπροσωπεύει ένα SDR με όχι μόνο τη δυνατότητα να προσαρμόζεται στη διαθεσιμότητα φάσματος, τα πρωτόκολλα, και τη διαμόρφωση του σήματος αλλά και την ικανότητα να ενημερώνεται για τις διαμορφώσεις σήματος και τα πρωτόκολλα, να προσαρμόζεται στην τοπική δραστηριότητα φάσματος, και να μαθαίνει τις τρέχουσες ανάγκες του χρήστη του. Η τεχνολογία CR επιτρέπει το ίδιο το radio να μάθει, επιτρέποντας το να εκτελέσει "γνωστικές" λειτουργίες όπως ο προσδιορισμός και η χρησιμοποίηση του κενού φάσματος για να επικοινωνεί αποτελεσματικότερα. Τα Cognitive Radios (ή αλλιώς Γνωστικά Συστήματα Ραδιοεπικοινωνιών) είναι έξυπνα-

ευφυή συστήματα τα οποία έχουν την ικανότητα να αντιλαμβάνονται τα χαρακτηριστικά του περιβάλλοντός τους και να προσαρμόζουν κατάλληλα τις παραμέτρους λειτουργίας τους με στόχο τη βελτίωση της επικοινωνίας. Τα συστήματα αυτά μπορούν να ανιχνεύουν το φάσμα, να εντοπίζουν τις ζώνες συχνοτήτων οι οποίες δε χρησιμοποιούνται από τους αδειοδοτημένους χρήστες τους και να τις αξιοποιούν για την πραγματοποίηση των μεταδόσεών τους.

Στη συνέχεια στο τέταρτο κεφάλαιο θα αναφερθούμε εκτενώς στο πρωτόκολλο IEEE 802.22 παραθέτοντας τόσο τα κίνητρα για την ανάπτυξής του, όσο και τα χαρακτηριστικά του.

Προχωρώντας προς το τέλος της εργασίας στο πέμπτο κεφάλαιο θα μιλήσουμε για την ασφάλεια των CR, αναλύοντας τα θεμελιώδη δομικά στοιχεία ασφάλειας επικοινωνίας και τον ρόλο που παίζουν στα CR . Για την ανάλυση της ασφάλειας των γνωστικών δικτύων, ξεκινάμε με την εισαγωγή ορισμένων βασικών εννοιών ασφάλειας στο πλαίσιο των CR. Μερικά από τα θεμελιώδη δομικά στοιχεία ασφάλειας επικοινωνίας θεωρούμε ότι είναι η διαθεσιμότητα, η ακεραιότητα, η ταυτοποίηση, ο έλεγχος ταυτότητας, η άδεια, η εμπιστευτικότητα και η μη-αναγνώριση. Επίσης παραθέτουμε λύσεις για ασφαλή συστήματα επικοινωνίας και τις αναλύουμε. Τέλος αναφερόμαστε στα στάδια της ασφαλής επικοινωνίας στα CR που είναι : ο έλεγχος ταυτότητας του συστήματος γνωστικών ραδιοεπικοινωνιών, ο έλεγχος ταυτότητας των χρηστών που είναι σε επικοινωνία καθώς και η διασφάλιση της ασφάλειας κατά το χρονικό διάστημα επικοινωνίας των χρηστών.

Στο έκτο κεφάλαιο θα ασχοληθούμε με τις επιθέσεις που μπορεί να δεχτεί ένα CR και τους στόχους τους . Θέτοντας ως στόχο την έγχυση ψευδή στοιχείων, την τροποποίηση των δεδομένων, την πρόσβαση σε προσωπικά δεδομένα, τις χαμένες ευκαιρίες για δευτερεύοντες χρήστες ή ακόμη και την απαράδεκτη παρέμβαση για άδεια κύριων χρηστών, ένας κακόβουλος χρήστης μπορεί εύκολα να επιτεθεί σε ένα CR. Στο κεφάλαιο αυτό θα αναλύσουμε τις ειδικές επιθέσεις που συναντάμε στα CR: Primary User Emulation Attacks (PUEA), Επιθέσεις στην αντικειμενική συνάρτηση (Objective Function Attacks,OFA), Επιθέσεις ελέγχου κοινών δεδομένων (Common Control Data Attacks, CCDA) καθώς και Επιθέσεις ψευδούς ανατροφοδότησης (False Feedback), αλλά και επιθέσεις Lion.

Και τέλος στο έβδομο και όγδοο κεφάλαιο θα αναπτύξουμε τρόπους διασφάλισης των γνωστικών επικοινωνιών και θα παραθέσουμε τα συμπεράσματά μας.

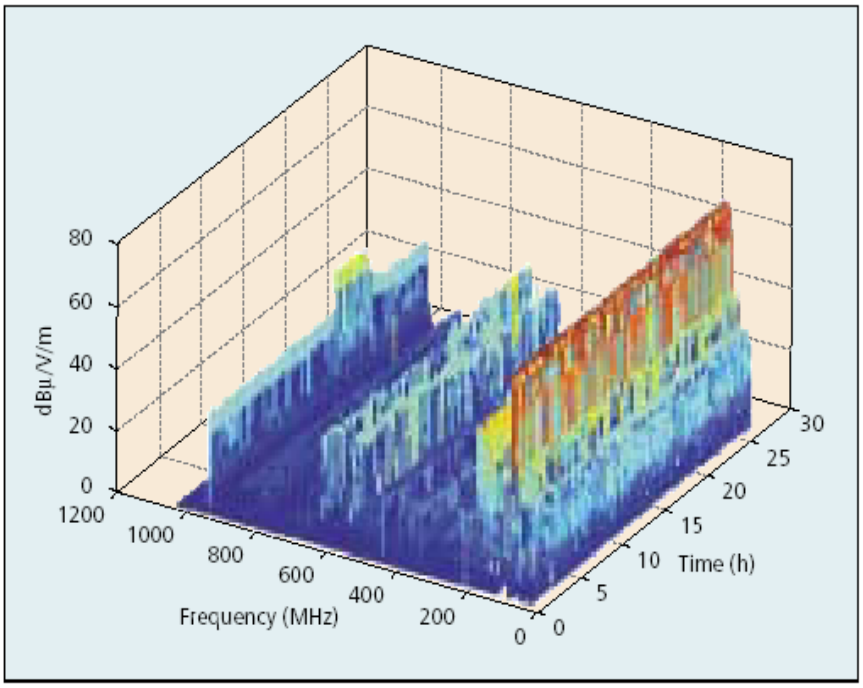
2 Γενικά

2.1 Χρησιμοποίηση του φάσματος ραδιοσυχνοτήτων

Το διαθέσιμο φάσμα ραδιοσυχνοτήτων αποτελεί πεπερασμένο φυσικό πόρο, η εκχώρηση του οποίου ανήκει στην αρμοδιότητα των κυβερνήσεων και των ρυθμιστικών αρχών των διαφόρων χωρών. Ο έλεγχος της χρήσης του περιορίζεται στα εθνικά σύνορα, αλλά εποπτεύεται και καθορίζεται από διεθνείς οργανισμούς, που συντελούν στην αρμονική χρησιμοποίησή του και στο συντονισμό των εθνικών ρυθμιστικών αρχών.

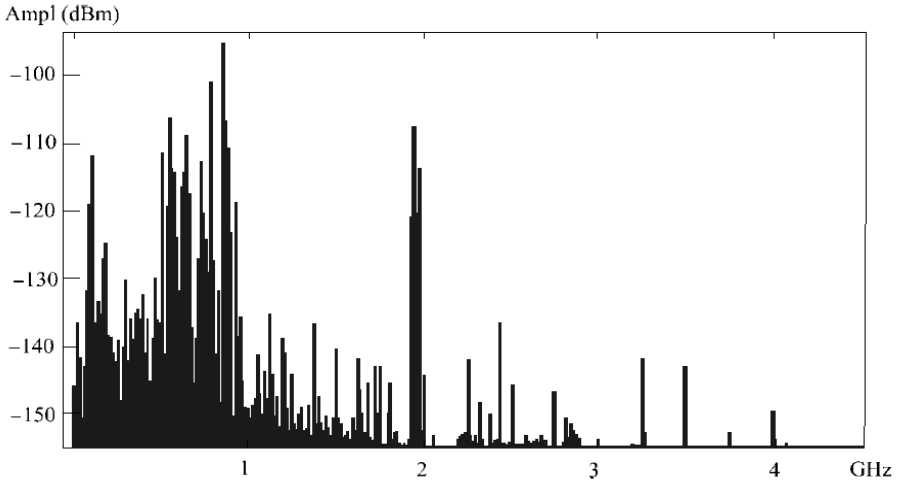
Η αλματώδης ανάπτυξη των ασύρματων ραδιοεπικοινωνιών έχει οδηγήσει στην αύξηση των απαιτήσεων για ελεύθερες ζώνες συχνοτήτων. Επικρατεί ευρέως η αντίληψη ότι σήμερα το διαθέσιμο ραδιοφάσμα είναι ιδιαίτερα ανεπαρκές και ότι το μεγαλύτερο τμήμα του έχει ήδη εκχωρηθεί και χρησιμοποιείται εκτεταμένα. Είναι αλήθεια ότι ο στατικός κατακερματισμός του φάσματος σε τμήματα τα οποία έχουν εκχωρηθεί σε δημόσιους και ιδιωτικούς φορείς με αδειοδότηση δεν αφήνει τεράστια περιθώρια για εκχώρηση πολλών νέων ελεύθερων ζωνών. Παρόλα αυτά, μετρήσεις που έχουν διενεργηθεί τόσο στην Ευρώπη όσο και στις ΗΠΑ έχουν δείξει ότι μεγάλα τμήματα του φάσματος, αν και έχουν εκχωρηθεί με άδεια σε χρήστες, στην πραγματικότητα παραμένουν αχρησιμοποίητα για αρκετά μεγάλα χρονικά διαστήματα.

Το 2001 στη Γερμανία πραγματοποιήθηκε μία σειρά από μετρήσεις οι οποίες έδειξαν ότι οι φασματικοί πόροι χρησιμοποιούνται σποραδικά. Το **σχήμα 1** δείχνει τη χρησιμοποίηση της ζώνης 50MHz – 1GHz κατά τη διάρκεια ενός εικοσιτετραώρου (βλ. [1]). Παρατηρούμε λοιπόν ότι ορισμένες περιοχές συχνοτήτων χρησιμοποιούνται εκτεταμένα, όπως π.χ. οι συχνότητες κάτω των 300 MHz που έχουν εκχωρηθεί για τη μετάδοση αναλογικών σημάτων ήχου και εικόνας ή οι συχνότητες στην περιοχή των 900 MHz που χρησιμοποιούνται από το σύστημα κινητών επικοινωνιών GSM (European 2G Global System for Mobile Communications). Ταυτόχρονα όμως ζώνες συχνοτήτων μεγάλου εύρους εμφανίζουν πολύ χαμηλή χρήση.



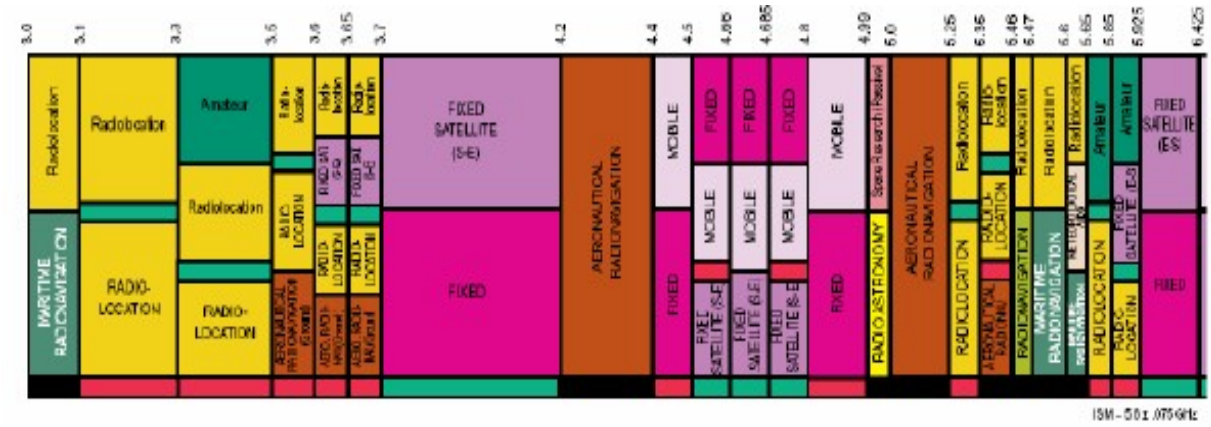
Σχήμα 1. Χρησιμοποίηση της ζώνης 50MHz - 1GHz

Το Νοέμβριο του 2002, η Ομοσπονδιακή Υπηρεσία Επικοινωνιών των ΗΠΑ FCC (Federal Communications Commission) δημοσίευσε μία αναφορά η οποία στόχευε στο να βελτιώσει τον τρόπο με τον οποίο γίνεται η διαχείριση του φάσματος (βλ. [2]). Τη σύνταξη της αναφοράς ανέλαβε μια ομάδα που αποτελείτο από οικονομολόγους, μηχανικούς και δικηγόρους. Στην τρίτη σελίδα της αναφοράς αυτής γίνεται καθαρά λόγος για την υπο-χρησιμοποίηση του φάσματος. Συγκεκριμένα αναφέρεται: «Σε πολλές ζώνες, η πρόσβαση στο φάσμα είναι πιο σημαντικό πρόβλημα από τη φυσική ανεπάρκεια του φάσματος, κυρίως λόγω των παραδοσιακών κανονισμών «διαταγής και ελέγχου» (command-and-control) που περιορίζουν την ικανότητα των υποψήφιων χρηστών του φάσματος να αποκτήσουν πρόσβαση σε αυτό». Επιπλέον, ο Ed Thomas, πρώην αρχιμηχανικός της FCC έχει δηλώσει τα εξής: «Αν δει κανείς όλες τις ραδιοσυχνότητες μέχρι τα 100GHz και λάβει ένα στιγμιότυπο οποιαδήποτε χρονική στιγμή, θα δει ότι μόνο το 5 με 10% αυτών χρησιμοποιείται» (βλ. [3]). Στο **σχήμα 2** φαίνεται ένα τέτοιο στιγμιότυπο του χρησιμοποιούμενου φάσματος, μέχρι τα 6 GHz. Είναι προφανές ότι πράγματι τη δεδομένη στιγμή οι περισσότερες από τις συχνότητες δε χρησιμοποιούνταν (βλ. [3]).



Σχήμα 2. Στιγμιότυπο της χρησιμοποίησης του φάσματος μέχρι τα 6GHz

Αξιοσημείωτο είναι ότι αυτή η χαμηλή χρησιμοποίηση του φάσματος δεν είναι συνεπής με το διάγραμμα εκχώρησης συχνοτήτων της ομοσπονδιακής επιτροπής των Ηνωμένων Πολιτειών (FCC) **(σχήμα 3)**, στο οποίο διακρίνεται ότι υπάρχουν πολλαπλές εκχωρήσεις σε όλες τις ζώνες συχνοτήτων για πληθώρα ασυρμάτων υπηρεσιών.

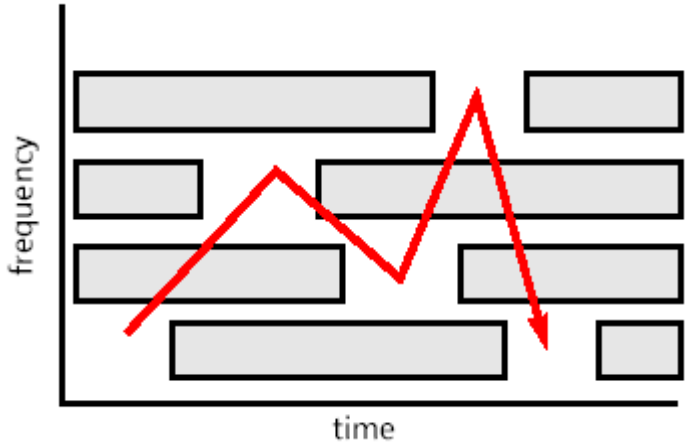


Σχήμα 3. Εκχώρηση συχνοτήτων σε ασύρματες υπηρεσίες έως τα 6 GHz

Από όλα τα παραπάνω, συμπεραίνουμε ότι η τρέχουσα πολιτική χρήσης του φάσματος είναι μη αποτελεσματική. Άλλες ζώνες συχνοτήτων είναι απόλυτα ελεύθερες στο μεγαλύτερο ποσοστό του χρόνου, άλλες είναι μερικά απασχολημένες ενώ άλλες είναι υπερφορτωμένες. Ένας από του λόγους της υπο-χρησιμοποίησης ορισμένων ζωνών είναι ότι, αν και οι ζώνες αυτές έχουν εκχωρηθεί με άδεια σε συγκεκριμένους φορείς, αυτοί χρησιμοποιούν μόνο κλάσματα των ζωνών αυτών και σε συγκεκριμένες χρονικές στιγμές. Τον υπόλοιπο χρόνο οι συχνότητες αυτές παραμένουν αχρησιμοποίητες κι έτσι ένα πολύτιμο δημόσιο αγαθό σπαταλείται.

Ορισμός. Ορίζουμε ως *«φασματική οπή»* (spectrum hole) μια ζώνη συχνοτήτων η οποία έχει ανατεθεί σε ένα αδειοδοτημένο χρήστη, αλλά, σε μια συγκεκριμένη χρονική στιγμή και σε μια συγκεκριμένη τοποθεσία, η εν λόγω ζώνη δε χρησιμοποιείται από το χρήστη αυτό (βλ. [4]). Άλλοι όροι που χρησιμοποιούνται για να περιγράψουν τη

φασματική οπή είναι οι *«λευκό φάσμα»* (white spectrum) και *«φασματική ευκαιρία»* (spectrum opportunity). Οι φασματικές οπές περιγράφονται συνήθως σε ένα χώρο δύο διαστάσεων, του χρόνου και της συχνότητας, όπως φαίνεται και στο **σχήμα 4**. Έτσι, οπή σημαίνει αχρησιμοποίητη ζώνη συχνοτήτων σε δεδομένη χρονική στιγμή. Άλλες διαστάσεις όμως μπορεί να είναι η τοποθεσία (όπως ήδη αναφέρθηκε και στον ορισμό) ή ακόμα και ο κώδικας διασποράς, στην περίπτωση που χρησιμοποιείται σχήμα πολλαπλής πρόσβασης με διαίρεση κώδικα



Σχήμα 4. Φασματικές οπές σε δύο διαστάσεις

Είναι λοιπόν σαφές ότι είναι αναγκαία μια νέα τεχνολογία η οποία θα εκμεταλλεύεται με αποδοτικό τρόπο τις φασματικές οπές. Τα τερματικά που θα εφαρμόζουν τη νέα αυτή τεχνολογία θα πρέπει να έχουν τη δυνατότητα να χρησιμοποιούν το φάσμα όταν οι αδειούχοι δεν το εκμεταλλεύονται και να το απελευθερώνουν όποτε κάποιος αδειούχος επιθυμεί να επικοινωνήσει. Σε κάθε περίπτωση, οι αδειούχοι δεν θα πρέπει να παρενοχλούνται στην επικοινωνία τους. Η νέα αυτή τεχνολογία δεν είναι άλλη από το Cognitive Radio (CR). Ο εντοπισμός και αναγνώριση των «φασματικών οπών» από CR τερματικά αποτελεί μια μεγάλη πρόκληση και αποτελεί πεδίο έντονου ερευνητικού ενδιαφέροντος. Η εκμετάλλευση των φασματικών οπών – ευκαιριών φάσματος από τα CR αναφέρεται συχνά και ως οπορτουνιστική χρήση του φάσματος.

2.2 Software-Defined Radio

Ορισμός. Ένας πομποδέκτης ονομάζεται *software radio* (SR) εάν όλες οι τηλεπικοινωνιακές του λειτουργίες πραγματοποιούνται αποκλειστικά από προγράμματα τα οποία εκτελούνται σε έναν κατάλληλο επεξεργαστή (βλ. [5]) .

Ο ορισμός αυτός δόθηκε από τον Mitola το 1995. Σε ένα SR, υλοποιούνται ως λογισμικό πάνω σε μια κοινή πλατφόρμα υλικού διαφορετικοί αλγόριθμοι εκπομπής και λήψης, οι οποίοι συνήθως αντιστοιχούν σε συγκεκριμένα πρότυπα. Η διαδικασία της ψηφιοποίησης πραγματοποιείται αμέσως μετά τη λήψη του σήματος στην κεραία του δέκτη και όλη η επεξεργασία του σήματος γίνεται από το λογισμικό. Αν και η ιδέα του SR αναφέρεται σε όλα τα στρώματα της στοίβας πρωτοκόλλων, οι περισσότερες ερευνητικές προσπάθειες εστίασαν στο φυσικό στρώμα (physical layer).

Ορισμός. Ένα *Software-Defined Radio* (SDR) αποτελεί μια πιο εφαρμόσιμη εκδοχή του ιδεατού Software Radio. Αποτελεί ουσιαστικά μια υλοποίηση του SR με κάποιες παραδοχές. Η κύρια διαφορά του SDR από το SR είναι ότι στο SDR τα λαμβανόμενα σήματα περνούν από ένα κατάλληλο ζωνοπερατό φίλτρο προτού γίνει η δειγματοληψία και η επεξεργασία τους με αποτέλεσμα ένα μικρό τμήμα του φάσματος (η ζώνη ενδιαφέροντος) να ψηφιοποιείται. Η ψηφιοποίηση γίνεται πολλές φορές μετά τη βαθμίδα ενδιάμεσης συχνότητας.

Στο σημείο αυτό πρέπει να γίνει η εξής διευκρίνιση. Ορίσαμε το SDR ως την παρούσα πρακτική υλοποίηση της ιδέας του SR. Το SR όπως περιγράφεται στον ορισμό του δεν μπορεί να υλοποιηθεί σήμερα, διότι ο *μετατροπέας σημάτων από αναλογικά σε ψηφιακά* (analog-to-digital converter, ADC) που απαιτείται από ένα SR δεν έχει κατασκευαστεί, δεν υπάρχει δηλ. ADC το οποίο να ψηφιοποιεί απευθείας το λαμβανόμενο σήμα, προτού αυτό διέλθει από ένα ζωνοπερατό φίλτρο περιοριζόμενο έτσι σε εύρος. Στην πραγματικότητα, η κατασκευή ενός τέτοιου ADC και του αντίστοιχου Software Radio δεν είναι καν επιθυμητή. Κι αυτό γιατί η ψηφιοποίηση όλων των σημάτων που εκτείνονται σε ένα τεράστιο εύρος ζώνης, το μεγαλύτερο μέρος του οποίου δεν είναι χρήσιμο, δεν έχει τίποτα να προσφέρει ούτε από επιστημονικής αλλά ούτε και από εμπορικής πλευράς. Εξ άλλου, κι αν ακόμα γινόταν ψηφιοποίηση των μη χρήσιμων σημάτων, η συγκεκριμένη ψηφιακή πληροφορία θα φιλτραρόταν στο πρώτο στάδιο της ψηφιακής επεξεργασίας σήματος που θα ακολουθούσε (βλ. [5]).

Συχνά, οι όροι SR και SDR συγχέονται και πολλές φορές χρησιμοποιούνται και οι δύο για να περιγράψουν το ίδιο πράγμα, δηλ. τα SDR συστήματα τα οποία έχουν υλοποιηθεί. Η ανάπτυξη και η εξέλιξη των SDR συστημάτων γίνεται υπό τη σκέπη του SDR Forum (βλ. [6]).

Τα συστήματα Cognitive Radio αποτελούν εξέλιξη των SDR. Η τεχνολογία CR στηρίχθηκε πάνω στην τεχνολογία των SDR και την επέκτεινε. Ουσιαστικά, ένα CR είναι ένα SDR το οποίο μπορεί επιπλέον να αντιλαμβάνεται το περιβάλλον του, να εντοπίζει τις αλλαγές που λαμβάνουν χώρα σε αυτό και να προσαρμόζεται σε αυτές αναλόγως. Για το λόγο αυτό, η κατανόηση του CR απαιτεί πρώτα μια περιγραφή της λειτουργίας του SDR.

2.2.1 Ιστορικά Στοιχεία

Όπως αναφέρθηκε, μια πρώτη παρουσίαση της ιδέας των software radios δόθηκε το 1995 από τον Mitola. Ένα από τα πρώτα SDRs σχεδιάστηκε στα πλαίσια του SpeakEasy, ενός έργου που ξεκίνησε από το στρατό των ΗΠΑ το 1992 (βλ. [7]). Πρωταρχικός στόχος του SpeakEasy ήταν να χρησιμοποιήσει προγραμματιστική λογική για να εξομοιώσει μια σειρά από συστήματα ραδιοεπικοινωνιών (περισσότερα από 10 σε πλήθος), τα οποία λειτουργούσαν στις ζώνες συχνοτήτων μεταξύ 2 και 200MHz. Άλλος στόχος του προγράμματος ήταν να καταφέρει μελλοντικά να ενσωματώσει στα συστήματα αυτά νέες τεχνικές κωδικοποίησης και διαμόρφωσης, έτσι ώστε τα στρατιωτικά συστήματα επικοινωνιών να είναι ενημερωμένα με την τελευταία τεχνολογία.

Στην πρώτη φάση του προγράμματος SpeakEasy, κατασκευάστηκε ένα σύστημα ραδιοεπικοινωνιών για χρήση από τον αμερικανικό στρατό, το οποίο είχε την ικανότητα να επικοινωνεί με τέσσερις διαφορετικές τεχνολογίες πρόσβασης: το δίκτυο του στρατού ξηράς, το δίκτυο του ναυτικού, το δίκτυο της αεροπορίας και το δορυφορικό σύστημα. Στο νέο αυτό ραδιοσύστημα, ήταν δυνατή η εγκατάσταση νέων προγραμμάτων. Το διαθέσιμο εύρος ζώνης υποδιαιρέθηκε σε μία σειρά από υπο-ζώνες (subbands). Ο δέκτης, αμέσως μετά την κεραία λήψης, αποτελείτο διαδοχικά από: έναν ενισχυτή, έναν υποβιβαστή (down converter), έναν αυτόματο ελεγκτή

κέρδους (Automatic Gain Controller), έναν A/D μετατροπέα και ένα υπολογιστικό σύστημα το οποίο περιελάμβανε μια συστοιχία από *ψηφιακούς επεξεργαστές σήματος (*Digital Signal Processors, DSPs).

Στη δεύτερη φάση του προγράμματος SpeakEasy τέθηκε ως στόχος ο σχεδιασμός μιας πιο γρήγορα επαναπρογραμματίσιμης (reconfigurable) αρχιτεκτονικής η οποία θα επέτρεπε την ύπαρξη πολλών ταυτόχρονων συνομιλιών, τη χρήση ανοικτού λογισμικού και τη διασύνδεση διαφορετικών καναλιών. Επίσης, το σύστημα θα έπρεπε να γίνει μικρότερο σε μέγεθος, ελαφρύτερο και φθηνότερο. Οι στόχοι επιτεύχθηκαν, το πρόγραμμα είχε θεαματικά αποτελέσματα και η νέα τεχνολογία, που λειτουργούσε στη ζώνη συχνοτήτων 4 MHz έως 400 MHz, διατέθηκε στο εμπόριο. Περιελάμβανε δε πολλές εξελιγμένες υπηρεσίες όπως η κρυπτογράφηση και η επεξεργασία φωνής.

Ακολούθησε το πρόγραμμα JTRS (Joint Tactical Radio System) το οποίο έγινε για λογαριασμό των ΗΠΑ και του ΝΑΤΟ και είχε ως στόχο την παραγωγή ευέλικτων ραδιοσυστημάτων που να μπορούν να επαναπροσαρμόζονται με τη βοήθεια λογισμικού. Αποτέλεσμα του προγράμματος ήταν η κατασκευή νέων πιο εξελιγμένων SDRs, με τη βοήθεια ενός νέου εργαλείου, του “Software Communications Architecture” (SCA). Το SCA είναι ένα ανοιχτό αρχιτεκτονικό πλαίσιο το οποίο υποδεικνύει στους σχεδιαστές τον τρόπο με τον οποίο υλικό και λογισμικό συνεργάζονται αρμονικά σε ένα SDR.

2.2.2 Χαρακτηριστικά των SDR

Ένα Software-Defined Radio είναι ένα σύστημα ραδιοεπικοινωνιών που έχει την ικανότητα να μεταβάλλει τα χαρακτηριστικά λειτουργίας του, όπως π.χ.:

- το εύρος ζώνης συχνοτήτων στο οποίο λειτουργεί
- το είδος διαμόρφωσης των σημάτων που εκπέμπει και λαμβάνει
- την ισχύ των εκπεμπόμενων σημάτων

Η επαναπρογραμματισιμότητα (reconfiguration) αυτή του συστήματος επιτυγχάνεται με τη βοήθεια πακέτων λογισμικού τα οποία έχουν εγκατασταθεί πάνω στο υλικό. Η κοινή αυτή πλατφόρμα υλικού αποτελείται από ψηφιακούς επεξεργαστές σήματος, καθώς και άλλους μικροεπεξεργαστές γενικού σκοπού. Το λογισμικό αποσκοπεί στο να προσαρμόζει τις παραμέτρους της λειτουργίας του συστήματος και έτσι να ελέγξει βασικές επικοινωνιακές λειτουργίες όπως είναι η διαμόρφωση και η αποδιαμόρφωση. Με την εγκατάσταση νέου λογισμικού είναι δυνατή η εκτέλεση νέων πρωτοκόλλων και λειτουργιών από το σύστημα.

Είναι επομένως προφανές ότι το βασικότερο πλεονέκτημα που προσφέρει η τεχνολογία SDR είναι αυτή η δυνατότητα της επί τόπου (on-the-fly) επαναπρογραμματισιμότητας των χαρακτηριστικών ενός τηλεπικοινωνιακού συστήματος. Παρόλα αυτά, το SDR έχει και μία σειρά από μειονεκτήματα όπως π.χ. η υψηλότερη κατανάλωση ισχύος, οι υψηλότερες απαιτήσεις σε υπολογιστική ισχύ και το υψηλότερο αρχικό κόστος (βλ. [8]).

Ένα SDR μπορεί να είναι (βλ. [5]):

- ένα *σύστημα πολλών ζωνών* (multiband system) το οποίο υποστηρίζει περισσότερες από μία ζώνες συχνοτήτων στα πλαίσια ενός προτύπου (π.χ. GSM 900, GSM 1800, GSM 1900)
- ένα *σύστημα πολλών προτύπων* (multistandard system) το οποίο υποστηρίζει δύο ή περισσότερα διαφορετικά πρότυπα. Τα πρότυπα αυτά μπορούν να ανήκουν στην ίδια οικογένεια προτύπων (π.χ. τα UTRA-FDD

και UTRA-TDD πρότυπα που ανήκουν στην οικογένεια του UMTS) ή να είναι εντελώς ανεξάρτητα και να αναφέρονται σε διαφορετικά δίκτυα.
- ένα σύστημα πολλών καναλιών (multichannel system) το οποίο υποστηρίζει την ταυτόχρονη ύπαρξη δύο ή περισσοτέρων αμφίδρομων δίαυλων χωρίς αυτό να υλοποιείται από το πρωτόκολλο
- ένα σύστημα πολλών υπηρεσιών (multiservice system) το οποίο παρέχει διαφορετικές υπηρεσίες όπως π.χ. υπηρεσίες φωνής, μεταφορά δεδομένων κ.λ.π.

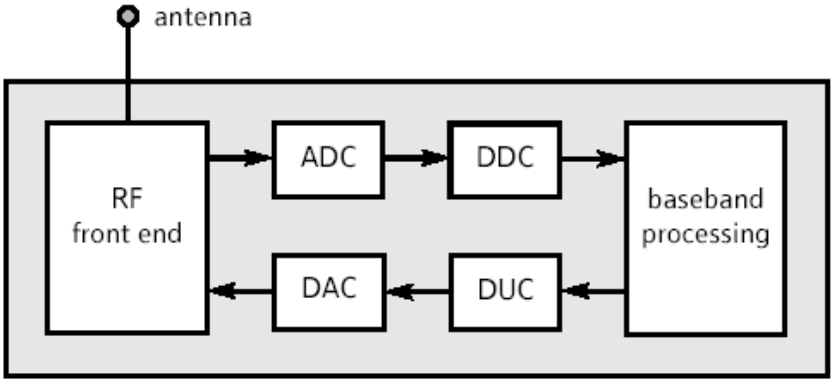
Ορισμός. Ένα σύστημα που είναι ταυτόχρονα multiband και multistandard χαρακτηρίζεται ως multimode δηλ. πολλών τρόπων λειτουργίας. Τα multimode συστήματα αναφέρονται συχνά και ως Composite Radios (Σύνθετα Συστήματα Ραδιοεπικοινωνιών).

Όπως έχουμε ήδη επισημάνει, το κυριότερο ίσως χαρακτηριστικό ενός SDR είναι η ικανότητά του να επαναπροσαμρόζεται - επεναπρογραμματίζεται, η επονομαζόμενη reconfigurability. Ο όρος reconfigurability περιλαμβάνει (βλ.[9]), [4]):
- Την προσαρμογή της διεπαφής του ραδιοσυστήματος στις μεταβολές του περιβάλλοντος
- Την ενσωμάτωση νέων εφαρμογών και υπηρεσιών
- Την ενσωμάτωση των τελευταίων εξελίξεων στην τεχνολογία λογισμικού
- Την εκμετάλλευση των ευέλικτων ετερογενών υπηρεσιών που παρέχονται από τα δίκτυα ραδιοεπικοινωνιών

Ένα SDR μπορεί να διαθέτει τέσσερα διαφορετικά επίπεδα προσαρμογής (βλ. [5]):
- Το πρώτο επίπεδο είναι η ρύθμιση του συστήματος λίγο πριν την αποστολή του στον πελάτη, ώστε να παραμετροποιηθεί με βάση τα χαρακτηριστικά τα οποία ζήτησε ο πελάτης κατά την αγορά του προϊόντος. Είναι προφανές ότι το επίπεδο αυτό δεν αποτελεί ουσιαστική επαναπρογραμματισιμότητα.
- Προσαρμογή με διακοπή της λειτουργίας: Τέτοιου είδους προσαρμογή γίνεται σπάνια και σε εξαιρετικές περιπτώσεις όπως είναι η αλλαγή της υποδομής του δικτύου. Απαιτεί τη διακοπή της λειτουργίας του συστήματος και μπορεί να διαρκέσει αρκετά δευτερόλεπτα.
- Προσαρμογή πριν την εκκίνηση μιας νέας κλήσης: Η προσαρμογή γίνεται πριν την έναρξη ενός νέου διαλόγου με ένα απομακρυσμένο τερματικό και δεν απαιτεί τη διακοπή της λειτουργίας του συστήματος. Στην περίπτωση αυτή δε μπορούν να επαναπρογραμματιστούν όλα τα χαρακτηριστικά του συστήματος αλλά μόνο μερικά από αυτά.
- Προσαρμογή σε οποιαδήποτε χρονική στιγμή: Εδώ η προσαρμογή μπορεί να λάβει χώρα ακόμα και κατά τη διάρκεια μιας κλήσης,

2.2.3 Δομή ενός SDR

Στο **σχήμα 5** δείχνει το λειτουργικό διάγραμμα ενός γενικού *Ψηφιακού Συστήματος Ραδιοεπικοινωνιών* (Digital Radio, DR) (βλ. [8]).

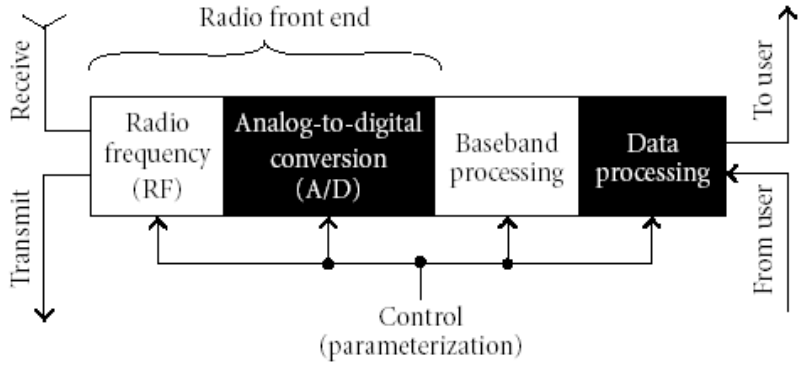


Σχήμα 5. Συμβατικό Ψηφιακό Σύστημα Ραδιοεπικοινωνιών

Το DR αποτελείται από:

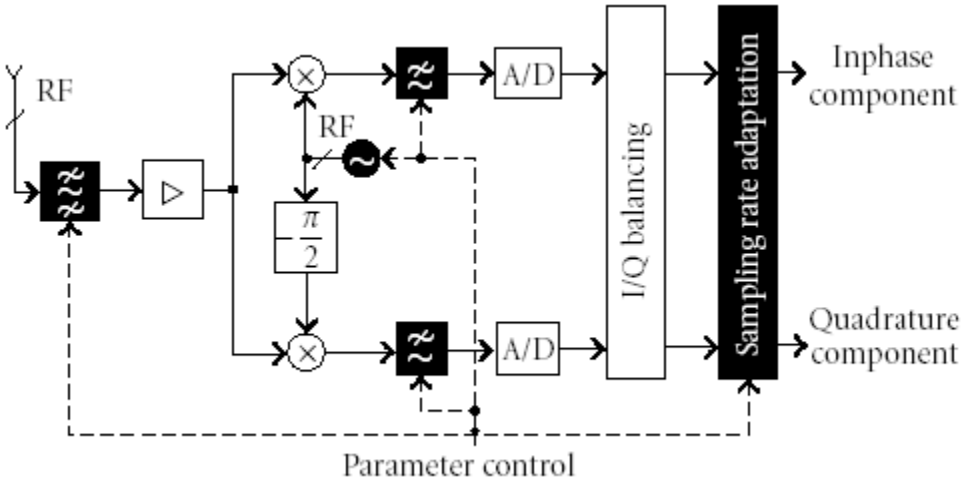
- Το μετωπιαίο άκρο ραδιοσυχνοτήτων (Radio Frequency front end). Το τμήμα αυτό είναι υπεύθυνο για τη μετάδοση και τη λήψη των σημάτων μέσω της κεραίας και για τη μετατροπή των σημάτων σε σήματα ενδιάμεσης συχνότητας (Intermediate Frequency, IF).
- Το τμήμα ADC/DAC. Ο μετατροπέας ADC πραγματοποιεί τη μετατροπή των σημάτων από αναλογικά σε ψηφιακά ενώ ο μετατροπέας DAC την μετατροπή τους από ψηφιακά σε αναλογικά.
- Το τμήμα DDC/DUC (Digital Down/Up Converter). Η μονάδα DDC πραγματοποιεί εφόσον χρειάζεται περαιτέρω κάτω μετατροπή συχνότητας στο ψηφιακό πλέον σήμα ενώ η DUC πραγματοποιεί την αντίστοιχη άνω μετατροπή συχνότητας.
- Το τμήμα επεξεργασίας βασικής ζώνης (baseband processing). Είναι υπεύθυνο για λειτουργίες βασικής ζώνης όπως η διαμόρφωση / αποδιαμόρφωση, ο σχηματισμός παλμών, η ισοστάθμιση, η μεταπήδηση συχνότητας και η αυτοσυσχέτιση. Επίσης, υλοποιεί ένα μεγάλο μέρος του πρωτοκόλλου του στρώματος ζεύξης δεδομένων όπως π.χ. τη διαυλοποίηση.

Τα συμβατικά Ψηφιακά Συστήματα Ραδιοεπικοινωνιών DRs υλοποιούν με υλικό τόσο τις λειτουργίες DDC/DUC όσο και τις λειτουργίες βασικής ζώνης. Στα ονομαζόμενα *Προγραμματίσιμα Ψηφιακά Συστήματα Ραδιοεπικοινωνιών* (Programmable Digital Radios, PDRs) οι λειτουργίες DDC/DUC πραγματοποιούνται με υλικό ενώ η επεξεργασία βασικής ζώνης υλοποιείται με τη βοήθεια λογισμικού. Στα SDR συστήματα τόσο οι λειτουργίες DDC/DUC όσο και οι λειτουργίες βασικής ζώνης εκτελούνται μέσω λογισμικού.



Σχήμα 6. Ένα PaC SDR

Στο **σχήμα 6** παρουσιάζει έναν SDR πομποδέκτη. Η διαφορά του με τον απλό DR πομποδέκτη του **σχήματος 5** είναι η ύπαρξη ενός *διαύλου ελέγχου* (control bus) ο οποίος τροφοδοτεί όλες τις μονάδες του συστήματος με πληροφορίες ελέγχου. Μέσω του διαύλου είναι δυνατός ο δυναμικός επαναπρογραμματισμός του συστήματος και η προσαρμογή όλων των παραμέτρων του. Ο εν λόγω πομποδέκτης πολλές φορές αποκαλείται και *SDR Ελεγχόμενο μέσω Παραμέτρων* (Parameter-Controlled SDR, PaC SDR) (βλ. [5]). Ακολουθεί μια αναλυτικότερη παρουσίαση των δύο πρώτων blocks της εικόνας 6, δηλ. της RF και A/D επεξεργασίας, τα οποία στην εικόνα χαρακτηρίζονται ως front end (*μετωπιαίο άκρο*). Θα εστιάσουμε στο δέκτη, αφού αυτός παρουσιάζει το μεγαλύτερο ενδιαφέρον.



Σχήμα 7. Πρόσθιο άκρο ενός δέκτη SDR

Το **σχήμα 7** δείχνει το μετωπιαίο άκρο ενός SDR δέκτη. Το RF σήμα λαμβάνεται αρχικά από την κεραία. Διέρχεται από ένα ζωνοπερατό φίλτρο το οποίο αποκόπτει τις περιττές συχνότητες και στη συνέχεια ενισχύεται. Το σήμα που προκύπτει ακολουθεί δύο διαφορετικές διαδρομές: στην άνω διαδρομή, που καλείται *συμφασική* (inphase, I), πραγματοποιείται αναλογική μίξη του σήματος με ένα ημιτονοειδές σήμα a(t) συχνότητας RF. Στην κάτω διαδρομή, που καλείται και *ορθογώνια* (quadrature, Q), γίνεται μίξη του σήματος με ένα ημιτονοειδές σήμα b(t) συχνότητας RF του οποίου η φάση έχει ολισθήσει κατά -π/2 σε σχέση με τη φάση του σήματος a(t). Τόσο η

ομοφασική I όσο και η ορθογώνια Q συνιστώσα διέρχονται από βαθυπερατά φίλτρα και στη συνέχεια μετατρέπονται από αναλογικές σε ψηφιακές. Ο ρυθμός δειγματοληψίας των ADC μετατροπέων πρέπει να είναι κοινός για όλα τα σήματα. Θα πρέπει επίσης να πληρούνται οι αρχές του Θεωρήματος Δειγματοληψίας του Nyquist-Shannon όπως σε όλα τα σήματα. Ακολούθως, θα πρέπει να υπάρξει κατάλληλη εξισορρόπηση των δύο συνιστωσών του σήματος I και Q (I/Q Balancing). Έπεται προσαρμογή του ρυθμού δειγματοληψίας (Sampling Rate Adaptation) στο κατάλληλο πρότυπο.

Η προσαρμογή αυτή απαιτείται γιατί ο ψηφιακός επεξεργαστής σήματος DSP θα πρέπει να λειτουργεί με τον ελάχιστο δυνατό ρυθμό. Για ένα δεδομένο πρότυπο ο ελάχιστος αυτός ρυθμός εξαρτάται από το ρυθμό συμβόλων fc=1/Tc . Συνήθως ένας ρυθμός fs=4fc είναι αρκετός για την επεξεργασία σήματος που ακολουθεί, δεδομένου μάλιστα και του υποτετραπλασιασμού του ρυθμού αμέσως μετά το τέλος της διαδικασίας συγχρονισμού. Μετά την προσαρμογή του ρυθμού, λαμβάνει χώρα η αποδιαμόρφωση και η αποκωδικοποίηση του σήματος. Η διαδικασία ολοκληρώνεται με την επεξεργασίας της ληφθείσας πληροφορίας.

Ο SDR πομπός επιτελεί περίπου την αντίστροφη διαδικασία (βλ. [5]).

3 Γνωστικά Συστήματα Ραδιοεπικοινωνιών – Cognitive Radio

3.1 Ιστορική αναδρομή

Αν και ο όρος “cognitive radio” προέκυψε σχετικά πρόσφατα, η ιδέα για κατασκευή έξυπνων συστημάτων ραδιοεπικοινωνιών δεν είναι νέα. Ήδη από τη δεκαετία του 1980 είχαν αναπτύχθηκαν δέκτες οι οποίοι εμφάνιζαν αρκετά χαρακτηριστικά ευφυΐας όπως π.χ. η αυτόματη αναγνώριση του είδους διαμόρφωσης των λαμβανόμενων σημάτων.

Αρκετά επιτεύγματα της τεχνολογίας επικοινωνιών που προηγήθηκαν του CR έχουν αρκετές ομοιότητες με την κεντρική ιδέα πίσω από το CR (βλ. [3]). Ένα παράδειγμα παλαιότερης τεχνολογίας που εμφανίζει χαρακτηριστικά παρόμοια με το CR είναι η *δυναμική επιλογή καναλιού* (dynamic channel selection/allocation) που έχει χρησιμοποιηθεί στα κυψελωτά συστήματα κινητών επικοινωνιών. Σε αυτή, όλα τα διαθέσιμα κανάλια συγκεντρώνονται σε μια κοινή δεξαμενή (pool). Κάθε νέο κινητό τερματικό που επιθυμεί να μεταδώσει λαμβάνει ένα ελεύθερο κανάλι από τη δεξαμενή. Το κανάλι επιστρέφεται στη δεξαμενή μετά το τέλος της μετάδοσης. Ο μηχανισμός που περιγράφηκε εμφανίζει πολλές ομοιότητες με το Spectrum Pooling, το οποίο θα αναλυθεί στη συνέχεια. Φυσικά το CR διαθέτει πολύ μεγαλύτερη νοημοσύνη από τα παλαιότερα συστήματα που αναφέρθηκαν.

Το Cognitive Radio αποτελεί εξέλιξη του Software-Defined Radio (SDR). Στηρίχθηκε στις αρχές του SDR και τις επέκτεινε με άμεση εφαρμογή την αξιοποίηση του ανεκμετάλλευτου φάσματος. Επομένως αν θέλει κανείς να καταγράψει την ιστορία του CR, θα πρέπει πρώτα να ξεκινήσει με την ιστορία του SDR, η οποία παρουσιάσθηκε παραπάνω. Όλα τα βήματα της εξέλιξης του SDR, όπως αναλύθηκαν παραπάνω, οδήγησαν αργά και σταθερά στο Cognitive Radio.

Όπως έχουμε ήδη αναφέρει ο πρώτος ορισμός των CR δόθηκε στη διατριβή του Mitolao (βλ. [10]).

Το 2002, όπως αναφέραμε και παραπάνω, η FCC διαπίστωσε την υπο-χρησιμοποίηση του φάσματος. Προέκυψε επομένως η ανάγκη για εκσυγχρονισμό των συστημάτων και διαδικασιών εκχώρησης φάσματος. Ο τρόπος με τον οποίο θα γινόταν η διαχείριση του φάσματος, ο τρόπος με τον οποίο θα βρισκόταν νέο φάσμα, το εάν το φάσμα αυτό θα έπρεπε να εκχωρηθεί στα πλαίσια αδειοδοτήσεων ή όχι, καθώς και άλλα παρόμοια ζητήματα προκάλεσαν αρκετές διχογνωμίες. Στις 20 Δεκεμβρίου του 2002 η FCC άνοιξε το ζήτημα της χρησιμοποίησης των τηλεοπτικών διαύλων για μη αδειοδοτημένη χρήση, με την προϋπόθεση ότι οι τηλεοπτικές μεταδόσεις δε θα δέχονταν παρεμβολές.

Ακολούθησαν και άλλες κινήσεις της FCC στις οποίες δηλώθηκε η πρόθεσή της να προωθήσει την ανάπτυξη του CR. Εκδόθηκαν αρκετές NPRMs (Notices of Proposed Rulemaking, Γνωστοποιήσεις Πρότασης για Θέσπιση Νέων Κανόνων) οι οποίες επεξεργάστηκαν πολλά από τα ζητήματα του CR. Η NPRM της 13^{ης} Νοεμβρίου του 2003 παρουσίασε ένα νέο μοντέλο υπολογισμού της θερμοκρασίας παρεμβολών (interference temperature) ενώ η NPRM της 17^{ης} Δεκεμβρίου του 2003 τόνισε την αξία της οπορτουνιστικής χρήσης του φάσματος από τα γνωστικά τερματικά (βλ. [3]). Μια από τις πιο σημαντικές εξελίξεις στην ιστορία του Cognitive Radio έλαβε χώρα το 2004 όταν η FCC δημοσίευσε μία ακόμη NPRM, στην οποία προτάθηκε το ενδεχόμενο να επιτραπεί σε μη αδειοδοτημένους χρήστες να δανειστούν προσωρινά φάσμα από

αδειοδοτημένους χρήστες, και πάλι με τον όρο ότι οι κάτοχοι αδειών δε θα δέχονταν παρεμβολές.

Παράλληλα με την FCC, η IEEE προχωρούσε και αυτή στην προτυποποίηση του Cognitive Radio. Μια πρόσφατη επέκταση του προτύπου IEEE 802.11, το IEEE 802.11h, ενσωμάτωσε τις λειτουργίες DFS (Dynamic Frequency Selection) και TPC (Transmit Power Control) για λειτουργία στα 5GHz. Οι DFS και TPC αποτελούν κύριες συνιστώσες του Cognitive Radio και θα αναλυθούν παρακάτω. Επίσης έχει εδώ και καιρό συσταθεί ομάδα εργασίας για την προτυποποίηση (802.22) της λειτουργίας τηλεπικοινωνιακού συστήματος πάνω από τηλεοπτικό φάσμα χωρίς την πρόκληση παρεμβολών στις τηλεοπτικές μεταδόσεις. Παράλληλα, η ιδέα του CR βρήκε πολύ μεγάλη ανταπόκριση από την επιστημονική και την ακαδημαϊκή κοινότητα, καθώς επίσης και από τη βιομηχανία των επικοινωνιών.

Σήμερα, η FCC έχει προτείνει τα ακόλουθα σε σχέση με το CR:

- Να ανοίξουν τρεις νέες ζώνες συχνοτήτων για χρήση από μη αδειοδοτημένους χρήστες. Οι τρεις ζώνες είναι: η ζώνη 6525-6700 MHz, η ζώνη 12.75-13.15 GHz και η ζώνη 13.2125-13.25 GHz.
- Να επιτραπεί η αύξηση της ισχύος εκπομπής των CR τερματικών που λειτουργούν στη ζώνη ISM (Industrial Scientific and Medical Radio Bands) Αν η ζώνη δεν είναι συνωστισμένη, η ισχύς εκπομπής μπορεί να αυξηθεί μέχρι και 6 φορές.
- Να οριστεί ως αχρησιμοποίητη ζώνη συχνοτήτων κάθε ζώνη στην οποία το ολικό λαμβανόμενο σήμα έχει ισχύ μικρότερη των -83 dBm (με συχνότητα αναφοράς τα 1.25 MHz)

3.2 Ορισμός

Ορισμός. Οι γνωστικές ραδιοεπικοινωνίες προσφέρουν τη δυνατότητα ευκαιριακής κάλυψης των ζωνών ραδιοσυχνοτήτων από δευτερεύοντες χρήστες στους οποίους δεν έχει εκχωρηθεί σταθερή ζώνη συχνοτήτων.

Συνεπώς, οι γνωστικές ραδιοεπικοινωνίες αποτελούν μια καινούργια φιλοσοφία σχεδίασης που περιλαμβάνει έξυπνη ανίχνευση φασματικών κενών και στη συνέχεια καθορισμό και προσαρμογή των παραμέτρων μετάδοσης μιας ομάδας δευτερογενών χρηστών.

Οι όροι γνωστικές ραδιοεπικοινωνίες και *συγκέντρωση φάσματος* (spectrum pooling) εισήχθηκαν αρχικά από τον Joseph Mitola (βλ. [10]), όπου προτάθηκε ο εξής ορισμός : **Ορισμός.** «Ο όρος γνωστικές ραδιοεπικοινωνίες ταυτίζεται με το σημείο εκείνο όπου τα ασύρματα PDAs (personal digital assistants, προσωπικοί ψηφιακοί βοηθοί) και τα σχετικά με αυτά δίκτυα διαθέτουν αρκετή υπολογιστική νοημοσύνη όσον αφορά την αξιοποίηση των ράδιο-πόρων και τη σχετική επικοινωνία μεταξύ υπολογιστών, ώστε να ανιχνεύουν τις τηλεπικοινωνιακές ανάγκες των χρηστών ως συνάρτηση του περιβάλλοντος χρήσης και να παρέχουν ράδιο-πόρους και ασύρματες επικοινωνίες που να είναι κατάλληλες να ικανοποιήσουν τις ανάγκες αυτές». Έτσι λοιπόν, οι γνωστικές ραδιοεπικοινωνίες είναι ικανές να επιλέγουν αυτόματα την καλύτερη υπηρεσία και να καθυστερήσουν ή να προωθήσουν άμεσα ορισμένες ασύρματες μεταδόσεις ανάλογα με τους διαθέσιμους ή προβλεπόμενους πόρους.

Η ομοσπονδιακή επιτροπή επικοινωνιών των Ηνωμένων Πολιτειών (FCC – Federal Communication Committee) πρότεινε αργότερα ένα λιγότερο γενικό ορισμό, όπου κάθε τηλεπικοινωνιακό σύστημα με ικανότητα μάθησης του φασματικού περιβάλλοντος και προσαρμογής αναφέρεται με τον όρο γνωστικό σύστημα ραδιοεπικοινωνιών.

Ορισμός. «Ως γνωστικό σύστημα ραδιοεπικοινωνιών καλείται κάθε σύστημα που μπορεί να αλλάξει τις παραμέτρους εκπομπής του, βασιζόμενο στην αλληλεπίδραση με το περιβάλλον στο οποίο λειτουργεί. Η πλειοψηφία των γνωστικών συστημάτων ραδιοεπικοινωνιών βασίζεται σε συστήματα λογισμικού (software defined radio – SDR), αλλά ούτε η ύπαρξη λογισμικού ούτε προγραμματισμού αποτελούν αναγκαίες απαιτήσεις των γνωστικών ραδιοεπικοινωνιών».

Η ομάδα έρευνας σε θέμα γνωστικών ορισμών του πανεπιστημίου της Βιρτζίνια (βλ. [5]) αναφέρει τον παρακάτω ορισμό :
Ορισμός. «cognitive radio είναι το προσαρμοστικό τηλεπικοινωνιακό σύστημα με δυνατότητες επίγνωσης του περιβάλλοντος, κατανόησης και μάθησης των επιδράσεων κάθε απόφασης, ανάκλησης και συσχέτισης των προηγούμενων ενεργειών, επιδόσεων και χαρακτηριστικών περιβάλλοντος για την επίτευξη βέλτιστης λειτουργίας».

Συμπληρωματικά, ο Simon Haykin σε μια δημοσίευσή του (βλ. [4]) δίνει τον εξής ορισμό:
Ορισμός. «Σύστημα γνωστικών ραδιοεπικοινωνιών είναι ένα έξυπνο ασύρματο σύστημα επικοινωνιών που έχει γνώση για το περιβάλλον του (δηλαδή, για τον εξωτερικό κόσμο) και χρησιμοποιεί τη μέθοδο ‘’κατανοώ οικοδομώντας‘’ (understanding-by-building) για να μάθει από το περιβάλλον και να προσαρμόσει τις εσωτερικές του καταστάσεις στις στατιστικές μεταβολές των εισερχόμενων RF ερεθισμάτων, κάνοντας αντίστοιχες αλλαγές σε συγκεκριμένες λειτουργικές παραμέτρους (π.χ. στην ισχύ μετάδοσης, την συχνότητα των φερόντων και το σχήμα διαμόρφωσης) σε πραγματικό χρόνο και έχοντας δυο κύριους στόχους:

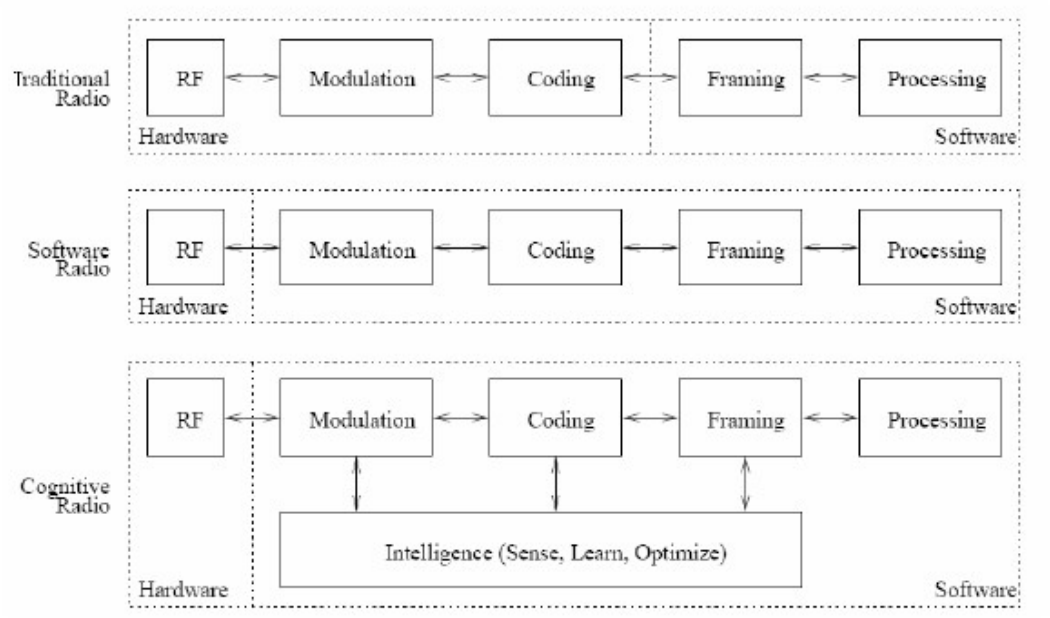
- Υψηλής αξιοπιστίας επικοινωνίες οποτεδήποτε και οπουδήποτε χρειαστεί
- Αποδοτική χρήση του φάσματος ραδιοσυχνοτήτων»

Τέλος το 2007 η ομάδα εργασίας IEEE 1900.1 , που δημιουργήθηκε για το καθορισμό ορολογιών και εννοιών, πρότεινε τον επόμενο ορισμό (βλ. [11]) για τις γνωστικές ραδιοεπικοινωνίες:
Ορισμός. «Οι γνωστικές ραδιοεπικοινωνίες είναι ένα είδος ασύρματου συστήματος ραδιοεπικοινωνιών που μπορεί να ανιχνεύει και να κρίνει αυτόνομα το περιβάλλον του και προσαρμόζεται ανάλογα σε αυτό. Το ασύρματο αυτό σύστημα επικοινωνιών θα μπορούσες να χρησιμοποιεί αναπαράσταση γνώσης, αυτοματοποιημένη κρίση και μηχανισμό μάθησης για την εγκατάσταση, διεξαγωγή και τερματισμό επικοινωνίας με άλλα ασύρματα συστήματα επικοινωνιών. Τα γνωστικά συστήματα ραδιοεπικοινωνιών μπορούν δυναμικά και αυτόνομα να προσαρμόζουν τις λειτουργικές τους παραμέτρους».

3.3 Χαρακτηριστικά

Τα τελευταία χρόνια, η ενσωμάτωση λογισμικού σε τηλεπικοινωνιακά συστήματα είχε ως αποτέλεσμα τη δημιουργία ευέλικτων συσκευών με ικανότητα μετάδοσης και λήψης, χρησιμοποιώντας μια ποικιλία πρωτοκόλλων και σχημάτων διαμόρφωσης. Στη βιβλιογραφία, τα τηλεπικοινωνιακά συστήματα ελεγχόμενα από λογισμικό (SDR), αναφέρονται ως συστήματα που περιλαμβάνουν πομπό, του οποίου οι λειτουργικές παράμετροι (όπως εύρος συχνοτήτων, είδος διαμόρφωσης, ισχύς εκπομπής κτλ) μπορούν να μεταβληθούν μέσω λογισμικού χωρίς την αλλαγή υλικού. Τα βασικά τους προτερήματα είναι η ευελιξία αλλαγής από ένα πρότυπο σε άλλο και η ευκολία προσαρμογής στις εκάστοτε συνθήκες περιβάλλοντος. Η ανάπτυξη και η χρησιμοποίηση της τεχνολογίας αυτής είναι τόσο ραγδαία που επηρεάζει την υπάρχουσα κατάσταση στον τομέα των τηλεπικοινωνιών.

Τα συστήματα ραδιοεπικοινωνιών που οραματίστηκε ο Mitola το 2000 αποτελούν μια εξέλιξη στην τεχνολογία SDR, έτσι ώστε ένα σύστημα να μπορεί να πάρει αποφάσεις όσον αφορά το δίκτυο, τη διαμόρφωση και την κωδικοποίηση βασιζόμενο στο εξωτερικό περιβάλλον. Στο παρακάτω **σχήμα 8** περιγράφεται και συγκρίνεται γραφικά η εξέλιξη των παραδοσιακών τηλεπικοινωνιακών συστημάτων στα υποσχόμενα συστήματα γνωστικών ραδιοεπικοινωνιών.



Σχήμα 8. Λογικό διάγραμμα σύγκρισης παραδοσιακού πομποδέκτη, τηλεπικοινωνιακού συστήματος βασισμένου σε λογισμικό και συστήματος γνωστικών ραδιοεπικοινωνιών

Η τεχνολογία των γνωστικών ραδιοεπικοινωνιών έχει τη δυνατότητα παροχής ενός αριθμού πλεονεκτημάτων που μπορούν να συμβάλουν στην αποδοτικότερη πρόσβαση στο φάσμα και συνεπώς στη διάθεση στο κοινό νέων εξελιγμένων τηλεπικοινωνιακών υπηρεσιών. Τα χαρακτηριστικά που οι γνωστικές ραδιοεπικοινωνίες μπορούν να ενσωματώσουν ώστε να επιτρέψουν αποτελεσματικότερη και πλέον ευέλικτη χρήση του φάσματος, όπως αναφέρεται και από την ομοσπονδιακή επιτροπή επικοινωνιών των Ηνωμένων Πολιτειών είναι τα εξής (βλ. [12]):

- **Μεταβλητότητα Συχνότητας** (Frequency Agility): η ικανότητα του συστήματος να μπορεί να μεταβάλλει τη συχνότητα λειτουργίας του, προκειμένου να πετύχει βέλτιστη ειτουργία στις εκάστοτε συνθήκες περιβάλλοντος.
- **Δυναμική Επιλογή Συχνότητας** (Dynamic Frequency Selection, DFS): η δυνατότητα ανίχνευσης σημάτων από γειτονικές συσκευές κατά την προσπάθεια επιλογής βέλτιστου λειτουργικού περιβάλλοντος.
- **Προσαρμοστική Διαμόρφωση** (Adaptive Modulation): η ικανότητα τροποποίησης χαρακτηριστικών μετάδοσης και κυματομορφών ώστε να αξιοποιηθούν ευκαιρίες χρησιμοποίησης φάσματος.
- **Έλεγχος Ισχύος Εκπομπής**(Transmit Power Control, TPC): μετάδοση στα όρια πλήρους ισχύος όταν είναι επιτρεπτό, αλλά και δυνατότητα περιορισμού

ισχύος εκπομπής σε χαμηλότερα επίπεδα ώστε να αποφεύγονται παρεμβολές και άσκοπη κατανάλωση ενέργειας των φορητών συσκευών.

- **Γνώση για την Τοποθεσία** (Location Awareness): η ικανότητα του συστήματος να αναγνωρίζει τη θέση του και τη θέση των υπολοίπων συσκευών που χρησιμοποιούν την ίδια ζώνη συχνοτήτων και η δυνατότητα αλλαγής λειτουργικών παραμέτρων ανάλογα με την πληροφορία τοπολογίας του δικτύου.
- **Χρήση υπό Διαπραγμάτευση** (Negotiated Use): το σύστημα γνωστικών ραδιοεπικοινωνιών περιλαμβάνει αλγορίθμους και μηχανισμούς που επιτρέπουν τον καταμερισμό του φάσματος στα πλαίσια προσυμφωνημένων κανόνων μεταξύ των δικαιούχων και δευτερογενών χρηστών. Τελικώς, τα γνωστικά συστήματα ενδεχομένως να μπορέσουν να διαπραγματεύονται την εκχώρηση φάσματος σε πραγματικό χρόνο, χωρίς προηγούμενες συμφωνίες μεταξύ των χρηστών.

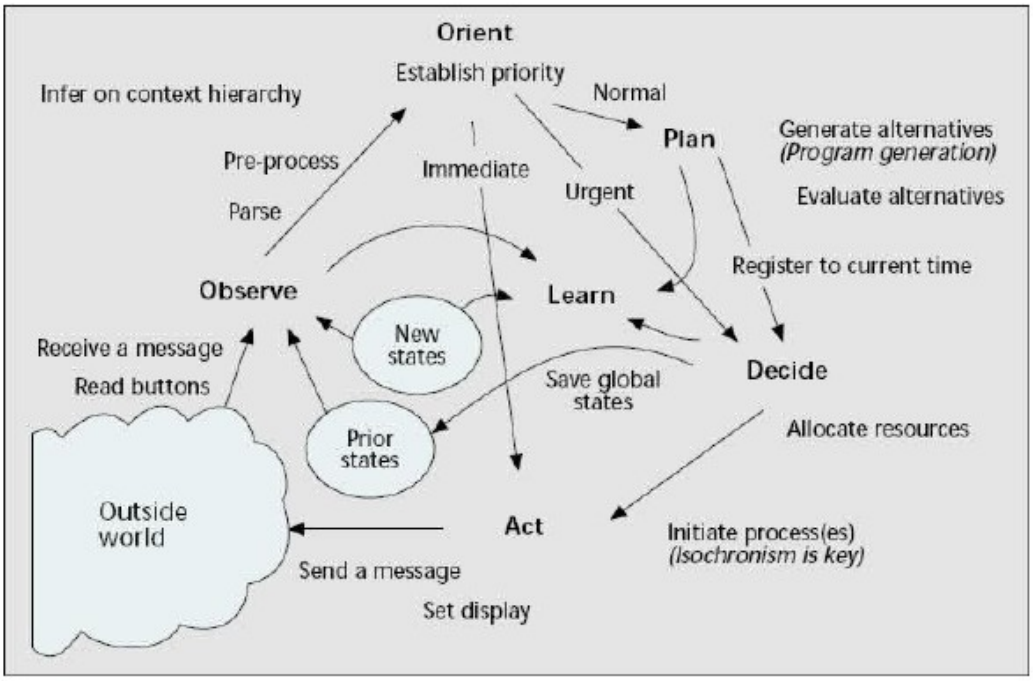
3.4 Αρχές Λειτουργίας ΓΕ – Κύκλος Γνώσης

Οι διαφορές στους ορισμούς για τις ΓΕ μπορούν να αποδοθούν κατά ένα μεγάλο μέρος στις διαφορές στις προσδοκίες της λειτουργίας που ένα σύστημα ΓΕ θα έχει. Στη διατριβή του, ο Joseph Mitola εξετάζει τα εννέα επίπεδα της αυξανόμενης ραδιολειτουργίας που παρουσιάζεται στον **πίνακα 1**, που κυμαίνεται από ένα software radio ως ένα σύνθετο self-aware radio.

Level	Capability	Comments
0	Pre-programmed	A software radio
1	Goal Driven	Chooses Waveform According to Goal. Requires Environment Awareness.
2	Context Awareness	Knowledge of What the User is Trying to Do
3	Radio Aware	Knowledge of Radio and Network Components, Environment Models
4	Capable of Planning	Analyze Situation (Level 2& 3) to Determine Goals (QoS, power), Follows Prescribed Plans
5	Conducts Negotiations	Settle on a Plan with Another Radio
6	Learns Environment	Autonomously Determines Structure of Environment
7	Adapts Plans	Generates New Goals
8	Adapts Protocols	Proposes and Negotiates New Protocols

Πίνακας 1. Επίπεδα λειτουργιών των ΓΕ

Αναφορικά με το πώς ένα CR θα μπορούσε να επιτύχει αυτά τα επίπεδα λειτουργίας, ο Mitola εισήγαγε τον *κύκλο γνώσης* (cognition circle),(βλ. [10]) που φαίνεται στο παρακάτω **σχήμα 9** :



Σχήμα 9. Ο κύκλος της Γνώσης

Στον κύκλο αυτό διακρίνονται έξι βασικά στάδια: Παρατήρηση (Observe), Προσανατολισμός (Orient), Σχεδιασμός (Plan), Απόφαση (Decide), Δράση (Act), και Μάθηση (Learn).

Παρατήρηση (Observe): Ένα σύστημα ΓΕ παρατηρεί το περιβάλλον του αναλύοντας τα εισερχόμενα ερεθίσματα. Επίσης συσχετίζει τους αισθητήρες θέσης, θερμοκρασίας, φωτεινότητας και ούτω καθ΄εξής για να συμπεράνει το γενικό τηλεπικοινωνιακό πλαίσιο. Αυτή η φάση συνδέει αυτά τα ερεθίσματα με προηγούμενες εμπειρίες με σκοπό να καλύψει μοτίβα σε βάθος χρόνου. Το σύστημα ΓΕ συγκεντρώνει εμπειρίες με το να «θυμάται» τα πάντα. Ολόκληρη η πληροφορία του ήχου, τα e-mail, οι τηλεπικοινωνιακές καταστάσεις στις οποίες μπορεί να βρεθεί ο χρήστης σε διάστημα ενός χρόνου καταλαμβάνουν μερικές εκατοντάδες gigabytes, ανάλογα με το επιθυμητό επίπεδο λεπτομέρειας. Επομένως η αρχιτεκτονική μνήμης και ταχείας συσχέτισης της τρέχουσας εμπειρίας με όλες τις προηγούμενες είναι μια κεντρική ικανότητα του συστήματος ΓΕ.

Προσανατολισμός (Orient): Η φάση προσανατολισμού καθορίζει την σπουδαιότητα μιας παρατήρησης, συνδέοντάς την με ένα σύνολο ερεθισμάτων γνωστό εκ των προτέρων. Όταν υπάρχει απόλυτο ταίριασμα ανάμεσα στην τρέχουσα παρατήρηση και την προηγούμενη εμπειρία, έχουμε αναγνώριση ερεθίσματος. Η επακόλουθη αντίδραση μπορεί να είναι είτε σωστή είτε λανθασμένη. Κάθε ερέθισμα ανήκει σε ένα ευρύτερο πλαίσιο , το οποίο περιλαμβάνει πρόσθετα ερεθίσματα και σχετικές εσωτερικές καταστάσεις συμπεριλαμβανομένου του χρόνου. Μερικές φορές η φάση προσανατολισμού προκαλεί την άμεση εκκίνηση μιας ενέργειας ως ένα είδος αντανακλαστικής συμπεριφοράς. Μια ξαφνική απώλεια ηλεκτρικής ισχύς, για παράδειγμα, θα μπορούσε να προκαλέσει την άμεση αποθήκευση των δεδομένων του χρήστη (το “immediate” μονοπάτι προς την φάση ‘’Act” στην εικόνα). Μια μη αντιμετωπίσιμη απώλεια σήματος σε ένα δίκτυο θα προκαλούσε επανεκχώρηση

πόρων, για παράδειγμα, από την ανάλυση φωνής ως την αναζήτηση εναλλακτικών καναλιών. Αυτό αντιστοιχεί στο μονοπάτι “Urgent” στην εικόνα.

Η σύνδεση συμβαίνει όταν υπάρχει ένα σχεδόν πλήρες ταίριασμα μεταξύ του παρόντος συνόλου ερεθισμάτων και μιας προηγούμενης εμπειρίας, ενώ ταυτόχρονα ισχύουν κάποια πολύ γενικά κριτήρια για την εφαρμογή της προηγούμενης εμπειρίας στην τρέχουσα κατάσταση. Ένα τέτοιο κριτήριο είναι το πλήθος των μη-αντιστοιχισμένων χαρακτηριστικών στην παρούσα σκηνή. Αν ένα μόνο χαρακτηριστικό δεν ταιριάζει, τότε η σύνδεση μπορεί να είναι το πρώτο βήμα στο σχεδιασμό μιας συμπεριφοράς παρόμοιας με τη συμπεριφορά στην πιο πρόσφατη συγκρίσιμη σκηνή.

Σχεδιασμός (Plan): Τα περισσότερα ερεθίσματα αντιμετωπίζονται με προμελετημένο τρόπο παρά αντανακλαστικά. Ένα εισερχόμενο μήνυμα από το δίκτυο θα αντιμετωπιζόταν με τη δημιουργία ενός σχεδίου (το κανονικό μονοπάτι). Τυπικά, οι αντανακλαστικές αντιδράσεις είναι προγραμματισμένες εκ των προτέρων ή μαθαίνονται μέσω ρητών εντολών του χρήστη, ενώ οι υπόλοιπες προμελετημένες αντιδράσεις μέσω σχεδίου. Σχεδιαστικά εργαλεία όπως το OPRS (Open Procedural Reasoning System) επιτρέπουν τη σύνθεση συμπεριφορών πρόσβασης στο φάσμα και στην πληροφορία με βάση την αντίληψη του περιβάλλοντος, τους κανόνες της μηχανής μάθησης και τις προτιμήσεις του χρήστη που έχουν γίνει γνωστές από προηγούμενη χρήση.

Απόφαση (Decide): Η φάση απόφασης διαλέγει ανάμεσα στα υποψήφια σχέδια. Το σύστημα ΓΕ θα μπορούσε να ειδοποιήσει το χρήστη για ένα εισερχόμενο μήνυμα ή να αναβάλει τη διακοπή για αργότερα (ενεργώντας όπως ένας γραμματέας που φιλτράρει τις κλήσεις κατά τη διάρκεια μιας σημαντικής συνάντησης).

Δράση (Act): Αυτή η φάση ξεκινά τις επιλεγμένες διαδικασίες χρησιμοποιώντας ενεργοποιητές που προσπελαύνουν τον έξω κόσμο ή τις εσωτερικές καταστάσεις του συστήματος ΓΕ. Πρόσβαση στον έξω κόσμο σημαίνει κυρίως τη σύνθεση μηνυμάτων, είτε προφορικών που απευθύνονται στο τοπικό περιβάλλον είτε γραπτών που απευθύνονται σε ένα άλλο σύστημα ΓΕ ή σε ένα Γνωστικό δίκτυο (Cognitive Network,CN), γραμμένων σε RKRL, RXML(Radio XML) ή σε κάποιο άλλο πρότυπο ανταλλαγής γνώσης. Η δράση πάνω σε εσωτερικές καταστάσεις περιλαμβάνει τον έλεγχο πόρων όπως τα ασύρματα κανάλια.

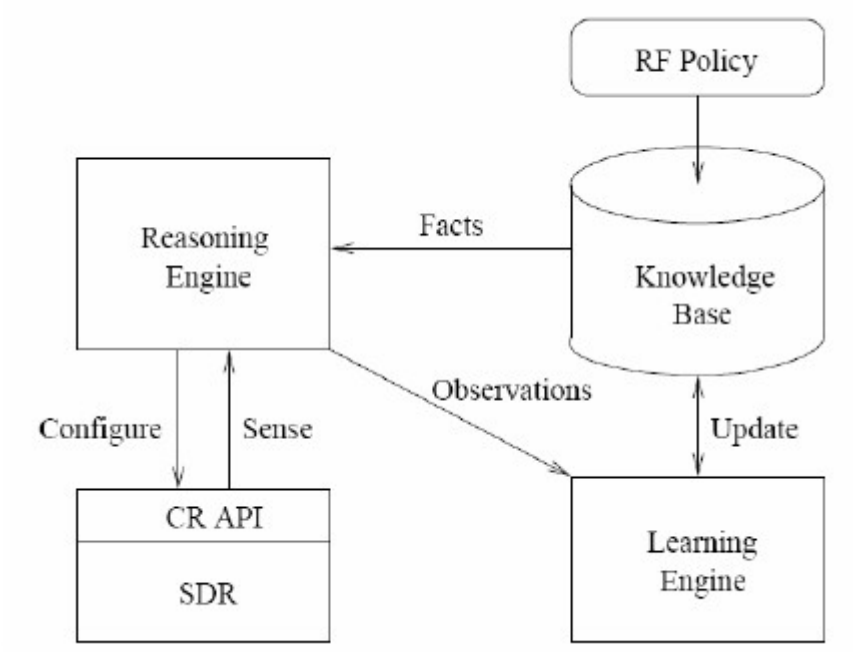
Μάθηση (Learn): Αρχικά η μάθηση εξυπηρετείται από τη φάση παρατήρησης όπου η πληροφορία από τους αισθητήρες συσχετίζεται με όλη την προηγούμενη εμπειρία. Κατόπιν το σύστημα ΓΕ μαθαίνει καθ’ όλη τη διάρκεια του κύκλου, δηλαδή από το σχεδιασμό, από τις αποφάσεις και από τη δημιουργία νέων καταστάσεων που ενσωματώνονται στην ήδη αποθηκευμένη γνώση.

Από τα παραπάνω γίνεται φανερό ότι το cognitive radio επιδεικνύει την ικανότητα επαναδιάρθρωσης της δομής και της λειτουργίας του. Δεν είναι τυχαίο λοιπόν η σχεδόν καθολική θεώρηση ότι το σύστημα CR χτίζεται πάνω στην πλατφόρμα του SDR.

Τέλος συνοψίζοντας για τον κύκλο γνώσης θα μπορούσαμε να πούμε ότι το τηλεπικοινωνιακό σύστημα αποκτά πληροφορίες σχετικά με το εξωτερικό περιβάλλον (outside world) μέσω άμεσων παρατηρήσεων ή μέσω σηματοδοσίας. Στη συνέχεια, οι πληροφορίες αυτές εκτιμώνται (Orient) ώστε να εκτιμηθεί η σπουδαιότητά τους. Με την αποτίμηση των πληροφοριών γίνεται ο σχεδιασμός των εναλλακτικών στρατηγικών (Plan) και στη συνέχεια με κριτήριο τη βελτιστοποίηση του τελικού στόχου, επιλέγεται (Decide) και εκτελείται (Act) η κατάλληλη ενέργεια. Τα αποτελέσματα των ενεργειών αυτών αντικατοπτρίζονται στις επιδόσεις του συστήματος και στις ενδεχόμενες ανεπιθύμητες παρεμβολές που παρουσιάζονται στο εξωτερικό περιβάλλον. Το ασύρματο σύστημα επικοινωνιών, τέλος, χρησιμοποιεί τα αποτελέσματα και τις εκάστοτε αποφάσεις κατά τη διαδικασία μάθησης (Learn), με σκοπό τη βελτίωση της

λειτουργίας του, δημιουργώντας νέες μοντελοποιημένες καταστάσεις και παράγοντας νέες εναλλακτικές στρατηγικές που ταιριάζουν καλύτερα στις συνθήκες του περιβάλλοντος λειτουργίας.

Οι έννοιες που προαναφέρθηκαν και η συνολική λειτουργία ενός συστήματος γνωστικών ραδιοεπικοινωνιών παρουσιάζονται σαφέστερα στο επόμενο **σχήμα 10**. Μέσω ενός συνόλου προγραμματιστικών εφαρμογών (API-Application Programming Interface) γίνεται πρόσβαση στην πλατφόρμα λογισμικού (SDR), παρέχοντας τη δυνατότητα στη μηχανή γνωστικών ραδιοεπικοινωνιών να ρυθμίσει το σύστημα και να ανιχνεύσει το περιβάλλον της. Η βασισμένη στην εκάστοτε πολιτική εκχώρησης ‘’συλλογιστική μηχανή’’ (reasoning engine) λαμβάνει δεδομένα από μια βάση πληροφοριών, προκειμένου να αποφασιστεί σχετικά με τις ευκαιρίες πρόσβασης στο φάσμα ραδιοσυχνοτήτων. Επιπλέον μια μηχανή μάθησης (learning engine) παρατηρεί τις μεταβολές του ραδιοφάσματος, τη συμπεριφορά του συστήματος και τις επιδόσεις των εκάστοτε ενεργειών, ώστε να προσαρμόσει τα δεδομένα στη βάση πληροφοριών που χρησιμοποιείται για τη λήψη αποφάσεων.



Σχήμα 10. Λειτουργικό διάγραμμα αρχιτεκτονικής συστήματος γνωστικών ραδιοεπικοινωνιών

3.5 Το μοντέλο αναφοράς OSI και το σύστημα ΓΕ

Τα συμβατικά συστήματα επικοινωνιών καθορίζονται και τυποποιούνται χρησιμοποιώντας επτά επίπεδα του ISO(International Organization for Standardization)/OSI(Open System Interconnection). Το μοντέλο OSI έχει επτά επίπεδα τα οποία είναι : το φυσικό επίπεδο, το επίπεδο συνδέσμου μετάδοσης δεδομένων, το επίπεδο δικτύου, το επίπεδο μεταφοράς, το επίπεδο συνδιάλεξης, το επίπεδο παρουσίασης και το επίπεδο εφαρμογών. Στη συνέχεια παρουσιάζονται συνοπτικά όλα τα προαναφερθέντα επίπεδα OSI.

Το *φυσικό επίπεδο* (physical layer) ασχολείται με την μετάδοση ανεπεξέργαστων δυαδικών ψηφίων μέσω ενός καναλιού επικοινωνίας. Τα ζητήματα σχεδίασης ταυτίζονται με την εξασφάλιση ότι όταν μια φορά στέλνει το bit 1, αυτό θα λαμβάνεται από την άλλη πλευρά ως bit 1 και όχι ως bit 0.

Συνεχίζοντας, το κύριο καθήκον του *επιπέδου συνδέσμου μετάδοσης δεδομένων* (data link layer) είναι να μμετασχηματίζει μια υπηρεσία μετάδοσης ανεπεξέργαστων δεδομένων σε μια γραμμή η οποία φαίνεται στο επίπεδο δικτύου ότι δεν έχει τον κίνδυνο μη εντοπισμένων σφαλμάτων μετάδοσης. Ο στόχος αυτός επιτυγχάνεται με την αποστολή πλαισίων δεδομένων και τη λήψη πλαισίων επιβεβαίωσης για τα πλαίσια που φτάνουν επιτυχώς στον παραλήπτη.

Το επίπεδο δικτύου (network layer) ελέγχει τη λειτουργία του υποδικτύου. Ένα βασικό ζήτημα σχεδίασης είναι ο καθορισμός του τρόπου δρομολόγησης των πακέτων από την προέλευση στον προορισμό.

Η βασική λειτουργία *του επιπέδου μεταφοράς* (transport layer) είναι να δέχεται δεδομένα από το ανώτερο επίπεδο, να τα διασπά αν τα χρειάζεται σε μικρότερες μονάδες, να τα μεταβιβάζει στο επίπεδο δικτύου και να εξασφαλίζει ότι όλα τα τμήματα φτάνουν σωστά στο άλλο άκρο.

Επιπρόσθετα, *το επίπεδο συνδιάλεξης* (session layer) επιτρέπει σε χρήστες διαφορετικών μηχανών να εγκαθιδρύουν συνδιαλέξεις μεταξύ τους. Οι συνδιαλέξεις αυτές περιλαμβάνουν διάφορες υπηρεσίες όπως ο έλεγχος διαλόγου (dialog control, η παρακολούθηση αυτού που έχει σειρά για μετάδοση), η διαχείριση σκυτάλης (token management, η αποτροπή των δύο πλευρών στο να επιχειρήσουν ταυτόχρονα την εκτέλεσης της ίδιας λειτουργίας) και ο συγχρονισμός (synchronization, η τήρηση σημείων ελέγχου σε μακρόχρονες μεταδόσεις, έτσι ώστε αυτές να μπορούν να συνεχιστούν από το σημείο που διακόπηκαν, μετά από κατάρρευση του συστήματος).

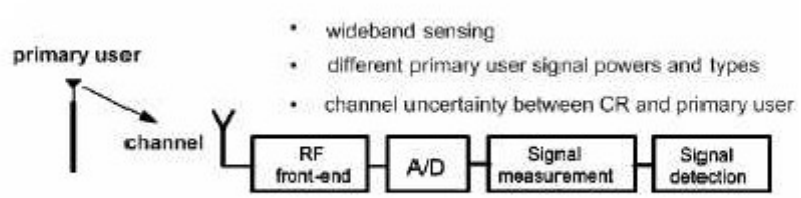
Το επίπεδο παρουσίασης (presentation layer) ασχολείται με την σύνταξη και τη σημασιολογία των μεταδιδόμενων πληροφοριών.

Τέλος, *το επίπεδο εφαρμογών* (application layer) περιέχει μια ποικιλία πρωτοκόλλων που απαιτούνται συχνά από τους χρήστες. Ένα γνωστό πρωτόκολλο εφαρμογής είναι το Πρωτόκολλο Μεταφοράς Υπερκειμένου ή HTTP (HyperText Transfer Protocol), το οποίο είναι η βάση του Παγκόσμιου Ιστού.

Εστιάζοντας στο cognitive radio, ακόμα κι αν τα συστήματα ΓΕ είναι αρκετά διαφορετικά από τα παραδοσιακά ασύρματα radios, είναι λογικό να υποτεθεί ότι ένα cognitive radio framework θα βασιζόταν στην μεθοδολογία διαστρωμάτωσης ISO/OSI. Ένα περαιτέρω πλεονέκτημα της διαστρωμάτωσης θα μπορούσε να είναι η ενίσχυση των υπαρχόντων στρωμάτων των συμβατικών radio με μοναδικές γνωστικές λειτουργίες. Πρώτα απ' όλα, κάποιος πρέπει να αρχίσει τις γνωστικές λειτουργίες στο φυσικό επίπεδο προκειμένου να γίνουν κατανοητές οι ικανότητες και οι περιορισμοί της εφαρμογής τους, έτσι ώστε τα ανώτερα στρώματα να μπορούν να σχεδιαστούν χρησιμοποιώντας ρεαλιστικά πρότυπα.

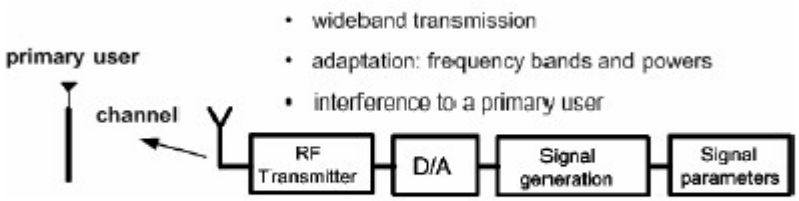
Η cognitive ραδιοεπικοινωνία βασίζεται στην αξιόπιστη ανίχνευση του μη κατειλημμένου φάσματος. Το γεγονός αυτό καθιερώνει έναν νέο τύπο λειτουργίας στο φυσικό επίπεδο για την *ανίχνευση φάσματος* (spectrum sensing) σε όλες τις παραμέτρους (χρόνος, συχνότητα, και διάστημα) προκειμένου να προσδιοριστούν οι ζώνες συχνότητας διαθέσιμες για τη μετάδοση. Η αντίληψη φάσματος απαιτεί το radio να λαμβάνει ένα ευρείας ζώνης σήμα μέσω front-end RF, να κάνει δειγματοληψία μέσω

αναλογικού σε ψηφιακού μετατροπέα (A/D converter), και να παίρνει μετρήσεις για την ανίχνευση των σημάτων αρχικών χρηστών, όπως διευκρινίζεται στο **σχήμα 11**.



Σχήμα 11. Δέκτης ΓΕ

Μετά τον προσδιορισμό ενός διαθέσιμου τμήματος φάσματος, ένα σύστημα ΓΕ πρέπει να χρησιμοποιήσει σχέδια διαμόρφωσης που παρέχουν καλύτερη χρησιμοποίηση φάσματος αποφεύγοντας την παρέμβαση σε οποιοδήποτε αρχικό χρήστη. Επιπλέον, το επιθυμητό σχέδιο μετάδοσης πρέπει να είναι ευέλικτο ώστε να επιτρέψει αναθέσεις οποιασδήποτε ζώνης σε οποιοδήποτε χρήστη, και κλιμακωτό σε σχέση με τον αριθμό χρηστών και ζωνών. Στην ιδανική περίπτωση, αυτή η ευέλικτη ευρείας ζώνης μετάδοση θα πραγματοποιούνταν μέσω ψηφιακής σύνθεσης κυματοειδούς περιοχών, όπου ένα σύνολο παραμέτρων διευκρινίζει τις ζώνες μετάδοσης και τον έλεγχο ισχύος. Στο **σχήμα 12** επεξηγεί την αρχιτεκτονική ενός ευρυζωνικού πομπού σημάτων. Η κύρια πρόκληση είναι να δημιουργηθεί ένα σήμα όπου, χωρίς εξωτερικά αναλογικά φίλτρα, αλλάζει προσαρμοστικά το κατειλημμένο εύρος ζώνης και δεν παρεμβάλλει σε άλλους ενεργούς αρχικούς χρήστες.



Σχήμα 12. Πομπός ΓΕ

Η σημασία της αξιόπιστης ανίχνευσης των αρχικών χρηστών έχει δύο πτυχές:

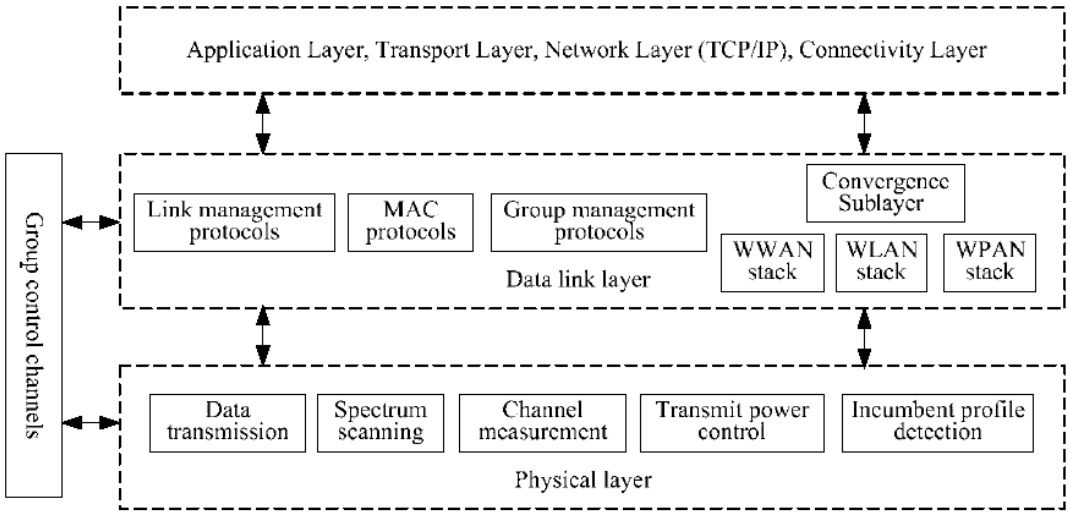
- εξασφαλίζει ότι τα CRs δεν θα παρεμποδίζουν τους αρχικούς χρήστες, το οποίο επιτρέπει τη δευτεροβάθμια χρήση του φάσματός τους
- δημιουργεί ευκαιρίες φάσματος για την αύξηση της χωρητικότητας των δικτύων ΓΕ.

Προκειμένου να πραγματοποιηθεί αυτή η λειτουργία, τα συστήματα ΓΕ πρέπει να έχουν σημαντικά καλύτερη ευαισθησία και ευφυΐα στις ευρυζωνικές συχνότητες απ' ότι

τα συμβατικά radios. Επομένως, μια εφαρμογή της αντίληψης φάσματος απαιτεί καινούριο σχεδιασμό όχι μόνο των κυκλωμάτων ευρείας ζώνης RF/analog, αλλά και τεχνικές ψηφιακής επεξεργασίας σήματος και συνεργασία δικτύων προκειμένου να καλυφθούν τέτοιες προκλητικές απαιτήσεις.

3.6 Ιεραρχία Πρωτοκόλλων

Σε ένα σύστημα ΓΕ τα στρώματα που συγκεντρώνουν το μεγαλύτερο ενδιαφέρον είναι αυτά που σχετίζονται με την διαχείριση φάσματος, δηλαδή το φυσικό στρώμα (physical layer) και το στρώμα ζεύξης δεδομένων (data link layer). Στο **σχήμα 13** παρουσιάζονται τα δύο κατώτερα στρώματα της στοίβας πρωτοκόλλων.



Σχήμα 13. Φυσικό Στρώμα και Στρώμα Σύνδεσης Δεδομένων σε ένα σύστημα ΓΕ

Όπως παρατηρούμε στην παραπάνω εικόνα στα πλαίσια του φυσικού στρώματος επιτελούνται οι εξής λειτουργίες:

- **Ανίχνευση του φάσματος** (Spectrum Scanning): Αποτελεί την πλέον βασική λειτουργία του φυσικού στρώματος ενός συστήματος ΓΕ. Ένα μεγάλο εύρος συχνοτήτων σαρώνεται και αναλύεται στο πεδίο της συχνότητας, του χώρου και του χρόνου. Όπως έχει ήδη αναφερθεί, τα αποτελέσματα της ανίχνευσης πολλές φορές ανταλλάσσονται μεταξύ των σταθμών ενός δικτύου ΓΕ.
- **Μέτρηση του καναλιού** (Channel Measurement): Πραγματοποιούνται μετρήσεις με στόχο να καθοριστεί η ποιότητα των διαύλων. Με βάση τις μετρήσεις αυτές θα ρυθμιστούν στη συνέχεια οι διάφορες παράμετροι του συστήματος ΓΕ, όπως π.χ. ο ρυθμός συμβόλων (bit rate) και η ισχύς μετάδοσης.
- **Μετάδοση των δεδομένων** (Data Transmission): Στα πλαίσια της μετάδοσης επιτελούνται λειτουργίες όπως η επιλογή του ρυθμού μετάδοσης, της τεχνικής διαμόρφωσης, της τιμής της ισχύος εκπομπής και της τεχνικής κωδικοποίησης που ενδεχομένως θα χρησιμοποιηθεί. Μπορεί επίσης να γίνει χρήση της OFDM τεχνικής αλλά και μηχανισμών MIMO (multiple-input multiple-output, πολλαπλών-εισόδων πολλαπλών-εξόδων).

- **Έλεγχος ισχύος εκπομπής** (TPC – Transmit Power Control): Χρησιμοποιείται για την αποφυγή παρεμβολών και την άσκοπη κατανάλωση ενέργειας των φορητών συσκευών.
- **Επικείμενη ανίχνευση προφίλ** (IDP – Incumbent Profile Detection)

Παράλληλα, παρατηρούμε ότι στο στρώμα ζεύξης δεδομένων περιλαμβάνονται οι εξής λειτουργίες:

- **Πρωτόκολλα Διαχείρισης Ομάδων** (Group Management Protocols): Κάθε χρήστης ΓΕ ανήκει σε μια ομάδα χρηστών που σχηματίζει ένα δευτερεύον δίκτυο. Τα πρωτόκολλα διαχείρισης ομάδων χρησιμοποιούνται για να συντονίσουν όλους τους χρήστες που ανήκουν στην ίδια ομάδα. Κάθε νέος χρήστης που εισέρχεται στην ομάδα θα πρέπει να λάβει όλες τις απαραίτητες πληροφορίες που αφορούν την ομάδα αυτή μέσω των πρωτοκόλλων.
- **Πρωτόκολλα Διαχείρισης Ζεύξης** (Link Management Protocols): Τα πρωτόκολλα αυτά φροντίζουν για την εγκατάσταση και της συντήρηση της ζεύξης μεταξύ δύο χρηστών ΓΕ.
- **Πρωτόκολλα MAC** (Medium Access Control, Ελέγχου Πρόσβασης στο Μέσο): Ελέγχουν την πρόσβαση των χρηστών στο φυσικό μέσο.
- **Υπόστρωμα Σύγκλισης** (Convergence Sublayer): Το υπόστρωμα αυτό δίνει τη δυνατότητα στο σύστημα ΓΕ να λειτουργεί σε εντελώς διαφορετικά ασύρματα περιβάλλοντα όπως π.χ. Ασύρματα Τοπικά Δίκτυα (WLANs), Ασύρματα Προσωπικά Δίκτυα (WPANs) και Ασύρματα Δίκτυα Ευρείας Περιοχής (WWANs).

3.7 Λειτουργίες CR

3.7.1 Ανίχνευση Φάσματος

Μία από τις κύριες απαιτήσεις των γνωστικών δικτύων είναι η ικανότητά τους να σαρώνουν τη φασματική ζώνη και να εντοπίζουν τα κενά των καναλιών που διατίθενται για ευκαιριακή μετάδοση. Καθώς ο αρχικός χρήστης του δικτύου είναι φυσικά διαχωρισμένος από το δευτερεύον δίκτυο χρηστών, οι δευτερογενείς χρήστες δεν παίρνουν καμία άμεση ανατροφοδότηση από χρήστες σχετικά με τη μετάδοσή τους. Οι δευτερεύοντες χρήστες πρέπει να εξαρτώνται από τη δική τους ατομική ή συνεργατική ικανότητα ανίχνευσης για τον εντοπισμό πρωτογενούς μετάδοσης χρήστη. Δεδομένου ότι οι αρχικοί χρήστες μπορεί να εξαπλωθούν σε μια τεράστια γεωγραφική περιοχή, η ανίχνευση του συνόλου της φασματικής ζώνης είναι ένα δύσκολο έργο (βλ. [15],[16]). Οι δευτερεύοντες χρήστες πρέπει να βασίζονται σε αδύναμα πρωτογενή σήματα μετάδοσης για να αξιολογήσουν την παρουσία τους. Το μεγαλύτερο μέρος της έρευνας σχετικά με τις τεχνικές ανίχνευσης ραδιοφάσματος εμπίπτει σε τρεις κατηγορίες: την ανίχνευση του πομπού, την συνεργατική ανίχνευση και τη παρέμβαση με βάση την ανίχνευση (βλ. [17]) . Ο κύριος στόχος όλων αυτών των τεχνικών είναι να αποφευχθούν οι παρεμβολές στις πρωτογενείς μεταδόσεις. Η ποσότητα της παρεμβολής που προκαλείται από όλους τους δευτερεύοντες χρήστες σε ένα σημείο στο διάστημα αναφέρεται ως θερμοκρασία παρεμβολής , σε εκείνο το σημείο (βλ. [18]). Όταν ένας πρωτογενής χρήστης μετάδοσης λαμβάνει χώρα, η θερμοκρασία παρεμβολής πρέπει να είναι κάτω από ένα συγκεκριμένο επίπεδο κοντά στους πρωτογενείς δέκτες. Ωστόσο, αυτό δεν είναι εύκολο να επιτευχθεί, καθώς η θέση του

πρωτογενούς δέκτη δεν είναι γνωστή στους δευτερεύοντες χρήστες. Επιπλέον, όταν επικαλύπτονται πολλαπλά δευτερεύοντα δίκτυα, οι δευτερεύοντες χρήστες που σαρώνουν το φάσμα δεν θα πρέπει να συγχέουν μεταδόσεις από δευτερεύοντες χρήστες σε άλλα δευτερεύοντα δίκτυα με πρωτεύον μεταδόσεις.

3.7.2 Ανάλυση Φάσματος και Απόφαση

Κάθε ζώνη του φάσματος έχει μερικά μοναδικά χαρακτηριστικά λόγω της περιοχή συχνοτήτων της και του αριθμό των χρηστών (τόσο των αρχικών όσο και δευτερευόντων) που χρησιμοποιούν τη ζώνη. Η ευαισθησία του φάσματος καθορίζει έναν κατάλογο ζωνών του φάσματος που είναι διαθέσιμες. Ωστόσο, οι δευτερεύοντες χρήστες αποφασίζουν για την πλέον κατάλληλη ζώνη από τη λίστα των διαθέσιμων ζωνών. Εκτός από την κοινώς χρησιμοποιούμενη παράμετρο SNR, μερικά από τα χαρακτηριστικά των ζωνών φάσματος (συχνοτήτων) που μπορούν να χρησιμοποιηθούν για να αξιολογηθεί η αποτελεσματικότητά τους είναι η παρεμβολή, η απώλεια διαδρομής, τα σφάλματα ασύρματου δεσμού, η καθυστέρηση του στρώματος ζεύξης καθώς και ο χρόνος αναμονής (αναμενόμενη διάρκεια που ο δευτερεύον χρήστης μπορεί να καταλάβει τη συχνότητα).

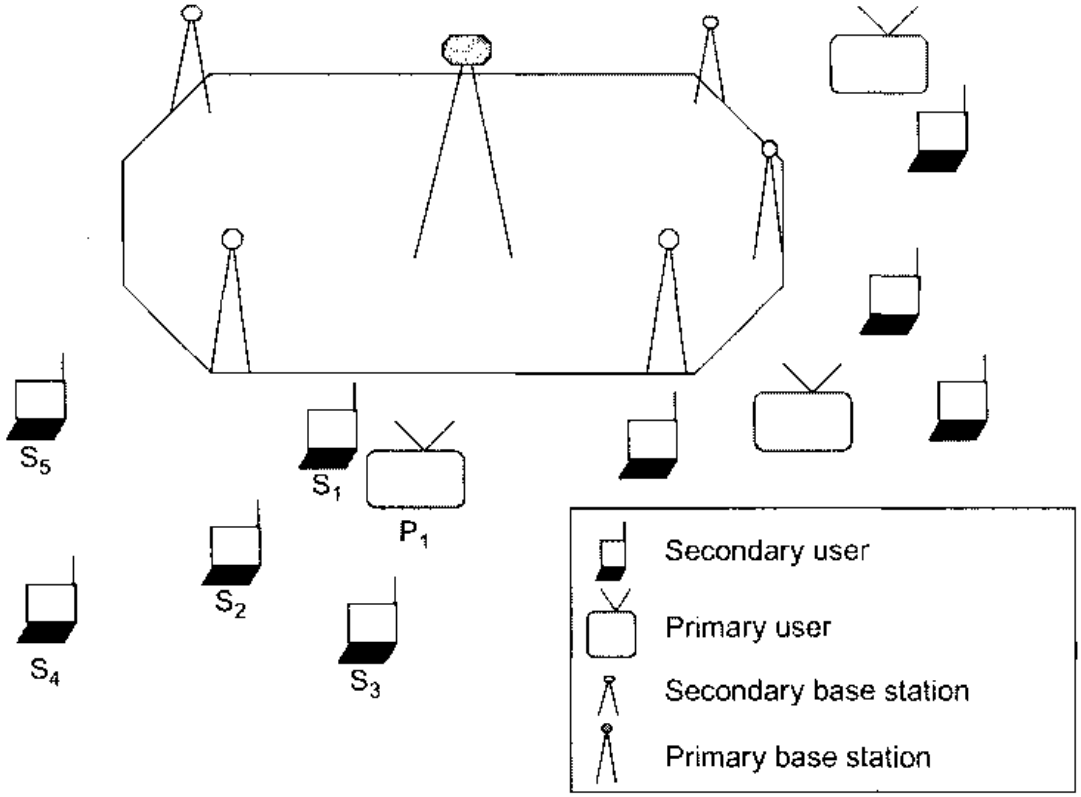
3.7.3 Κινητικότητα Φάσματος

Η κινητικότητα φάσματος αναφέρεται στην ευελιξία των συστημάτων ΓΕ σε δυναμική εναλλαγή μεταξύ πρόσβασης του ραδιοφάσματος. Καθώς οι δευτερεύοντες χρήστες δεν είναι πιστοποιημένοι σε συνεχή πρόσβαση στη συχνότητα σε οποιαδήποτε από τις επιτρεπόμενες ζώνες και η διαθεσιμότητα των κενών φασματικών ζωνών αλλάζει συχνά με την πάροδο του χρόνου, η κινητικότητα του φάσματος γίνεται ένας σημαντικός παράγοντας κατά το σχεδιασμό των πρωτοκόλλων ΓΕ. Ένας από τους κύριους παράγοντες που επηρεάζουν την κινητικότητα του φάσματος είναι η καθυστέρηση που σημειώνετε κατά την μεταβίβαση του φάσματος. Αυτή η καθυστέρηση επηρεάζει αρνητικά τα πρωτόκολλα που χρησιμοποιούνται σε διάφορα στρώματα της στοίβας πρωτοκόλλου επικοινωνίας. Ένας άλλος σημαντικός παράγοντας που πρέπει να εξεταστεί στην κινητικότητα του φάσματος είναι η διαφορά χρόνου μεταξύ του δευτερεύοντος δικτύου που ανιχνεύει μια πρωτογενή μετάδοση και των δευτερευόντων χρηστών που εκκενώνουν την φασματική ζώνη. Μεταδόσεις από τους δευτερεύοντες χρήστες κατά τη διάρκεια αυτής της περιόδου θα προκαλέσουν επιβλαβείς παρεμβολές στους πρωτεύοντες χρήστες. Η FCC (βλ. [19]) έχει ορίσει ανώτατα όρια για τη διάρκεια εκπομπής φάσματος για να αποφευχθεί η παρατεταμένη παρέμβαση στους αρχικούς χρήστες.

3.8 Τύποι ΓΕ

3.8.1 Κεντρικά συστήματα ΓΕ

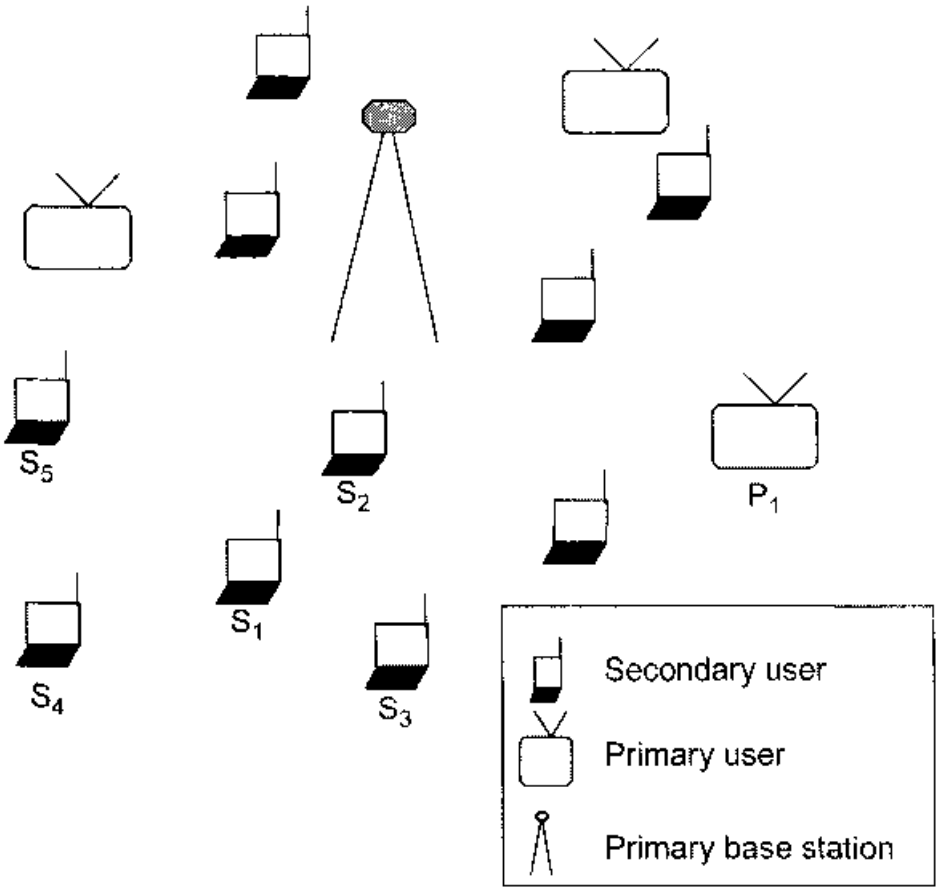
Σε μια κεντρική αρχιτεκτονική, ο δευτερεύων χρήστης δικτύου είναι μια προσανατολισμένη υποδομή. Δηλαδή, το δίκτυο διαιρείται σε κελιά. Κάθε κελί διαχειρίζεται μέσω ενός δευτερεύοντος σταθμού βάσης. Οι σταθμοί αυτοί βάσης ελέγχουν το μέσο πρόσβασης και τους δευτερεύοντες χρήστες, όπως φαίνεται στο **σχήμα 14**. Οι δευτερεύοντες χρήστες συγχρονίζονται με τους σταθμούς βάσης και μπορούν να εκτελούν τις λειτουργίες του περιοδικού φάσματος ανίχνευσης. Οι δευτερεύοντες σταθμοί βάσης μπορούν να διασυνδέονται μέσω ενός ενσύρματου δικτύου κορμού.



Σχήμα 14. Κεντρικά δίκτυα ΓΕ

3.8.2 Αποκεντρωμένα συστήματα ΓΕ

Σε μια αποκεντρωμένη αρχιτεκτονική, οι δευτερεύοντες χρήστες δεν διασυνδέονται μεταξύ τους με μια υποδομή-προσανατολισμένου δικτύου. Το **σχήμα 15** αντιπροσωπεύει ένα αποκεντρωμένο δίκτυο, όπου οι δευτερεύοντες χρήστες επικοινωνούν μεταξύ τους με ad-hoc τρόπο. Δύο δευτερεύοντες χρήστες που βρίσκονται εντός της εμβέλειας επικοινωνίας μπορούν να ανταλλάσσουν πληροφορίες άμεσα, ενώ οι δευτερεύοντες χρήστες που δεν βρίσκονται εντός εμβέλειας άμεσης επικοινωνίας μπορούν να ανταλλάσσουν πληροφορίες σε πολλαπλά πηδήματα hops.



Σχήμα 15. Αποκεντρωμένα δίκτυα ΓΕ

Στα κατανεμημένα συστήματα ΓΕ, οι δευτερεύοντες χρήστες αποφασίζουν σχετικά με τις ζώνες του φάσματος, την ισχύ εκπομπής, κλπ. βασιζόμενοι είτε σε τοπικές παρατηρήσεις, είτε σε συνεργασία με ορισμένες λειτουργίες βοηθητικού προγράμματος για να πάρουν τη βέλτιστη απόδοση για όλους τους δευτερεύοντες χρήστες. Για να παρουσιάσουμε τα βασικά στοιχεία μιας συνεργατικής προσέγγισης, εξετάζουμε το ακόλουθο παράδειγμα (βλ. **σχήμα 15**), όπου δύο δευτερεύοντες χρήστες (Si και S2) λειτουργούν σε μια επιτρεπόμενη ζώνη σε έναν πρωτεύοντα σταθμό βάσης. Si είναι στο όριο του εύρους μετάδοσης του πρωτογενούς σταθμού βάσης ενώ S2 είναι κοντά στον πρωτεύοντα σταθμό βάσης. Συνεπώς το S2 θα ανιχνεύσει την παρουσία των πρωτογενών χρηστών γρήγορα και εύκολα σε σύγκριση με Si. Συνεργατικές τεχνικές ανίχνευσης υπογραμμίζουν το γεγονός ότι αν οι δευτερογενείς χρήστες μοιράζονται πληροφορίες σε σχέση με τους ανιχνευτές, τότε η συνολική πρωτογενή ανίχνευση χρήστη για το σύστημα ΓΕ μπορεί να βελτιωθεί. Ωστόσο, αυτά τα πρωτόκολλα δεν θεωρούνται κακόβουλοι χρήστες στο δίκτυο. Αργότερα θα δούμε ότι συνεργαζόμενα πρωτόκολλα μπορούν να χρησιμοποιηθούν από κακόβουλους χρήστες για να προκαλέσουν παραβιάσεις της ασφάλειας των συστημάτων ΓΕ.

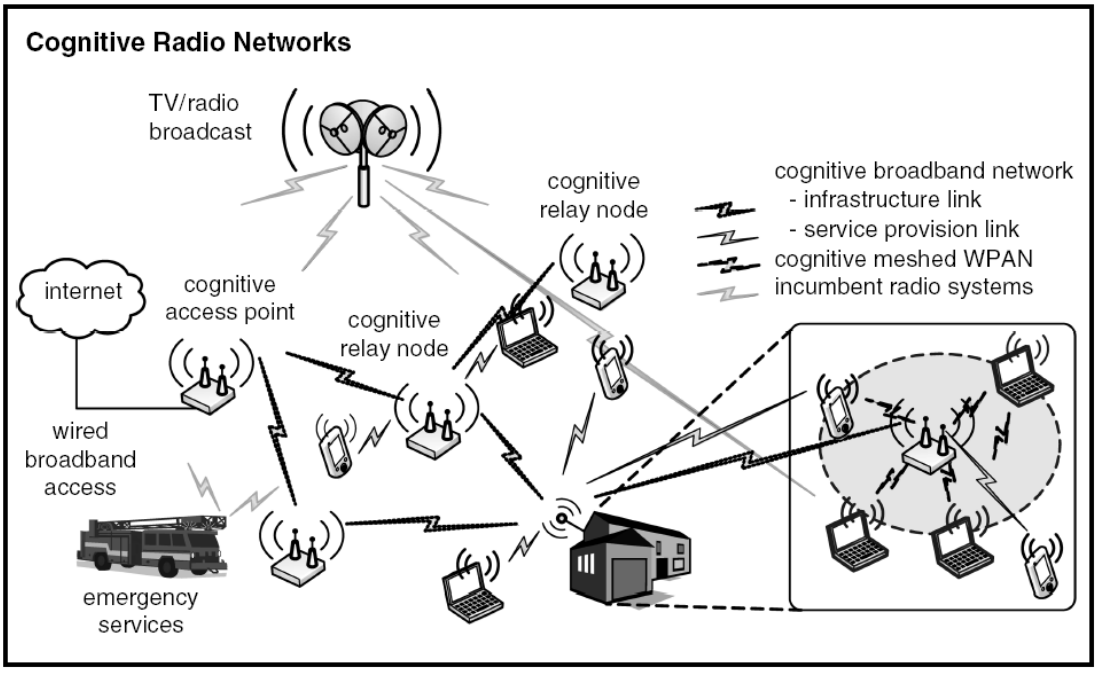
Μια υποκατηγορία των αποκεντρωμένων συστημάτων ΓΕ είναι τα δίκτυα μερισμού φάσματος, όπου δύο ασύρματα δίκτυα συνυπάρχουν σε μια ζώνη χωρίς άδεια(βλ. [20]). Ένα παράδειγμα ενός τέτοιου δικτύου είναι η συνύπαρξη του IEEE 802.11 και 802.16 (βλ. [21]). Σε τέτοια δίκτυα, ένα κοινό κανάλι συντονισμού του φάσματος είναι

εγκατεστημένο για την ανταλλαγή πληροφοριών σχετικά με τις παραμέτρους ελέγχου του πομπού και του δέκτη. Η ταυτοποίηση των αρχικών χρηστών, η κινητικότητα φάσματος και διαχείριση λειτουργιών δεν είναι απαραίτητη σε αυτές τις κατηγορίες δικτύων.

3.9 Δίκτυα CR και τα χαρακτηριστικά τους

Ορισμός. Πολλά συστήματα ΓΕ που επικοινωνούν μεταξύ τους συγκροτούν ένα *Δίκτυο Γνωστικών Συστημάτων Ραδιοεπικοινωνιών* (Cognitive Radio Network). Το δίκτυο αποτελείται από τερματικά συστήματα ΓΕ, τα οποία μπορεί να είναι είτε σταθερά είτε κινητά. Τα τερματικά έχουν την ικανότητα να ανιχνεύουν το φάσμα των ραδιοσυχνοτήτων και να προσαρμόζουν κατάλληλα τη συχνότητα λειτουργίας. Ως εκ τούτου, το δίκτυο λειτουργεί κατά βάση οπορτουνιστικά, ανιχνεύοντας φασματικές οπές και αξιοποιώντας τις. Όσον αφορά την ανίχνευση του φάσματος, υπάρχουν δύο επικρατούσες τάσεις στην επιστημονική κοινότητα σήμερα. Η πρώτη υποστηρίζει τη χρήση αυτόνομων τεχνικών ανίχνευσης ενώ η δεύτερη τη συνεργασία των σταθμών για την οικοδόμηση μιας κοινής βάσης δεδομένων που να περιέχει πληροφορίες σχετικές με τη χρήση του φάσματος.

Η περιοχή κάλυψης του δικτύου μπορεί να επεκταθεί αν δημιουργηθεί η κατάλληλη υποδομή με τη χρήση *Γνωστικών Σημείων Πρόσβασης* (Service Access Points, CAPs) και *Γνωστικών Κόμβων Αναμετάδοσης* (Cognitive Relay Nodes, CRNs) . Στο παρακάτω **σχήμα 16** παρουσιάζεται ένα σύνολο από Δίκτυα ΓΕ .



Σχήμα 16. Δίκτυα ΓΕ

Παρατηρούμε την ύπαρξη ενός Γνωστικού Σημείου Πρόσβασης το οποίο συνδέεται ενσύρματα με το Internet. Επίσης, μία σειρά από Γνωστικούς Κόμβους Αναμετάδοσης επεκτείνουν το δίκτυο σε μία ευρεία περιοχή. Ένα υποδίκτυο ΓΕ στο κάτω δεξιά μέρος

της εικόνας συνδέεται με το κυρίως δίκτυο υποδομής μέσω των κόμβων αναμετάδοσης και λειτουργεί οπορτουνιστικά. Συγκεκριμένα, οι σταθμοί του υποδικτύου μπορούν να ανιχνεύουν το φάσμα και να καταλαμβάνουν τις ζώνες που δε χρησιμοποιούνται από τα πρωτεύοντα δίκτυα, τα οποία στη συγκεκριμένη περίπτωση είναι ένα δίκτυο μετάδοσης σημάτων τηλεόρασης και ένα δίκτυο υπηρεσιών έκτακτης ανάγκης.

Ένα σωστά δομημένο και πετυχημένο δίκτυο ΓΕ διαθέτει τα ακόλουθα χαρακτηριστικά:

- Αυτό-διάρθρωση (Self-Configuration). Τα CAPs και τα CRNs εγκαθίστανται αυτόματα αμέσως μόλις τεθούν σε λειτουργία και ο χρήστης δεν παρεμβαίνει στη διαδικασία της διάρθρωσης τους. Επίσης, μπορούν να κατεβάζουν (download) αυτόματα τις τελευταίες ενημερώσεις του λογισμικού τους και να ανακάμπτουν μόνα τους από ενδεχόμενη κατάρρευση.
- Χαμηλή Κατανάλωση Ισχύος: Η στοίβα των πρωτοκόλλων και γενικά όλες οι λειτουργίες των συστημάτων ΓΕ θα πρέπει να έχουν σχεδιαστεί ώστε να καταναλώνουν όσο το δυνατόν μικρότερη ισχύ. Έτσι, θα είναι δυνατή η μεταφερσιμότητα των συσκευών.
- Υλικό μικρό σε μέγεθος. Τα CAPs και τα CRNs είναι μικρές και διακριτικές συσκευές που μπορούν να στηθούν σε τοίχους, ενώ τα κινητά τερματικά έχουν αρκετά μικρό μέγεθος ώστε να εξασφαλίζεται η μεταφερσιμότητά τους.
- Υλικό χαμηλού κόστους: Ακόμα και οι συσκευές CAP και CRN δεν ξεπερνούν σε κόστος τα 100 δολάρια.
- Διαφάνεια προς το χρήστη

3.10 Δυναμική εκχώρηση φάσματος (DSA)

Η δύναμη των Cognitive Radios έγκειται στην ικανότητά τους να αναγνωρίζουν την ύπαρξη φασματικών οπών και να λειτουργούν σε αδειοδοτημένες ζώνες συχνοτήτων, όταν αυτές δε χρησιμοποιούνται από τα αντίστοιχα πρωτεύοντα συστήματα. Τα συστήματα ΓΕ μπορούν να εντοπίζουν την ύπαρξη τέτοιων ζωνών, να τις καταλαμβάνουν και να τις αποδεσμεύουν δυναμικά, ανάλογα με τη συμπεριφορά των πρωτευόντων συστημάτων. Αυτός ο πανίσχυρος μηχανισμός μπορεί να περιγραφεί συνοπτικά με τον όρο *Δυναμική Εκχώρηση Φάσματος* (Dynamic Spectrum Access, DSA).

Ορισμός. Ορίζουμε ως Δυναμική Πρόσβαση στο Φάσμα την τεχνολογία εκείνη που επιτρέπει τη χρήση υπο-χρησιμοποιούμενων αδειοδοτημένων ζωνών συχνοτήτων με την προϋπόθεση ότι δεν εισάγονται παρεμβολές στα αδειοδοτημένα συστήματα. Η λέξη «Δυναμική» χρησιμοποιείται για να αποδώσει τα εξής δύο χαρακτηριστικά:

- η πρόσβαση ενός τερματικού Χ σε μια αδειοδοτημένη ζώνη γίνεται μόνο εφόσον διαπιστωθεί ότι αυτή είναι ελεύθερη τη συγκεκριμένη χρονική στιγμή
- αν ο πρωτεύων χρήστης θελήσει να κάνει χρήση των δικαιωμάτων του, ο Χ θα πρέπει να αποδεσμεύσει τη ζώνη

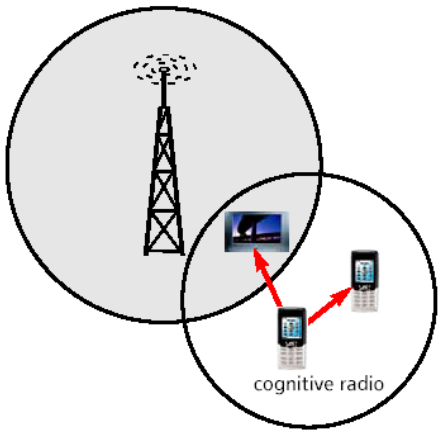
Το κύριο χαρακτηριστικό των DSA συστημάτων είναι η ικανότητά τους να εκμεταλλεύονται τη γνώση που έχουν για το ηλεκτρομαγνητικό περιβάλλον τους για να προσαρμόσουν κατάλληλα τη λειτουργία τους και την πρόσβασή τους στο φάσμα. Είναι λοιπόν εμφανές ότι ένα σύστημα ΓΕ είναι κατά βάση και DSA σύστημα. Τα DSA συστήματα επιτυγχάνουν την αποτελεσματική αξιοποίηση του φάσματος σε κάθε του διάσταση (χρόνο, χώρο, συχνότητα, κώδικα).

Τα δίκτυα DSA συστημάτων μπορούν να διακριθούν σε τρεις κύριες κατηγορίες, οι οποίες αναλύονται διεξοδικά στη συνέχεια.

3.10.1 Αυτόνομα DSA δίκτυα

Εδώ τα τερματικά ΓΕ που αποτελούν το δίκτυο λειτουργούν αυτόνομα, ενώ το ίδιο το δίκτυο μπορεί να σχηματιστεί από μόνο του, χωρίς εξωτερική παρέμβαση. Η βασική ιδέα είναι η εξής: κάθε συσκευή ΓΕ ανιχνεύει το φάσμα που επιθυμεί να χρησιμοποιήσει και διαπιστώνει την πιθανή παρουσία πρωτευόντων χρηστών ή άλλων συσκευών ΓΕ. Με βάση το αποτέλεσμα της ανίχνευσης, η συσκευή αναγνωρίζει τις φασματικές ευκαιρίες και μεταδίδει προσπαθώντας να αποφύγει να εισάγει παρεμβολές τόσο στους πρωτεύοντες όσο και σε γειτονικούς δευτερεύοντες χρήστες. Η ανίχνευση γίνεται ανεξάρτητα και αυτόνομα από τον κάθε σταθμό. Η εν λόγω λειτουργία θα πρέπει φυσικά να υπακούει σε κανονισμούς που έχουν τεθεί από τους διεθνείς φορείς και οι οποίοι διασφαλίζουν τη δίκαια κατανομή του φάσματος.

Η ανίχνευση των φασματικών οπών δεν είναι εύκολη υπόθεση, όπως έχουμε ήδη δει. Διαφορετικοί τύποι πρωτευόντων χρηστών απαιτούν διαφορετικές μεθόδους ανίχνευσης. Γενικά, η ευαισθησία των συστημάτων ΓΕ θα πρέπει να είναι πολύ μεγάλη ώστε να αποφεύγεται το πρόβλημα των κρυμμένων τερματικών. Μια απεικόνιση του προβλήματος των κρυμμένων τερματικών για DSA συστήματα φαίνεται στο **σχήμα 17**. Όπως βλέπουμε στην εικόνα, ένας πρωτεύον τηλεοπτικός δέκτης βρίσκεται στην εμβέλεια του συστήματος ΓΕ. Το σύστημα ΓΕ δε δύναται να ανιχνεύσει τη μετάδοση του τηλεοπτικού πομπού κι έτσι διαπιστώνει λανθασμένα την ύπαρξη μιας φασματικής οπής, η οποία στην πραγματικότητα δεν υπάρχει. Το σύστημα ΓΕ θα ξεκινήσει έτσι να μεταδίδει και θα εισάγει παρεμβολές στον τηλεοπτικό δέκτη.



Σχήμα 17. Πρόβλημα κρυμμένων τερματικών σε DSA συστήματα

Αν και γενικά είναι προτιμότερο τα συστήματα ΓΕ να μπορούν να συντονίσουν μόνα τους την πρόσβαση στο φάσμα, υπάρχουν περιπτώσεις που τα πρωτεύοντα συστήματα βοηθούν. Αυτό μπορεί να γίνει π.χ. με τη χρησιμοποίηση σημάτων ραδιοφάρου (beacon signals). Σε μια τέτοια υλοποίηση, το πρωτεύον σύστημα εκπέμπει σήματα ραδιοφάρου μέσω των οποίων μπορεί να δώσει άδεια στα δευτερεύοντα συστήματα να χρησιμοποιήσουν συγκεκριμένες ζώνες συχνοτήτων ή να τους απαγορέψει την πρόσβαση σε αυτές. Με τον τρόπο αυτό, τα συστήματα ΓΕ δε χρειάζεται να ανιχνεύουν το φάσμα. Το σενάριο που περιγράψαμε μπορεί να εμφανίσει προβλήματα αξιοπιστίας, καθώς τα CRs μπορεί να μη λάβουν ποτέ το σήμα ραδιοφάρου, ή μπορεί να το λάβουν και να μην το ερμηνεύσουν σωστά.

3.10.2 Συνεργατικά DSA δίκτυα

Μία εναλλακτική μορφή DSA δικτύων είναι αυτή στην οποία οι σταθμοί συνεργάζονται μεταξύ τους τόσο κατά τη φάση της ανίχνευσης του φάσματος όσο και κατά τη φάση της χρησιμοποίησής του. Η από κοινού ανίχνευση του φάσματος επιτυγχάνεται με τη βοήθεια ανταλλαγής πλαισίων συντονισμού. Ένα μειονέκτημα των συνεργατικών DSA δικτύων είναι το επιπλέον τηλεπικοινωνιακό φορτίο που εισάγει η χρήση των σχετικών πλαισίων συντονισμού. Τα εν λόγω δίκτυα είναι ιδανικά για την εφαρμογή της spectrum pooling τεχνικής, η οποία αναλύεται σε άλλη ενότητα.

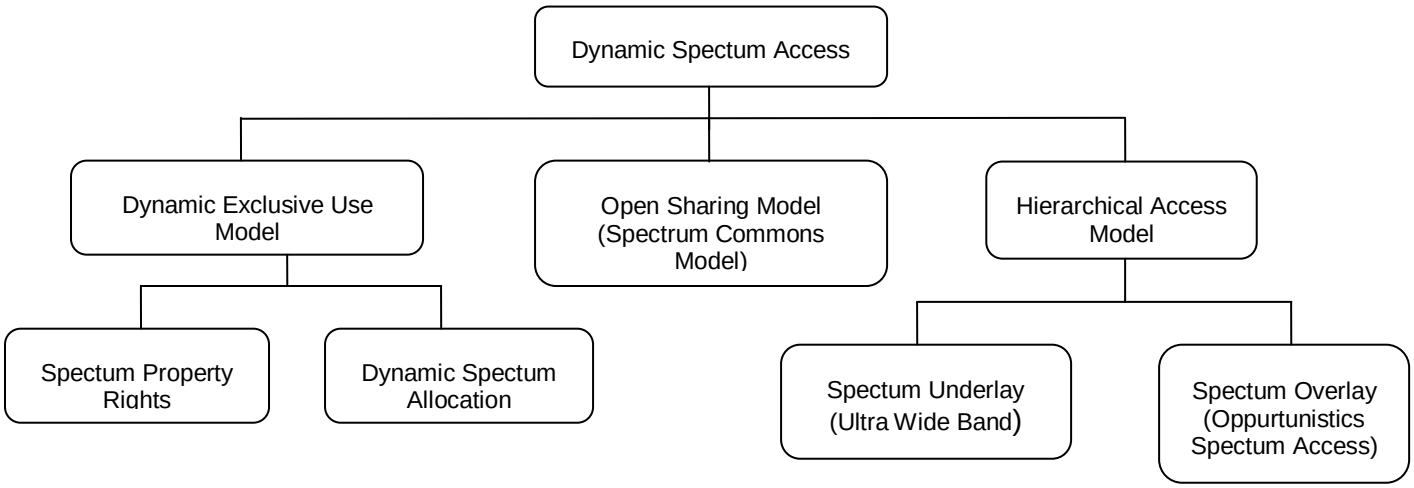
Διακρίνουμε δύο κατηγορίες συνεργατικών DSA δικτύων:

- Δίκτυα κεντρικά ελεγχόμενα. Εδώ υπάρχει ένα κεντρικός σταθμός βάσης – σημείο πρόσβασης. Τα ασύρματα τερματικά ΓΕ πραγματοποιούν διαρκώς ανίχνευση του φάσματος και μεταδίδουν τα αποτελέσματα της ανίχνευσής τους στο σημείο πρόσβασης. Στη συνέχεια, το σημείο πρόσβασης χρησιμοποιεί τις πληροφορίες αυτές και σε συνδυασμό με τις δικές του μετρήσεις προσδιορίζει με μεγαλύτερη βεβαιότητα την κατάσταση του καναλιού.
- Κατανεμημένα δίκτυα. Στην αρχιτεκτονική αυτή, τα τερματικά ΓΕ σχηματίζουν μια ομάδα και συντονίζονται μεταξύ τους, δεν υπάρχει δηλ. σημείο πρόσβασης

3.10.3 DSA δίκτυα με διαχειριστή

Στην αρχιτεκτονική αυτή πραγματοποιείται δυναμική πρόσβαση σε φάσμα το οποίο διαχειρίζονται οι ρυθμιστικές αρχές. Ένας φορέας είναι ο απόλυτος κάτοχος του φάσματος και έχει τη δυνατότητα να μισθώσει (νοικιάσει) τμήματα αυτού σε χρήστες για συγκεκριμένα χρονικά διαστήματα. Ερευνητές της Bell Labs πρότειναν την εφαρμογή της αρχιτεκτονικής αυτής σε κυψελωτά συστήματα τηλεπικοινωνιών. Δύο διαφορετικά μοντέλα έχουν προταθεί. Στο πρώτο και απλούστερο μοντέλο, μόνο ο διαχειριστής ενός δικτύου μπορεί να ζητήσει την ενοικίαση φάσματος. Στο δεύτερο και πολυπλοκότερο μοντέλο, τα τερματικά συμμετέχουν και αυτά στη διαδικασία μίσθωσης του φάσματος και μπορούν να ζητήσουν να τους εκχωρηθούν ζώνες συχνοτήτων για να επικοινωνήσουν. Μεταξύ των διαθέσιμων συχνοτήτων, υπάρχουν και ορισμένες συχνότητες που χρησιμοποιούνται για την ανταλλαγή πληροφοριών ελέγχου που αφορούν τη μίσθωση του φάσματος.

Σε αντίθεση με την τρέχουσα πολιτική διαχείρισης του ραδιοφάσματος, ο όρος δυναμική φασματική πρόσβαση περιλαμβάνει διάφορες προσεγγίσεις ρύθμισης του φάσματος. Όπως παρουσιάζεται και στο **σχήμα 18**, οι στρατηγικές δυναμικής εκχώρησης μπορούν να κατηγοριοποιηθούν σε τρία διαφορετικά επίπεδα.



Σχήμα 18. Ταξινόμηση στρατηγικών δυναμικής πρόσβασης στο φάσμα

- Μοντέλο Αποκλειστικής Δυναμικής Χρήσης

Διατηρεί τη βασική δομή της υφιστάμενης πολιτικής ρύθμισης του φάσματος, όπου ζώνες συχνοτήτων αδειοδοτούνται σε υπηρεσίες για αποκλειστική χρήση. Η βασική ιδέα είναι η εισαγωγή ευελιξίας για βελτίωση της φασματικής απόδοσης. Δύο προσεγγίσεις έχουν προταθεί για αυτό το μοντέλο : φασματικά δικαιώματα ιδιοκτησίας και δυναμική κατανομή φάσματος. Η πρώτη προσέγγιση επιτρέπει στους δικαιούχους (licensees-primary users) να εμπορεύονται το φάσμα και να επιλέγουν ελεύθερα την τεχνολογία. Η οικονομία και η αγορά , επομένως, θα διαδραματίσουν ένα σημαντικό ρόλο στην αποδοτικότερη χρησιμοποίηση του περιορισμένου αυτού πόρου.

Η δεύτερη προσέγγιση της δυναμικής κατανομής φάσματος διατυπώθηκε από το ευρωπαϊκό σχέδιο DRIVE (βλ. [13]). Στόχος της είναι η βελτίωση της αποτελεσματικής χρησιμοποίησης του φάσματος μέσω της δυναμικής εκχώρησης , αξιοποιώντας τα χωρικά και χρονικά στατιστικά κίνησης διαφόρων υπηρεσιών. Δηλαδή, για μια συγκεκριμένη περιοχή και για δεδομένο χρόνο, το φάσμα διατίθεται σε υπηρεσίες για αποκλειστική χρήση. Η εκχώρηση αυτή διαφέρει της τρέχουσας πολιτικής στις ταχύτερες αλλαγές κατανομής συχνοτήτων που απαιτούνται.

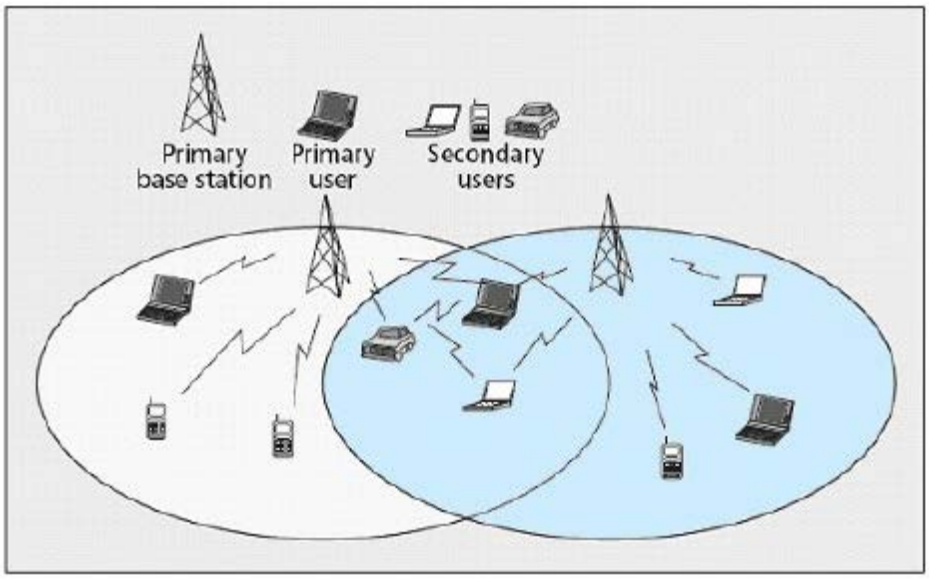
Ωστόσο, με βάση μόνο το μοντέλο αποκλειστικής χρήσης δεν είναι δυνατό να αντιμετωπιστούν και να αξιοποιηθούν τα λευκά φασματικά διαστήματα (white spaces) που προκύπτουν από την εκρηκτική φύση της ασύρματης τηλεπικοινωνιακής κίνησης

- Μοντέλο Ανοικτής Ανταλλαγής

Αναφέρεται επίσης και ως μοντέλο κοινού φάσματος και χρησιμοποιεί την ανοικτή ανταλλαγή φάσματος μεταξύ ομότιμων χρηστών ως βάση για την διαχείριση μιας φασματικής περιοχής. Οι υποστηρικτές του μοντέλου αυτού τάσσονται υπέρ της χρησιμοποίησής του λόγω της αδιαμφισβήτητης επιτυχίας των ασύρματων υπηρεσιών (π.χ. WiFi) που λειτουργούν στην μη αδειοδοτημένη βιομηχανική, επιστημονική και ιατρική μπάντα ραδιοσυχνοτήτων (ISM – Intustrial Scientific and Medical Radio Bands). Συγκεντρωτικές και κατανεμημένες στρατηγικές κατανομής φάσματος έχουν αρχικά διερευνηθεί για την αντιμετώπιση των τεχνολογικών προκλήσεων στο πλαίσιο του συγκεκριμένου μοντέλου διαχείρισης ραδιοφάσματος.

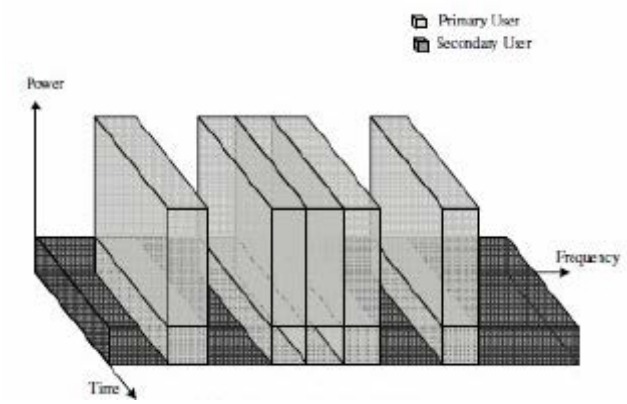
- Μοντέλο Ιεραρχικής Πρόσβασης

Το μοντέλο αυτό υιοθετεί μια ιεραρχική δομή πρόσβασης με πρωτεύοντες και δευτερεύοντες χρήστες. Η βασική ιδέα είναι η δυνατότητα χρησιμοποίησης αδειοδοτημένου φάσματος από δευτερεύοντες χρήστες εφόσον περιορίζονται επαρκών οι παρεμβολές που αντιλαμβάνονται οι πρωτεύοντες χρήστες (δικαιούχοι), όπως φαίνεται στο **σχήμα 19**.

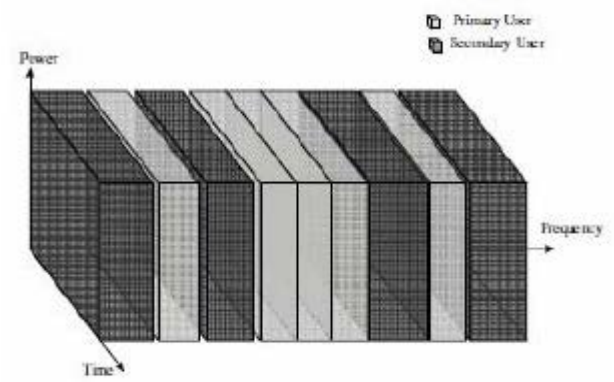


Σχήμα 19. Απεικόνιση δικτύων που ακολουθούν το μοντέλο ιεραρχικής πρόσβασης

Δύο προσεγγίσεις κατανομής καταμερισμού του φάσματος μεταξύ κύριων και δευτερευόντων χρηστών έχουν εξεταστεί : η *τεχνική φασματικής υπόστρωσης* (spectrum underlay) και η *τεχνική φασματικής επίστρωσης* (spectrum overlay) , όπως φαίνονται και στο **σχήμα 20 και 21**.



Σχήμα 20. Η προσέγγιση φασματικής υπόστρωσης (spectrum underlay)



Σχήμα 21. Η προσέγγιση φασματικής επίστρωσης (spectrum overlay)

Η προσέγγιση φασματικής υπόστρωσης επιβάλλει αυστηρούς περιορισμούς σχετικά με την ισχύ μετάδοσης των δευτερογενών χρηστών ώστε να λειτουργούν κάτω από το επίπεδο θορύβου των κύριων χρηστών. Με τη φασματική εξάπλωση των μεταδιδόμενων σημάτων σε μια ευρεία ζώνη ραδιοσυχνοτήτων (UWB), οι δευτερογενείς χρήστες μπορούν δυνητικά να πετυχαίνουν υψηλούς ρυθμούς μετάδοσης με εξαιρετικά χαμηλή ισχύ εκπομπής. Η δεύτερη προσέγγιση ιεραρχικής πρόσβασης (overlay approach) αρχικά επινοήθηκε από τον Mitola (βλ. [14]) υπό τον όρο συγκέντρωση φάσματος (spectrum polling) και στη συνέχεια ερευνήθηκε από τον οργανισμό προηγμένων ερευνητικών έργων του υπουργείου άμυνας των Ηνωμένων Πολιτειών (DARPA) και το πρόγραμμα «επόμενης γενιάς» με την ονομασία της ευκαιριακής φασματικής πρόσβασης (opportunistic spectrum access). Η διαφορά με την προηγούμενη προσέγγιση είναι ότι δεν υποβάλλει αναγκαστικά αυστηρούς περιορισμούς στην ισχύ εκπομπής των δευτερογενών χρηστών αλλά καθορίζει πότε και πού μπορούν αν εκπέμπουν. Η προσέγγιση αυτή στοχεύει άμεσα στα χρονικά και χωρικά φασματικά κενά διαστήματα (λευκά), επιτρέποντας στους δευτερογενείς χρήστες να αναγνωρίζουν και να αξιοποιούν τοπικές και στιγμιαίες φασματικές διαθεσιμότητες υπό την προϋπόθεση ότι δεν προκαλούν παρεμβολές σε αδειοδοτημένους χρήστες.

Συγκρινόμενο με τα υπόλοιπα μοντέλα της δυναμικής αποκλειστικής χρήσης και της ανοικτής ανταλλαγής, το μοντέλο της ιεραρχικής πρόσβασης είναι ίσως η πιο συμβατή προσέγγιση εφαρμογής της δυναμικής εκχώρησης συχνοτήτων, δεδομένης της τρέχουσας πολιτικής διαχείρισης του ραδιοφάσματος και της κληρονομιάς των ασύρματων συστημάτων. Επιπρόσθετα, οι δυο ξεχωριστές τεχνικές ιεραρχικής πρόσβασης μπορούν ενδεχομένως στο μέλλον να εφαρμοστούν συνδιαστικά για την περαιτέρω βελτίωση της φασματικής απόδοσης.

4 Γνωστικές επικοινωνίες και το πρωτόκολλο IEEE 802.22

4.1 Το πρωτόκολλο IEEE 802.22

Η Ομοσπονδιακή Επιτροπή Επικοινωνιών των Ηνωμένων Πολιτειών (FCC), που είναι υπεύθυνη για τη δέσμευση των συχνοτήτων στο φάσμα των ραδιοσυχνοτήτων, έχοντας υπόψη όλα τα παραπάνω, προχώρησε το Μάιο του 2004 σε μία πρόταση για τη θέσπιση κανόνων (Notice of Proposed Rule Making - NPRM) σύμφωνα με την οποία γινόταν δυνατή η χρήση των ραδιοσυχνοτήτων που χρησιμοποιούνται για τις τηλεοπτικές υπηρεσίες από μη αδειοδοτημένους χρήστες – συσκευές. Ο μόνος αυστηρός κανόνας που θα έπρεπε να τηρηθεί αφορούσε τη χρήση αυτή των ραδιοσυχνοτήτων από τους μη αδειοδοτημένους χρήστες-συσκευές, η οποία δε θα πρέπει να προκαλεί επιζήμιες παρεμβολές στους πρωτεύοντες χρήστες (Primary Users – PUs) των συχνοτήτων αυτών, δηλαδή στις μεταδόσεις των τηλεοπτικών σταθμών. Αυτό αποτελεί ένα θέμα μείζονος σημασίας, καθώς θα πρέπει να διασφαλιστεί η ποιότητα των υπηρεσιών των τηλεοπτικών σταθμών, οι οποίοι έχουν πληρώσει για να έχουν άδεια τηλεοπτικών μεταδόσεων.

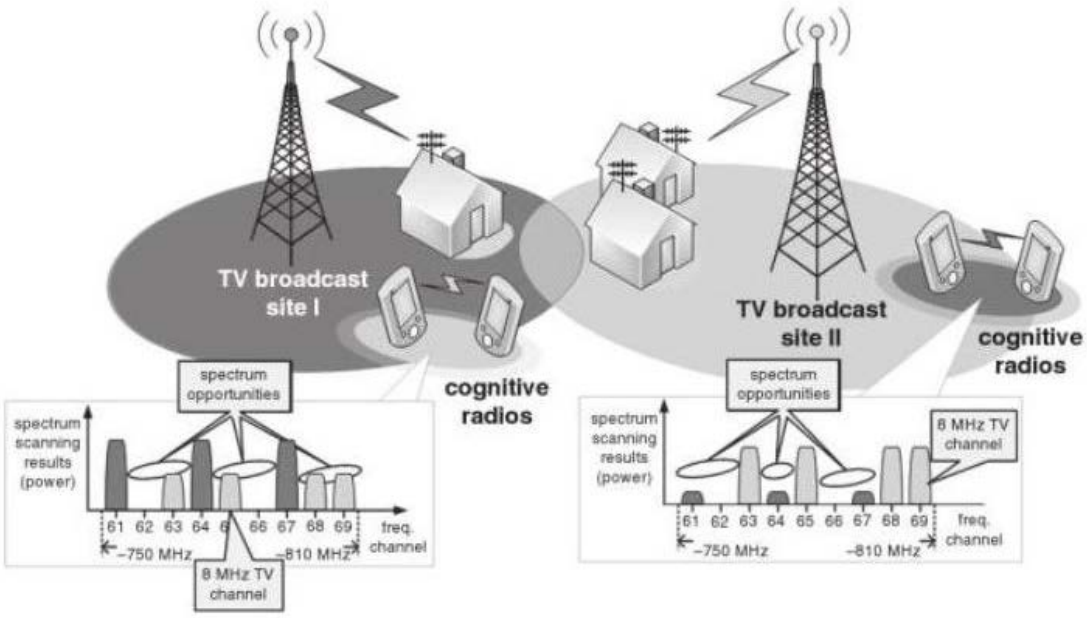
Η μερική μη αδειοδοτημένη χρήση των συχνοτήτων που χρησιμοποιούνται από τις τηλεοπτικές υπηρεσίες (οι συχνότητες μεταξύ 54 και 698MHz) οφείλεται σε δύο παράγοντες-κλειδιά :

- Στην πολύ χαμηλή χρήση των συγκεκριμένων συχνοτήτων σε πολλές περιοχές της υφηλίου. Αυτή η χαμηλή χρήση αναμένεται να γίνει ακόμα μικρότερη καθώς η αναλογική τηλεόραση αναμένεται να αντικατασταθεί σταδιακά σε πολλές χώρες με την ψηφιακή. Οι εκπομπές της ψηφιακής τηλεόρασης είναι πιο ανεκτικές στις παρεμβολές, ενώ επιπλέον προκαλούν και λιγότερες παρεμβολές. Συνεπώς, το φάσμα των συχνοτήτων που θα χρησιμοποιείται από τις ψηφιακές μεταδόσεις αναμένεται να μειωθεί αρκετά. Για την παροχή της ίδιας ποιότητας υπηρεσιών η χρήση του φάσματος θα είναι 4 φορές μικρότερη. Συγκεκριμένα, στις Ηνωμένες Πολιτείες αναμένεται να ελευθερωθούν 108 MHz φάσματος από αυτή τη «συμπίεση» των τηλεοπτικών καναλιών, ενώ στο Βερολίνο, που έχει ήδη συμβεί, ελευθερώθηκαν 35 MHz, που αναμένεται φυσικά να αδειοδοτηθούν για διαφορετική χρήση. Όσον αφορά το φάσμα που ελευθερώθηκε στις Ηνωμένες Πολιτείες, θεωρείται αρκετά μεγάλο, αν αναλογιστεί κάποιος ότι το σύνολο της χρήσης των ραδιοσυχνοτήτων AM στις Ηνωμένες Πολιτείες είναι μόλις 1.2 MHz, ενώ όλα τα τοπικά ασύρματα δίκτυα που χρησιμοποιούν τα πρωτόκολλα IEEE 802.11 b/g απασχολούν 83.5 MHz.
- Ένα άλλο πολύ σημαντικό χαρακτηριστικό που έχουν οι συγκεκριμένες συχνότητες είναι τα ιδιαίτερα χαρακτηριστικά διάδοσής τους. Τα σήματα αυτά των συχνοτήτων μπορούν να διαδοθούν με μικρότερη ενέργεια σε μεγαλύτερες αποστάσεις, ενώ η διεισδυτικότητά τους στα κτίρια είναι μεγαλύτερη. Έτσι είναι δυνατή η μετάδοση, με (Line-of-sight - LOS) ή χωρίς οπτική επαφή με τον πομπό (Non-Line-of-Sight - NLOS), παρέχοντας τη δυνατότητα χρήσης πολύ λιγότερων αναμεταδοτών για να επιτευχθεί η κάλυψη των επιθυμητών περιοχών, γεγονός που παίζει ιδιαίτερα σημαντικό ρόλο στο κόστος λειτουργίας ενός συστήματος που χρησιμοποιεί αυτό το φάσμα (βλ. [54], [55]).

Έτσι λίγο μόλις καιρό μετά από αυτή την ανακοίνωση (το Νοέμβριο του 2004) η IEEE δημιούργησε μια ομάδα για να ορίσει ένα καινοτόμο πρωτόκολλο για ασύρματες τηλεπικοινωνίες, στο φυσικό επίπεδο (PHY) αλλά και στο επίπεδο πρόσβασης στο

μέσο (MAC), το οποίο θα βασιζόταν στην τεχνολογία του cognitive radio και θα χρησιμοποιούσε τις συχνότητες των τηλεοπτικών υπηρεσιών. Με αυτό τον τρόπο θα ήταν δυνατή η δημιουργία ασυρμάτων δικτύων μεγάλης εμβέλειας (Wireless Regional Area Network – WRAN) λόγω των χαρακτηριστικών των τηλεοπτικών συχνοτήτων που αναφέρθηκαν παραπάνω.

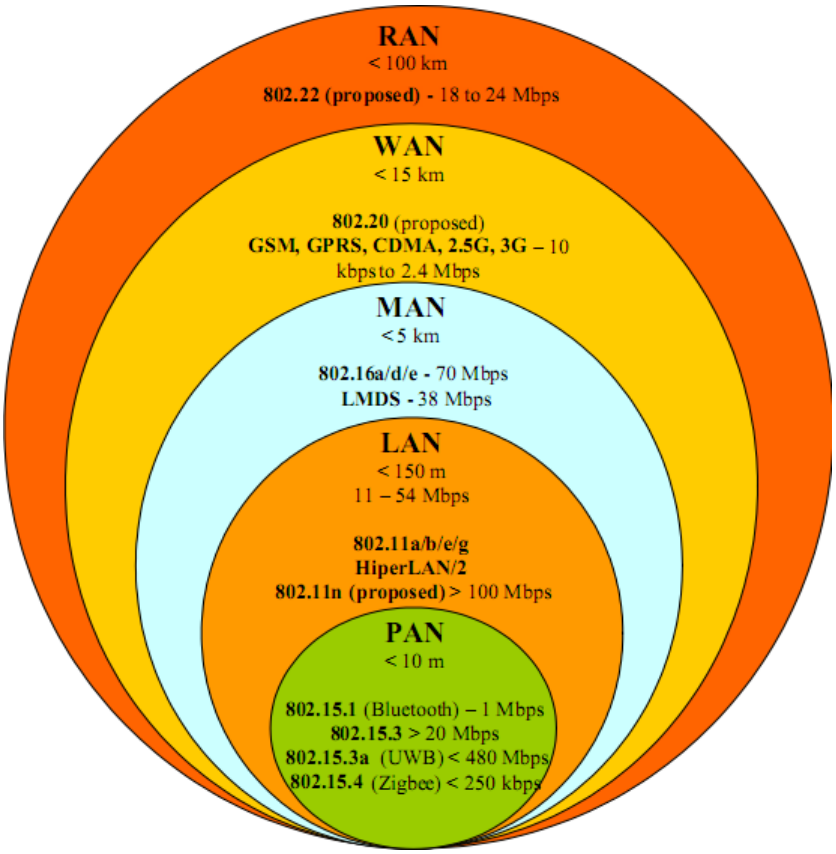
Βάσει των παραπάνω στοιχείων, η ερευνητική ομάδα του 802.22 στοχεύει στην προτυποποίηση της μη αδειοδοτημένης πρόσβασης στις τηλεοπτικές συχνότητες. Χαρακτηριστικό είναι το παράδειγμα στο **σχήμα 22**, στο οποίο παριστάνονται δύο παρακείμενες περιοχές εμβέλειας τηλεοπτικών σημάτων και δύο ζεύγη συσκευών που υλοποιούν το cognitive radio, ανεξάρτητα μεταξύ τους. Οι cognitive radio συσκευές εντοπίζουν τοπικά αχρησιμοποίητο φάσμα (τηλεοπτικές συχνότητες στην προκειμένη περίπτωση) θεωρώντας το υποψήφιο για μετάδοση (γνωστό και ως spectrum opportunities, όπως φαίνεται και στην παρακάτω εικόνα). Ύστερα από ανταλλαγή πληροφοριών, τα ζεύγη επικοινωνούν μεταξύ τους, χρησιμοποιώντας τις «ελεύθερες» συχνότητες, ενώ ελέγχουν το φάσμα σε τακτά χρονικά διαστήματα για την παρουσία σημάτων από πρωτεύοντες χρήστες(βλ. [56]).



Σχήμα 22. Συσκευές cognitive radio που λειτουργούν στο πεδίο των τηλεοπτικών συχνοτήτων. Σε διαφορετικές τοποθεσίες, οι συσκευές εντοπίζουν και διαφορετικές μη χρησιμοποιημένες συχνότητες.

4.1.1 Κίνητρα για την ανάπτυξη του πρωτοκόλλου

Το κίνητρο για την ανάπτυξη αυτού του πρωτοκόλλου είναι η κάλυψη περιοχών που είναι δυσπρόσιτες, και κυρίως μη αστικές περιοχές, με ευρυζωνικά δίκτυα, δεδομένου ότι τα κενά του φάσματος σε αυτές τις περιοχές είναι μεγαλύτερα. Χαρακτηριστικό είναι ότι σε πολύ μεγάλες περιοχές των Ηνωμένων Πολιτειών μεγάλο μέρος αυτού του φάσματος παραμένει αχρησιμοποίητο, λόγω της ευρείας χρήσης της δορυφορικής και της καλωδιακής τηλεόρασης. Ανάπτυξη τέτοιων συστημάτων μπορεί να γίνει και σε περιοχές αναπτυσσόμενων χωρών για τον ίδιο λόγο.



Σχήμα 23. Εμβέλειες διαθέσιμων πρωτοκόλλων ασυρμάτων δικτύων

Είναι γεγονός ότι η παροχή ευρυζωνικών υπηρεσιών θα ήταν ικανή να καλύψει μόνο τις ανάγκες μιας οικίας, μιας μικρής επιχείρησης ή για εργασία στο σπίτι. Η συγκεκριμένη τεχνολογία όμως μπορεί να αποτελέσει και τη βάση για την ανάπτυξη νέων ειδών επιχειρήσεων οι οποίες θα παρέχουν υπηρεσίες διαδικτύου μέσω ασύρματων δικτύων (Wireless Internet Service Providers). Τα έξοδα αυτών περιορίζονται αρκετά αν ληφθεί υπόψη και η μη αδειοδοτημένη χρήση του τηλεοπτικού φάσματος. Έτσι, απαλλάσσονται από τα έξοδα για αδειοδοτήσεις που πιθανόν να χρειάζονται (όπως στην περίπτωση του WiMAX). Όπως αναφέρθηκε και προηγουμένως, τα έξοδα περιορίζονται και από τον περιορισμένο εξοπλισμό που θα χρησιμοποιείται λόγω της μεγάλης εμβέλειας των συστημάτων (βλ. [57]).

4.1.2 Κανονιστικό πλαίσιο

Το πρωτόκολλο, εφόσον πραγματοποιεί μη αδειοδοτημένη χρήση των τηλεοπτικών συχνοτήτων για τις μεταδόσεις του, οφείλει να υπακούει στον μοναδικό και αυστηρό κανόνα, της μη επιβλαβούς παρενόχλησης των εκπομπών των μεταδόσεων των τηλεοπτικών σταθμών. Πέρα όμως από τους τηλεοπτικούς σταθμούς, υπάρχει και μια σειρά άλλων συσκευών και υπηρεσιών που χρησιμοποιούν και αυτές χωρίς άδεια τις ελεύθερες τηλεοπτικές συχνότητες. Αυτές είναι τα ασύρματα μικρόφωνα αλλά και υπηρεσίες σχετικές με τη δημόσια ασφάλεια αλλά και εφαρμογές μικρής εμβέλειας όπως η ασύρματη ενδοεπικοινωνία μέσα σε κάποια επιχείρηση. Σε κάθε περίπτωση όμως το σύνολο των υπηρεσίων που προαναφέρθηκαν αποτελούν τον πρωτεύον χρήστη αυτών των συχνοτήτων, με το πρωτόκολλο να είναι ο δευτερεύον χρήστης. Ο

χαρακτηρισμός των συσκευών αυτών ως πρωτευόντων χρηστών είναι λογικός, αν ληφθεί υπόψη το γεγονός πως οι συσκευές αυτές δεν έχουν δυνατότητα αλλαγής των χαρακτηριστικών της μετάδοσής τους.

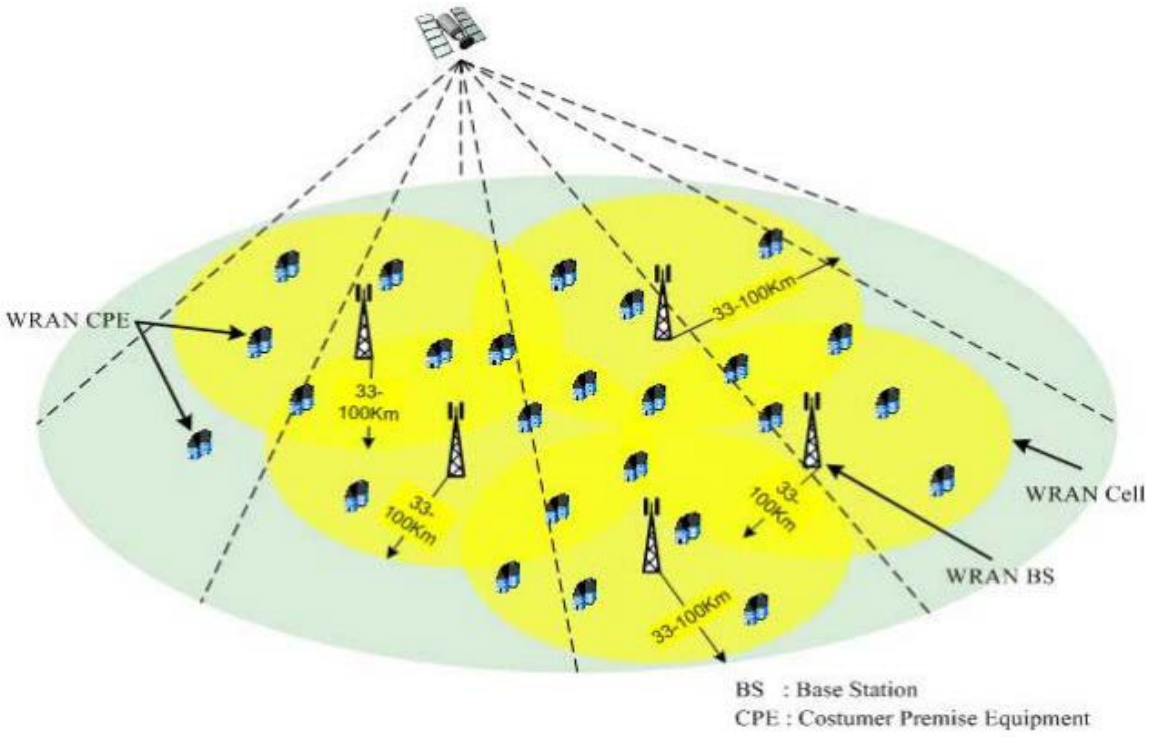
4.1.3 Χαρακτηριστικά του 802.22

4.1.3.1 Οντότητες του 802.22

Βασική μονάδα στο πρωτόκολλο 802.22 θεωρείται ο *Σταθμός Βάσης* (Base Station – BS). Είναι μια διάταξη η οποία θα εγκαθίσταται και θα συντηρείται από κάποιον επαγγελματία και είναι η συσκευή που είναι υπεύθυνη για όλο το δίκτυο το οποίο δημιουργεί με την παρουσία της. Αυτό το δίκτυο αλλιώς ονομάζεται και *κυψέλη* (cell). Κάθε κυψέλη αποτελείται από ένα σταθμό βάσης και από μία ή περισσότερες συσκευές πελατών οι οποίες είναι συσχετισμένες με αυτόν (Consumer Premise Equipments – CPE).

Ο σταθμός βάσης είναι αυτός που καθορίζει όλα τα χαρακτηριστικά λειτουργίας και μετάδοσης ενός δικτύου, αλλά και τη διαχείριση και το διαμοιρασμό του διαθέσιμου φάσματος στις συσκευές των πελατών. Τα κινητά τερματικά μπορούν να στείλουν δεδομένα μόνο στο σταθμό βάσης με τον οποίο είναι συσχετισμένα, στο χρόνο και με τα χαρακτηριστικά που έχουν καθοριστεί. Καμία συσκευή πελάτη δεν μπορεί να αποστείλει δεδομένα αν δεν έχει συσχετιστεί προηγουμένως με κάποιον σταθμό βάσης. Με αυτό τον τρόπο, δημιουργείται μια διεπαφή Σημείου προς πολλά Σημεία (Point-to-Multipoint – PMP) μεταξύ του σταθμού βάσης και των συσκευών των πελατών που έχουν συσχετιστεί με αυτόν.

Οι συσκευές των πελατών, πέρα από την αποστολή των δεδομένων, συμμετέχουν μαζί με το σταθμό βάσης στην ανίχνευση (sensing) για την ύπαρξη ή όχι πρωτευόντων χρηστών αλλά και άλλων δικτύων 802.22 στις συχνότητες που χρησιμοποιούνται για μετάδοση, σύμφωνα με οδηγίες που παίρνουν από αυτούς. Έτσι, οι σταθμοί βάσης με βάση τα δεδομένα που λαμβάνονται, φτιάχνουν μια βάση δεδομένων για το χάρτη κατοχής καναλιών. Αυτός ο χάρτης εμπλουτίζεται με πληροφορίες από βάσεις δεδομένων που αφορούν τη χρήση καναλιών στην περιοχή που βρίσκεται ο εκάστοτε σταθμός βάσης. Συνοψίζοντας, όλα τα παραπάνω, μπορεί να θεωρηθεί ότι η σχέση του σταθμού βάσης με τις συσκευές των πελατών είναι μία σχέση αφέντη – σκλάβου (master-slave). Όλες οι οντότητες που περιγράφτηκαν προηγουμένως παριστάνονται σχηματικά στο **σχήμα 24**.



Σχήμα 24. Πιθανό σενάριο ανάπτυξης ενός δικτύου 802.22

Μια ιδιαίτερη διαφορά που έχουν οι συσκευές των πελατών με το σταθμό βάσης αφορά το είδος και τον αριθμό των κεραιών που έχουν. Συγκεκριμένα, οι σταθμοί βάσης διαθέτουν μόνο μία κεραία, πανδιευθυντική (Omni-directional).Αντίθετα, οι συσκευές των πελατών διαθέτουν δυο είδη κεραίας, Μια κατευθυντική (directional), με την οποία γίνονται οι επικοινωνίες μεταξύ των συσκευών των πελατών και των σταθμών βάσης και μια πανδιευθυντική που χρησιμοποιείται για τον εντοπισμό των πρωτευόντων αλλά και των υπολοίπων δευτερευόντων χρηστών. Η χρήση της κατευθυντικής κεραίας περιορίζει τις απώλειες ενέργειας που μπορεί να υπάρξουν κατά την διάρκεια της επικοινωνίας μεταξύ των σταθμών βάσης και των συσκευών των πελατών, ενώ ελαχιστοποιείται παράλληλα και ο κίνδυνος συγκρούσεων (collision).Έτσι, καταναλώνεται η ελάχιστη δυνατή ενέργεια για τη μεταξύ τους επικοινωνία.

4.1.3.2 Κάλυψη

Όπως αναφέρθηκε και προηγουμένως, το πρωτόκολλο 802.22 προορίζεται να καλύπτει μεγάλες περιοχές. Η κάλυψη, όπως φαίνεται στο **σχήμα 24**, μπορεί να φτάσει στα 33km με ενέργεια εκπομπής τα 4 Watt EIRP(Equivalent Isotropically Radiated Power). Η κάλυψη αυτή μπορεί να επεκταθεί μέχρι τα 100km αν δεν τίθενται περιορισμοί, είτε όσον αφορά την κατανάλωση ενέργειας (καθώς θα είναι αυξημένη), είτε από παρεμβολές, λόγω της αυξημένης ενέργειας εκπομπής.

4.1.3.3 Δυνατότητες Υπηρεσιών

Στο 802.22 η απόδοση του φάσματος (spectral efficiency) προσδιορίζεται στο εύρος 0.5-5 bit/(s/Hz).Βάση του εύρος αυτού, αν οριστεί μια μέση τιμή για την απόδοση στα 3 bit/(s/Hz) και λαμβάνοντας υπόψη ότι το ελάχιστο εύρος των καναλιών είναι 6 MHz

(όσο είναι και το εύρος των καναλιών στις Ηνωμένες Πολιτείες), τότε ο ρυθμός μετάδοσης δεδομένων στο φυσικό επίπεδο (PHY) θα κυμαίνεται στα18 Mbps. Ο ρυθμός αυτός μπορεί να αυξηθεί ακόμα περισσότερο αν χρησιμοποιηθούν μεγαλύτερου εύρους, των 7 ή 8 MHz, φτάνοντας στη μέγιστη τιμή των 24 Mbps.Συνεπώς, αν υπάρχουν 12 συσκευές πελάτη συνδεδεμένες με ένα σταθμό βάσης, η ελάχιστη δυνατή κάλυψη μπορεί να επιτευχθεί με ένα ρυθμό μετάδοσης δεδομένων της τάξης των 1.5 Mbps/384 Kbps για το downstream/ upstream αντίστοιχα για κάθε συσκευή πελάτη. Ο ρυθμός αυτός αντιστοιχεί σε ποιότητα υπηρεσιών που παρέχεται από τεχνολογίες Xdsl εξασφαλίζοντας ωστόσο πολύ μεγαλύτερη κάλυψη.

4.1.3.4 Εξασφάλιση ποιότητας υπηρεσιών

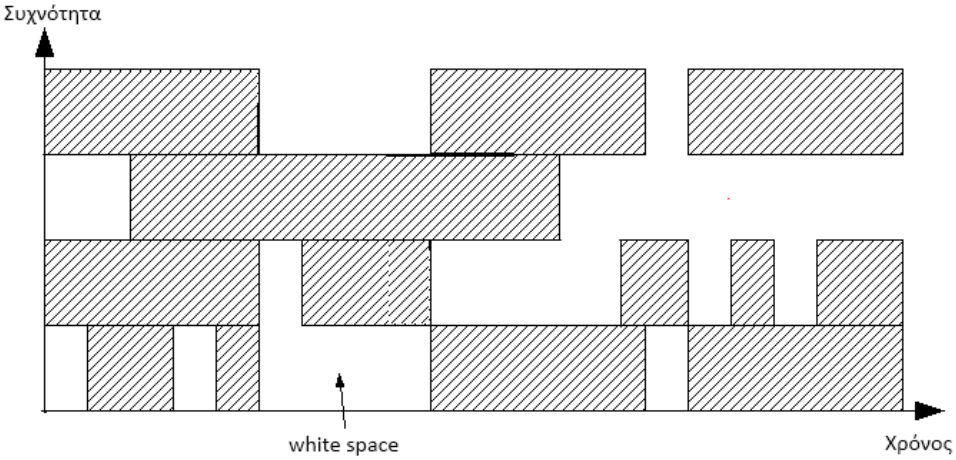
Ένα ακόμα κοινό σημείο μεταξύ των πρωτοκόλλων της οικογένειας 802.16 και του 802.22 είναι ο τρόπος με τον οποίο διασφαλίζεται η ποιότητα των υπηρεσιών, με τον κατάλληλο προγραμματισμό των εκπομπών ανάλογα με το είδος των υπηρεσιών που ζητούνται από το σύστημα. Έτσι οι εφαρμογές που υποστηρίζονται από το σταθμό βάσης διαχωρίζονται σε πέντε (5) κλάσεις προσφοράς υπηρεσιών :

1. UGS (Unsolicited Grant Service) : Για υπηρεσίες σταθερού ρυθμού εκπομπής. Τέτοιες υπηρεσίες είναι οι τηλεδιασκέψεις, διασκέψεις μέσω τηλεφώνου (χωρίς silence suppression) ή κάθε υπηρεσία έπειτα από αίτηση (on-demand) όπως διαδραστική (interactive) φωνή και ήχος.
2. rtPS (real-time Polling Service) : Για υπηρεσίες με μεταβλητό ρυθμό εκπομπής. Σε αυτή την κατηγορία εντάσσεται το video streaming σε συμπιεσμένο format και με μεταβλητό ρυθμό δεδομένων.
3. nrtPS (non-real-time Polling Service) : Για υπηρεσίες μη πραγματικού χρόνου με μεταβλητό ρυθμό εκπομπής. Σ' αυτές τις υπηρεσίες ανήκουν οι μεταδόσεις FTP.
4. ertPS (extended-real-time Polling Service) : Για υπηρεσίες Voice over IP (VoIP) με silence suppression.
5. BE (Best Effort) : Για υπηρεσίες χωρίς απαιτήσεις σχετικά με καθυστερήσεις ή με το ρυθμό μετάδοσης. Σε αυτή την κατηγορία ανήκει και η περιήγηση στο διαδίκτυο (αν δεν υπάρχει κάποια διαφορετική απαίτηση) (βλ. [58]).

4.1.4 Το φυσικό επίπεδο και το επίπεδο πρόσβασης στο μέσο του 802.22

4.1.4.1 Το φυσικό επίπεδο (PHY)

Όπως έχει αναφερθεί, οι οντότητες του 802.22 θα πρέπει να προγραμματίζουν τις μεταδόσεις τους στις τηλεοπτικές συχνότητες κατά τη διάρκεια των κενών διαστημάτων των μεταδόσεων των πρωτευόντων χρηστών. Ωστόσο, δεν υπάρχει ένας ντετερμινιστικός τρόπος καθορισμού του χρόνου εμφάνισης αυτών των διαστημάτων. Στην παρακάτω εικόνα φαίνεται παραστατικά ο τυχαίος τρόπος με τον οποίο εμφανίζονται τα παρακάτω κενά διαστήματα στο φάσμα. Το χαρακτηριστικό αυτό επηρεάζει το σχεδιασμό τόσο του φυσικού επιπέδου της μετάδοσης, όσο κα του επιπέδου πρόσβασης στο μέσο (βλ. [59].



Σχήμα 25. Εμφάνιση κενών διαστημάτων μετάδοσης στο φάσμα

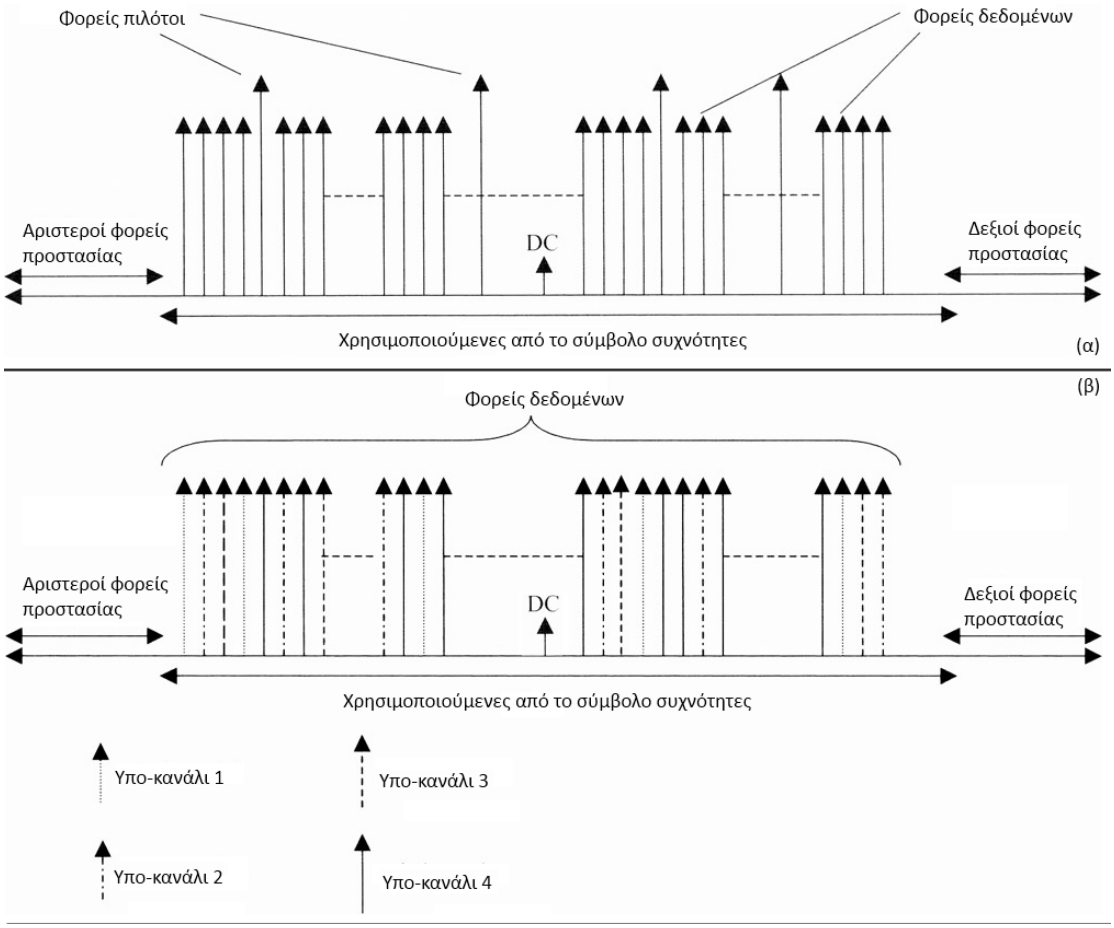
Τα κενά μεταξύ των μεταδόσεων των πρωτευόντων χρηστών πρέπει να χρησιμοποιούνται με τον καλύτερο τρόπο, διασφαλίζοντας με αυτόν τον τρόπο την ποιότητα των υπηρεσιών. Σημαντικό στοιχείο αποτελεί και η δυνατότητα μετάδοσης από πολλές συσκευές πελατών προς το σταθμό βάσης ταυτόχρονα αλλά και προς την αντίθετη κατεύθυνση. Τα προαναφερθείσα χαρακτηριστικά ενσωματώνονται στη διαμόρφωση OFDMA (Orthogonal Frequency Division Multiple Access – Ορθογώνια διαίρεση συχνότητας πολλαπλής πρόσβασης), που χρησιμοποιείται από το 802.22. Η διαμόρφωση OFDMA χρησιμοποιείται για τη μεταφορά δεδομένων τόσο από το σταθμό βάσης προς τις συσκευές των πελατών (downlink), όσο και από τις συσκευές των πελατών προς το σταθμό βάσης (uplink). Η επικοινωνία μεταξύ της συσκευής πελάτη και του σταθμού βάσης υλοποιείται με την αμφίδρομη λειτουργία διαίρεσης χρόνου (Time Division Duplex – TDD) στην οποία χρησιμοποιούνται οι ίδιες συχνότητες για τις εκατέρωθεν μεταφορές δεδομένων, σε διαφορετικές όμως χρονικές στιγμές. Είναι πιθανό στο μέλλον να υποστηριχθεί επιπλέον και η δυνατότητα αμφίδρομης λειτουργίας διαίρεσης συχνότητας (Frequency Division Duplex – FDD), στην οποία χρησιμοποιούνται διαφορετικές συχνότητες την ίδια χρονική στιγμή για να γίνει η μετάδοση των δεδομένων μεταξύ σταθμού βάσης και των συσκευών των πελατών (βλ. [60].

Με αυτόν τον τρόπο εξασφαλίζεται ένας ευέλικτος και δυναμικός τρόπος για τη διαχείριση των πόρων του δικτύου. Επιπλέον με το διαχωρισμό τόσο στο χρόνο όσο και στην συχνότητα, επιτρέπεται η πρόσβαση πολλαπλών συσκευών πελατών στο φάσμα. Έτσι οι «σχισμές» (slots) στις οποίες μπορούν να γίνουν μεταφορές δεδομένων ορίζονται τόσο στον άξονα του χρόνου όσο και αυτόν της συχνότητας. Προκάτοχος του OFDMA είναι η κωδικοποίηση OFDM (Orthogonal Frequency Division Multiplexing – Ορθογώνια Πολυπλεξία Διαίρεσης Συχνότητας). Στην κωδικοποίηση OFDM και κατ' επέκταση και στο OFDMA υπάρχουν τεσσάρων διαφορετικών ειδών φορείς (carriers) στο πεδίο της συχνότητας σε κάθε σύμβολο (είτε OFDM είτε OFDMA) :

1. Οι φορείς δεδομένων (Data Subcarriers) : Οι φορείς αυτοί, όπως μαρτυρά και το όνομα τους, χρησιμοποιούνται για τη μεταφορά των δεδομένων.
2. Οι φορείς πιλότοι (Pilot Subcarriers) : Οι φορείς αυτοί χρησιμοποιούνται για τη λειτουργία του συγχρονισμού.
3. Οι κενοί φορείς (Null Subcarriers) : Οι φορείς αυτοί χρησιμοποιούνται για προστασία στον άξονα της συχνότητας.
4. Ένας ειδικός κενός φορέας είναι ο φορέας DC (Direct Current). Ο φορέας DC έχει συχνότητα ίδια με την κεντρική συχνότητα του σταθμού μετάδοσης. Για να

απλουστευτεί η μετατροπή από Αναλογικό σε Ψηφιακό και από Ψηφιακό σε Αναλογικό ο φορέας αυτός είναι κενός.

Σε αντίθεση με τη διαμόρφωση OFDM, στη διαμόρφωση OFDMA δημιουργούνται υποσύνολα αυτών των φορέων δεδομένων, που αποτελούν τα υπο-κανάλια. Συνεπώς, στο OFDMA ορίζεται και το υπο-κανάλι, που είναι ουσιαστικά η ελάχιστη μονάδα μετάδοσης ενός συμβόλου OFDMA. Οι διαφορές επισημαίνονται στο παρακάτω **σχήμα 26** (βλ. [58] [61].

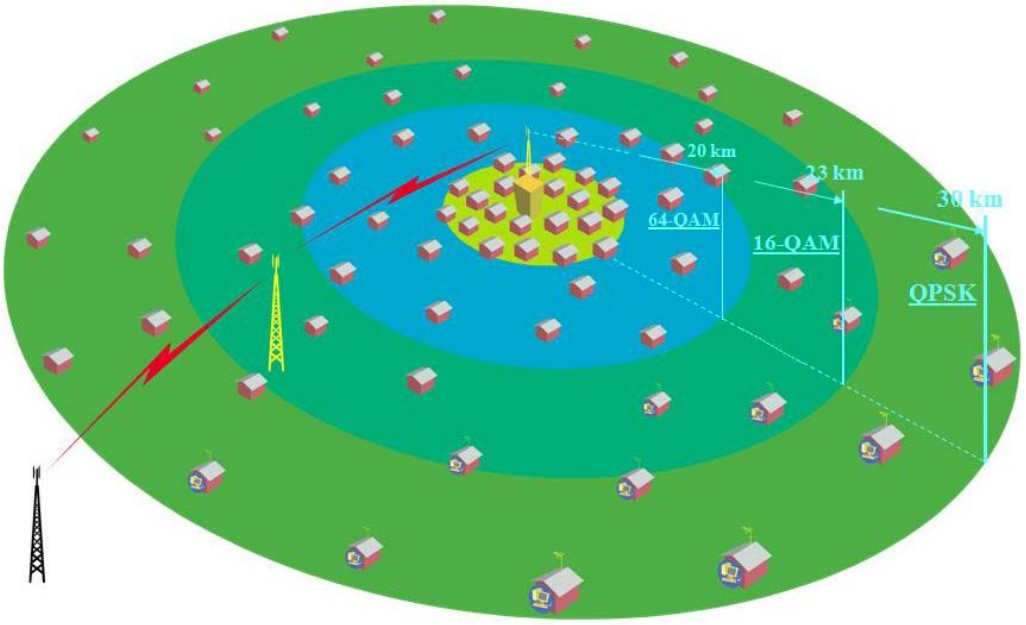


Σχήμα 26. Διαφορές μεταξύ ενός συμβόλου OFDM (α) – OFDMA (β).

Μια ακόμη παράμετρος που παίζει σημαντικό ρόλο στην υψηλή αποδοτικότητα του φάσματος είναι ο αριθμός των μετασχηματισμών Fourier (Fast Fourier Transformations – FFT) που πραγματοποιούνται σε κάθε σύμβολο. Αύξηση του αριθμού των μετασχηματισμών Fourier συνεπάγεται και μείωση των απαιτούμενων φορέων προστασίας για την αποφυγή θορύβων. Έτσι, αυξάνεται το ποσοστό των φορέων δεδομένων επί του συνόλου των φορέων του κάθε συμβόλου OFDMA. Στο 802.22 έχει προταθεί η χρήση 2048 FFT για κάθε σύμβολο κατά κύριο λόγο ενώ, προαιρετικά, να μπορούν να χρησιμοποιηθούν 1024 και 4096 FFT.

Ένα επιπλέον χαρακτηριστικό που υποστηρίζεται από τη διαμόρφωση OFDMA και υποστηρίζεται και από το πρωτόκολλο 802.22, είναι η διαφορετική κωδικοποίηση στις μεταφορές δεδομένων ανάμεσα στο σταθμό βάσης και τις συσκευές των πελατών. Ο

παράγοντας από τον οποίο εξαρτάται αυτό, είναι η απόσταση που υπάρχει μεταξύ του σταθμού βάσης και της συσκευής πελάτη και κατ' επέκταση ο λόγος Σήματος – Θορύβου (Signal to Noise Ratio – SNR). Αυτός είναι ακόμα ένας τρόπος για να αυξηθεί η αποδοτικότητα του συστήματος. Υποχρεωτικά οι συσκευές που θα χρησιμοποιούν το πρωτόκολλο 802.22 θα πρέπει να υποστηρίζουν υποχρεωτικά τις κωδικοποιήσεις που φαίνονται στο **σχήμα 27**, δηλ 64-QAM (Quadrature Amplitude Modulation – Τετραγωνική διαμόρφωση πλάτους με μετάδοση 6 bits/σύμβολο διαμόρφωσης), 16-QAM (Τετραγωνική διαμόρφωση πλάτους με μετάδοση 4 bits/σύμβολο διαμόρφωσης) και QPSK ή 4-QAM (Τετραγωνική διαμόρφωση πλάτους με μετάδοση 2 bits/σύμβολο διαμόρφωσης). Όπως γίνεται κατανοητό, η μετάδοση δεδομένων έχει φθίνων ρυθμό σε σχέση με την απόσταση. Αυτό όμως που υπάρχει σαν κέρδος είναι η διαφοροποίηση των υπηρεσιών. Έτσι, αυτοί που βρίσκονται κοντά στο σταθμό βάσης μπορούν και απολαμβάνουν υψηλότερους ρυθμούς μετάδοσης δεδομένων, ενώ αυτοί που βρίσκονται μακριά από αυτόν απολαμβάνουν μεγαλύτερη ανοχή στην περιόδευση (multi-path), έχοντας με αυτόν τον τρόπο πιο εύρωστες μεταδόσεις. Ωστόσο, αν τα δίκτυα που αναπτύσσονται είναι αρκετά μεγάλα υπάρχει η δυνατότητα να αυξηθεί η χωρητικότητα και η ακτίνα κάλυψης των δικτύων με χρήση ψηφιακών επαναληπτών (repeaters).



Σχήμα 27. Κωδικοποιήσεις ανάλογα με την απόσταση

Ένας άλλος τρόπος για την αύξηση της χωρητικότητας του συστήματος είναι η συνένωση πολλών τηλεοπτικών καναλιών (channel bonding), όπου αυτό είναι δυνατό, είτε αυτά βρίσκονται σε συνεχόμενες συχνότητες είτε όχι. Κυρίως έχει δοθεί βαρύτητα στη χρήση συνεχόμενων καναλιών. Θεωρητικά θα μπορούσαν να συνενωθούν πολλά κανάλια, αλλά πρακτικά ο μέγιστος αριθμός που μπορούν να συνενωθούν είναι τρία. Επειδή ο βασικός περιορισμός στον οποίο υπακούει το πρωτόκολλο είναι η προστασία των τηλεοπτικών μεταδόσεων, θα πρέπει να υπάρχουν τουλάχιστον τρία ελεύθερα τηλεοπτικά κανάλια για να μπορέσει να λειτουργήσει ένα WRAN, είτε χρησιμοποιείται η συνένωση των καναλιών είτε όχι. Αν δε χρησιμοποιείται συνένωση καναλιών, το ένα από τα τρία κανάλια χρησιμοποιείται για τις μεταδόσεις των δεδομένων ενώ τα άλλα δύο για προστασία των τηλεοπτικών καναλιών. Όταν χρησιμοποιείται η συνένωση, τότε

χρησιμοποιούνται δύο κανάλια για προστασία, ένα πριν και ένα μετά τα κανάλια που χρησιμοποιούνται, ενώ τα υπόλοιπα για τις μεταδόσεις των δεδομένων. Ανάλογα με τον αριθμό των καναλιών που συνενώνονται, διαφοροποιείται και ο αριθμός των μετασχηματισμών Fourier που θα πρέπει να πραγματοποιηθούν. Στοιχεία σχετικά με αυτό φαίνονται στον παρακάτω **πίνακα 2** :

Αριθμός FFT / Αριθμό συνενωμένων καναλιών	1	2	3
1024	1024	2048	-
2048	2048	4096	6144
4096	4096	-	-

Πίνακας 2. Αριθμός FFT ανά αριθμό συνενωμένων καναλιών

Όταν κάποια συσκευή πελάτη προσπαθεί να συσχετιστεί με το σταθμό βάσης του και να συγχρονιστεί με αυτόν, θα πρέπει να γνωρίζει εκ των προτέρων αν χρησιμοποιείται η τεχνική της συνένωσης καναλιών. Γι' αυτό το λόγο έχει οριστεί η επικεφαλίδα ελέγχου της δομής superframe του επιπέδου πρόσβασης στο μέσο (MAC Superframe Control Header), που μεταδίδεται σε εύρος ζώνης ίσο με τη συχνότητα του καναλιού που χρησιμοποιείται για τη μετάδοση (6, 7 ή 8 MHz), ενημερώνοντας τις συσκευές των πελατών σχετικά με τη χρήση ή όχι αυτής της τεχνικής, καθώς και για τα κανάλια που συνενώνονται.

Ωστόσο, η συγκεκριμένη λύση για αύξηση της διαθέσιμης χωρητικότητας του δικτύου δεν μπορεί να χρησιμοποιηθεί πάντα. Βασικός λόγος αποτελεί το γεγονός πως πολλά κανάλια μπορεί να ψηφιοποιήσουν τις μεταδόσεις τους, αυξάνοντας τα κενά στο εύρος των ραδιοσυχνοτήτων και προσφέροντας υπηρεσίες όπως μεταδόσεις υψηλής ευκρίνειας, που απαιτούν μεγαλύτερο εύρος ζώνης για τη μετάδοσή τους. Αυτό θα έχει ως αντίκτυπο να μην είναι διαρκώς διαθέσιμα περισσότερα από τέσσερα κανάλια έτσι ώστε να είναι δυνατή η χρήση της τεχνικής της συνένωσης των καναλιών, παρά μόνο σε περιορισμένα χρονικά διαστήματα. Στον παρακάτω **πίνακα 3** εμφανίζονται συνοπτικά και συγκεντρωμένα τα χαρακτηριστικά που θα έχει το φυσικό επίπεδο του πρωτοκόλλου όπως αναφέρθηκαν παραπάνω.

Συχνότητες	54-862 MHz
Χωρητικότητα καναλιού	6, 7 ή 8 MHz με δυνατότητα συνένωσης καναλιών
Κωδικοποιήσεις	64-QAM, 16-QAM, 4-QAM (QPSK)
Πολλαπλή πρόσβαση	Μέσω OFDMA
Αριθμός FFT	Υποχρεωτικά 2048, προαιρετικά 1024 και 4096. Προσαρμογή ανάλογα με το αν χρησιμοποιείται συνένωση καναλιών.
Duplex	Μέσω TDD, πιθανόν και FDD αργότερα
Τοπολογία δικτύου	P-MP (point to multipoint)

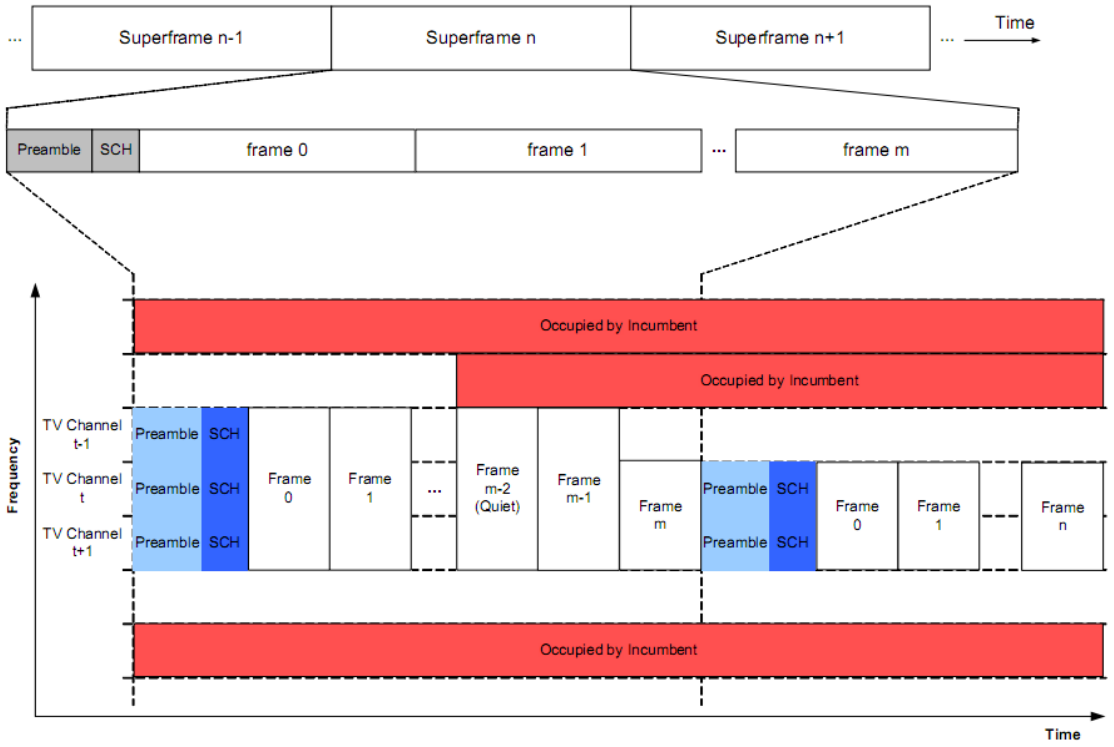
Πίνακας 3. Χαρακτηριστικά του φυσικού επιπέδου του 802.22

4.1.4.2 Επίπεδο πρόσβασης στο μέσο (MAC)

Οι μεταδόσεις στο επίπεδο πρόσβασης στο μέσο, όπως προαναφέρθηκε, πρέπει να έχουν έναν αρκετά δυναμικό χαρακτήρα, για να αντιδρούν γρήγορα και αποτελεσματικά στις αλλαγές του περιβάλλοντος στο οποίο λειτουργούν. Η ανάπτυξη του επιπέδου πρόσβασης στο μέσο, βασίστηκε κατά ένα μεγάλο βαθμό σε ήδη υπάρχοντα πρωτόκολλα και συγκεκριμένα στην οικογένεια πρωτοκόλλων του 802.16 (βλ. [62]). Σε αυτό έγιναν αρκετές βελτιώσεις και απλουστεύσεις έτσι ώστε να επιτευχθούν οι απαιτήσεις λειτουργίας του 802.22. Το επίπεδο πρόσβασης στο μέσο βασίζεται σε μια αρχιτεκτονική με χρήση super-frames η οποία θεωρείται αρκετά γενική για να είναι δυνατή η συνύπαρξη πολλών συστημάτων σε συνδυασμό με την ευελιξία και την αρκετά μεγάλη χωρητικότητα. Για να συνυπάρχουν τα συστήματα που χρησιμοποιούν το πρωτόκολλο 802.22 με τους πρωτεύοντες χρήστες των τηλεοπτικών συχνοτήτων, έχει οριστεί στο επίπεδο πρόσβασης στο μέσο μια σειρά από διαδικασίες με τις οποίες γίνεται ο εντοπισμός τους και άλλες με τις οποίες παρέχονται τα απαραίτητα χαρακτηριστικά για τη διαχείριση του φάσματος. Επιπλέον χαρακτηριστικά αυτού του επιπέδου περιλαμβάνονται για την υποστήριξη διαφόρων τύπων κυκλοφορίας με διαφορετικές απαιτήσεις ποιότητας υπηρεσιών (Quality of Service – QoS) (βλ. [63]).

4.1.4.2.1 Δομή Frame και Superframe

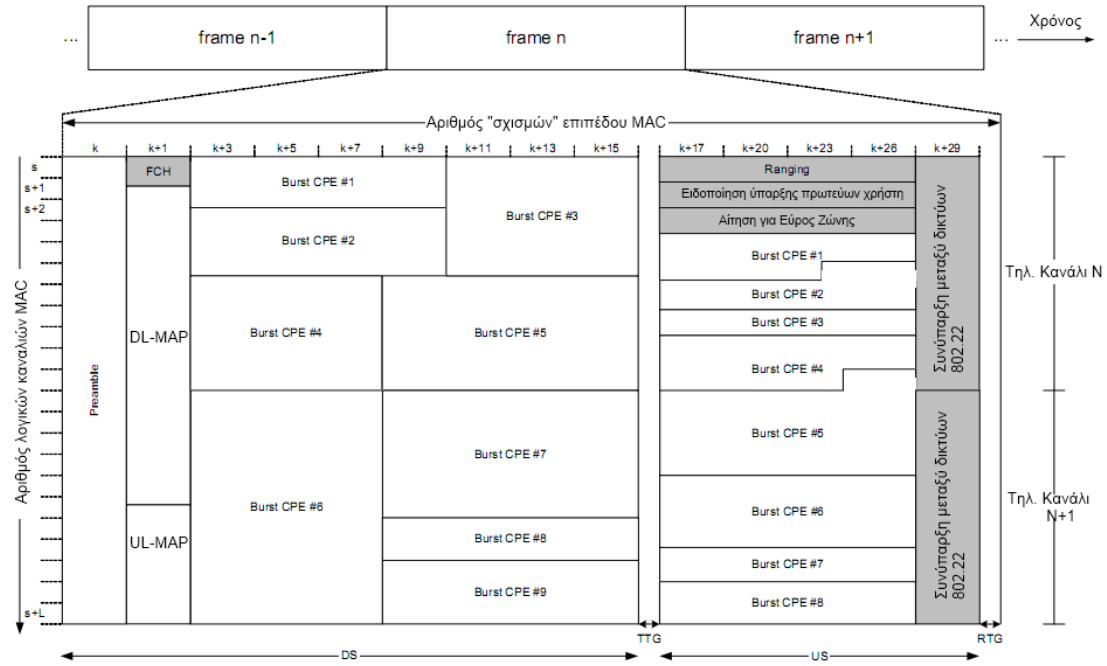
Η δομή του frame είναι η βασική δομή με την οποία οργανώνονται οι μεταφορές από τους σταθμούς βάσης προς τις συσκευές των πελατών και αντίστροφα. Η δομή του superframe αποτελεί μια εκτεταμένη δομή οργάνωσης των frames. Κάθε superframe αποτελείται από δεκαέξι (16) επιμέρους frames. Επειδή η διάρκεια που έχει οριστεί για κάθε frame είναι της τάξης των 10ms, με δεδομένο ότι κάθε superframe έχει 16 frames η διάρκεια του είναι 160ms. Στην αρχή κάθε superframe υπάρχει το τμήμα (preamble), το οποίο προαναγγέλλει την αρχή του superframe και χρησιμοποιείται για το συγχρονισμό. Στη συνέχεια ακολουθεί η επικεφαλίδα ελέγχου του superframe (Superframe Control Header), που όπως αναφέρθηκε παραπάνω, πέρα από ότι μεταδίδεται σε εύρος ζώνης ενός καναλιού (6, 7 ή 8 MHz), περιέχει πληροφορίες για το αν χρησιμοποιείται συνένωση καναλιών και για τα κανάλια που συνενώνονται. Αυτή είναι η βασική δομή που εκπέμπεται από το σταθμό βάσης και λαμβάνεται από τις συσκευές πελατών για να αρχίσει η διαδικασία συσχετισμού τους με το σταθμό βάσης. Μετά από την επικεφαλίδα ελέγχου του superframe ακολουθούν τα δεκαέξι frames που απαρτίζουν το κάθε superframe.



Σχήμα 28. Γενική δομή του superframe

Στο **σχήμα 28** φαίνεται η δομή του superframe όπως παρουσιάστηκε σε αυτή την παράγραφο, σε συνδυασμό με τις μεταδόσεις των πρωτευόντων χρηστών. Στην ίδια εικόνα παριστάνεται και η συνένωση των καναλιών, καθώς και μια αντίδραση του συστήματος. Όπως παρατηρείται, τη χρονική στιγμή t_1 κάποιος πρωτεύων χρήστης αρχίζει μεταδόσεις στο τηλεοπτικό κανάλι t-2 που χρησιμοποιείται, όπως προαναφέρθηκε νωρίτερα, ως συχνότητα προστασίας. Έτσι από τη χρονική στιγμή t_2 και μετά ο σταθμός βάσης χρησιμοποιεί συνενωμένα μόνο τα τηλεοπτικά κανάλια t και t+1.

Η γενική δομή του frame ενός superframe είναι αυτή που παριστάνεται στο **σχήμα 29**. Σε αυτή τη δομή εντοπίζονται δύο κύρια τμήματα. Το πρώτο είναι το τμήμα στο οποίο ο σταθμός βάσης αποστέλλει πληροφορίες προς τις συσκευές των πελατών (Downstream Subframe), ενώ το δεύτερο είναι το τμήμα που αποστέλλονται πληροφορίες από τις συσκευές των πελατών προς το σταθμό βάσης (Upstream Subframe). Τα δύο τμήματα χωρίζονται μεταξύ τους με ένα μικρό χρονικό διάστημα στο οποίο δεν πραγματοποιείται κάποια μετάδοση, γνωστό και ως χρονικό κενό μετάδοσης (Transmission Time Gap – TTG). Αξίζει να σημειωθεί ότι το Downstream Subframe αποτελείται από ένα και μόνο πακέτο στο φυσικό επίπεδο, ενώ το Upstream Subframe από ένα ή περισσότερα, ένα για κάθε συσκευή πελάτη που εκπέμπει στο εκάστοτε frame.



Σχήμα 29. Γενική δομή του frame

Όπως και το superframe έτσι και το frame ξεκινάει με ένα τμήμα που προαναγγέλλει την αρχή του (preamble). Επιπλέον, το μέγεθος του πρώτου frame κάθε superframe είναι μειωμένο κατά το χρόνο που διαρκεί η αρχή του superframe. Μετά το preamble ακολουθεί η επικεφαλίδα ελέγχου του frame (Frame Control Header – FCH), που περιέχει πληροφορίες σχετικά με τα χαρακτηριστικά των καναλιών που χρησιμοποιούνται. Στη συνέχεια, ακολουθούν οι κεφαλίδες χαρτογράφησης για το Downstream και το Ubstream Subframe, που ονομάζονται DL-MAP και UL-MAP αντίστοιχα. Το μέγεθος που έχουν αυτές οι κεφαλίδες χαρτογράφησης περιέχεται στην επικεφαλίδα ελέγχου του frame. Σε αυτές τις κεφαλίδες καταγράφονται και γνωστοποιούνται σε όλους τους χρήστες του δικτύου από το σταθμό βάσης πότε θα γίνουν οι μεταδόσεις προς τις συσκευές πελατών που υπάρχουν στο δίκτυο, όσο και πότε θα μεταδώσουν αυτές προς το σταθμό βάσης.

Το επόμενο βήμα είναι οι αποστολές των δεδομένων από το σταθμό βάσης προς τις συσκευές των πελατών, που γίνονται με τη μορφή ριπών (bursts). Κάθε ριπή είναι μία μετάδοση η οποία έχει μια σειρά κοινών χαρακτηριστικών :

- Της κωδικοποίησης που χρησιμοποιείται και
- Του κώδικα εκ των προτέρων διόρθωσης σφαλμάτων (Forward Error Correction – FEC).

Κάθε ριπή καταλαμβάνει συγκεκριμένο αριθμό λογικών καναλιών στο επίπεδο MAC (βλ. [64]).

Μετά και την παρέλευση του TTG, εκκινούν οι μεταφορές δεδομένων από την πλευρά των συσκευών των πελατών. Σε αυτό το σημείο, προτού αρχίσουν οι μεταφορές δεδομένων, οι πελάτες αναφέρουν αν εντοπίστηκε κάποιος πρωτεύων χρήστης, ενώ σε αυτό το σημείο γίνονται και οι αιτήσεις για μεγαλύτερο εύρος ζώνης από τη μεριά των συσκευών των πελατών για κάποια από τις ροές δεδομένων τους με το σταθμό βάσης. Ο σταθμός βάσης λαμβάνοντας υπόψη τις αιτήσεις για αύξηση του εύρους ζώνης σε διάφορες συνδέσεις, προγραμματίζει τις μεταφορές των δεδομένων από και προς τις συσκευές των πελατών, προσαρμόζοντας κατάλληλα το χρόνο που θα

αποφασίσει να κάνει την παύση των μεταδόσεών του (TTG). Έτσι, αν για παράδειγμα διαπιστωθεί ότι υπάρχει μεγαλύτερη ανάγκη για μεταφορές από το σταθμό βάσης προς τις συσκευές των πελατών, ο σταθμός βάσης μετατοπίζει το TTG προς τα δεξιά έτσι ώστε το Downstream Subframe να γίνει μεγαλύτερο και να ικανοποιήσει κατά συνέπεια την αυξημένη κίνηση. Αν η κίνηση είναι μεγαλύτερη για αποστολή δεδομένων από τις συσκευές πελατών προς το σταθμό βάσης, πράττει ανάλογα. Για λόγους μεγαλύτερης ευελιξίας, στο επίπεδο πρόσβασης στο μέσο οι σταθμοί βάσης έχουν τη δυνατότητα υποστήριξης συσκευών πελατών που λειτουργούν σε ένα ή περισσότερα κανάλια (βλ. [64], [65]).

4.1.4.2.2 Περίοδοι σιγής και έλεγχος για πρωτεύοντες χρήστες

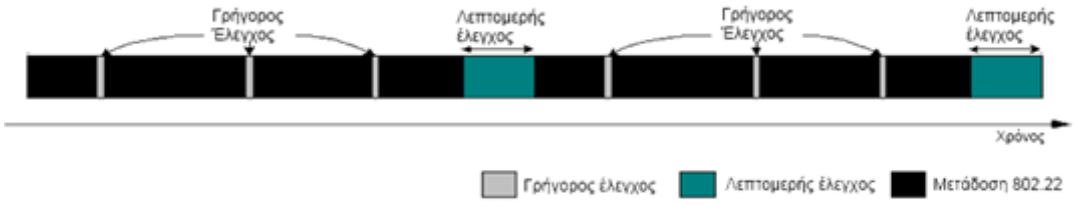
Για να διασφαλιστεί η απρόσκοπτη επικοινωνία των πρωτευόντων χρηστών του δικτύου αλλά και η σωστή λειτουργία των δικτύων που χρησιμοποιούν το πρωτόκολλο, προγραμματίζεται περιοδικός έλεγχος για παρουσία πρωτευόντων χρηστών. Ο έλεγχος για τυχόν πρωτεύοντες χρήστες διεξάγεται από τις συσκευές των χρηστών υπό την καθοδήγηση του σταθμού βάσης, ο οποίος ενημερώνει σχετικά με τα κανάλια που θα πρέπει να ελεγχθούν, καθώς και με τη διάρκεια του ελέγχου. Αφού συγκεντρωθούν οι απαραίτητες πληροφορίες από τις συσκευές των χρηστών, στη συνέχεια αποστέλλονται στο σταθμό βάσης, ο οποίος με τη σειρά του αποφασίζει για τα μέτρα που πρέπει να ληφθούν. Μπορούν να χρησιμοποιηθούν επιπλέον κάποιοι μηχανισμοί, που αφορούν τις οδηγίες που δίνει ο σταθμός βάσης προς τις συσκευές των πελατών, έτσι ώστε οι δράσεις τους να είναι συμπληρωματικές, διαμοιράζοντας με αυτόν τον τρόπο τον υπολογιστικό φόρτο. Όπως διαφαίνεται από τα προαναφερθέντα, έλεγχος για πρωτεύοντες χρήστες γίνεται τόσο στο κανάλι ή κανάλια που χρησιμοποιούνται από την κυψέλη όσο και από άλλα κανάλια.

Η διαδικασία αυτή του ελέγχου γίνεται σε δύο φάσεις, κατά τις οποίες διακόπτονται οι μεταδόσεις του σταθμού βάσης προς τις συσκευές και αντίστροφα :

- **Γρήγορος έλεγχος (fast-sensing) :** Ο γρήγορος έλεγχος γίνεται σε μία ή περισσότερες περιόδους οι οποίες έχουν πολύ μικρή διάρκεια (της τάξης του 1ms). Κατά τη διάρκεια αυτού του ελέγχου γίνεται ανίχνευση της ενέργειας που λαμβάνεται και ειδικότερα μέτρησή της, έτσι ώστε να διαπιστωθεί αν ξεπερνά κάποιο καθορισμένο κατώφλι (threshold). Αυτού του είδους ο έλεγχος πραγματοποιείται μόνο στο κανάλι(-ια) που χρησιμοποιείται από την κυψέλη. Ανάλογα με τις μετρήσεις που λαμβάνει ο σταθμός βάσης από τις συσκευές των πελατών, το σύστημα ορίζει αν θα πρέπει να πραγματοποιηθεί λεπτομερής έλεγχος (fine-sensing). Για παράδειγμα, αν παρατηρηθεί ότι η λαμβανόμενη ενέργεια στο κανάλι είναι πάντα κάτω από το επιτρεπόμενο όριο που έχει τεθεί μπορεί να αποφασίσει να ακυρώσει την επόμενη περίοδο λεπτομερούς ελέγχου. Αντίστοιχα, αν το σύστημα εντοπίζει υψηλή λαμβανόμενη ενέργεια τότε προγραμματίζει την εκπόνηση ενός λεπτομερούς ελέγχου. Όπως έχει σημειωθεί και στον ορισμό του προτύπου του 802.22, το σύστημα θα πρέπει να είναι ικανό να εντοπίσει την παρουσία πρωτευόντων χρηστών σε χρόνο λιγότερο από 2 sec. Συνεπώς, οι έλεγχοι θα πρέπει να πραγματοποιούνται περιοδικά με χρόνο που να μην ξεπερνά τα 2 sec.
- **Λεπτομερής έλεγχος (fine-sensing) :** Όπως προαναφέρθηκε, η φάση αυτή δεν είναι υποχρεωτική, αλλά αποφασίζεται δυναμικά από το σταθμό βάσης, ανάλογα με το αποτέλεσμα του fast-sensing. Η διάρκειά της κυμαίνεται στα 25ms κατά την οποία το σύστημα προσπαθεί να εντοπίσει συγκεκριμένες υπογραφές σημάτων που εκπέμπονται από πρωτεύοντες χρήστες αλλά και από άλλες κυψέλες 802.22. Η αντίδραση του σταθμού βάσης βέβαια διαφέρει ανάλογα με την περίπτωση. Αν πρόκειται για πρωτεύων χρήστη, τότε ο σταθμός βάσης εκκινεί τις διαδικασίες

αλλαγής καναλιού λειτουργίας, ενώ αν πρόκειται για άλλη κυψέλη 802.22, ξεκινούν κάποιες διαδικασίες για τη μεταξύ τους συνύπαρξη, που θα περιγραφούν παρακάτω. Τα σήματα που χρησιμοποιούνται για την επικοινωνία δεν είναι τελείως τυχαία. Περιέχουν κάποια στοιχεία που δεν είναι τυχαία, λόγω του συνδυασμού των διαμορφωμένων σημάτων με ημιτονικές φέρουσες κυμάτων. Τα σήματα αυτά θεωρούνται κυκλοστατικά (cyclostationary), καθώς τα στατιστικά τους στοιχεία παρουσιάζουν περιοδικότητα στο χρόνο. Η συνάρτηση πυκνότητας φασματικής συσχέτισης (spectral correlation density function – SCD function) μπορεί να εξάγει την κυκλοστατικότητα ενός σήματος. Σε αντίθεση με τα σήματα, ο θόρυβος δεν εμφανίζει καμία κυκλοστατικότητα. Συνεπώς, με την ανάλυση της συνάρτησης SCD μπορεί να διαπιστωθεί και ο τύπος του λαμβανόμενου σήματος. Πάνω σε αυτή την ανάλυση βασίζεται και η λειτουργία του fine-sensing. Διαφορετικοί τύποι σημάτων έχουν διαφορετικές μη μηδενικές κυκλικές συχνότητες. Για παράδειγμα, στην περίπτωση των αναλογικών τηλεοπτικών σημάτων, εμφανίζονται κυκλικές συχνότητες με ρυθμό πολλαπλάσιο του ρυθμού οριζόντιας σάρωσης (horizontal line – scan rate) που είναι 15.75 kHz στις Ηνωμένες Πολιτείες και 15.625 kHz στην Ευρώπη (βλ. [66]).

Στο **σχήμα 30** φαίνονται οι φάσεις αυτές που περιγράφηκαν παραπάνω σε σχέση με τις μεταδόσεις του πρωτοκόλλου (βλ. [59]).



Σχήμα 30. Τα δύο στάδια πραγματοποίησης ελέγχου για εντοπισμό πρωτευόντων χρηστών.

Ιδιαίτερη προσοχή έχει δοθεί και για την προστασία των υπόλοιπων συσκευών που χρησιμοποιούν το φάσμα, όπως ασύρματα μικρόφωνα και συσκευές ενδοεπικοινωνίας μικρής εμβέλειας, καθώς αυτές έχουν πολύ μικρή ενέργεια εκπομπής, καθιστώντας δύσκολο τον εντοπισμό τους. Για αυτό το λόγο έχουν προταθεί δύο ειδών λύσεις για τον εντοπισμό τους.

- Η πρώτη λύση αναφέρει την παρουσία μιας ξεχωριστής συσκευής που εκπέμπει πακέτα-φάρους (beacons) τα οποία θα επισημαίνουν την ύπαρξη τέτοιου είδους συσκευών.
- Στη δεύτερη λύση προτείνεται η ύπαρξη μιας ξεχωριστής συσκευής πελάτη που θα ενημερώνει τα δίκτυα 802.22 για την ύπαρξη αυτού του είδους συσκευών. Η συσκευή πελάτη θα ενημερώνει σχετικά με την ύπαρξη αυτών των συσκευών με πακέτο-φάρο που θα αποστέλλεται κατά τη διάρκεια κάποιας περιόδου σιγής προς το σταθμό βάσης, ο οποίος θα πρέπει με τη σειρά του να στέλνει και το ανάλογο πακέτο για να επιβεβαιώσει τη λήψη αυτού του πακέτου.

Παρόλα αυτά, επισημαίνεται ότι μεμονωμένη χρήση των δύο αυτών λύσεων δεν είναι τόσο αποτελεσματική. Ο συνδυασμός αυτών των δύο λύσεων θεωρείται προτιμότερος (βλ. [67]).

4.1.4.2.3 Συμπεριφορά δικτύων 802.22 που λειτουργούν στο ίδιο κανάλι

Πριν αναλυθούν οι μηχανισμοί συμπεριφοράς των δικτύων 802.22 που έχουν προταθεί, είναι σημαντικό να αναφερθούν ορισμένες υλοποιήσεις που έχουν προταθεί για το Cognitive Radio, οι οποίες μπορούν να εφαρμοστούν και στην περίπτωση του

802.22. Είναι γεγονός πως η ερευνητική ομάδα του 802.22 έχει αφήσει ανοιχτά αρκετά ζητήματα (όπως για παράδειγμα τη διαδικασία αλλαγής καναλιού στο δίκτυο), καταδεικνύοντας εμμέσως τη δυνατότητα υιοθέτησης πολλών προτάσεων. Στην περίπτωση του cognitive radio, ο τρόπος με τον οποίο διαμοιράζεται το φάσμα χωρίζεται σε δύο είδη :

- Κάθετος διαμοιρασμός φάσματος (vertical spectrum sharing) : Οι συσκευές πελατών αναζητούν περιοδικά το φάσμα για την παρουσία ελεύθερων καναλιών στα οποία μπορούν να μεταβούν και το δίκτυο να συνεχίσει τη λειτουργία του.
- Οριζόντιος διαμοιρασμός φάσματος (horizontal spectrum sharing) : Αν ένα δίκτυο 802.22 εντοπίσει κάποιο άλλο δίκτυο στο ίδιο κανάλι και τα ελεύθερα κανάλια στο φάσμα είναι περιορισμένα, τότε τα δίκτυα συναινούν σε έναν κοινό διαμοιρασμό του καναλιού (βλ. [68]).

Στη συνέχεια, αναλύονται οι μηχανισμοί που έχουν προταθεί για το 802.22. Σε περίπτωση που εντοπιστεί ότι κάποια κυψέλη 802.22 λειτουργεί στο ίδιο κανάλι με κάποια άλλη (ή κάποιες άλλες) ενεργοποιούνται κάποιοι μηχανισμοί έτσι ώστε να είναι δυνατή είτε η συνύπαρξή τους, είτε κάποια από τις δύο (ή περισσότερες) να αλλάξει κανάλι λειτουργίας. Η συμπεριφορά αυτή είναι μείζονος σημασίας για τη λειτουργία του πρωτοκόλλου. Ο λόγος είναι η μεγάλη περιοχή κάλυψης που αναμένονται να έχουν τα δίκτυα 802.22, που όπως προαναφέρθηκε μπορεί να φτάσει τα 100km. Η μεγάλη περιοχή κάλυψης καθιστά πολύ πιθανή την παρουσία δύο ή περισσότερων δικτύων 802.22 σε μια περιοχή. Σε μια τέτοια περίπτωση, οι λειτουργίες του fast και του fine sensing δε θα παρείχαν κανένα όφελος, καθώς το ένα δίκτυο θα εντόπιζε το άλλο κατά τις περιόδους ελέγχου, δυσχεραίνοντας επιπλέον και τον εντοπισμό των πρωτευόντων χρηστών στο κανάλι λειτουργίας. Για αυτό το λόγο έχει προστεθεί και η δυνατότητα του συγχρονισμού που αναλύεται στην επόμενη παράγραφο. Η υλοποίηση αυτών των μηχανισμών είναι πολύ σημαντική για την αποτελεσματική λειτουργία του πρωτοκόλλου, καθώς σε αντίθετη περίπτωση οι παρεμβολές μεταξύ αυτών των δικτύων θα είναι αρκετά μεγάλες, καθιστώντας τα συστήματα άχρηστα.

4.1.4.2.4 Συγχρονισμός μεταξύ των κυψελών

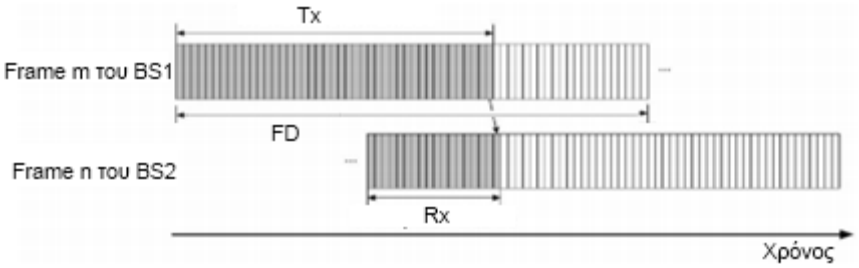
Ένας τρόπος έτσι ώστε να γίνει πιο εύκολος ο εντοπισμός πρωτευόντων χρηστών του δικτύου είναι ο συγχρονισμός των δύο φάσεων ελέγχου για πρωτεύοντες χρήστες, της γρήγορης αλλά και της λεπτομερούς φάσης, μεταξύ γειτονικών σταθμών βάσης. Με το συγχρονισμό των δικτύων μεταξύ τους τα frames θα εκκινούν την ίδια χρονική στιγμή και κατ' επέκταση θα πραγματοποιούνται ταυτόχρονα τα fast και fine sensing. Συνεπώς, είναι δυνατή η κατά περιόδους αδρανοποίηση οποιασδήποτε κίνησης από τη μεριά των δικτύων 802.22, καθιστώντας πιο αποτελεσματικό τον έλεγχο για πρωτεύοντες χρήστες χωρίς τις παρεμβολές άλλων δικτύων.

Ας υποτεθεί ότι υπάρχουν δύο επικαλυπτόμενες κυψέλες στις οποίες βρίσκονται δύο σταθμοί βάσης, ο BS1 και ο BS2, που επιθυμούν να συγχρονίσουν τις μεταδόσεις τους. Ο συγχρονισμός μεταξύ τους επιτυγχάνεται με τη χρήση ειδικών πακέτων-φάρων (inter-cell beacons). Όταν το BS1 αποστέλλει ένα beacon πακέτο, καταγράφει σε αυτό και το χρόνο που έχει μεσολαβήσει από την αρχή του frame μέχρι και τη στιγμή που άρχισε τη μετάδοση του beacon, έστω Tχ (γνωστό και ως transmission offset). Το BS2, αφού λάβει το beacon από το BS1, υπολογίζει το χρόνο που μεσολάβησε από την αρχή του δικού του frame μέχρι και τη στιγμή λήψης του πακέτου έστω Rx (γνωστό και ως reception offset). Έστω FD η διάρκεια του frame. Αφού το BS2 λάβει το beacon από το BS1, ο συγχρονισμός του με το BS1 επιτυγχάνεται ολισθαίνοντας τα frames με βάση τον ακόλουθο κανόνα :

- Αν $(FD - T_X + R_X) \leq [FD/2]$, τότε ολισθαίνει τα frames δεξιά κατά $FD - T_X + R_X$.

- Διαφορετικά ολισθαίνει τα frames αριστερά κατά $T_X - R_X$.

Στην παρακάτω εικόνα παριστάνεται η λειτουργία του συγχρονισμού με τον υπολογισμό των μεγεθών FD, Tχ, Rx με την εφαρμογή του προαναφερθέντος κανόνα.



Σχήμα 31. Συγχρονισμός επικαλυπτόμενων κυψελών

4.1.4.2.5 Δυναμικός διαμοιρασμός πόρων μεταξύ των κυψελών

Υπάρχει τρόπος να διαμοιραστούν το/τα κανάλια λειτουργίας των κυψελών. Γνώμονας γι' αυτό το διαμοιρασμό των καναλιών αποτελεί η εξασφάλιση της ποιότητας των υπηρεσιών που προσφέρουν οι κυψέλες. Για αυτό το λόγο στο 802.22 ορίζονται δύο διαφορετικές μέθοδοι διαμοιρασμού των καναλιών, η αποκλειστική και η μη αποκλειστική.

Στη μη αποκλειστική μέθοδο ο σταθμός βάσης θα πρέπει να αποφασίσει αν ο διαμοιρασμός του φάσματος είναι εφικτός με βάση το λόγο σήματος-παρεμβολής (Signal to Interference Ratio) και ένα κατώφλι που έχει οριστεί για αυτό, βάσει των υπηρεσιών που πρέπει να υποστηρίξει το δίκτυο. Αν ο λόγος σήματος-παρεμβολής είναι μεγαλύτερος από το καθορισμένο κατώφλι, τότε είναι δυνατός ο διαμοιρασμός του καναλιού λειτουργίας. Έτσι επιτυγχάνεται, ο διαμοιρασμός του καναλιού λειτουργίας με τον έλεγχο της ενέργειας μεταδόσεων, ελαχιστοποιώντας τις μεταξύ τους παρεμβολές. Η μέθοδος αυτή είναι γνωστή και ως spectrum sharing

Σε αντίθετη περίπτωση, κάποιος από τους δύο ή περισσότερους σταθμούς βάσης παύει να χρησιμοποιεί το συγκεκριμένο κανάλι και εκκινεί τις διαδικασίες για την αναζήτηση ενός άλλου ελεύθερου καναλιού. Το 802.22 αφήνει ανοιχτό τον τρόπο με τον οποίο θα γίνει η αναζήτηση των ελεύθερων καναλιών, αλλά και το ποιο δίκτυο θα εγκαταλείψει το συγκεκριμένο κανάλι. Ήδη, στη βιβλιογραφία περιλαμβάνονται αρκετές προτεινόμενες μέθοδοι. Μια αρκετά απλή μέθοδος περιγράφεται από το πρωτόκολλο ODSC (On-demand Spectrum Contention). Ειδικότερα, με την εφαρμογή του ODSC, ο σταθμός βάσης επιλέγει έναν τυχαίο αριθμό ανάμεσα στο 0 και το W ([0, W]), όπου το W είναι ένα άνω όριο, κοινό για όλους τους σταθμούς βάσης. Ο αριθμός αυτός χρησιμοποιείται για να καθοριστεί ο «νικητής» κάθε ζεύγους σταθμού βάσεων που διεκδικεί το χρησιμοποιημένο κανάλι. Αυτός ο αριθμός αποστέλλεται σε κάθε σταθμό βάσης που χρησιμοποιεί το ίδιο κανάλι. Για να κερδίσει τελικά το κανάλι, ο σταθμός βάσης που εκκίνησε τη διαδικασία θα πρέπει να νικήσει όλους τους επιμέρους «διαγωνισμούς» μεταξύ των σταθμών βάσεων. Νικητής θεωρείται ο σταθμός βάσης που έχει το μεγαλύτερο αριθμό όπως αυτός έχει επιλεχθεί τυχαία από το διάστημα [0, W]. Με την αποχώρηση του σταθμού βάσης από το κανάλι, εξασφαλίζεται μεγαλύτερος λόγος σήματος προς παρεμβολές τόσο για αυτόν όσο και για τις υπόλοιπες κυψέλες, αυξάνοντας τη δυνατότητα προσφοράς υπηρεσιών (βλ. [67]). Παρόλο που η συγκεκριμένη μέθοδος θεωρείται αρκετά δημοφιλής, θεωρείται αρκετά επιρρεπής σε επιθέσεις στις οποίες κάποιος κακόβουλος, αναλαμβάνοντας το ρόλο ενός

«πειραγμένου» BS, θα μπορούσε να επιλέγει έναν αριθμό (όχι τυχαία) κερδίζοντας συνεχώς τις διεκδικήσεις του χρησιμοποιημένου καναλιού.

4.1.5 Προοπτικές εφαρμογής του 802.22

Ενδιαφέρον παρουσιάζει και η μελέτη ερευνητικής ομάδας σχετικά με τις προοπτικές εφαρμογής του προτύπου 802.22 στην Ιαπωνία (βλ. [57]). Όπως είναι γνωστό, ο πρωταρχικός σχεδιασμός του 802.22 πραγματοποιήθηκε με βάση την τρέχουσα κατάσταση στις Ηνωμένες Πολιτείες σε αρκετούς τομείς μεταξύ των οποίων περιλαμβάνονται :

- Το κανονιστικό πλαίσιο με την απελευθέρωση των μη χρησιμοποιημένων τηλεοπτικών συχνοτήτων από την FCC.
- Γεωγραφικά κριτήρια τα οποία αναδεικνύουν το πρόβλημα που υπάρχει όσον αφορά την προσβασιμότητα στο διαδίκτυο σε μη αστικές περιοχές. Στις ΗΠΑ το πρόβλημα είναι αρκετά έντονο, καθώς υπάρχουν πολλές μη αστικές περιοχές, γεγονός που αντανακλάται και στο χάσμα (15%), όσον αφορά την ευρυζωνικότητα μεταξύ των αστικών και των μη αστικών περιοχών (βλ. [69]).
- Συγκεκριμένες τεχνολογίες που χρησιμοποιούνται (όπως για τη μετάδοση του τηλεοπτικού σήματος).

Συνεπώς, η δυνατότητα εφαρμογής του προτύπου και σε άλλες χώρες με ξεχωριστές ιδιαιτερότητες αποκτά ύψιστη σημασία. Στη μελέτη της συγκεκριμένης ερευνητικής ομάδας επισημαίνονται οι διαφορές που υπάρχουν ανάμεσα στις Ηνωμένες Πολιτείες και την Ιαπωνία, οι οποίες ωστόσο δεν καθιστούν σε καμιά περίπτωση απαγορευτική την εφαρμογή του 802.22

Σημαντικό στοιχείο για τον εντοπισμό των πρωτευόντων χρηστών στις Ηνωμένες Πολιτείες αποτελεί η δυνατότητα πρόσβασης σε πληροφορίες που αφορούν τους τηλεοπτικούς σταθμούς που εκπέμπουν, όπως η γεωγραφική τοποθεσία τους, η εμβέλειά τους, ακόμα και η ενεργή ακτινοβολούμενη ισχύς (Effective Radiated Power – ERP). Ωστόσο, τέτοιου είδους πληροφορίες δεν είναι διαθέσιμες στην Ιαπωνία, ρίχνοντας συνεπώς περισσότερο βάρος στη λειτουργία του sensing για τον εντοπισμό των πρωτευόντων χρηστών. Ο σταθμός βάσης δε θα έχει τη δυνατότητα λήψης πληροφοριών για τους τηλεοπτικούς σταθμούς, κάτι που θα ήταν εφικτό στις Ηνωμένες Πολιτείες. Η λειτουργία του sensing αποκτά μεγαλύτερη αξία, χωρίς ωστόσο το γεγονός αυτό να θεωρείται πως αποτελεί σημαντικό εμπόδιο.

Αξίζει να σημειωθεί πως η ρύθμιση του κανονιστικού πλαισίου για τις ελεύθερες τηλεοπτικές συχνότητες έχει πραγματοποιηθεί μόνο από τον κυβερνητικό φορέα των ΗΠΑ (FCC), χωρίς ο αντίστοιχος ιαπωνικός φορέας (MIC) να έχει προβεί σε ανάλογη ενέργεια. Ωστόσο, επικρατεί αισιοδοξία πως η MIC, με την ολοκλήρωση της πλήρους αντικατάστασης των αναλογικών με τις ψηφιακές εκπομπές τηλεοπτικών σημάτων, θα ελευθερώσει όλο το εύρος των VHF συχνοτήτων, επιτρέποντας κατ' επέκταση τη λειτουργία των 802.22 δικτύων. Ακόμα όμως και στην περίπτωση που δεν πραγματοποιηθεί η πλήρης απελευθέρωση των VHF συχνοτήτων, τα δίκτυα 802.22 θα συνυπάρχουν με τους πρωτεύοντες χρήστες βάσει των μεθόδων που έχουν αναλυθεί.

Σημαντική είναι η επισήμανση για την ανάγκη διεύρυνσης των τεχνικών εντοπισμού των τηλεοπτικών σημάτων, έτσι ώστε να συμπεριληφθούν και άλλοι τύποι σημάτων. Σε αντίθεση με τις Ηνωμένες Πολιτείες και την Ευρώπη που χρησιμοποιούν τα συστήματα ATSC και DVB-T για την ψηφιακή μετάδοση αντίστοιχα, στην Ιαπωνία έχει υιοθετηθεί το σύστημα ISDB-T, για το οποίο δεν έχει υλοποιηθεί κάποιος μηχανισμός εντοπισμού. Καθώς δεν υπάρχει η δυνατότητα λήψης γεωγραφικών πληροφοριών για τους τηλεοπτικούς σταθμούς, ούτε και η δυνατότητα ενημέρωσης των συστημάτων 802.22

για την παρουσία αδειοδοτημένων καναλιών, η επέκταση των τεχνικών εντοπισμού, φαντάζει η πιο ευέλικτη λύση.

5 Ασφάλεια

5.1 Δομικά στοιχεία ασφάλειας (ασύρματων) επικοινωνιών

Για την ανάλυση της ασφάλειας των γνωστικών δικτύων, ξεκινάμε με την εισαγωγή ορισμένων βασικών εννοιών ασφάλειας στο πλαίσιο των CR. Μερικά από τα θεμελιώδη δομικά στοιχεία ασφάλειας επικοινωνίας θεωρούμε ότι είναι η διαθεσιμότητα, η ακεραιότητα, η ταυτοποίηση, ο έλεγχος ταυτότητας, η εξουσιοδότηση, η εμπιστευτικότητα και η μη-αναγνώριση.

5.1.1 Διαθεσιμότητα (Availability)

Μία από τις θεμελιώδεις απαιτήσεις για κάθε τύπο δικτύου είναι η διαθεσιμότητα. Αν το δίκτυο είναι κλειστό και δεν δύναται να χρησιμοποιηθεί, ο σκοπός της ύπαρξής του είναι χαμένος. Οι περισσότερες από τις επιθέσεις που ακούμε αυτές τις ημέρες, όπως η άρνηση των επιθέσεων υπηρεσιών (DoS), οι επιθέσεις παρεμβολών, καθώς οι επιθέσεις υπερχείλισης buffer σε ουρές δικτύου, όλες στοχεύουν να καταστήσουν το δίκτυο μη διαθέσιμο είτε προσωρινά είτε μόνιμα (βλ. [43]). Ένα ζήτημα που συνδέεται στενά με τη διαθεσιμότητα του δικτύου είναι η διαθεσιμότητα των στοιχείων. Αυτή είναι η διαθεσιμότητα των δεδομένων (πληροφορίες για το χρήστη, πίνακες δρομολόγησης, κλπ.) για τους χρήστες του δικτύου.

Στα ασύρματα δίκτυα, η διαθεσιμότητα αναφέρεται συνήθως στη διαθεσιμότητα του ασύρματου μέσου μετάδοσης. Διάφορες τεχνικές χρησιμοποιούνται για να εξασφαλίσουν ότι το ασύρματο μέσο επικοινωνίας είναι διαθέσιμο για μετάδοση. Για παράδειγμα, ένας τυχαίος back-off μηχανισμός (βλ. [44]) χρησιμοποιείται για την πρόληψη της σύγκρουσης μεταξύ πολλών χρηστών στο μέσο υπόστρωμα ελέγχου πρόσβασης (MAC) του προτύπου IEEE 802.11 του στρώματος ζεύξης.

Στο πλαίσιο των ΓΕ, η διαθεσιμότητα αναφέρεται στην ικανότητα των πρωτογενών και δευτερογενών χρηστών να έχουν πρόσβαση στο φάσμα συχνοτήτων. Όσον αφορά τους πρωτογενείς (αδειοδοτημένους) χρήστες, η διαθεσιμότητα αναφέρεται στο να είναι σε θέση να μεταδώσουν στην παραχωρούμενη ζώνη χωρίς επιζήμιες παρεμβολές από τους δευτερεύοντες χρήστες. Από τον ορισμό των δυναμικών μεθόδων πρόσβασης στο ραδιοφάσμα , η διαθεσιμότητα φάσματος για τους πρωτογενείς χρήστες είναι εγγυημένη (βλ. [45]). Για τους δευτερεύοντες (χωρίς άδεια) χρήστες, η διαθεσιμότητα αναφέρεται στην ύπαρξη τμημάτων του φάσματος, όπου ο δευτερεύον χρήστης μπορεί να μεταδώσει χωρίς να προκαλεί επιβλαβείς παρεμβολές στους πρωτεύοντες χρήστες. Αν και οι μελέτες έχουν δείξει ότι μεγάλα τμήματα αδειοδοτημένου φάσματος συχνοτήτων είναι διαθέσιμα για ευκαιριακή χρήση, η διαθεσιμότητα του φάσματος προς τους δευτερεύοντες χρήστες δεν είναι εγγυημένη. Στα κεντρικά συστήματα ΓΕ, η διαθεσιμότητα αναφέρεται επίσης στην διαθεσιμότητα των δευτερευόντων σταθμών βάσης (βλ. [43]). Μηχανισμοί ασφαλείας θα πρέπει να διασφαλίζουν ότι οι επιθέσεις DoS (Denial-of-Service) εναντίον δευτερευόντων σταθμών βάσης αντιμετωπίζονται κατάλληλα.

5.1.2 Ακεραιότητα (Integrity)

Τα δεδομένα που είναι υπό διέλευση στο δίκτυο θα πρέπει να προστατεύονται από κακόβουλη τροποποίηση, προσθήκη, διαγραφή ή επανάληψη. Η ακεραιότητα είναι μια

διαβεβαίωση ότι τα δεδομένα που λαμβάνονται είναι ακριβώς όπως αυτά εστάλησαν από το εξουσιοδοτημένο πρόσωπο. Ωστόσο, ορισμένα τμήματα των δεδομένων είναι ευμετάβλητα, χρειάζονται δηλαδή να τροποποιηθούν νομίμως καθώς κινούνται από τον έναν κόμβο στον άλλο. Για το λόγο αυτό, οι περισσότερες από τις τεχνικές που χρησιμοποιούνται για να εξασφαλίσουν την ακεραιότητα εκτελούν επιλεκτική ακεραιότητα πεδίου (παρέχει ακεραιότητα μόνο για τα επιλεγμένα μη-ευμετάβλητά πεδία) (βλ. [46]).

Η ακεραιότητα είναι εξαιρετικά σημαντική σε ασύρματα δίκτυα, επειδή, σε αντίθεση με τα αντίστοιχα ενσύρματα, το ασύρματο μέσο είναι εύκολα προσβάσιμο από τους εισβολείς. Για αυτόν τον λόγο στα ασύρματα τοπικά δίκτυα προστίθεται ένα πρόσθετο στρώμα ασφάλειας το στρώμα ζεύξης, για να κάνει τις ασύρματες συνδέσεις τόσο ασφαλείς όσο και οι ενσύρματες συνδέσεις. Το πρωτόκολλο ασφαλείας που χρησιμοποιείται σε αυτό το στρώμα ονομάζεται CCMP (Counter mode encryption with CBC-MAC Protocol, κρυπτογράφηση με λειτουργία μετρητή με πρωτόκολλο ταυτοποίησης CBC-MAC) (βλ. [47]). Το πρωτόκολλο CCMP χρησιμοποιεί το προηγμένο πρότυπο κρυπτογράφησης (Advanced Encryption Standard,AES) (βλ. [48]) σε λειτουργία μπλοκ κρυπτογράφησης για να παράγει έναν έλεγχο ακεραιότητας μηνύματος (MIC) (βλ. [49]), ο οποίος χρησιμοποιείται για την επαλήθευση της ακεραιότητας του μηνύματος από τον παραλήπτη. Αυτές οι τεχνικές μπορούν επίσης να χρησιμοποιηθούν στις ΓΕ.

5.1.3 Ταυτοποίηση (Identification)

Η ταυτοποίηση είναι μία από τις βασικές απαιτήσεις ασφαλείας για κάθε συσκευή επικοινωνίας. Πρόκειται για μια μέθοδο που συνδέει ένα χρήστη / συσκευή με το όνομα ή την ταυτότητά της. Για παράδειγμα, σε δίκτυα κινητής τηλεφωνίας, οι κινητές συσκευές παρέχονται με ένα στοιχείο αναγνώρισης που ονομάζεται αναγνωριστικό διεθνή εξοπλισμού κινητού (International Mobile Equipment Identifier, IMEI). Αυτό το αναγνωριστικό χρησιμοποιείται για να προσδιορίσει μοναδικά τις κινητές συσκευές στα δίκτυα κινητής τηλεφωνίας. Ομοίως, ένας απαραβίαστος μηχανισμός αναγνώρισης θα πρέπει να βασίζεται στις δευτερεύουσες συσκευές των χρηστών στις ΓΕ.

5.1.4 Έλεγχος Ταυτότητας (Authentication)

Ο έλεγχος ταυτότητας είναι μια διασφάλιση ότι ο φορέας επικοινωνίας είναι αυτός που ισχυρίζεται ότι είναι. Ο πρωταρχικός στόχος ενός συστήματος ελέγχου ταυτότητας είναι να αποτρέψει μη εξουσιοδοτημένους χρήστες από το να αποκτήσουν πρόσβαση στα προστατευμένα συστήματα. Είναι μια απαραίτητη διαδικασία που επαληθεύει τόσο την ταυτότητα όσο και την εξουσιοδότηση. Από την πλευρά του φορέα παροχής υπηρεσιών, ο έλεγχος ταυτότητας προστατεύει το φορέα παροχής υπηρεσιών από μη εξουσιοδοτημένο εισβολέα στο σύστημα. Οι περισσότεροι από τους μηχανισμούς διασφάλισης ταυτότητας βασίζονται σε μια κεντρική αρχή έκδοσης πιστοποιητικών (Certificate Authority,CA) που είναι αποδεκτή από όλους τους χρήστες του δικτύου. Ένα τυπικό πρωτόκολλο ελέγχου ταυτότητας θα απαιτούσε από τους ομότιμους φορείς να πάρουν την ταυτότητά τους υπογεγραμμένη (χρησιμοποιώντας το δημόσιο κλειδί κρυπτογράφησης) από την (CA) και τα ψηφιακά υπογεγραμμένα πιστοποιητικά που ανταλλάσσονται και επαληθεύονται από τους άλλους για να διασφαλιστεί η αυθεντικότητα. Μόλις η αυθεντικότητα των συνομιλητών εγκατασταθεί ξεκινά η τακτική επικοινωνία.

Στα συστήματα ΓΕ, υπάρχει η ανάγκη να γίνει διάκριση μεταξύ αρχικών και δευτερευόντων χρηστών. Επομένως, ο έλεγχος ταυτότητας μπορεί να θεωρηθεί ως μία από τις βασικές προϋποθέσεις για τα γνωστικά δίκτυα. Στα κεντρικά γνωστικά δίκτυα,

όπου οι αρχικοί και δευτερεύοντες σταθμοί βάσης συνδέονται σε ένα ενσύρματο δίκτυο κορμού, μπορεί να είναι ευκολότερο να έχουμε (CA) συνδεδεμένο στον ενσύρματο σκελετό. Ωστόσο, σε κατανεμημένα γνωστικά δίκτυα με μια σειρά από δευτερεύοντες χρήστες διασκορπισμένους σε μια μεγάλη γεωγραφική περιοχή, η παροχή λειτουργιών (CA) μπορεί να είναι μια πρόκληση (βλ. [50]).

5.1.5 Εξουσιοδότηση (Authorization)

Διαφορετικές οντότητες του δικτύου έχουν διαφορετικά επίπεδα εξουσιοδότησης. Για παράδειγμα, το σημείο ασύρματης πρόσβασης έχει την άδεια για να αφαιρέσει ένα πιθανώς κακόβουλο χρήστη από την πρόσβαση στο δίκτυο. Άλλοι χρήστες στο δίκτυο δεν έχουν αυτό το προνόμιο. Η πολιτική ελέγχου πρόσβασης στο δίκτυο περιγράφει το επίπεδο της άδειας για κάθε μία από τις οντότητες. Στο πλαίσιο των γνωστικών δικτύων, έχουμε μια μοναδική απαίτηση αδειοδότησης που ονομάζουμε άδεια υπό όρους. Είναι υπό όρους, διότι οι δευτερεύοντες χρήστες επιτρέπεται να εκπέμπουν σε εξουσιοδοτημένες ζώνες μόνο εφόσον δεν έρχονται σε αντίθεση με τους βασικούς/αρχικούς χρήστες επικοινωνίας στην εν λόγω ζώνη. Δεδομένου ότι είναι δύσκολο να εντοπίσουμε ποιοί ακριβώς από τους δευτερεύοντες χρήστες είναι υπεύθυνοι για επιβλαβείς παρεμβολές στη μετάδοση των αρχικών, αυτός ο τύπος της άδειας είναι δύσκολο να εφαρμοστεί και, ακόμη περισσότερο, σε ένα κατανεμημένο περιβάλλον. Ως εκ τούτου, η υπό όρους άδεια συνιστά τη μοναδική επιλογή στην δυναμική πρόσβαση στο φάσμα.

5.1.6 Εμπιστευτικότητα (Confidentiality)

Η εμπιστευτικότητα είναι στενά συνδεδεμένη με την ακεραιότητα. Ενώ η ακεραιότητα διαβεβαιώνει ότι στα δεδομένα δεν πραγματοποιήθηκαν κακόβουλες αλλαγές κατά τη διαμετακόμιση, η εμπιστευτικότητα διασφαλίζει ότι τα δεδομένα (στη μετασχηματισμένη τους μορφή) είναι ακατανόητα σε μη-εξουσιοδοτημένη (και ενδεχομένως κακόβουλη) οντότητα. Αυτό επιτυγχάνεται με τη χρήση των αλγόριθμων κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων που πρέπει να διαβιβάζονται με ένα μυστικό κλειδί που μοιράζεται μόνο στους δικαιούχους. Τα κρυπτογραφημένα δεδομένα στη συνέχεια μεταδίδονται και μόνο οι παραλήπτες με ένα έγκυρο κλειδί μπορούν να τα αποκρυπτογραφήσουν και να τα διαβάσουν.

Δεδομένου ότι το ασύρματο μέσο είναι ανοιχτό για τους εισβολείς, το IEEE 802.11 LAN χρησιμοποιεί την κρυπτογράφηση AES σε κατάσταση λειτουργίας μετρητή στο CCMP πρωτόκολλο (βλ. [47]) για την κρυπτογράφηση των δεδομένων στο στρώμα ζεύξης ως ένα επιπλέον επίπεδο ασφάλειας. Η επιρρεπής σε λάθη και θορυβώδης φύση του ασύρματου μέσου αποτελεί μια μοναδική πρόκληση τόσο για την εμπιστευτικότητα όσο και για την ακεραιότητα των μηχανισμών. Αυτό συμβαίνει επειδή το σύνολο σχεδόν των τεχνικών εμπιστευτικότητας και ακεραιότητας βασίζονται σε αλγόριθμους κρυπτογράφησης που είναι ευαίσθητοι σε σφάλματα διαύλων και διαγραφών. Αυτή η ιδιότητα ευαισθησίας κάτω από θορυβώδεις συνθήκες ενεργοποιεί την υπερβολική αναμετάδοση καταναλώνοντας μεγάλο εύρος ζώνης του δικτύου (βλ. [51],[52]). Το θέμα αυτό είναι ακόμη πιο έντονο στα συστήματα ΓΕ, όπου η δευτερεύουσα πρόσβαση των χρηστών στο δίκτυο είναι ευκαιριακή και η διαθεσιμότητα του φάσματος δεν είναι εγγυημένη.

5.1.7 Μη αναγνώριση (Non-reputation)

Οι τεχνικές μη αναγνώρισης (βλ. [53]) εμποδίζουν είτε τον αποστολέα είτε τον παραλήπτη από το να αρνηθεί ένα μεταδιδόμενο μήνυμα. Επομένως, όταν ένα μήνυμα

στέλνεται, ο παραλήπτης μπορεί να αποδείξει ότι πράγματι το μήνυμα εστάλη από τον υποτιθέμενο αποστολέα. Ομοίως, όταν ένα μήνυμα λαμβάνεται, ο αποστολέας μπορεί στην πραγματικότητα να αποδείξει ότι τα στοιχεία είναι του υποτιθέμενου παραλήπτη. Στη ρύθμιση των συστημάτων ΓΕ, εάν διαπιστωθεί ότι κακόβουλοι δευτερογενείς χρήστες παραβιάζουν το πρωτόκολλο, τεχνικές μη-αναγνώρισης μπορούν να χρησιμοποιηθούν για να αποδείξουν την ανάρμοστη συμπεριφορά και να διαχωρίσουν ή να απαγορεύσουν τους κακόβουλους χρήστες από το δευτερεύον δίκτυο.

5.2 Ανάγκη για ασφαλή επικοινωνία

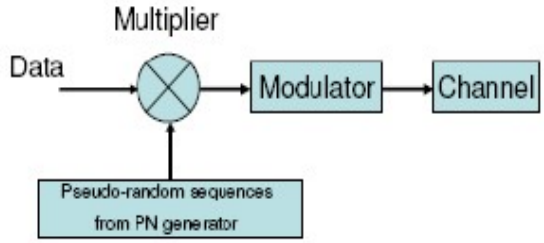
Σε αυτό το άκρως ανταγωνιστικό κόσμο, οι κίνδυνοι των οικονομικών και πολιτικών κατασκοπειών έχουν αυξηθεί πάρα πολύ βάζοντας έτσι πολλά κρατικά περιουσιακά στοιχεία καθώς και ατομικά σε κίνδυνο. Πολλές από τις τεχνικές που χρησιμοποιούνται για τη διεξαγωγή επικοινωνίας είναι επισφαλείς, με την έννοια ότι η ασφάλειά τους μπορεί να παραβιαστεί και κατά συνέπεια σημαντικές συζητήσεις μπορεί να ακούγονται ή να καταγράφονται. Ακόμα πολλές από αυτές τις τεχνικές δεν απαιτούν την πιστοποίηση του ατόμου που έρχονται σε επικοινωνία. Για παράδειγμα: οι GSM υπηρεσίες, αν και παρέχουν καλή συνδεσιμότητα, είναι επιρρεπείς σε πολλές απειλές κατά της ασφάλειας. Ακόμη και τα τυπικά κινητά τηλέφωνα δεν παρέχουν ασφάλεια από άκρο σε άκρο. Ως εκ τούτου, μπορούμε να πούμε ότι η ασφαλής επικοινωνία είναι απαραίτητη για τη σύνδεση και την παροχή της μετάδοσης, της επεξεργασίας, της καταγραφής και της παρακολούθησης για διάφορους σκοπούς, όπως: ο ασφαλής τηλεφωνικός και δικτυακός εξοπλισμός και η διαχείριση του κλειδιού κρυπτογράφησης, οι ασφαλείς συνδέσεις δεδομένων προς και από το έδαφος καθώς και τις δορυφορικά απομακρυσμένες πλατφόρμες, για τη συλλογή πληροφοριών σε πραγματικό χρόνο, καθώς και για την επικοινωνία μεταξύ των επανδρωμένων διαστημικών πτήσεων, κλπ.

5.2.1 Πιθανές λύσεις για ασφαλή συστήματα επικοινωνιών

Πολλές από τις υπάρχουσες τεχνολογίες έχουν τέτοια ικανότητα που αν συνδυαστεί με τη γνωστική τεχνολογία ραδιοεπικοινωνιών μπορεί να προσφέρει μια μορφή επικοινωνίας χωρίς κοινές απειλές για την ασφάλεια. Η τεχνική της εξάπλωση του διευρυμένου φάσματος είναι μία από αυτές. Ακόμη και οι βασικές τεχνολογίες κρυπτογράφησης, όπως το δημόσιο κλειδί και το ιδιωτικό κλειδί κρυπτογράφησης μπορούν να χρησιμοποιηθούν σε συνδυασμό με σύστημα ΓΕ για τέτοιους σκοπούς. Παρακάτω θα συζητήσουμε τη δυνατότητα μιας ασφαλούς μορφής επικοινωνίας με τη χρήση της τεχνικής εξάπλωσης του διευρυμένου φάσματος με συστήματα ΓΕ.

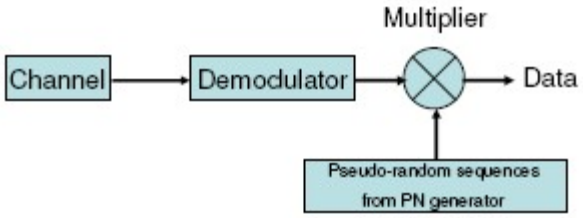
5.2.1.1 Διαμόρφωση διευρυμένου φάσματος

Ορισμός. "Διευρυμένο φάσμα (Spread Spectrum,SS) είναι ένα μέσο μετάδοσης στο οποίο ένα σήμα καταλαμβάνει ένα εύρος ζώνης σε περίσσεια του ελάχιστου αναγκαίου για την αποστολή πληροφοριών (η διάδοση της ζώνης επιτυγχάνεται με τη βοήθεια ενός κώδικα που είναι ανεξάρτητος από τα στοιχεία, και χρησιμοποιεί την συγχρονισμένη λήψη με τον κωδικό στο δέκτη για την ανασύνταξη και την επακόλουθη ανάκτηση των δεδομένων)". Όπως φαίνεται στο **σχήμα 32**, το σήμα δεδομένων πρώτα πολλαπλασιάζεται με μία ψευδοτυχαία ακολουθία γνωστή ως κώδικα διασποράς, στη συνέχεια διαμορφώνεται (χρησιμοποιώντας κωδικοποίηση μετατόπισης φάσης) και τέλος μεταδίδεται μέσω του καναλιού.



Σχήμα 32. Τμήμα πομπού στην τεχνική διεύρυνσης φάσματος

Στην πλευρά του δέκτη, όπως φαίνεται στο **σχήμα 33**, πρώτα το εισερχόμενο σήμα ελέγχεται για το εάν περιέχει κάποιο περιεχόμενο θορύβου (ανάλογα με τα χαρακτηριστικά θορύβου του διαύλου) και στην περίπτωση που περιέχει πρώτα απομακρύνεται πρώτα ο θόρυβος και στη συνέχεια αποδιαμορφώνεται το σήμα (με βάση την τεχνική διαμόρφωσης που έχει χρησιμοποιηθεί στην πλευρά του πομπού).



Σχήμα 33. Τμήμα δέκτη στην τεχνική διεύρυνσης φάσματος

Τώρα, το αποδιαμορφωμένο σήμα πολλαπλασιάζεται με την ίδια ψευδοτυχαία ακολουθία που χρησιμοποιήθηκε στην αρχή και έτσι παίρνουμε το τελικό σήμα πληροφοριών. Το τμήμα δέκτη είναι όπως φαίνεται παραπάνω. Βλέπουμε λοιπόν ότι σε μια τεχνική SS, για να ανακτηθεί το αρχικό σήμα που αποστέλλεται από την πλευρά του αποστολέα, είναι απαραίτητη η γνώση των ψευδοτυχαίων ακολουθιών. Επιπλέον τα δεδομένα, αφού έχουν πολλαπλασιαστεί με την αλληλουχία PN γίνεται να μετατραπούν σε ένα σήμα ευρείας ζώνης κερδίζοντας έτσι μορφή και χαρακτηριστικά παρόμοια με το θόρυβο. Αυτό το μοναδικό χαρακτηριστικό της τεχνικής διαμόρφωσης φασματικής διεύρυνσης την καθιστά ξεχωριστή από τις άλλες υπάρχουσες τεχνικές διαμόρφωσης με τέτοιο τρόπο ώστε να επιτρέπει στα δεδομένα που κρύβονται ανάμεσα στο τυχαίο θόρυβο που υπάρχει ή που παράγεται στο σύστημα και ως εκ τούτου παρέχει μια διαφυγή από οποιονδήποτε τρίτο (προσπαθώντας να γλιστρήσει στην εν εξελίξει επικοινωνία). Αυτή η ποιότητα του αλγορίθμου διαμόρφωσης φασματικής διεύρυνσης μπορεί να αξιοποιηθεί για να παρέχει ένα ασφαλές και αξιόπιστο περιβάλλον επικοινωνίας.

5.2.1.2 Τεχνικές κρυπτογράφησης

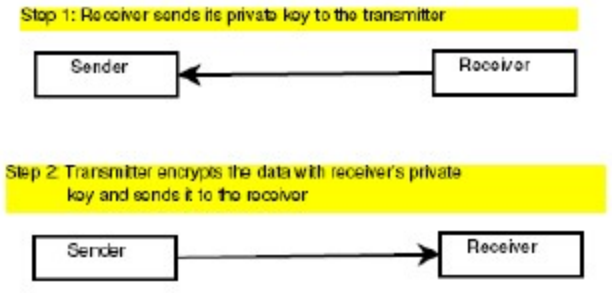
Έχει γίνει πια αναγκαιότητα το να κρατηθούν τα δεδομένα κρυμμένα από τα αδιάκριτα βλέμματα, προκειμένου να διατηρηθεί η ασφάλεια. Και για να επιτευχθεί αυτό έχουν προταθεί διάφορες τεχνικές κρυπτογράφησης (βλ. [70]). Κρυπτογράφηση (encryption)

είναι ο μετασχηματισμός των δεδομένων σε μορφή που δεν μπορεί να διαβαστεί από κανένα παρά μόνο από αυτόν που διαθέτει ένα κατάλληλο κλειδί. Υπάρχουν δύο μεγάλες οικογένειες αλγόριθμων κρυπτογράφησης, οι συμμετρικοί αλγόριθμοι (ή αλγόριθμοι ιδιωτικού κλειδιού) και οι ασύμμετροι (ή αλγόριθμοι δημόσιου κλειδιού).

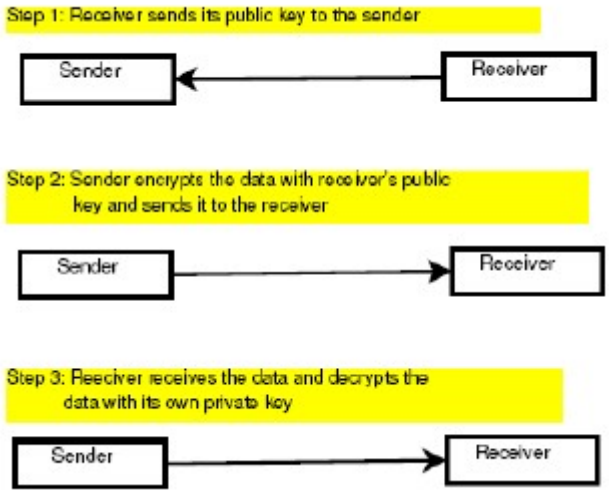
Στους συμμετρικούς αλγόριθμους το κλειδί κρυπτογράφησης μπορεί να υπολογιστεί από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση και το ανάποδο. Μάλιστα στις περισσότερες περιπτώσεις τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια. Αυτοί οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια. Η ασφάλεια των αλγόριθμων βασίζεται στην μυστικότητα αυτού του κλειδιού. Για όσο καιρό επιθυμούμε η επικοινωνία να παραμείνει μυστική, για τον ίδιο καιρό πρέπει και το κλειδί να παραμείνει μυστικό. Ο αλγόριθμος κρυπτογράφησης ιδιωτικού κλειδιού φαίνεται στο **σχήμα 34**. Οι συμμετρικοί αλγόριθμοι μπορούν να διαιρεθούν σε δύο υποκατηγορίες: α) αλγόριθμοι ροής (stream ciphers) οι οποίοι λειτουργούν bit προς bit και β) μπλοκ αλγόριθμοι (block ciphers) οι οποίοι λειτουργούν πάνω σε κομμάτια δεδομένων (συνήθως των 64 bit).Παραδείγματα συμμετρικών αλγορίθμων είναι οι DES, Triple-DEA, AES.

Οι ασύμμετροι αλγόριθμοι ή αλγόριθμοι δημόσιου κλειδιού είναι σχεδιασμένοι έτσι ώστε το κλειδί που χρησιμοποιείται για την κρυπτογράφηση να είναι διαφορετικό από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση. Πέρα από αυτό, το κλειδί αποκρυπτογράφησης δεν μπορεί να υπολογιστεί από το κλειδί κρυπτογράφησης. Οι αλγόριθμοι αυτοί καλούνται και "δημόσιου κλειδιού" γιατί το κλειδί κρυπτογράφησης μπορεί να δημοσιοποιηθεί. Ο καθένας μπορεί να κρυπτογραφήσει ένα μήνυμα με το δημόσιο κλειδί αλλά μόνο αυτός που διαθέτει το αντίστοιχο ιδιωτικό κλειδί μπορεί να το αποκρυπτογραφήσει. Η τεχνική κρυπτογράφησης του αλγόριθμου δημόσιου κλειδιού είναι όπως φαίνεται στο **σχήμα 35**. Παραδείγματα ασύμμετρων αλγορίθμων είναι οι RSA, ElGamal και DSA.

Οι συμμετρικοί αλγόριθμοι είναι πολύ πιο γρήγοροι από τους ασύμμετρους αλγόριθμους, εφαρμοσμένοι είτε σε υλικό είτε σε λογισμικό. Ως εκ τούτου οι συμμετρικοί αλγόριθμοι χρησιμοποιούνται για την κρυπτογράφηση του κυρίου μέρους των δεδομένων, ενώ οι αλγόριθμοι δημόσιου κλειδιού βρίσκουν κατάλληλη εφαρμογή σε πρωτόκολλα ανταλλαγής κλειδιών και ψηφιακών υπογραφών.



Σχήμα 34. Κρυπτογράφηση ιδιωτικού κλειδιού



Σχήμα 35. Κρυπτογράφηση δημοσίου κλειδιού

5.3 Ασφαλής επικοινωνία ΓΕ

Οι βασικές συνιστώσες ενός δικτύου ΓΕ είναι οι ακόλουθες:

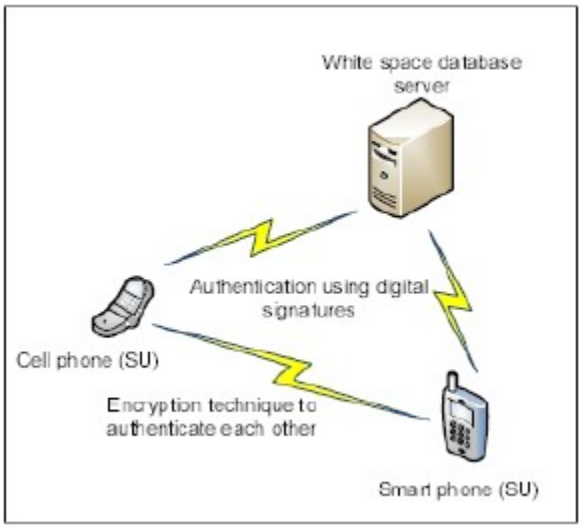
- Επιβεβλημένη προστασία των χρηστών με τη χρήση ανίχνευσης φάσματος,
- Λευκό διάστημα πρόσβασης σε βάσεις δεδομένων
- Ασφάλεια στην πρόσβαση σε βάση δεδομένων και αδειοδοτημένο φάσμα,
- Κοινή χρήση του ραδιοφάσματος

Για την τέλεια γνώση των πρωτογενών χρηστών στο αδειοδοτημένο φάσμα, οι δευτερεύοντες χρήστες αναμένεται να έχουν πρόσβαση σε βάση δεδομένων λευκού διαστήματος όπως στο **σχήμα 36**, δηλαδή, βάση δεδομένων που περιέχει πληροφορίες των πρωτογενών χρηστών σε κάθε αδειοδοτημένη ζώνη. Η FCC έχει αναθέσει την ανίχνευση φάσματος (βλ. [71]) καθώς και την πρόσβαση σε αυτό στη βάση δεδομένων λευκού διαστήματος. Η ανίχνευση φάσματος είναι μια τεχνική που χρησιμοποιείται από ένα σύστημα ΓΕ για την ανίχνευση οπών στο αδειοδοτημένο φάσμα. Οι υπάρχουσες ερευνητικές εργασίες έχουν προτείνει τη χρήση των χαρακτηριστικών του φυσικού στρώματος και του στρώματος ελέγχου πρόσβασης στο μέσο (MAC) του πρωτογενούς σήματος του χρήστη για να την ανίχνευση τέτοιων φασματικών οπών. Η διαδικασία ανίχνευσης φάσματος περιλαμβάνει δύο τύπους σφαλμάτων: mis-ανίχνευση (ύπαρξη του νόμιμου χρήστη σε μία ζώνη ανιχνεύεται για να είναι σε αδράνεια) και ψευδείς συναγερμούς (μια αδρανής ζώνη ανιχνεύεται ως κατεχόμενη ζώνη). Η ασφάλεια στο πλαίσιο των δικτύων ΓΕ μοιράζεται σε τρία στάδια:

• Έλεγχος ταυτότητας του συστήματος ΓΕ

• Έλεγχος ταυτότητας των δύο χρηστών που είναι σε επικοινωνία

• Διασφάλιση της ασφάλεια κατά το χρονικό διάστημα επικοινωνία μεταξύ των χρηστών.



Σχήμα 36. Ασφάλεια σε συστήματα ΓΕ

- **Βήμα 1:** Πιστοποίηση ενός συστήματος ΓΕ

Ο έλεγχος ταυτότητας ενός συστήματος ΓΕ μπορεί να διεξαχθεί χρησιμοποιώντας ψηφιακές υπογραφές (βλ. [70]).

- **Βήμα 2:** Έλεγχος ταυτότητας ενός γνωστικού χρήστη

Δημόσιες και ιδιωτικές βασικές τεχνικές κρυπτογράφησης κλειδιού χρησιμοποιούνται για τον έλεγχο ταυτότητας των ΓΕ.

- **Βήμα 3:** Ασφαλής γνωστικές επικοινωνίες

Μόλις ελεγθεί η ταυτότητα των ΓΕ, το επόμενο βήμα είναι να εξασφαλιστεί η ασφάλεια στη δυνατότητα ανταλλαγής πληροφοριών. Υποτίθεται ότι όλοι οι γνωστικοί χρήστες διαθέτουν ιστορικές πληροφορίες σχετικά με την πληρότητα των κύριων χρηστών στο επιθυμητό φάσμα. Από την άποψη της λειτουργίας ενός συστήματος ΓΕ ένα λειτουργικό φάσμα ραδιοσυχνοτήτων χωρίζεται σε N μη-επικαλυπτόμενες υποζώνες. Το σύνολο των υπο-ζωνών συμβολίζεται με Sub = {1, 2,. . . , N}. Με βάση την ιστορική πληροφορία, θεωρείται περαιτέρω ότι η πιθανότητα της πληρότητας του κύριου χρήστη σε κάθε υπο-συγκρότημα είναι γνωστή σε κάθε σύστημα ΓΕ. Ας ορίσουμε ως p_i την πιθανότητα της i-υποζώνης να είναι ελεύθερη σε κάθε στιγμή του χρόνου. Σύμφωνα με αυτές τις πιθανότητες των ελεύθερων υποζωνών, τα συστήματα ΓΕ διαχωρίζουν τις επιμέρους ζώνες σε τρεις διαφορετικές κατηγορίες: μικρή πιθανότητα, μεγάλη πιθανότητα, και μέτρια πιθανότητα να είναι ελεύθερη. Ο αριθμός των υποζωνών με μικρές πιθανότητες του να είναι ελεύθερη παριστάνεται ως $N_{freesmall}$, με μεγάλες πιθανότητες ως $N_{freelarge}$ και με μέτριες πιθανότητες ως $N_{freemod}$. Η διανομή του $N_{freesmall}$ (βλ. [72]), και η πιθανότητα ότι υπάρχουν k ελεύθερες υποζώνες είναι:

$$Pr(N_{free_{small}} = k) \simeq \frac{{\lambda_g}^k e^{-\lambda_g}}{k!} = Pr_{Poi}(N_{free_{small}} = k), \quad (1)$$

όπου $\lambda_g = \Sigma_{i \in Subsmall} p_i$. Αυτή η προσέγγιση ακολουθεί έναν αποκαλούμενο νόμο σπάνιων γεγονότων. Έχουμε επίσης το ακόλουθο λήμμα που δίνει ένα άνω φράγμα του σφάλματος της προσέγγισης. Η κατανομή των $N_{freemod}$ για τον Sub_{mod} (βλ. [72]) και η πιθανότητα να υπάρχουν k ελεύθερες υποζώνες είναι:

$$Pr(N_{free_{mod}} = k) \simeq \int_{k-\frac{1}{2}}^{k+\frac{1}{2}} \frac{1}{\sqrt{2\pi C_n}} e^{-\left(\frac{(x-\overline{N}_{mod})^2}{2C_n}\right)} dx = Pr_{Normal}(N_{free_{mod}} = k), \quad (2)$$

όπου n είναι το μέγεθος του Sub_{mod}, k = 0, 1, • • •, n, $N_{mod} = E[N_{freemod}] = \Sigma_{i2Submod} p_i$, και $C_n = \Sigma_{i2Submod} p_i (1- p_i)$ αντιπροσωπεύει τη διακύμανση του $N_{freemod}$. Η προσέγγιση της κατανομής του $N_{freelarge}$ ακολουθεί ουσιαστικά την πορεία που έθεσε $N_{freesmall}$. Σημειώστε ότι $(1 - p_i)$ είναι μικρή για i 2 Sub_{large}. Χρησιμοποιώντας το νόμο των Σπάνιων Γεγονότων, η κατανομή των $N_{freelarge}$ μπορεί επίσης να προσεγγιστεί από μια κατανομή Poisson. Το ακόλουθο λήμμα διευκολύνει τον υπολογισμό της κατανομής πιθανοτήτων των $N_{freelarge}$. Για k = 0, 1, • • •, (N-m - n), έχουμε

$$Pr(N_{free_{large}} = k) \simeq \frac{e^{-\lambda_l} \lambda_l^{[N-m-n-k)}}{(N-m-n-k)!} = Pr_{Poi}(N_{free_{large}} = k), \quad (3)$$

όπου $\lambda_1 = \Sigma_{i2Sublarge} (1- p_i)$. Συνεπώς, η πιθανότητα να είναι ελεύθερες k υπο-ζώνες σε οποιοδήποτε σημείο χρόνου δίνεται από: $P_r (N_{free} = k)$

$$= \sum Pr(N_{free_{small}} = k_1) Pr(N_{free_{mod}} = k_2) Pr(N_{free_{large}} = k_3) \quad (4)$$

όπου το άθροισμα λαμβάνεται πάνω από όλα $k_1 \geq 0$, $k_2 \geq 0$, και $k_3 \geq 0$ με $k_1 + k_2 + k_3 = k$. Με αυτή την προκαταρκτική γνώση, ένας γνωστικός χρήστης υπολογίζει το μέγιστο πιθανό αριθμό των ελεύθερων υποζωνών που διατίθενται για τις επικοινωνίες του. Η κεντρική ιδέα της υπολογισμό αυτής της πιθανότητας είναι για να υπολογιστεί ο πιθανός αριθμός των ελεύθερων υποζώνων τις οποίες ένα σύστημα ΓΕ αλλάζει κατά τη διάρκεια της επικοινωνίας. Ένας γνωστικός χρήστης χρησιμοποιεί αυτές τις πληροφορίες μαζί με τις πληροφορίες που λαμβάνονται από τη βάση δεδομένων του λευκού διαστήματος για να κατανοήσει την ακολουθία της αλλαγής του σχεδίου για την επικοινωνία του. Μόλις οι δύο γνωστικοί χρήστες έχουν πιστοποιηθεί οι ίδιοι για να είναι γνήσιοι, ο χρήστης που μεταδίδει μεταφέρει το χρονοπρόγραμμα που προορίζεται για τον παραλήπτη του. Η διαδικασία αυτή εξασφαλίζει ότι μόνο οι χρήστες που προορίζονται έχουν επίγνωση της μεταγωγής συχνοτήτων. Υποκλοπές μπορεί να

οδηγήσουν σε μερικό συμβιβασμό των πληροφοριών σε κακόβουλους χρήστες, αλλά όχι για όλα τα μέρη του.

- Συγχώνευση διαμόρφωσης διευρυμένου φάσματος με ΓΕ

Η τεχνολογία ΓΕ όταν συνδυάζεται με τις τεχνικές διαμόρφωσης διευρυμένου φάσματος (όπως Direct αλληλουχία, hopping συχνότητας και του χρόνου hopping) μπορεί να παρέχει μια λύση αποδίδοντας ασφαλή συστήματα επικοινωνιών. Αν και η τεχνολογία ΓΕ είναι πολύ προσαρμοστική, αλλάζοντας συνεχώς τις ζώνες συχνοτήτων με βάση τη διαθεσιμότητα τους, μπορεί να σχεδιαστεί ένα τέτοιο σύστημα που να μπορεί να παρακολουθήσει τα χαρακτηριστικά των λειτουργικών του συστήματος ΓΕ και ως εκ τούτου η μετάδοση να μπορεί να εντοπιστεί. Αλλά με τον συνδυασμό της τεχνικής διαμόρφωσης διευρυμένου φάσματος, οι πιθανότητες του εντοπισμού της μετάδοσης είναι πολύ λιγότερες. Στην τεχνική SS, το σήμα στενής ζώνη μεταμορφώνεται σε ένα ευρυζωνικό σήμα, για να πολλαπλασιάζεται ψευδοτυχαία με ένα σήμα (αρχικά ένα σήμα ευρείας ζώνη). Αυτό το μετασχηματισμένο σήμα ευρείας ζώνη έχει χαρακτηριστικά πολύ παρόμοια με το τυχαίο παρόν σήμα θορύβου στο περιβάλλον και ως εκ τούτου είναι πολύ δύσκολο από το παρεισφρέον μέρος να σχεδιάσει ένα τέτοιο σύστημα που θα μπορούσε να προσαρμοστεί σε σχέση με το θόρυβο (όπως είναι τυχαίο) και επομένως η μετάδοση παραμένει ανεπηρέαστη από οποιοδήποτε είδος παραβίασης.

6 Επιθέσεις

Η ασφάλεια είναι αναγκαία στα CRNs επειδή το κανάλι δεδομένων είναι εύκολα προσβάσιμο από έναν εισβολέα. Στο πλαίσιο των CRNs, ορίζουμε τις επιθέσεις ώς τις ενέργειες που συμβάλλουν στην επίτευξη τουλάχιστον ενός από τους ακόλουθους στόχους:

• **Απαράδεκτη παρέμβαση για άδεια κύριων χρηστών**: Λόγω της επίθεσης, η επικοινωνία των καναλιών των πρωτογενών / αδειοδοτημένων χρηστών της ζώνης συχνοτήτων μειώνεται ή απλά γίνεται άχρηστη (denial-of-service(DoS)επίθεση).

• **Χαμένες ευκαιρίες για τους δευτερεύον χρήστες:** Ένας εισβολέας θα μπορούσε να αποτρέψει δευτερεύον χρήστες από την χρήση των διαθέσιμων ζωνών φάσματος έτσι, για άλλη μια φορά, μειώνοντας την απόδοση του καναλιού ή απλώς με το να αρνηθεί υπηρεσία στους δευτερεύον χρήστες

• **Η πρόσβαση σε προσωπικά δεδομένα:** Ένας εισβολέας θα μπορούσε να προσπαθήσει να έχει πρόσβαση στα δεδομένα με μη εξουσιοδοτημένο τρόπο. Κατά συνέπεια τα δεδομένα πρέπει να εξασφαλίζονται με τη βοήθεια των κρυπτογραφικών αρχέτυπων.

• **Τροποποίηση των δεδομένων:** Ένας εισβολέας θα μπορούσε να προσπαθήσει να τροποποιήσει τα δεδομένα που ανταλλάσσονται μεταξύ διαφόρων οντοτήτων και προς όφελός του. Έτσι, η ακεραιότητα των δεδομένων πρέπει να εξασφαλίζεται.

• **Η έγχυση ψευδή στοιχείων:** Η έγχυση ψευδή στοιχείων θα μπορούσε να κάνει το CRN να εκτελέσει με πρωτοφανή τρόπο ή απλά να ακολουθήσει τις οδηγίες του εισβολέα. Ως εκ τούτου, η κύρωση των πηγών πληροφοριών πρέπει να είναι εγγυημένη.

ΣΤΡΩΜΑΤΑ				
ΕΠΙΘΕΣΕΙΣ	**ΦΥΣΙΚΟ**	**ΖΕΥΞΗΣ**	**ΔΙΚΤΥΟΥ**	**ΜΕΤΑΦΟΡΑΣ**
		Spoofing /Sybil		
	jamming		Packet injection	Jellyfish
	PUE attack	selfish		Lion
	OFA	Selective forwarding		
	CCDA	False feedback		
		Worn/sink - hole		

Πίνακας 4. Επιθέσεις στα CRNs

Δεδομένου ότι οι τελευταίοι τρεις στόχοι επίθεσης σε γενικές γραμμές έχουν μελετηθεί από την κρυπτογραφική κοινότητα, θα επικεντρωθούμε στα δύο πρώτα αυτά που έχουν πολύ σχέση με τη φύση των CRN. Στον παραπάνω **Πίνακα 4** παρέχουμε μια περίληψη των επιθέσεων σε CRNs, με σαφή προσδιορισμό των νέων κοινών επιθέσεων στα ασύρματα δίκτυα. Οι επιθέσεις έχουν ταξινομηθεί σύμφωνα με το στοχευόμενο στρώμα της στοίβας στο OSI (Open Systems Interconnection). Στη συνέχεια θα περιγράψουμε τις νέες ειδικές επιθέσεις για CRNs: Puea (Primary User emulation attacks, επιθέσεις εξομοίωσης κύριων χρηστών), OFA (Objective Function attacks, επιθέσεις στην αντικειμενική συνάρτηση), CCDA (Common Control

Data attacks, επιθέσεις ελέγχου κοινών δεδομένων), ψευδή ανατροφοδότηση (False Feedback),και επίθεση Lion.

6.1 Primary User Emulation Attacks (PUE Attacks)

Η γνωστή επίθεση παρεμβολών περιλαμβάνει την ακτινοβολία των ραδιοσημάτων που σκόπιμα διακόπτουν τις επικοινωνίες στο επιτιθέμενο δίκτυο. Αν οι παρεμβολές που δημιουργούνται είναι αρκετά μεγάλες, μπορούν να μειώσουν σημαντικά την απόδοση των επικοινωνιών ή ακόμη και να τις σταματήσουν τελείως εφαρμόζοντας μια DoS επίθεση. Η ανίχνευση των παρεμβολών είναι ακόμα πιο δύσκολο στα CRN καθώς οι παρεμβολές μπορούν να δημιουργηθούν με ψευδή κύριους χρήστες και επομένως η πηγή επίθεσης δύσκολα μπορεί να ανιχνευθεί. Επιπλέον, καθώς η επίθεση παρεμβολών απευθύνεται στις συχνότητες των θυμάτων, σε CRNs θα αναγκάσει πιθανότατα μια συχνότητα handoff να υποστεί σημαντική καθυστέρηση. CRS ή δευτερεύοντες χρήστες έχουν τη δυνατότητα να λειτουργούν σε αδειοδοτημένες ζώνες με βάση μη-παρέμβαση, και συνεπώς είναι απαραίτητο να ανιχνεύουν συνεχώς το μέσο με σκοπό την ανίχνευση της παρουσίας των πρωτογενών χρηστών. Λόγω αυτού, ένα από τα κλειδιά για την επιτυχία των CRNs είναι η ανάπτυξη αποτελεσματικών μηχανισμών ανίχνευσης φάσματος. Είναι όμως επίσης απαραίτητο, να έχουν την ικανότητα να διακρίνουν δευτερεύοντες χρήστες που συνδέονται με άλλα CRNs από κατεστημένους φορείς: αν ένα πρωτεύον σήμα ανιχνεύεται σε μία δεδομένη συχνότητα, δευτερεύοντες χρήστες πρέπει να στραφούν σε μία από τις κενές ζώνες (μια διαδικασία γνωστή ως μεταβίβαση φάσματος). Από την άλλη πλευρά, εάν ένας άλλος δευτερεύον χρήστης λειτουργεί ήδη σε τέτοια ζώνη, συνύπαρξη των μηχανισμών απαιτείται για να μοιραστεί δίκαια το φάσμα.

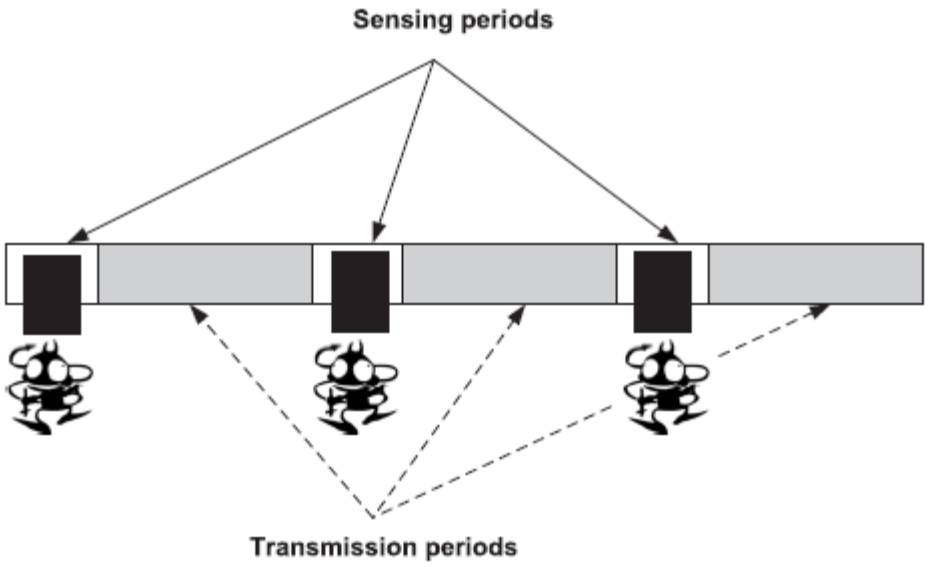
Το γεγονός αυτό δημιουργεί ένα κενό ασφαλείας στο σύστημα, καθώς ένας εισβολέας θα μπορούσε να προσποιηθεί ότι είναι ένας εν ενεργεία χρήστης με την εκπομπή ενός σήματος με παρόμοια χαρακτηριστικά με ένα πρωτογενές σήμα, εμποδίζοντας έτσι δευτερεύοντες χρήστες να χρησιμοποιούν κενές ζώνες. Η επίθεση αυτή, επινοήθηκε (βλ. [24]), σαν PUE attack, και είναι αρκετά ρεαλιστική, δεδομένης της ευελιξίας που προσφέρουν τα CRs ως προς τις παραμέτρους μετάδοσης. Η δυνατότητα αυτή ενισχύει την ανάγκη για μηχανισμούς ανιχνεύσεως που να αναγνωρίζουν αποτελεσματικά πρωτογενή σήματα.

Υπάρχουν πολλές προσεγγίσεις για την ανίχνευση φάσματος (βλ. [25]). Η πιο συνηθισμένη, η ανίχνευση της ενέργειας βασίζεται στην απλότητα, με την οποία το σήμα ανιχνεύεται σε σύγκριση με την έξοδο του ανιχνευτή με ένα όριο. Εξαιτίας αυτού, ο μηχανισμός ανίχνευσης είναι ιδιαίτερα ευαίσθητος σε μεταβαλλόμενα επίπεδα θορύβου, και εύκολα οδηγεί σε ψευδώς θετικά αποτελέσματα. Επιπλέον, παρουσιάζει άλλα μειονεκτήματα, όπως η ανικανότητα διάκρισης μεταξύ των σημάτων, των παρεμβολών και του θορύβου, και το γεγονός ότι δεν λειτουργεί για την ανίχνευση φασματικής εξάπλωσης, έχει ως άμεση συνέπεια, την αναπήδηση των σημάτων συχνότητας. Στην περίπτωση των CRNs με την ενέργεια να βασίζεται στην ανίχνευση φάσματος, ένας εισβολέας θα πρέπει απλώς να μεταδώσει οποιοδήποτε είδος σήματος όταν δεν υπάρχουν πρωτογενείς μεταδόσεις που να λαμβάνουν χώρα και να εμφανιστεί ως κατεστημένος φορέας για δευτερεύοντες χρήστες.

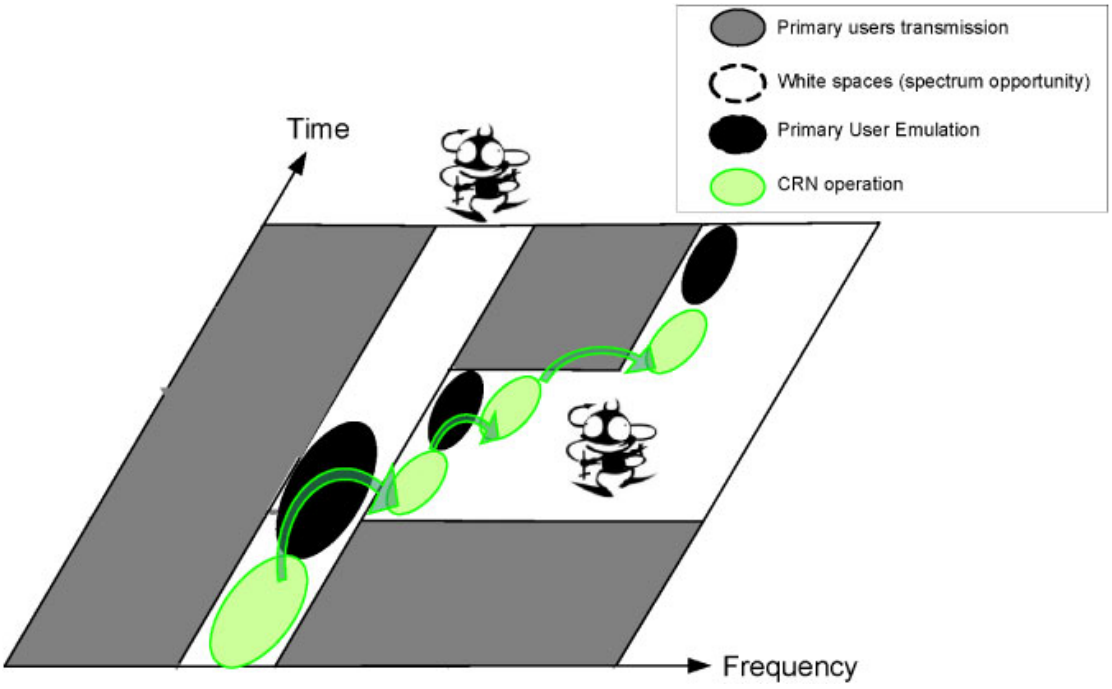
Υπάρχουν και άλλοι μηχανισμοί, όπως του προσαρμοσμένου φίλτρου, του κυκλοστάσιμου χαρακτηριστικού ανίχνευσης, ή της κυματομορφής που βασίζονται στην ανίχνευση φάσματος, και είναι πιο αποτελεσματική λύση αλλά σε αντίθεση απαιτούν κάποια προηγούμενη γνώση του σήματος. Ως εκ τούτου, αυτό θα σήμαινε αποθήκευση

των πληροφοριών των συστημάτων ΓΕ σχετικά με τα πρότυπα του σήματος όλων των τύπων των πρωτογενών μεταδόσεων. Τα προγράμματα αυτά μπορεί να περιπλέξουν μια PUE attack αλλά όχι να την αποφύγουν, αφού ένας εισβολέας μπορεί να εξακολουθεί να μεταδώσει ένα σήμα με τα ίδια φασματικά χαρακτηριστικά ως νόμιμο πρωτογενές σήμα.
Ενδεικτικά, ο εισβολέας θα μπορούσε να μεταδώσει εύκολα ένα τηλεοπτικό σήμα χρησιμοποιώντας ένα πομπό TV Ultra High Frequency (UHF) ή απλά να επαναλάβει ένα πραγματικό τηλεοπτικό σήμα.

Έχοντας κάποια γνώση του CRN μπορούμε να εκτελέσουμε μια πιο συγκεκριμένη PUE attack. Για παράδειγμα, στα IEEE 802.22 δίκτυα, ο εισβολέας θα μπορούσε να εκμεταλλευτεί το συγχρονισμό των δευτερογενών χρηστών που απαιτούνται κατά τη διάρκεια των περιόδων ανίχνευσης. Στο 802.22, ο σταθμός βάσης είναι υπεύθυνος για τις ήσυχες χρονικές περιόδους στις οποίες οι μεταδόσεις δεν επιτρέπεται να διεξάγουν ανίχνευση φάσματος και να εντοπίσουν πρωτογενή σήματα. Κάθε μετάδοση που εντοπίζεται κατά τη διάρκεια αυτής της περιόδου μπορεί να θεωρηθεί ως πρωτογενές σήμα. Έτσι, ένας κακόβουλος χρήστης θα μπορούσε να μεταδώσει μόνο κατά τη διάρκεια των περιόδων ανίχνευσης για να εκτελέσει την επίθεση DoS όπως φαίνεται στο **Σχήμα 37**.



Σχήμα 37. Ασύγχρονη μεταφορά



Σχήμα 38. Dos μέσω διαδοχικών PUEA

Ένα άλλο παράδειγμα (βλέπε **Σχήμα 38**) είναι ένας εισβολέας που εκτελεί νέες PUE attacks όποτε οι CRN εναλλάσσονται από το ένα κανάλι στο άλλο (μεταβίβαση συχνότητας) υποβαθμίζοντας έτσι την απόδοση δεδομένων στο CRN ή οδηγώντας σε DoS. Θεωρείται δεδομένο ότι ο εισβολέας θα βρεί το επόμενο κανάλι λειτουργία CRN σε ένα περιορισμένο χρονικό διάστημα που καθορίζεται από:

• **την ανίχνευση των μέσων ενημέρωσης μέχρι την εύρεση του νέου καναλιού της λειτουργίας**.
Ο εισβολέας θα μπορούσε να απορρίψει κάποια πολύ απίθανα κανάλια ή απλώς να απαγορεύσει κανάλια (σε χρήση από τα πρωτογενή σήματα) για την ελαχιστοποίηση του χρόνου αναζήτησης του καναλιού. Επιπλέον, ο εισβολέας μπορεί να εκτιμήσει το πιο πιθανό νέο κανάλι CRN βασιζόμενος στις τοπικές ανιχνεύσεις.

• **Ο επιτιθέμενος αποκτά το επόμενο hop από υποκλοπές των κοινών στοιχείων ελέγχου του CRN (CCDA).**

Ο αντίκτυπος της PUE attack εξαρτάται από πολλούς παράγοντες, όπως η θέση του επιτιθέμενου και η ευαισθησία των ΓΕ στις μετρήσεις τους. Επιλέγοντας μια βέλτιστη θέση για να εκτελέσει την επίθεση θα προκαλέσει πολλούς δευτερογενείς χρήστες να καταλήξουν στο συμπέρασμα ότι μια δεδομένη ζώνη είναι απασχολημένη και να αναζητούν ένα άλλο μη κατειλημμένο τμήμα του φάσματος. Από την άλλη πλευρά, όταν μια μέθοδος βασισμένη στην ενέργεια χρησιμοποιείται για την ανίχνευση κύριων χρηστών, η οριακή τιμή θα παίξει επίσης σημαντικό ρόλο: όσο χαμηλότερο είναι το όριο τόσο πιο εύκολο να εκτελεστεί μια PUE attack. Σύμφωνα με το στόχο της επίθεσης, ταξινομούμε PUE attacks σε κακόβουλες επιθέσεις ή εγωιστικές. Ο στόχος των κακόβουλων επιθέσεων είναι να αποτρέψουν τους δευτερεύοντες χρήστες από τον εντοπισμό κενών ζωνών και τη χρήση τους (DoS), ενώ οι εγωιστικές επιθέσεις στοχεύουν στη μεγιστοποίηση της χρήσης του ραδιοφάσματος από τον εισβολέα.

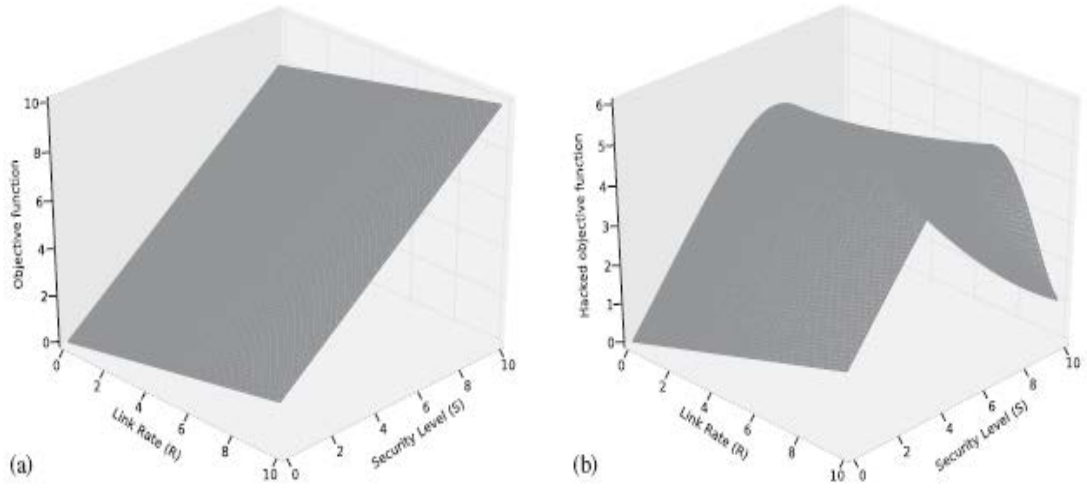
6.2 Επιθέσεις στην αντικειμενική συνάρτηση (Objective Function Attacks,OFA)

Μέσα σε ένα CRN, οι κατεστημένοι φορείς ελέγχουν διάφορες παραμέτρους ραδιοφάσματος για να ενισχύσουν την απόδοση του δικτύου. Η επιλογή των παραμέτρων γίνεται συχνά με τη βοήθεια αλγόριθμου τεχνητής νοημοσύνης (AI), όπως genetic, hill-climbing, ή random walks ή γενικότερα αλγορίθμου βελτιστοποίησης (βλ. [26]). Τέτοιοι αλγόριθμοι κάνουν ελαφρές τροποποιήσεις αρκετών παραγόντων εισόδου για την εύρεση των βέλτιστων τιμών που μεγιστοποιούν μια αντικειμενική συνάρτηση ή στόχο. Στο πλαίσιο των συστημάτων ΓΕ, παράγοντες εισόδου μπορεί να είναι η συχνότητα, το εύρος ζώνης, η ισχύς, ο τύπος διαμόρφωσης, ο ρυθμός κωδικοποίησης του πρωτόκολλου πρόσβασης στο κανάλι, ο τύπος κρυπτογράφησης, ο τύπος πιστοποίησης, ο κωδικός μηνύματος ακεραιότητας και το μέγεθος του πλαισίου (βλ. [42]).

Εντός μίας από τις απλούστερες προσεγγίσεις μπορούμε να οριοθετήσουμε μια αντικειμενική συνάρτηση βασισμένη στο βάρος με μόνο δύο στόχους: το υψηλό ποσοστό σύνδεσης και την ασφάλεια. Ως παράδειγμα μπορούμε να ορίσουμε μια αντικειμενική συνάρτηση βασισμένη στο βάρος, στην οποία οι διαφορετικές απαιτήσεις της κάθε υπηρεσίας θα καθορίζουν το βάρος που ανατίθεται σε κάθε στόχο. Από τη μία πλευρά, σε μεταδόσεις πολυμέσων υψηλό ποσοστό σύνδεσης θα είχε και το μεγαλύτερο βάρος, αλλά από την άλλη πλευρά, τα δεδομένα των συναλλαγών θα απαιτούσαν περισσότερη ασφάλεια. Με αυτούς τους στόχους μπορούμε να υποδηλώσουμε μια συνάρτηση βάρους, όπως στην **έκφραση(1)**, όπου R το ποσοστό σύνδεσης, S το προκαθορισμένο επίπεδο ασφάλειας, και ω_i το βάρος της παραμέτρου i.

$$f(R, S)=\omega_R R+\omega_S S \quad \textbf{(1)}$$

Για την ασφάλεια των συναλλαγών των δεδομένων, μια αντικειμενική συνάρτηση βαρών θα μπορούσε να οριστεί, π.χ. ω_R=0,2 και ω_S=0.8. Υπό κανονικές συνθήκες σεναρίου, το σύστημα ΓΕ θα μεταβάλει τις παραμέτρους του ραδιοφάσματος για την εύρεση του μέγιστου της αντικειμενικής συνάρτησης που είναι προφανώς οτι επιτυγχάνεται όταν οι δύο τιμές πάρουν τη μέγιστη δυνατή πιθανή τιμή. Το **Σχήμα 39 α** αντιπροσωπεύει f (R, S), R ∈ [0, 10], S ∈ [0, 10], ω_R=0,2 και ω_S=0,8.



Σχήμα 39. (α) αντικειμενικές λειτουργίες (β) αντικειμενικές λειτουργίες μετά από OFA

Το επίπεδο ασφαλείας S ορίζεται ως ένας χρήστης/πολιτική εισόδου, αλλά αντίθετα ο ρυθμός σύνδεσης R σχετίζεται περισσότερο με τις συνθήκες του καναλιού. Έτσι, επηρεάζοντας το κανάλι, ένας εισβολέας μπορεί να χειριστεί το ρυθμό σύνδεσης με τη παρεμβολή παρασίτων στο κανάλι. Τώρα φανταστείτε ότι ένας εισβολέας είναι σε θέση να υποκλέψει (hack) ένα επίπεδο ασφαλείας s1, αλλά όχι κάτι περισσότερο από αυτό. Για να απαγορευτεί S>s1, ο εισβολέας μπορεί να παρεμβάλει παράσιτα στο κανάλι κάθε φορά που το επίπεδο ασφαλείας S≥ s1. Ο αντίπαλος χρειάζεται μόνο να πάρει την αντικειμενική συνάρτηση και να είναι όσο στην **έκφραση(2).**

$$f(R, S)=\omega_R R+\omega_S S < \omega_R r_1+\omega_S s_1 \;\forall\; S>s_1 \quad (2)$$

Αυτό σημαίνει ότι ο επιτιθέμενος πρέπει να παρεμβάλει παράσιτα στο κανάλι για να διατηρήσει ένα ρυθμό μετάδοσης, όπως της **έκφρασης(3).**

$$0\leq R<r_1+ (\omega_S / \omega_R) (s_1- S) \;\forall\; S>s_1 \quad (3)$$

Ας υποθέσουμε ότι λόγω της επίθεσης η αναπαράσταση της αντικειμενικής συνάρτησης είναι αυτή στο **Σχήμα 34(β)**. Τώρα, ο αλγόριθμος (AI) θα προσαρμόζει τις παραμέτρους ραδιοφάσματος μέχρι να βρει τις τιμές που μεγιστοποιούν την αντικειμενική συνάρτηση. Ωστόσο, δεν μπορεί να πάρει τα καλύτερα αποτελέσματα, λόγω της παραπλάνησης της αντικειμενικής συνάρτησης, η συσκευή ΓΕ θέτει ένα επίπεδο ασφαλείας της s1, το οποίο μπορεί να υποκλαπεί από τον εισβολέα.

Είναι αναγκαίο να παρατηρήσουμε ότι η απόδοση OFA είναι πολύ σχετική με την ποσότητα του online εκμάθησης του CRN. Η online μάθηση αναφέρεται σε μια online βελτιστοποίηση του χώρου αναζήτησης. Από την άλλη πλευρά, τα ραδιοφάσματα που εκτελούν offline μάθηση παρατηρούν το περιβάλλον μόνο μία φορά, και στη συνέχεια, αναζητούν μια βέλτιστη διαμόρφωσης offline (π.χ. μόνο μετά από μια προκαθορισμένη πολιτική ραδιοφάσματος), καθώς η διαμόρφωση αυτών των ραδιοσυχνοτήτων είναι ανεξάρτητα από τις παρατηρήσεις τους, η offline μάθηση δεν επηρεάζεται από την OFAs. Ωστόσο, οι συσκευές ραδιοφάσματος που χρησιμοποιούν μόνο offline μάθηση δεν απαιτούν ένα μηχανισμό θεωρητικής μάθησης και συνεπώς δεν μπορούν να θεωρηθούν, σαν συστήματα ΓΕ. Έτσι, κάθε CRN είναι εκτεθειμένη σε επιθέσεις OFA.

6.3 Επιθέσεις ελέγχου κοινών δεδομένων (Common control data attacks, CCDA)

Σε ορισμένες προσεγγίσεις, ένα αποκλειστικό κανάλι χρησιμοποιείται για την ανταλλαγή πληροφοριών ανίχνευσης: (α) μεταξύ του σταθμού βάσης και των δευτερευόντων χρηστών, εάν το CRN είναι κεντρικό και (β) μεταξύ των δευτερευόντων χρηστών, εάν είναι κατανεμημένο. Ένας κακόβουλος χρήστης θα μπορούσε να παρεμβάλει παράσιτα στο κανάλι, διαταράσσοντας τελείως όλες τις μεταδόσεις και την πρόληψη των στοιχείων εντός του CRN από την ανταλλαγή πληροφοριών σχετικά με τη χρήση φάσματος (βλ. [22]). Η έλλειψη γνώσης για τις διαθέσιμες φασματικές ζώνες διατηρεί το CRN από λειτουργικές (DoS επίθεσης). Επιπλέον, υποκλοπές στα δεδομένα ελέγχου παρέχονται στον εισβολέα με όλες τις απαραίτητες πληροφορίες για τον εντοπισμό σε ποιο νέο κανάλι CRN να στραφούν. Η ανάγκη για διασφάλιση των κοινών στοιχείων ελέγχου είναι, ως εκ τούτου πασιφανές. Στο 802.22 η ομάδα εργασίας έχει επίγνωση αυτής της απειλής και έχει προτείνει μηχανισμούς για την προστασία αυτών των πληροφοριών (βλ. [27]). Θεωρούμε ότι ο αντίκτυπος αυτής της επίθεσης είναι πιο σημαντικός σε κεντρικά CRN καθώς κάποιος εισβολέας μπορεί να επικεντρωθεί στην παρεμβολή παρασίτων του καναλιού ελέγχου εντός της περιοχής του σταθμού βάσης (μοναδικό σημείο αποτυχίας) και επηρεάζοντας έτσι εύκολα το σύνολο του δικτύου.

6.4 Ψευδής ανατροφοδότηση (False feedback)

Μέσα σε ένα πλαίσιο συνεργασίας, όπου οι δευτερεύοντες χρήστες ανταλλάσσουν πληροφορίες ανίχνευσης, ψευδείς πληροφορίες από έναν ή μια ομάδα από κακόβουλους χρήστες θα μπορούσαν να οδηγήσουν το CRN να λάβει ακατάλληλες ενέργειες (βλ. [23]). Για παράδειγμα, το CRN θα μπορούσε να συμπεράνει ότι μια συγκεκριμένη ζώνη συχνοτήτων καταλαμβάνεται από ένα κύριο χρήστη όταν στην πραγματικότητα αυτό δεν συμβαίνει ή το αντίθετο, θα μπορούσε να θεωρηθεί ως μια κενή ζώνη όταν χρησιμοποιείται από ένα πρωτεύον δίκτυο. Στην πρώτη περίπτωση, ο εισβολέας εμποδίζει το CRN από τη χρήση μιας διαθέσιμης ζώνης. Στην τελευταία ,αν το CRN αποφασίσει να χρησιμοποιήσει την εν λόγω ζώνη να λειτουργεί, μεταδόσεις των δευτερογενών χρηστών θα μπορούσαν να επηρεάσουν αρνητικά τα πρωτογενή σήματα. Κατά τη γνώμη μου, ο κίνδυνος αυτός είναι ιδιαίτερα σημαντικός για πλήρως κατανεμημένο CRN επειδή ψευδή ανατροφοδότηση θα μπορούσε να διαδοθεί, επηρεάζοντας έτσι ένα μεγάλο τμήμα του δικτύου. Ένα τέτοιο αποτέλεσμα συχνά αναφέρεται ως ένας ιός που οφείλεται σε ανεπιθύμητη διανομή του, αλλά αντιθέτως με έναν «παραδοσιακό» ιό, εφαρμόζεται στο στρώμα συνδέσμου αντί για αυτό της εφαρμογής.

Από την άλλη πλευρά, σε κεντρικά δίκτυα, 802,22 ο σταθμός συλλέγει μετρήσεις ανίχνευσης από όλα τα συστήματα ΓΕ για να καθορίσει ποιες είναι οι ζώνες συχνοτήτων που καταλαμβάνονται. Παρά το γεγονός ότι το πρότυπο IEEE 802.22 ορίζει ότι η τελική απόφαση σχετικά με τη διαθεσιμότητα ενός καναλιού πρέπει να εκτελείται στο σταθμό βάσης, δεν προσδιορίζει πώς θα πρέπει να γίνει. Γενικά σε αυτή την περίπτωση ένας κακόβουλος χρήστης θα μπορούσε εύκολα να εντοπιστεί, καθώς οι πληροφορίες που παρέχονται μπορεί να είναι άτοπες. Ωστόσο, εξακολουθούν να υπάρχουν πολλές περιπτώσεις κατά τις οποίες μια ψεύτικη έκθεση από ένα μεμονωμένο χρήστη μπορεί να έχει αρνητική επίδραση στη λειτουργία του CRN: λαμβάνοντας υπόψη τη μεγάλη περιοχή κάλυψης του δικτύου 802.22, είναι πολύ

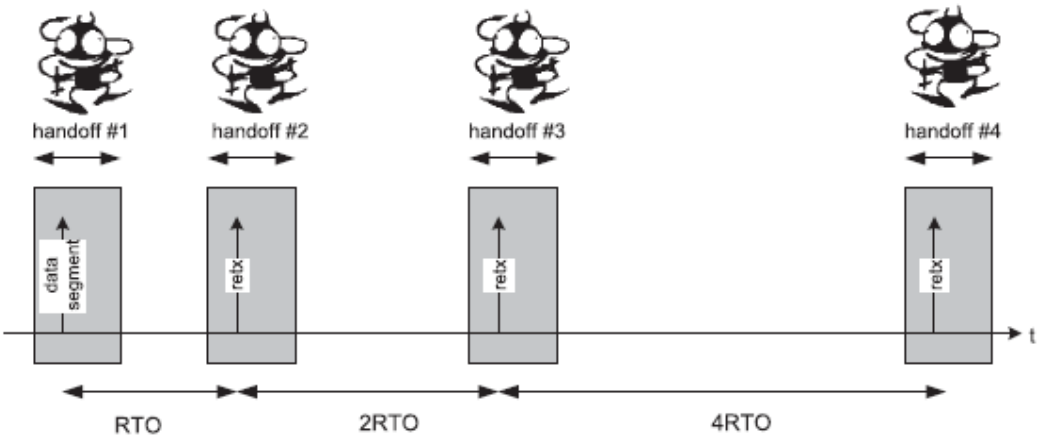
πιθανό ότι οι δύο δευτερεύοντες χρήστες λαμβάνουν εντελώς διαφορετικές μετρήσεις αν βρίσκονται, για παράδειγμα, ο ένας κοντά στο σταθμό βάσης και ο άλλος στα όρια της περιοχής κάλυψης. Σε τέτοιου είδους σενάρια, θα είναι σημαντικά δυσκολότερο να ανιχνευθεί αν μια συγκεκριμένη έκθεση είναι αξιόπιστη ή όχι.

6.5 Επιθέσεις Lion

Ορίσαμε την επίθεση Lion ως μια στοχευμένη παρεμβολή για τη μείωση της απόδοσης του Πρωτόκολλου Ελέγχου Μετάδοσης (TCP) με τον καταναγκασμό μεταβιβάσεων συχνότητας. Η διαδικασία μεταβίβασης περιλαμβάνει το μέσο ανίχνευσης να ψάχνει για κενά κανάλια και να επιλέγει το καλύτερο σύμφωνα με ορισμένα κριτήρια, αναλαμβάνοντας έτσι πολύ μεγάλες καθυστερήσεις έως ότου η μετάδοση να βρεθεί σε συνέχεια. Ένας κακόβουλος χρήστης που προσπαθεί να διαταράξει μια σύνδεση TCP από ένα δευτερεύον χρήστη μπορεί να εκτελέσει μια Puea για να αναγκάσει μια μεταβίβαση της CRN. Καθώς το στρώμα μεταφοράς δεν είναι ενήμερο για την αποσύνδεση, αυτό συνεχίζει να στέλνει τα τμήματα δεδομένων που βρίσκονται σε σειρά αναμονής σε χαμηλότερα στρώματα, αλλά δεν μεταδίδονται και έτσι TCP τμήματα μπορεί να καθυστερήσουν ή ακόμη και να χαθούν. Δεδομένου ότι ο αποστολέας TCP επιτρέπει να μεταδίδουν τα νέα δεδομένα μετά τη λήψη των αναγνωρίσεων, η απώλεια ή καθυστέρηση των τμημάτων μπορεί να οδηγήσει σε μια περίοδο αδράνειας.

Είναι καλά γνωστό ότι το TCP ενεργοποιεί ένα χρονόμετρο αναμετάδοσης (Retransmission Timer, RTO) για κάθε εκκρεμή τμήμα, το οποίο καθορίζει το χρόνο που ο αποστολέας περιμένει για την αντίστοιχη αναγνώριση προτού εξετάσει το τμήμα που έχει χαθεί. Αν το χρονόμετρο αναμετάδοσης λήγει για ένα δεδομένο τμήμα, ο TCP αποστολέας αναμεταδίδει και μειώνει το παράθυρο συμφόρησης, δεδομένου ότι θεωρείται ως ένα σήμα συμφόρησης. Η αξία που αποδίδεται στο χρονόμετρο αναμετάδοσης εξαρτάται από την εκτίμηση του γύρου του χρόνου ταξιδιού (Round Trip Timer, RTT) που εκτελείται από τον αποστολέα TCP και συνεπώς, εάν η περίοδος ελεγχοδότησης είναι αρκετά μεγάλη αυτό θα οδηγήσει στην λήξη των πολλών χρονομετρητών και την υποβάθμιση της απόδοσης. Όσο μεγαλύτερη είναι η διάρκεια μεταβίβασης τόσο πιο δραστική είναι η μείωση της απόδοσης του.

Επιπλέον, ο εισβολέας μπορεί να εκτελέσει μια έξυπνη επίθεση Lion αν καταφέρει να εκτελέσει μια μεταβίβαση όταν ο αποστολέας TCP προσπαθεί να μεταδώσει μια δεδομένη κατηγορία. Σε γενικές γραμμές, το RTO είναι μια μεταβλητή που εξαρτάται από την εκτίμηση RTT, των TCP υλοποιήσεων που ορίζουν μια ελάχιστη τιμή για το RTO. Στο (βλ. [28]) η συνιστώμενη τιμή είναι 1s και οι εφαρμογές χρησιμοποιούν τυπικές τιμές που κυμαίνονται από 100 έως 200ms. Σε κάθε περίπτωση, η ελάχιστη RTO είναι πολύ υψηλότερη από τα RTT δειγμάτων που λαμβάνονται για μια δεδομένη σύνδεση εντός της CRN (της τάξεως των μικροδευτερολέπτων ή λίγα χιλιοστά του δευτερολέπτου). Κατά συνέπεια, μια σταθερή τιμή RTO θα χρησιμοποιείται για όλα τα τμήματα και θα διπλασιάζεται για κάθε ανεπιτυχείς αναμετάδοση. Έτσι, ένας εισβολέας μπορεί να επωφεληθεί από αυτή την πληροφορία και να ενδυναμώσει μεταβιβάσεις σε συγκεκριμένες στιγμές του χρόνου στις οποίες ο αποστολέας TCP αναμεταδίδει δεδομένα, οδηγώντας στην λιμοκτονία του αποστολέα TCP (βλέπε **σχήμα 40**). Για την κατανόηση μας, το γεγονός αυτό δείχνει σαφώς την ανάγκη για cross-layer μηχανισμούς που θα καταστήσουν τα πρωτόκολλα μεταφοράς να αντιλαμβάνονται τις συνθήκες του δικτύου (**βλ. Ενότητα 4.4).**



Σχήμα 40. Ευφυής επίθεση Lion βασισμένη στη πρόβλεψη των χρονομετρών αναμετάδοσης

6.6 Σκοπός των επιθέσεων

Ο **πίνακας 5** παρουσιάζει μία ταξινόμηση των επιθέσεων ακολουθώντας το μοντέλο CIA (εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα). Αυτό σημαίνει ότι οι επιθέσεις που ταξινομούνται ανάλογα με το αν ο στόχος τους θέτει σε κίνδυνο το απόρρητο των αποθηκευμένων / παραδομένων δεδομένων, αλλάζοντας την ακεραιότητα των δεδομένων αυτών, και /ή διακόπτοντας τη διαθεσιμότητα των επικοινωνιών του θύματος. Ο πίνακας δείχνει σαφώς ότι ο κοινός στόχος για τις παρουσιαζόμενες νέες ειδικές επιθέσεις για να CRNs είναι να επηρεάζουν αρνητικά τη διαθεσιμότητα των επικοινωνιών: οι PUE attacks αναγκάζουν μεταβιβάσεις συχνότητας και κατά συνέπεια τη διακοπή των επικοινωνιών προσωρινά, οι OFA, π.χ. εξαπατούν τον αλγόριθμο μάθησης των ΓΕ σε μη βέλτιστη χρήση των παραμέτρων μετάδοσης, οι CCDA χρησιμοποιούν τα δεδομένα που έχουν κρυφακούσει για να συνεχίσουν και να επιτίθονται στο δίκτυο του θύματος, οι ψευδής ανατροφοδότησης επιτίθενται λόγω των χαμένων, πιθανώς καλύτερων ευκαιριών και τέλος η Lion επιτίθεται καθώς υποβαθμίζει την απόδοση των TCP συνδέσεων. Αλλά εκτός από τις επιθέσεις για διαθεσιμότητα, η CCDA είναι επίσης μια απειλή για την εμπιστευτικότητα, καθώς παρέχει στον εισβολέα τη τρέχουσα και τη μελλοντική συμπεριφορά του δικτύου του θύματος, και οι OFAs μπορούν επίσης να επηρεάσει την εμπιστευτικότητα και την ακεραιότητα μειώνοντας το επίπεδο ασφάλειας του επιτιθέμενου δικτύου (βλέπε το παράδειγμα στο 6.2).

Εμπιστευτικότητα (Confidentiality)	**Διαθεσιμότητα (Availability)**	**Ακεραιότητα (Integrity)**
	PUE attack	
OFA	OFA	OFA
CCDA	CCDA	
	False feedback attacks	
	Lion attacks	

Πίνακας 5. Σκοπός των επιθέσεων από την άποψη του CIA μοντέλου

Όσον αφορά τον τύπο του CRN (από την άποψη της κατανομής φάσματος), πιστεύουμε ότι, σε γενικές γραμμές, ιεραρχικά ή μη κατανεμημένα δίκτυα (δηλαδή με ένα σταθερό σταθμό βάσης) θα επηρεάζονται πιο εύκολα από τις περισσότερες από τις επιθέσεις από τα κατανεμημένα. Για παράδειγμα, σε ένα μη κατανεμημένο IEEE 802.22 δίκτυο ο σταθμός βάσης συλλέγει ανίχνευση πληροφοριών που διαβιβάζονται σε όλους τους δευτερεύοντες χρήστες και καθορίζει το χρονικό βήμα στο οποίο ο καθένας επιτρέπεται να μεταδίδει. Η απόφαση έχει σκοπό παγκόσμιας εμβέλειας και οι παράμετροι μοιράζονται από όλους τους συμμετέχοντες CRN. Έτσι, εάν ο σταθμός βάσης λαμβάνει πολλά ψευδή μέτρα που σχετίζονται με μια συγκεκριμένη ζώνη συχνοτήτων (λόγω PUE attack ή ψευδή ανατροφοδότησης επίθεσης), μπορεί να τα θεωρήσει ως μη κατάλληλα για τη μετάδοση, και έτσι κανένας σταθμός δε θα τα χρησιμοποιήσει. Από την άλλη πλευρά, σε ένα κατανεμημένο δίκτυο, δευτερογενείς χρήστες ανταλλάσσουν ανίχνευση πληροφοριών. Στην περίπτωση αυτή, ο αριθμός των χρηστών που επηρεάζονται από PUE attacks ή ψευδή επίθεσης ανατροφοδότηση όχι μόνο θα εξαρτηθεί απο το πρωτόκολλο που χρησιμοποιείται για την αποστολή / λήψη πληροφοριών προς/από άλλους κόμβους (ανίχνευση πληροφορίας που ανταλλάσσονται ανάμεσα σε όλους τους χρήστες ή μόνο μεταξύ των γειτόνων), αλλά και για το αν οι αποφάσεις του φάσματος παίρνονται σε τοπικά ή σε ένα συλλογικό τρόπο. Για παράδειγμα, αν ένας CR εξετάζει μόνο πληροφορίες που αποστέλλονται από hop κόμβους των οποίων τα μέτρα δεν έχουν επηρεαστεί από την επίθεση, μπορεί να συνεχίσει να χρησιμοποιεί αυτή τη ζώνη, ενώ άλλα ΓΕ μπορεί να την απορρίψουν.

Ένας άλλος παράγοντας που πρέπει να ληφθεί υπόψη είναι η λειτουργία του χρησιμοποιούμενου γνωστικού τρόπου για τη λήψη αποφάσεων (δηλαδή για να αποφασίσετε ποιο είναι το καλύτερο κομμάτι του φάσματος για τη μετάδοση). Εάν ένας εισβολέας συνεχίζει να μιμείται κατεστημένα σήματα σε μια δεδομένη ζώνη, τα συστήματα ΓΕ θα μάθουν ότι αυτή η ζώνη είναι πάντα διαθέσιμη και μπορούν να αποφασίσουν να μην την χρησιμοποιούν πια, έτσι ώστε η επίθεση να συνεχιστεί στο χρόνο, ακόμη και αν ο επιτιθέμενος δεν εκτελεί καμία ενέργεια. Κριτήρια, όπως ο αριθμός των μετρήσεων ανίχνευσης και του βάρους ανατίθονται σε καθένα από αυτά, επίσης θα επηρεαστεί στο πεδίο της επίθεσης από άποψη χρόνου και ο αριθμός των χρηστών που επηρεάζονται. Για παράδειγμα, σε μια OFA το μήκος της επίθεσης εξαρτάται σε μεγάλο βαθμό από την ποσότητα των μνημών που χρησιμοποιούνται στη διαδικασία της μάθησης.

7 Securing CR

Σε αυτή την ενότητα θα συζητήσουμε και θα προτείνει αντίμετρα για τις πιθανές επιθέσεις στα CRNs.

7.1 Αντιμετώπιση των επιθέσεων παρεμβολής

Οι περισσότερες από τις επιθέσεις στα CRNs βασίζονται στην παρεμβολή παρασίτων σε συγκεκριμένες συχνότητες. Ασφαλή πρωτόκολλα μπορούν να μετριάσουν πολλούς από τους στόχους του εισβολέα, αλλά δεν μπορούν να αντιμετωπιστούν αποτελεσματικά τις DoS ή το κανάλι υποβάθμισης λόγω των παρεμβολών. Επομένως, ένα παράλληλο σύστημα για την εύρεση της πηγής επίθεσης είναι απαραίτητο. Τα συστήματα ανίχνευσης εισβολών (Intuition Detection Systems, IDSs) αποτελούν πολύτιμα εργαλεία για την ανίχνευση τέτοιων επιτιθέμενων. Τα IDSs μπορούν να ανιχνεύσουν ποιοι κόμβοι είναι ύποπτοι ή κακόβουλοι, και να παρέχουν τις εν λόγω πληροφορίες σε άλλα πρωτόκολλα του κόμβου (π.χ. δρομολόγησης, ή ομαδοποίησης). Η αναζήτηση για τα κατάλληλα IDSs είναι ένα καυτό θέμα σήμερα και πολλές προτάσεις έχουν εμφανιστεί στη βιβλιογραφία.

Στα CRNs, η ανατροφοδότηση από τις συσκευές ΓΕ μπορεί να ενισχύσει την αποτελεσματικότητα των IDSs. Ο πλεονασμός του δικτύου χρησιμοποιείται ως πλεονέκτημα, επειδή η ανατροφοδότηση πολλών συμμετεχόντων μπορεί να οδηγήσει σε μια πιο εύκολη ανίχνευση της πηγής παρεμβολής. Όπως αναφέρεται στο (βλ. [29]), μια αρχιτεκτονική για την καλύτερη ανίχνευση εισβολής για τα ασύρματα δίκτυα ad-hoc πρέπει να είναι κατανεμημένη και συνεργάσιμη. Για την κατανόηση μας, ο ίδιος ισχυρισμός ισχύει και για τα CRNs όπου η συνεργασία είναι εγγενής στη φύση τους. Η καλύτερη προσέγγιση είναι πιθανόν βασισμένη στην ανίχνευση της μη φυσιολογικής λειτουργίας μέσω της ανάλυσης της κυκλοφορίας και της συνεργασίας. Προκειμένου να εκπληρώσει την αποστολή αυτή, τα IDSs πρέπει να λειτουργούν σε κάθε στρώμα δικτύωσης σε ένα cross-layer τρόπο. Διάφορες προσεγγίσεις IDSs (βλ. [29-31]) πληρούν αυτές τις απαιτήσεις, αλλά η συγκεκριμενοποίηση τους στα CRNs εξακολουθεί να είναι μια πρόκληση.

7.2 Αντιμετώπιση των PUE επιθέσεων

Η προστασία από τις επιθέσεις Puea είναι απαραίτητη και επομένως ο σχεδιασμός ισχυρών τεχνικών για την επαλήθευση της αυθεντικότητας των πρωτογενών σημάτων γίνεται πιο απαραίτητος. Ο απλούστερος τρόπος είναι να ενσωματωθεί μια υπογραφή σε ένα επικείμενο σήμα ή να χρησιμοποιηθεί ένα πρωτόκολλο ελέγχου ταυτότητας μεταξύ των αρχικών και των δευτερευόντων χρηστών. Ωστόσο, αυτές οι προσεγγίσεις δεν είναι σύμφωνες με τις απαιτήσεις της FCC (βλ. [32]), η οποία αναφέρει ότι καμιά τροποποίηση στο υφιστάμενο σύστημα δεν θα πρέπει να απαιτείται για να φιλοξενηθεί ευκαιριακή χρήση του φάσματος από τους δευτερογενείς χρήστες. Μια εναλλακτική λύση είναι, όταν πρωτογενείς πομποί έχουν μια σταθερή θέση, όπως το TV συστήματα μετάδοσης, να εκτιμηθεί η θέση τους από την πηγή του σήματος για να ελεγθεί η ταυτότητά τους. Σε αυτήν την περίπτωση, έχοντας προηγούμενη γνώση της θέσης όλων των TV towers θα επιτραπεί να διακρίνουν τους επικείμενους νόμιμους φορείς από τους κακόβουλους χρήστες στην προσπάθεια να εκτελεστεί μια PUE attack. Θα πρέπει να σημειωθεί, ωστόσο, ότι ένας εισβολέας θα μπορούσε να εκπέμπει ακόμη και

σε γειτονικό TV tower για να πάρει γύρω από αυτή τη μέθοδο. Για να αντιμετωπίσει αυτή η συγκεκριμένη PUE attack, οι συγγραφείς στο (βλ. [41]), προτείνουν να χρησιμοποιηθεί εκτός από την εντόπιση των πομπών και το σήμα ανιχνεύσεως επιπέδου ενέργειας. Η προσέγγιση αυτή βασίζεται στις ακόλουθες παραδοχές: (1) ότι πρωτογενείς πομποί είναι TV towers με μια σταθερή γνωστή θέση και με ισχυρή ισχύ μετάδοσης (στην περιοχή των εκατοντάδων κιλοβάτ) και (2) ότι τα CR είναι συσκευές με περιορισμένη ισχύ εκπομπής (που κυμαίνονται από μερικά milliwatts σε λίγα watt). Κατά συνέπεια η ανίχνευση επιπέδου ενέργειας μπορεί σίγουρα να είναι ένα ισχυρό κριτήριο για την επικύρωση της γνησιότητας των πρωτογενών μεταδόσεων.

Παρ' όλα αυτά, το σύστημα αυτό στηρίζεται στην ύπαρξη ενός συνόλου κόμβων μέσα στα CRN που ονομάζονται ελεγκτές θέσης (Location Verifiers, LV), οι οποίοι είναι υπεύθυνοι για τη διεξαγωγή μετρήσεων της ισχύς του σήματος που λαμβάνεται (Received Signal Strength, RSS). Προκειμένου να καθοριστεί αποτελεσματικά η θέση του πομπού απαιτούνται, πολλές μετρήσεις RSS από διαφορετικές LVs. Το γεγονός αυτό δημιουργεί την ανάγκη για ασφαλή ανταλλαγή πληροφοριών μεταξύ των LVs, για την αποφυγή πιθανών επιθέσεων, όπως οι υποκλοπές, η εισαγωγή, η τροποποίηση, ή η επανάληψη επιθέσεων. Επιπλέον, είναι επίσης αναγκαίο να διατηρηθεί μυστική η θέση των LVs ως επιτιθέμενος, γνωρίζοντας ότι θα μπορούσε στρατηγικά να επιλέξει τη θέση μετάδοσης για να παρακάμψει το σύστημα επαλήθευσης. Έτσι, οι συγγραφείς προτείνουν ως αντίμετρο για την επίθεση αυτή τη χρήση cover LVs, που είναι εκείνοι των οποίων η θέση είναι γνωστή μόνο στην αρχή που είναι υπεύθυνη για την διαδικασίας επαλήθευσης. Κατά τη γνώμη μου, ένα άλλο μειονέκτημα αυτής της πρότασης είναι ότι δεν λειτουργεί σε περιβάλλον δικτύου όπου οι κύριοι χρήστες είναι κινητοί και διαβιβάζουν με χαμηλή ισχύ μεταφοράς , π.χ. τα ασύρματα μικρόφωνα.

Υπάρχουν εναλλακτικά αντίμετρα, όπως η λήψη των δακτυλικών αποτυπωμάτων ραδιοσυχνοτήτων (Radio Frequency Fingerprinting, RFF), η οποία έχει ευρέως αναφερθεί στην βιβλιογραφία ως μία τεχνική για την ταυτοποίηση του πομπού (βλ. [33,34]). Το αποτύπωμα μιας ραδιο-συσκευής αναφέρεται στα μοναδικά χαρακτηριστικά του σήματος που εκπέμπεται από μια συγκεκριμένη συσκευή. Ορισμένες τεχνικές δακτυλικών αποτυπωμάτων βασίζονται στην μεταβατική συμπεριφορά που παρουσιάζεται από το σήμα σε σχέση με τη στιγμιαία συχνότητα και το πλάτος, όταν η συσκευή αρχίζει τη μετάδοση. Ακόμη και πομποί του ίδιου τύπου, θα εμφανίζουν διαφορετικά χαρακτηριστικά κατά τη διάρκεια μιας μεταβατικής χρονικής περιόδου εξαιτίας παραγόντων, όπως η ηλικία ή τα επίπεδα ανοχής, τα οποία επιτρέπουν να προσδιοριστεί μοναδικά κάθε ενιαίος πομπός. Ωστόσο, το πρόβλημα έγκειται στην εκτίμηση με ακρίβεια της διάρκειας της παροδικής περιόδου. Από την άλλη πλευρά, ορισμένοι υποστηρίζουν ότι δεν είναι πάντα δυνατόν να γίνει διάκριση μεταξύ παρόμοιων διατάξεων (βλ. [35]) λόγω της δυσκολίας της περιόδου αυτής και προτείνουν τεχνικές που βασίζονται στα χαρακτηριστικά σταθερής κατάστασης των σημάτων. Σήμερα, σταθερή ανάλυση της κατάστασης του σήματος είναι εφικτή, διότι ψηφιακοί πομποί εισάγουν συχνά επαναλαμβανόμενες αλληλουχίες όπως σκέψεις για την απλοποίηση του σχεδιασμού του δέκτη.

Ένας άλλος κλάδος της έρευνας θα μπορούσε να είναι η χρήση της ανοχής σε βλάβες συστημάτων ψηφιακής υπογραφής (βλ. [36]) που εφαρμόζονται στα σήματα για τον εντοπισμό εξουσιοδοτημένων πηγών δεδομένων, ανεξάρτητα από το αν είναι κύριοι ή δευτερεύοντες χρήστες. Δηλαδή ότι το σήμα περιέχει μία ψηφιακή υπογραφή η οποία επιτρέπει σε κάθε δέκτη να ελέγξει αν η πηγή είναι ένας νόμιμος χρήστης ή όχι μέσα σε ένα ορισμένο όριο. Η υψηλή παρουσία σφαλμάτων στις ασύρματες συνδέσεις δικαιολογεί τη χρήση των συστημάτων αυτών, αντί της «παραδοσιακής» ψηφιακής υπογραφής. Ωστόσο, οι λύσεις αυτές δεν μπορούν να εφαρμοστούν τουλάχιστον σήμερα για τους κύριους χρήστες, αφού η FCC, όπως αναφέρθηκε πριν, δηλώνει

σαφώς στο (βλ. [32]), ότι η παρουσία των εισερχόμενων CRNs δεν πρέπει να επηρεάσει τα τρέχοντα πρωτογενή σήματα.

7.3 Αντιμετώπιση των OFA επιθέσεων

Οι επιθέσεις OFAs απευθύνονται στην online εκμάθηση του AI πρωτοκόλλου που χρησιμοποιείται από τις συσκευές ΓΕ. Μια OFA μεταβάλλει τη συμπεριφορά των ασύρματων μέσων (με τη δημιουργία παρεμβολών σε συγκεκριμένο χρόνο και συχνότητες) σε σχέση με την πολιτική παραμέτρων που έχει καθοριστεί (π.χ. το επίπεδο της ασφάλειας), και ως εκ τούτου τροποποιεί την καμπύλη μάθησης προς όφελος του εισβολέα (π.χ. επίτευξη χαμηλού επιπέδου ασφάλειας). Κατά τη γνώμη μου, κανένας αλγόριθμος μάθησης που βασίζεται στην παρατήρηση ενός εκτεθειμένου μέσου δε θα πρέπει να εμπιστεύεται εντελώς τα συλλεχθέντα δεδομένα. Ως εκ τούτου, η καμπύλη μάθησης πρέπει να προστατεύεται ώστε να μην επιτυγχάνονται μη αποδεκτά επίπεδα ορισμένων παραμέτρων. Επομένως θα μπορούσαμε να προτείνουμε ως μια απλή λύση τον καθορισμό των τιμών κατωφλίου για κάθε ράδιο-παράμετρο με δυνατότητα αναβάθμισης, αποτρέποντας έτσι την επικοινωνία όταν μία παράμετρος ή μια σειρά από παραμέτρους δεν πληρούν το προκαθορισμένο όριό του. Σε κάθε περίπτωση, η λύση αυτή μετατρέπει μόνο την OFA σε μια DoS επίθεση αλλά δεν την εμποδίζει καθόλου. Για άλλη μια φορά η ανάγκη για μια καλή IDS είναι ολοφάνερη.

7.4 Αντιμετώπιση των επιθέσεων Lion

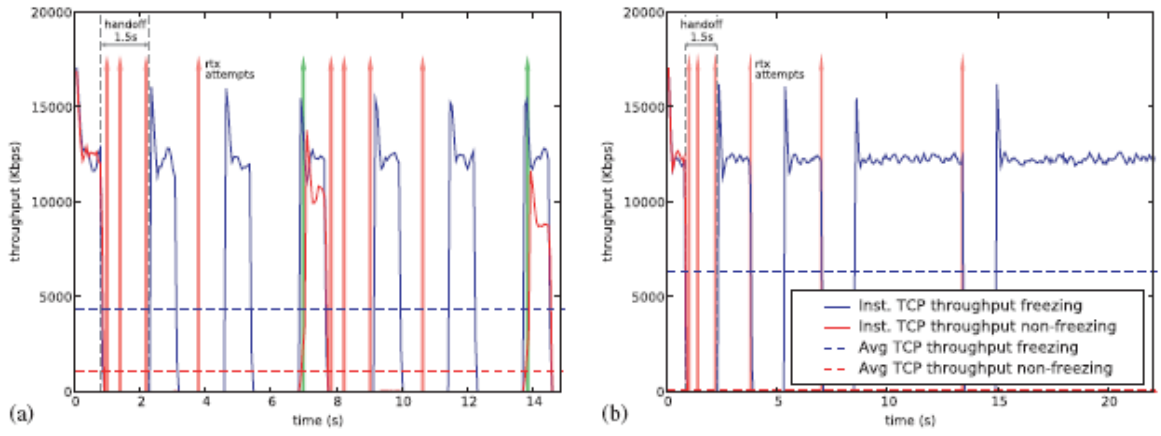
Όπως εξηγείται στη παράγραφο 6.5, η TCP διακίνηση είναι ειδικά υποβαθμισμένη λόγω των μεταβιβάσεων συχνότητας επειδή το στρώμα μεταφοράς δεν έχει καμία πληροφορία σχετικά με το φυσικό στρώμα ή το στρώμα ζεύξης και παρερμηνεύει μια αποσύνδεση σαν μια συμφόρηση του δικτύου. Συνεπώς, υπάρχει μία ανάγκη για cross-layers λύσεις για την αντιμετώπιση αυτού του προβλήματος. Αρκετές cross-layers λύσεις έχουν προταθεί στη βιβλιογραφία (βλ. [37]) για την βελτίωση των επιδόσεων του TCP στο πλαίσιο των ασύρματων δικτύων, ειδικά στα ad-hoc δίκτυα. Αυτές οι προτάσεις αντιμετωπίζουν τα τυπικά προβλήματα των ασύρματων ζεύξεων, όπως οι απώλειες, οι δραστικές αλλαγές στα δρομολόγια, ή η χρονική απώλεια σύνδεσης, οι οποίες μπορούν να επηρεάσουν δραματικά την απόδοση του πρωτοκόλλου TCP, εξαιτίας της αλληλεπίδρασης με τους μηχανισμούς ελέγχου συμφόρησης του. Κάνοντας TCP γνωρίζοντας τι συμβαίνει στα χαμηλότερα επίπεδα και τροποποιώντας τη συμπεριφορά του να αντιδρά ανάλογα με τις συνθήκες δικτύου, είναι δυνατόν να βελτιωθεί η απόδοσή του. Κατά την άποψή μου, αυτές οι τεχνικές μπορούν να χρησιμοποιηθούν ως κατευθυντήρια γραμμή για το σχεδιασμό νέων πρωτοκόλλων κατάλληλων για CRNs, αυξάνοντας έτσι την αποδοτικότητα και κάνοντας την περισσότερο ανθεκτική στις crosslayer επιθέσεις. Μεταξύ αυτών, αξίζει να αναφερθεί το Freeze-TCP (βλ. [38]), μια παραλλαγή του TCP που σχεδιάστηκε για να βελτιώσει την απόδοση TCP σε κινητά περιβάλλοντα, όπου οι χρονικές αποσυνδέσεις συμβαίνουν συχνά λόγω της εξασθένισης του σήματος ή της κίνησης των κόμβων. Στο Freeze-TOP, ο δέκτης είναι υπεύθυνος για τον έλεγχο της ισχύος του σήματος για να προβλέψει αποσυνδέσεις και να διαφημίζει μηδενικό παράθυρο για τον αποστολέα πριν λάβει χώρα η αποσύνδεση. Μετά τη λήψη του μηδενικού μεγέθους του παραθύρου, ο αποστολέας εισέρχεται στη ZWP (Zero Window Probe) κατάσταση, στην οποία «παγώνει» τη μετάδοση παραμέτρων και δεν επιτρέπεται να μεταδίδει οποιοδήποτε τμήμα των δεδομένων (μόνο οι ανιχνευτές παραθύρου). Μέσω αυτού του μηχανισμού, είναι δυνατό να αποφευχθούν πιθανές ζημιές και το παράθυρο

συμφόρησης να μην πέσει σε ένα τμήμα επειδή δεν χρειάζονται αναμεταδόσεις. Όταν η σύνδεση συνεχίζεται, ο δέκτης διαφημίζει ένα μη μηδενικό παράθυρο που επιτρέπει στον αποστολέα για να συνεχίσει τη μετάδοσή του.

Μια παρόμοια προσέγγιση για Freeze-TCP μπορεί να χρησιμοποιηθεί σε CRNs για τον περιορισμό της επίδρασης του φάσματος μεταβιβάσεων, υπό την προϋπόθεση ότι ο κόμβος δέκτης μπορεί να προβλέψει πότε θα προκύψει η μεταβίβαση, π.χ. προληπτική μεταβίβαση. Ωστόσο, υποθέτοντας ότι όλοι οι κόμβοι που συνδέονται με μια δεδομένη CRN μοιράζονται την ίδια πληροφορία, ο αποστολέας θα μπορούσε επίσης να γνωρίζει ότι υπάρχει μια εισερχόμενη μεταβίβαση. Λαμβάνοντας υπόψη αυτό, δεν έχει νόημα να περιμένουμε διαφήμιση για μηδενικό παράθυρο για να παγώσει τις παραμέτρους μετάδοσης του αποστολέα, καθώς ο αποστολέας θα μπορούσε να το κάνει ο ίδιος. Επίσης, ένα άλλο σημαντικό θέμα που δεν καλύπτεται από Freeze-TCP είναι το πώς τα χαρακτηριστικά σύνδεσης διαφέρουν ανάλογα με τη μεταβίβαση. Μία μεταβολή των παραμέτρων μετάδοσης, όπως η συχνότητα ή η κωδικοποίηση, μπορεί να περιλαμβάνει μία παραλλαγή του διαθέσιμου εύρους ζώνης. Λόγω αυτού, το ότι διατηρεί τις ίδιες τιμές για τις παραμέτρους TCP σύνδεση μπορεί να μην είναι κατάλληλο. Για παράδειγμα, μια απότομη μείωση του εύρους ζώνης θα οδηγήσει σε πολλαπλές απώλειες, αν ο αποστολέας δεν μειώσει το παράθυρο συμφόρησης.

Εξαιτίας αυτού, η πραγματική έκδοση των Freeze-TCP δεν είναι η βέλτιστη για αυτό το περιβάλλον, και μια πιθανή λύση θα μπορούσε να είναι μια νέα παραλλαγή του TCP που βασίζεται σε δύο βασικές διαφορές: (1) όπως όλα τα μέλη CRN έχουν επίγνωση των μεταβίβαση συχνότητας, έτσι κάθε σύστημα ΓΕ μπορεί να παγώσει τις δικές του παραμέτρους του TCP χωρίς να έχει προειδοποίηση από τον δέκτη και (2) όπως κάθε συμμετέχων έχει πληροφορία σχετικά με την επόμενη ζώνη όσον αφορά το διαθέσιμο εύρος ζώνης, τη σχέση του σήματος προς θόρυβο, κλπ. έτσι θα πρέπει να τροποποιήσει τη TCP σύνδεση του αναλόγως με τις παραμέτρους.

Τα σχήματα 41(α,β) δείχνουν, αντίστοιχα τα αποτελέσματα της επίθεσης Lion στη διακίνηση του TCP όταν μεταβιβάσεις γίνονται περιοδικά και με έξυπνο τρόπο (ταιριάζουν με τις προσπάθειες αναμετάδοσης). Η διάρκεια ελεγχοδότησης υποτίθεται ότι είναι 1,5s, η μέγιστη μεταβίβαση, επιτεύξιμη από τη TCP σύνδεση σε 17Mbps και τη BER10-6. Όπως μπορεί να φανεί, η απόδοση του TCP είναι σε μεγάλο βαθμό μειωμένη όταν συμβαίνουν μεταβιβάσεις, ακόμη και πεθαίνουν από την πείνα όταν ο επιτιθέμενος εκτελεί μια ευφυή Lion επίθεση.



Σχήμα 41. Ελεγχοδότηση επίδρασης στην απόδοση TCP, με freezing, και non-freezing των παραμέτρων TCP:(α) Lion επίθεση βασισμένη σε περιοδικές PUEAs και (β) έξυπνη Lion επίθεση

7.5 Γενική αντιμετώπιση των επιθέσεων

Ένα από τα κύρια χαρακτηριστικά του CRNs είναι η συνεργασία των συμμετεχόντων να βρουν ευκαιρίες στο φάσμα. Οι πληροφορίες που ανταλλάσσονται με το σκοπό αυτό συχνά μεταφέρουν κοινόχρηστα δεδομένα και ως εκ τούτου μονής διανομής επικοινωνίες πρέπει να αντικατασταθούν με εκπομπή ή ομαδικές επικοινωνίες. Επομένως, υπάρχει η ανάγκη για την προστασία αυτών των δεδομένων μόνο κατά των ξένων της ομάδας και όχι εντός των μελών της ομάδας, και αυτό είναι αυτό που ονομάζεται ασφάλεια της ομάδας. Ασφάλεια της ομάδας είναι, ως εκ τούτου, με στόχο την παροχή απορρήτου στην ομάδα και την πιστοποίηση της ομάδας: τα δεδομένα προστατεύονται από τους ξένους και οι μοναδικές πηγές της επικοινωνίας είναι τα μέλη της ομάδας. Ως αποτέλεσμα, είναι ότι απλώς βασίζεται στην χρήση ενός κοινόχρηστου κοινού μυστικού που ονομάζεται το κλειδί κύκλου ή το πλήκτρο της ομάδας. Αυτό το πλήκτρο επιτρέπει σε κάθε ομάδα μέλος (1) να στείλει κρυπτογραφημένα δεδομένα (2) να αποκρυπτογραφήσει δεδομένα που έλαβε, και (3) να πιστοποιείται ως ομάδα μέλος, όπως η γνώση του κλειδιού περιόδου λειτουργίας εγγυάται ότι ανήκει στην ομάδα. Δεδομένου ότι μόνο τα σημερινά μέλη της ομάδας θα πρέπει να γνωρίζουν το κλειδί περιόδου λειτουργίας, καθώς το κλειδί αυτό πρέπει να ενημερώνεται κάθε φορά που η ιδιότητα του μέλους της ομάδας αλλάζει. Η ομάδα διαχείρισης κλειδιών (GKM) μελετά την παραγωγή και ενημέρωση του κρυπτογραφικού υλικού που χρησιμοποιείται για την εξασφάλιση της ομάδας κατά τη διάρκεια ολόκληρης της ζωής του (βλ. [39]). Είμαστε βέβαιοι ότι η εφαρμογή των γνωστών τεχνικών GKM (group Key Management) για τα CRN θα εξασφαλίσει την ανταλλαγή κρίσιμων δεδομένων, ενώ θα υφίσταται μικρό αντίκτυπο στην απόδοση του δικτύου. Επιπροσθέτως, η μελέτη των κατανεμημένων και αυτόνομων GKM πρωτοκόλλων (βλ. [40]) είναι απαραίτητη για να καλύψει όλες τις αρχιτεκτονικές CRN.

Επιπλέον, πιστεύουμε ότι είναι απαραίτητο οι κόμβοι να εκτελούν κρυπτογραφικές λειτουργίες που βασίζονται σε αρχέτυπα, όπως το συμμετρικό κλειδί κρυπτογράφησης (Symmetric Key Encryption, SKE), τις συναρτήσεις κατακερματισμού, και τη κρυπτογραφία δημόσιου κλειδιού (Public Key Cryptography, PKC). Χωρίς αυτά τα αρχέτυπα, δεν θα ήταν δυνατό να παρέχουν τις απαραίτητες υπηρεσίες ασφαλείας όπως η εμπιστευτικότητα του καναλιού επικοινωνίας, ο έλεγχος ταυτότητας των κόμβων που συμμετέχουν σε μια ανταλλαγή πληροφοριών, και η ακεραιότητα των μηνυμάτων, μεταξύ άλλων.

8 Επίλογος

Το βασικό κίνητρο πίσω από τις γνωστικές ραδιοεπικοινωνίες ήταν να αυξήσουν τη χρησιμοποίηση του φάσματος, επιτρέποντας στους χωρίς άδεια (δευτερεύοντες) χρήστες να έχουν πρόσβαση ευκαιριακά στη ζώνη συχνοτήτων, που στην πραγματικότητα ανήκει στους αδειοδοτημένους (πρωτογενής) χρήστες. Σε αντίθεση με άλλες αρχιτεκτονικές ασφάλεια των δικτύων, στα δίκτυα ΓΕ, οι χρήστες κατηγοριοποιούνται σε δύο διακριτές κατηγορίες: στους πρωτεύοντες και τους δευτερεύοντες χρήστες. Δείξαμε λοιπόν ότι αυτή η κατηγοριοποίηση δημιουργεί διάφορα ζητήματα ασφάλειας που είναι μοναδικά στα δίκτυα ΓΕ. Συζητήσαμε, επίσης, τις διάφορες πτυχές της ασφάλειας, όπως η πιστοποίηση και η αδειοδότηση των χρηστών, η εμπιστευτικότητα και η ακεραιότητα της επικοινωνίας καθώς και ο εντοπισμός και η μη-αναγνώριση των συσκευών γνωστικών χρηστών.

8.1 Μελλοντικές κατευθύνσεις

Τέλος σε αυτό το κεφάλαιο θα παρέχουμε κάποιες μελλοντικές κατευθύνσεις που πρέπει να ληφθούν για να γίνουν πιο ασφαλή τα δίκτυα ΓΕ τόσο κατά των τυχαίων όσο και κατά των εκ προθέσεως επιθέσεων. Οι περισσότερες λύσεις που προτείνονται μας είναι εύκολο να εφαρμοστούν (για παράδειγμα, χρησιμοποιώντας τα υπάρχοντα πρωτόκολλα ασφάλειας). Ωστόσο, προτείνουμε επίσης λύσεις (για παράδειγμα, την ανάπτυξη αναλογικών αρχέτυπων κρυπτογράφησης) που απαιτούν περισσότερη δουλειά.

8.1.1 Χρησιμοποιώντας τα υπάρχοντα πρωτόκολλα ασφάλειας

Οι υπηρεσίες ασφαλείας που παρέχονται σε κυψελοειδή δίκτυα, όπως τα WLAN και τα ασύρματα ad-hoc μπορούν να εφαρμοστούν και στα γνωστικά δίκτυα. Σε μια αρχιτεκτονική κεντρικού ασύρματου δικτύου, το δίκτυο κορμού είναι συνήθως ένα ενσύρματο μέσο. Ως εκ τούτου, ισχυροί μηχανισμοί ασφαλείας υπάρχουν για να προστατεύουν αυτό το δίκτυο. Αυτό που πρέπει να προστατευτεί είναι η τελευταία αναμετάδοση μεταξύ των ασύρματων σταθμών βάσης και των ασύρματων τερματικών. Καθώς τα κυψελοειδή δίκτυα είναι κεντρικά, λύσεις ασφαλείας στα υπάρχοντα κυψελοειδή δίκτυα (3G ιδίως) θα μπορούσαν να χρησιμοποιηθούν ως πρότυπο για να παρέχουν ασφάλεια στα γνωστικά δίκτυα. Στα δίκτυα κινητής τηλεφωνίας, η ταυτότητα του χρήστη επιτυγχάνεται με τη χρήση μιας προσωρινής ταυτότητας που ονομάζεται διεθνής κινητή ταυτότητα του χρήστη. Ο έλεγχος ταυτότητας επιτυγχάνεται με ένα μηχανισμό απόκρισης χρησιμοποιώντας ένα μυστικό κλειδί. Ένας τέτοιος μηχανισμός απόκρισης υπάρχει όταν μια οντότητα στο δίκτυο αποδεικνύει ότι μια άλλη οντότητα γνωρίζει ένα συγκεκριμένο μυστικό χωρίς όμως να το αποκαλύψει. Η πιστοποίηση UMTS και το κλειδί συμφωνία (UMTS AKA) χρησιμοποιείται για να επιτευχθεί αυτή η πιστοποίηση. Η εμπιστευτικότητα παρέχεται χρησιμοποιώντας τον αλγόριθμο εμπιστευτικότητας , γνωστό ως f8, και το κλειδί κρυπτογράφησης του μυστικού (CK) που ανταλλάσσεται ως μέρος της διαδικασίας AKA. Η ακεραιότητα παρέχεται με τη χρήση του αλγορίθμου ακεραιότητας f9 και το κλειδί ακεραιότητας (IK). Ένα μπλοκ κρυπτογράφησης είναι το δομικό στοιχείο των f8 και f9 αλγορίθμων, λειτουργεί σε 64 bit μπλοκ και χρησιμοποιεί 128-bit για το μυστικό κλειδί. Μια παρόμοια εγκατάσταση μπορεί να χρησιμοποιηθεί σε κεντρικά δίκτυα ΓΕ για τον καθορισμό των βασικών απαιτήσεων ασφαλείας μεταξύ των δευτερευόντων χρηστών και του δευτερεύοντος σταθμού βάσης.

Σε αποκεντρωμένα δίκτυα, οι δευτερεύοντες χρήστες επικοινωνούν μεταξύ τους σε ένα ή περισσότερα hops. Λόγω της έλλειψης υποδομών, αυτά τα δίκτυα, αναφέρονται ως ad-hoc δίκτυα. Αυτοί οι τύποι δικτύων χρησιμοποιούν συνήθως ένα μηχανισμό ασφαλείας δύο επιπέδων. Το ένα επίπεδο ασφάλειας παρέχεται στο στρώμα ζεύξης για την προστασία κάθε hop της επικοινωνίας και το άλλο επίπεδο ασφάλειας απασχολείται στο στρώμα εφαρμογής ή μεταφοράς του δικτύου για την προστασία της end-to-end διαδρομής επικοινωνίας. Δύο πιο περίπλοκες εργασίες στα ad-hoc ασύρματα δίκτυα είναι η διαχείριση του κλειδιού και η ασφαλής δρομολόγηση. Τα αποκεντρωμένα γνωστικά δίκτυα θα μπορούσαν να χρησιμοποιήσουν τους μηχανισμούς ασφαλείας που χρησιμοποιούνται στα ad-hoc ασύρματα δίκτυα. Μερικά από τα ζητήματα, όπως η έλλειψη ενός κοινού καναλιού ελέγχου και η χρήση διαφορετικών ζωνών συχνοτήτων από διαφορετικούς δευτερεύοντες χρήστες μπορούν να επιβάλλουν πρόσθετους περιορισμούς στα υφιστάμενα πρωτόκολλα ασφαλείας.

8.1.2 Χρησιμοποιώντας κρυπτογραφικά πρότυπα

Οι περισσότερες από τις επιθέσεις που πραγματοποιούνται στο στρώμα ζεύξης περιλαμβάνουν μια κακόβουλη οντότητα που μεταμφιέζεται ως κύριος χρήστης. Ως εκ τούτου ο έλεγχος ταυτότητας του πρωτογενούς χρήστη είναι πολύ σημαντικό τόσο για τα κεντρικά όσο και για τα αποκεντρωμένα γνωστικά δίκτυα. Έτσι προτείναμε παραπάνω στην εργασία μας τη χρήση ψηφιακής υπογραφής που βασίζεται στο μηχανισμό αναγνώρισης του κύριου χρήστη, και η οποία μπορεί να χρησιμοποιηθεί από δευτερεύοντες χρήστες για να διακρίνουν τις κακόβουλες μεταδόσεις από πριν. Περαιτέρω έρευνα πρέπει να γίνει για τη χρήση των κρυπτογραφικών αρχέτυπων για να λυθούν εγγενή ζητήματα ασφάλειας στα δίκτυα ΓΕ.

8.1.3 Χρησιμοποιώντας αντιδραστικούς μηχανισμούς ασφάλειας

Επίσης θα πρέπει να αναπτυχθούν αντιδραστικοί μηχανισμοί ασφαλείας που να εντοπίζουν κακόβουλη δραστηριότητα στα δίκτυα ΓΕ. Για παράδειγμα, οι μηχανισμοί που μπορούν να ανιχνεύσουν ασυνήθιστα υψηλές μεταβιβάσεις φάσματος είναι χρήσιμο να αποτρέπουν την παρεμβολή παρασίτων και τις επιθέσεις στη μεταβίβαση φάσματος. Αυτοί οι μηχανισμοί ανίχνευσης επιτρέπουν στους δευτερεύοντες χρήστες να εντοπίζουν και να μπλοκάρουν κακόβουλους χρήστες από το δίκτυο.

8.1.4 Γνωρίζοντας την φασματική προσέγγιση

Υπάρχουν δύο τρόποι για να χειριστούμε την κινητικότητα του φάσματος και τις συναφείς καθυστερήσεις. Ο ένας είναι να κάνουμε την ανίχνευση φάσματος, την ανάλυση και τη διαδικασία μεταβίβασης γρήγορα και με διαφανή τρόπο στα πρωτόκολλα του ανώτερου στρώματος. Ωστόσο, η ανίχνευση φάσματος και οι διαδικασίες μεταβίβασης είναι στα αρχικά τους στάδια και αυτό θα πάρει πολύ χρόνο για να υλοποιηθούν τέτοιου είδους προσεγγίσεις . Μια άλλη προσέγγιση είναι μια cross-layer μεθοδολογία να ενσωματώσει την κινητικότητα του φάσματος, σαν μια κατάσταση της πληροφορίες στα πρωτόκολλα που λειτουργούν στα ανώτερα στρώματα. Αν και αυτή η προσέγγιση αυξάνει τις cross-layer εξαρτήσεις, αυτό θα κάνει όλο το φάσμα πρωτοκόλλου επικοινωνίας γνωστό και ως εκ τούτου καλύτερη την υπεράσπιση κάποιων επιθέσεων στα ανώτερα πρωτόκολλα επιπέδου στια δίκτυα ΓΕ. Για παράδειγμα, μια δρομολόγηση θα πρέπει να εξετάσει τη λειτουργική ζώνη φάσματος και τα χαρακτηριστικά της και το στρώμα μεταφοράς θα πρέπει να εξετάσει την επίδραση της μεταβίβασης του φάσματος στο RTT και αντίστοιχα να προσαρμόσει το παράθυρο αναμετάδοσης.

8.1.5 Αναπτύσσοντας αναλογικά κρυπτογραφικά πρότυπα

Μία από τις προκλήσεις στην ενσωμάτωση μηχανισμών ασφάλειας στα δίκτυα ΓΕ είναι ότι σε ορισμένες ζώνες συχνοτήτων, όπως η τηλεοπτική ζώνη, οι πρωτογενείς σταθμοί βάσεως μεταδίδουν αναλογικά σήματα (με την εξαίρεση των HDTVs). Δεδομένου ότι τα περισσότερα από τα κρυπτογραφικά πρότυπα λειτουργούν στον ψηφιακό τομέα, μπορεί να μην είναι καν δυνατό να ενσωματωθούν σε αναλογικά τηλεοπτικά σήματα. Ως εκ τούτου, πρότυπα κρυπτογράφησης που εργάζονται σε αναλογικούς τομείς πρέπει να αναπτυχθούν.

8.1.6 Χρησιμοποιώντας light-weight πρωτόκολλα ασφαλείας και πρότυπα

Αν οι δευτερεύοντες χρήστες στα δίκτυα ΓΕ έχουν κινητό εξοπλισμό με περιορισμένη επεξεργαστική ισχύ και πόρους, θα ήταν μια πρόκληση για να παρέχουν τόσο τη γνωστική δυνατότητα ραδιοεπικοινωνιών όσο και την ασφάλεια σε πραγματικό χρόνο. Έτσι light-weight πρωτόκολλα ασφαλείας θα πρέπει να αναπτυχθούν για την ενδυνάμωση περιβαλλόντων με περιορισμένους πόρους.

9 Βιβλιογραφία

[01] Ye Zhuan, Grosspietsch John, Memik Gokemik, Spectrum Sensing Using Cyclostationary Spectrum Density for Cognitive Radios, Signal Processing Systems , IEEE 2007 Workshop

[02] Γκερπινής Γ. Κωνσταντίνος, Κατανεμημένο Πρωτόκολλο Ελέγχου Πρόσβασης στο Μέσο σε Περιβάλλον Δυναμικής Εκχώρησης Φάσματος για συστήματα Cognitive Radio , ΕΜΠ, Οκτώβριος 2007

[03] Chen V. and M. Guizani , Next Generation Wireless Systems and Networks, John Wiley & Sons Ltd. , 2006

[04] I.G. Proakis and M. Salehi, Συστήματα Τηλεπικοινωνιών

[05] S. Haykin, "Cognitive Radio: Brain – Empowered Wireless Communications", IEEE JSAC, vol. 23, no. 2, Feb. 2005, pp. 201-220

[06] F. K. Jondral, Software-Defined Radio–Basics and Evolution to Cognitive Radio, EURASIP Journal on Wireless Communications and Networking, 2005, pp 275-283

[07] SDR Forum, http: www.sdrforum.org, September 2007

[08] Wikipedia, The free Encyclopedia, www.wikipedia.org

[09] M. Nekovee, Dynamic Spectrum access-concepts and future architecture, BT Technology Journal, Vol. 24, No2, April 2006, pp. 111-116

[10] B. H. Walke, S. Mangold and L. Berlemann, IEEE 802 Wireless Systems, John Wiley & Sons Ltd., 2006

[11] Mitola III, "Cognitive Radio: an integrated agent architecture for software defined radio", Doctor of technology, Royal Inst. Technol (KTH), Stockholm, Sweden, 2000

[12] Draft Document, "Standard Definitions and Concepts for Spectrum Management and Advance Radio System Technologies", June 2006

[13] L. Xu, R. Tonjes, T. Paila, W. Hansmann, M. Frank and M. Albrecht, "DRIVE- ing to the Internet: Dynamic Radio for IP services in Vehicular Enviroments" , in Proc. Of 25th Annual IEEE Conference on Local Computer Networks, pp. 281-289, Nov. 2000

[14] J. Mitola, Cognitive radio for flexible mobile multimedia communications, in Proc IEEE Int. Workshop Mobile Multimedia Communications, 1999, pp. 3-10

[15] Cabric, D., Mishra, S. and Brodersen, R., Implementation issues in spectrum sensing for cognitive radios. *Signals, Systems and Computers, 2004*

[16] Digham, M.A.F. and Simon, M. , On the energy detection of unknown signals over fading channels.Proceedings of the IEEE ICC, vol. 5, 2003, pp. 3575–9.

[17] Akyildiz, I., Lee, W.-Y., Vuran, M.C. and Mohanty, S. , Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey. Computer Networks, 2006, 50(13), 2127–59.

[18] Xing, Y., Mathur, C., Haleem, M., Chandramouli, R., and Subbalakshmi, K., Priority based dynamic spectrum access with QoS and interference temperature

constraints. Proceedings of the IEEE International Conference on Communications, vol. 10, 2006, pp. 4420–5.

[19] FCC, Notice of proposed rule making and order, ET docket no 03-222, December 2003

[20] Etkin, R., Parekh, A. and Tse, D. ,Spectrum sharing for unlicensed bands. Proceedings of the IEEE DySPAN, November 2005, pp. 251–8

[21] X. Jing, D. Raychaudhuri, Spectrum co-existence of IEEE 802.22b and 802.16a networks using CSCC etiquette protocol. Proceedings of the IEEE DySPAN, November 2005, pp. 243–50

[22] Zhang Y, Xu G, Geng X. Security threats in cognitive radio networks.10th IEEE International Conference on High Performance Computing and Communications. HPCC 2008, 2008, 1036–104

[23] Mathur CN, Subbalakshmi KP. Security issues in cognitive radio networks. COGNITIVE NETWORKS: Towards Self-Aware Networks. Wiley: New York, 2007, 284–293.

[24] Chen R, Park JM. Ensuring trustworthy spectrum sensing in cognitive radio networks. First IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR), 2006, 110–119.

[25] Cabric D, Mishra S, Brodersen R. Implementation issues in spectrum sensing for cognitive radios. Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, vol. 1, 2004, 772–776

[26] Russell S, Norvig P. Artificial Intelligence: A Modern Approach (2nd edn). Prentice-Hall: Englewood Cliffs, NJ,2002

[27] Mody A, Reddy R, Kiernan T. Recommended text for security in 802.22. 802.22 WG on WRANs—doc.:IEEE 802.22-08/0174r18. Available at: https://mentor.ieee.org/802.22/dcn/08/22-08-0174-18-0000-recommended-text-forsection-7-on-security-in-802-22.doc, May 2009.

[28] Paxson V, Allman M. Computing TCP's retransmission timer. Network Working Group—RFC2988, November 2000.

[29] Zhang Y, Lee W. Intrusion detection in wireless ad-hoc networks. MobiCom '00: Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking. ACM: New York, NY, U.S.A., 2000, 275–283

[30] Mishra A, Nadkarni K, Patcha A. Intrusion detection in wireless ad hoc networks. Wireless Communications, IEEE 2004, 48–60

[31] Bhuse V, Gupta A. Anomaly intrusion detection in wireless sensor networks. Journal of High Speed Networks 2006, 33–51

[32] Federal Communications Commission. Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies. FCC 03-322. ET Docket No. 03-108, December 2003.

[33] Ureten O, Serinken N. Wireless security through rf fingerprinting. Electrical and Computer Engineering, Canadian Journal of Winter 2007, 27–33.

[34] Toonstra J, Kinsner W. A radio transmitter fingerprinting system odo-1. Canadian Conference on Electrical and Computer Engineering 1996, 60–63

[35] Kennedy I, Scanlon P, Buddhikot M. Passive steady state rf fingerprinting: a cognitive technique for scalable deployment of co-channel femto cell underlays.

Third IEEE Symposium on the New Frontiers in Dynamic Spectrum Access Networks, 2008, DySPAN 2008, October 2008, 1–12

[36] Zhang C. Integrated approach for fault tolerance and digital signature in rsa. Computers and Digital Techniques, IEE Proceedings 1999, 151–159

[37] Al Hanbali A, Altman E, Nain P. A survey of tcp over ad hoc networks. Communications Surveys and Tutorials, IEEE Quarter 2005, 22–36.

[38] Goff T, Moronski J, Phatak D, Gupta V. Freeze-TCP: a true end-to-end TCP enhancement mechanism for mobile environments. INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies vol. 3, 2000, 1537–1545

[39] Wallner D, Harder E, Agee R. Key management for multicast: issues and architectures. National Security Agency, Network Working Group—RFC 2627, June 1999

[40] Hernandez-Serrano J, Pegueroles J, Soriano M. Shared self-organized GKM protocol for MANETs. Journal of Information Science and Engineering (JISE) 2008, 1629–1646.

[41] Chen R, Park JM, Reed J. Defense against primary user emulation attacks in cognitive radio networks. IEEE Journal on Selected Areas in Communications 2008, 25–37

[42] Clancy T, Goergen N. Security in cognitive radio networks: threats and mitigation. Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), 2008, 1–8.

[43] Ferguson, N. and Schneier, B. (2003) Practical Cryptography, John Wiley & Sons, Inc., New York, USA.

[44] Natkaniec, M. and Pach, A.R. (2000) An analysis of the back-o mechanism used in IEEE 802.11 net-works. Proceedings of the Fifth IEEE Symposium on Computers and Communications, p. 444, Washington, DC, USA.

[45] FCC (2003), Notice of proposed rule making and order, ET docket no 03-222, December.

[46] Zapata, M.G. and Asokan, N. (2002) Securing ad hoc routing protocols. Proceedings of the 3rd ACM Workshop on Wireless Security, pp. 1–10, New York, USA.

[47] Cam-Winget, N., Housley, R., Wagner, D. and Walker, J. (2003) Security flaws in 802.11 data link protocols. ACM Communications, 46(5), 35–9.

[48] FIPS (2001) Specification for the advanced encryption standard (AES). Federal Information Processing Standards Publication 197. http://csrc.nist.gov/publications/ ps/ ps197/ ps-197.pdf.

[49] Schneier, B. (1995) Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., New York, USA.

[50] Zhou, D. (2003), Security Issues in Ad Hoc Networks, CRC Press, Inc., Boca Raton, FL, USA.

[51] Nanjunda, C., Haleem, M. and Chandramouli, R. (2005) Robust encryption for secure image transmission over wireless channels. Proceedings of the IEEE International Conference on Communications, vol. 2, May.

[52] Reason, J.M. and Messerschmitt, D.G. (2001) The impact of confidentiality on quality of service in heterogeneous voice over IP. Lecture Notes in Computer Science, 2216, 175.

[53] Stallings, W. (1999) Cryptography and Network Security: Principles and Practice, Prentice-Hall, Upper Saddle River, NJ, USA.

[54] Robert M. Rast. The dawn of digital TV, 2005. Retrieved from IEEE Spectrum December 6, 2009.

http://spectrum.ieee.org/consumer-electronics/audiovideo/the-dawn-of-digital-tv/2

[55] Carl R. Stevenson , Response of IEEE 802.18/SG1 to the Comments from IEEE 802.16 on "Proposed PAR for IEEE 802.xx Regional Area Network TV Band Specification". IEEE, 2004.

[56] Berlemann L., Mangold S. Cognitive Radio for Dynamic Spectrum Access, John Wiley and Sons Ltd., 2009

[57] Kimtho Po, Jun-ichi Takada, Study of Applicability of IEEE 802.22 in Japan. Technical Report of IEICE, July 2006.

[58] Loutfi Nuyami, WiMax: Technology for Broadband Wireless Access, John Wiley & Sons, 2007

[59] Carlos Cordeiro, Kiran Challapali, Dagnachew Birru. IEEE 802.22: An introduction to the first Wireless Standard based on Cognitive Radios. Journal of communications, 1(1).38-47.

[60] Time Division Duplex (TDD) Vs Frequency Division Duplex (FDD) in Wireless Backhauls,(N.D), November 27, 2009 Netkrom Technologies: http://www.netkrom.com/support/whitepapers/TDD_vs_FDD_in_wireless_backhaul_white_ paper.pdf.

[61] Carlos Cordeiro, Kiran Challapali, Dagnachew Birru, Vasanth Gaddam, Gene Turkenich, Martial Bellec, Patrick Pirat, Luis Escobar, Denis Callonnec, François Marx. "IEEE 802.22 WRAN Standard PHY/MAC Proposal", IEEE, 2005.

[62] C. Eklund, R. Marks, K. Stanwood. IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access. IEEE Communications Magazine, 40(6). 98-107

[63] Draft IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE P802.16-REVd/D5-2004, IEEE, May,2004.

[64] Andrews, J. G., Ghosh, A., and Muhamed, R. 2007 Fundamentals of Wimax: Understanding Broadband Wireless Networking (Prentice Hall Communications Engineering and Emerging Technologies Series). Prentice Hall PTR.

[65] J. Thiel, Metropolitan and Regional Wireless Networking: 802.16, 802.20 and 802.22, October 20, 2009 , Department of Computer Science and Engineering of Washington University in St. Louis: http://www.cse.wustl.edu/~jain/cse574-06/ftp/wimax/index.html

[66] Yang Xiao, Fei Hu, Cognitive Radio Networks, Taylor & Francis Group. 2009

[67] Bian, K. and Park, J. ". 2008. Security vulnerabilities in IEEE 802.22. In Proceedings of the 4th Annual international Conference on Wireless internet (Maui, Hawaii, November 17 - 19, 2008). ACM International Conference

Proceeding Series. ICST (Institute for Computer Sciences Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, 1-9.

[68] Kwang-Cheng Chen, Ramjee Prasad. Cognitive Radio Networks, John Wiley and Sons Ltd. 2009

[69] Meinrath S., Calabrese M. Unlicensed Broadband Device Technologies: "White Space Device" Operations on the TV Band and the Myth of Harmful Interference, 2007 , October 10, 2009, New America Foundation: http://wirelessfuture.newamerica.net/publications/policy/unlicensed_broadband

[70] C. N. Mathur and K. Subbalakshmi, "Digital signatures for centralized DSA networks," Proc. First IEEE Workshop on Cognitive Radio Net- works, CCNC), Las Vegas, NE, Jan. 11,2007.

[71] K. Arshad and K. Moessner, "Collaborative Spectrum Sensing for Cognitive Radio," IEEE International Conference on Communications Workshop, pp. 1-5, June 2009.

[72] C. Ghosh, Innovative Approaches to Spectrum Selection, Sensing, andSharing in Cognitive Radio Networks, PhD Thesis, University of Cincinnati, May 2009.