
ΠΕΡΙΛΗΨΗ

Σελίδα | i

Ο τομέας των τηλεπικοινωνιών τα τελευταία χρόνια στηρίζεται σε ένα μεγάλο βαθμό στην ανάπτυξη των ασύρματων δικτύων. Σημαντικό ρόλο σε αυτή την συνεχή και επιταχυνόμενη ανάπτυξη παίζει το διαδίκτυο και η αντίστοιχη συνεχής εξάπλωσή του. Τα δυο παραπάνω γεγονότα έχουν ως αποτέλεσμα τη δημιουργία νέων ασύρματων πρωτοκόλλων που έχουν ως σκοπό να καλύψουν τις διαρκώς αυξανόμενες, τόσο σε εύρος ζώνης όσο και σε ταχύτητα, ανάγκες για δικτύωση. Παρόλη όμως αυτή την αύξηση των ασύρματων επικοινωνιών, και ως εκ τούτου των διαφορετικών ραδιοσυχνοτήτων που χρησιμοποιούνται σε αυτά, υπάρχουν περιοχές του χάρτη ραδιοσυχνοτήτων που παραμένουν αχρησιμοποίητες ή που χρησιμοποιούνται μεν αλλά με μη αποδοτικό τρόπο. Μια από αυτές είναι και οι μπάντες συχνοτήτων που χρησιμοποιούν για τις μεταδόσεις τους οι τηλεοπτικοί σταθμοί. Οι συγκεκριμένες συχνότητες παρουσιάζουν και ένα επιπλέον χαρακτηριστικό το οποίο τις κάνει ακόμα πιο σημαντικές. Έχουν χαρακτηριστικά μετάδοσης που καταστούν τις μεταδόσεις που γίνονται στις συγκεκριμένες συχνότητες να έχουν μεγάλη ακτίνα εκπομπής, ενώ η καταναλισκόμενη ενέργεια για αυτές είναι σχετικά μικρή. Το πλήθος των αχρησιμοποίητων καναλιών αναμένεται να αυξηθεί καθώς γίνεται πραγματικότητα η ψηφιακή τηλεόραση, αντικαθιστώντας την αναλογική. Η δυνατότητα χρήσης των τηλεοπτικών συχνοτήτων από χρήστες διαφορετικούς από τους αδειοδοτημένους έχει επιτραπεί σε συσκευές ασύρματης επικοινωνίας, οι οποίες έχουν περιορισμένη ακτίνα εκπομπής. Ερωτηματικό όμως αποτελεί ωστόσο αν και κατά πόσο η απελευθέρωση της χρήσης του φάσματος των τηλεοπτικών ραδιοσυχνοτήτων θα έχει αρνητικές επιπτώσεις στις μεταδόσεις των τηλεοπτικών σταθμών.

Η τεχνολογία του Γνωστικού Ραδιοφώνου (*Cognitive Radio*) αποτελεί μια τεχνολογία βασισμένη στο Software Radio με την βοήθεια της οποίας δίνεται η δυνατότητα για πολύ ευέλικτες τηλεπικοινωνίες. Αυτό οφείλεται στο γεγονός ότι οι μεταδόσεις του *Cognitive Radio* προσαρμόζονται άκρως δυναμικά, καθώς τέτοιες συσκευές έχουν την δυνατότητα να εντοπίζουν από μόνες τους τα χαρακτηριστικά του ραδιοσυχνοτικού τους οικοσυστήματος. Αυτό έγινε δυνατό με τον συνδυασμό της τεχνολογίας των τηλεπικοινωνιών με άλλους τομείς της επιστήμης των υπολογιστών, όπως της τεχνητής νοημοσύνης αλλά και του υλικού των υπολογιστών και της αντίστοιχης ραγδαίας ανάπτυξης που έχει παρουσιαστεί σε αυτούς τους τομείς. Βλέποντας όλη αυτή την ανάπτυξη γύρω από τον τομέα των τηλεπικοινωνιών η Ομοσπονδιακή Επιτροπή Επικοινωνιών των Ηνωμένων Πολιτειών της Αμερικής πήρε το Μάιο του 2004 την απόφαση να απελευθερώσει το φάσμα των ραδιοηλεκτρικών συχνοτήτων σε μη αδειοδοτημένους χρήστες. Ο αυστηρός, αλλά πλέον εφικτός περιορισμός, που έθεσε είναι να μην γίνονται παρεμβολές στους πρωτεύοντες χρήστες των συχνοτήτων αυτών συμπεριλαμβανομένων και των συσκευών που χρησιμοποιούν μη αδειοδοτημένα το φάσμα, αλλά έχουν περιορισμένη ακτίνα εκπομπής. Η απάντηση του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (*Institute of Electrical and Electronic Engineers – IEEE*) σ' αυτή την πρόκληση ήρθε άμεσα, το Νοέμβριο του ίδιου έτους, προωθώντας την ανάπτυξη ενός πρωτοτύπου ασύρματων επικοινωνιών, του 802.22, για δημιουργία δικτύων σε μεγάλες ακτίνες κάνοντας έτσι εφικτή την κάλυψη, με δίκτυα υψηλών ταχυτήτων, περιοχών που είναι ιδιαιτέρως δυσπρόσιτες λόγω της γεωγραφικής τους θέσης.

Προεργασία για την ανάπτυξη των δικτύων των πολύ μεγάλων αποστάσεων είχε ήδη γίνει καθώς ένα πρωτόκολλο για μεγάλες αποστάσεις προϋπήρχε και αυτό ήταν το 802.16 – Wimax. Σ' αυτό όμως θα έπρεπε να γίνουν οι απαραίτητες τροποποιήσεις για να υιοθετηθεί αυτή η δυναμική συμπεριφορά που θα πρέπει να έχει το νέο αυτό πρωτόκολλο. Όπως και στο

802.16 βασική οντότητα για την δημιουργία ενός δικτύου είναι ο σταθμός βάσης ο οποίος σχετίζεται με μια ή περισσότερες συσκευές πελατών. Όλες οι οντότητες ενός δικτύου θα πρέπει να εξασφαλίζουν ότι με την λειτουργία τους δεν θα δημιουργούν παρεμβολές σε αδειοδοτημένους χρήστες. Για να είναι αυτό δυνατό θα πρέπει αυτές να πραγματοποιούν περιοδικά κάποιους ελέγχους για τον εντοπισμό τους. Επιπλέον, λόγω της μεγάλης ακτίνας δράσης των δικτύων αυτών είναι συχνό το φαινόμενο της κάλυψης μιας περιοχής από περισσότερα του ενός δίκτυα που λειτουργούν σε ίδιο ή ίδια κανάλια με αποτέλεσμα να πρέπει να υπάρχει μέριμνα για μηχανισμούς που θα επιτρέπουν την συνύπαρξη των δικτύων αυτών.

Σελίδα | ii

Καθώς το 802.22 δεν έχει ακόμα προτυποποιηθεί πλήρως για κάποιες από αυτές τις λειτουργίες που αναφέρονται παραπάνω, αλλά και για τις γενικές λειτουργίες των δικτύων αυτών, έχουν προταθεί κάποιες λύσεις ενώ για άλλες γίνεται ακόμα έρευνα από διαφορετικές ερευνητικές ομάδες οι οποίες ασχολούνται με την ανάπτυξη του πρωτοκόλλου. Έχει διαπιστωθεί όμως ότι το συγκεκριμένο πρωτόκολλο έχει κάποιες ευπάθειες στον τομέα της ασφάλειας. Αυτές κυρίως έχουν σχέση με την διαχείριση των πόρων. Ήδη έχει γίνει έρευνα και σε αυτό τον τομέα, πάνω στις προτάσεις που έχουν γίνει για κάποιες λειτουργίες, με ερευνητές να αναφέρουν πιθανά σενάρια διακοπής της εύρυθμης λειτουργίας των δικτύων 802.22. Στην διπλωματική αυτή εργασία γίνεται ανάλυση κάποιων τέτοιων σεναρίων που έχουν εντοπιστεί από άλλους ερευνητές αλλά γίνονται και κάποιες προτάσεις για την αποτελεσματικότερη αντιμετώπισή των απειλών αυτών. Έχει γίνει προσπάθεια έτσι ώστε οι όποιες λύσεις προτείνονται να προκαλούν την ελάχιστη δυνατή επιβάρυνση στο δίκτυο.

Πέρα όμως από την ανάλυση αυτών των επιθέσεων σε θεωρητικό επίπεδο υπήρξε ανάγκη για να ελεγχθεί η αποτελεσματικότητα των αντιμέτρων, η οποία θα γινόταν με την βοήθεια κάποιων μετρήσεων. Γι' αυτό το λόγο χρησιμοποιήθηκε ο γνωστός προσομοιωτής δικτύων ns-2 με μια επιπλέον επέκταση έτσι ώστε να είναι δυνατή η προσομοίωση του πρωτοκόλλου 802.22. Ο ns-2 είναι ένας προσομοιωτής δικτύων ανοιχτού κώδικα, δίνοντας με αυτό τον τρόπο σε πλήθος ερευνητών ανά τον κόσμο να επεκτείνουν την λειτουργία του αυξάνοντας την λειτουργικότητα του σε όλα τα επίπεδα ενός δικτύου (φυσικού μέσου, πρόσβασης στο μέσο κλπ). Για το συγκεκριμένο όμως πρωτόκολλο δεν υπάρχει ακόμα διαθέσιμη κάποια επέκταση για να υποστηρίξει την λειτουργικότητα του 802.22. Γι' αυτό το λόγο στα πλαίσια της διπλωματικής αυτής εργασίας πρώτου γίνεται η ανάλυση των ευπαθειών και η αξιολόγηση των αντιμέτρων που λήφθηκαν θα έπρεπε να υλοποιηθεί το σύνολο της λειτουργικότητας του πρωτοκόλλου στο περιβάλλον του ns-2.

Καθώς το πρωτόκολλο 802.22 είναι ένα πρωτόκολλο επιπέδου πρόσβασης στο μέσο (*Medium Access Control protocol – MAC protocol*), η λειτουργικότητα που αναπτύχθηκε αφορούσε κατά κύριο λόγο αυτό το επίπεδο δικτύου. Έτσι πρωταρχικός σκοπός ήταν να αναπτυχθεί η βασική λειτουργικότητα του πρωτοκόλλου όπως τα πακέτα που ανταλλάσσονται από τις οντότητες ενός δικτύου κατά την διάρκεια ενός frame και ο τρόπος που οι οντότητες αυτές αντιδρούν σε αυτά, οι περιοδικοί έλεγχοι για την αναζήτηση πρωτευόντων χρηστών των συχνοτήτων. Στη συνέχεια επεκτάθηκε η υπάρχουσα λειτουργία με τα αντίμετρα που προτάθηκαν και αναθεωρήθηκαν τόσο οι λειτουργίες που έχουν ήδη ενσωματωθεί στο πρωτόκολλο όσο και τα αντίμετρα αυτά καθαυτά. Η αποτελεσματικότητα κρίνεται τόσο με βάση την αποτελεσματικότητά τους τις επιθέσεις όσο και στην επιβάρυνση που δημιουργούν στο δίκτυο, καθώς και οι δυο αυτοί παράγοντες είναι σημαντικοί για την απρόσκοπτη λειτουργία των δικτύων. Οι αλλαγές που έγιναν σε επίπεδο φυσικού μέσου αφορούσαν κυρίως την δυνατότητα εκπομπής των συσκευών του δικτύου σε πολλά κανάλια αλλά και στην υιοθέτηση της διαίρεσης συχνότητας πολλαπλής πρόσβασης (*OFDMA*), που όπως ορίζεται από το ίδιο το πρότυπο, θα χρησιμοποιηθεί για μεγαλύτερη αποτελεσματικότητα όσον αφορά τη χρήση του φάσματος.

Με βάση αυτά που αναφέρθηκαν παραπάνω η παρούσα διπλωματική εργασία έχει χωριστεί σε δυο κύρια μέρη. Στο πρώτο αναφέρονται οι λεπτομέρειες που αφορούν το θεωρητικό

κομμάτι του πρωτοκόλλου αλλά και οι απαραίτητες πληροφορίες που αφορούν τον προσομοιωτή δικτύων 802.22. Για να είναι δυνατή η ανάπτυξη της επέκτασης για το 802.22 μελετήθηκαν προηγουμένως και άλλα πρότυπα που υπήρχαν υλοποιημένα στον ns-2, όπως το 802.16 με το οποίο παρουσιάζουν και πολλές ομοιότητες, με στοιχεία που θα ήταν δυνατό να επαναχρησιμοποιηθούν για την διευκόλυνση της ανάπτυξής του. Το δεύτερο μέρος της διπλωματικής αναλύεται ο τρόπος με τον οποίο έγινε δυνατή η υλοποίηση της επέκτασης και των δυνατοτήτων που ορίζονται ότι θα έπρεπε να έχει το πρωτόκολλο. Πέρα όμως από αυτό γίνεται εξήγηση υλοποίησης συγκεκριμένων σεναρίων επίθεσης και των αντιμέτρων σε συνδυασμό με την αξιολόγησή τους.

Σελίδα | iii

Αθήνα, Φεβρουάριος 2010.

SUMMARY

Σελίδα | iv

In the recent years, the telecommunications sector growth has been based to a great extent on the development of wireless networks. One of the main reasons for this continuous and rapid development is Internet and its respective development. The above facts have led to the creation of a big number of wireless protocols aiming to cover the increasing needs for networking both in terms of bandwidth capacity and speed. However, despite this unprecedented growth of wireless telecommunications and, thus, of the different radiofrequency bands used for protocols communication, there are still some unused or not efficiently used bands. One of these not efficiently used bands is the band used for television emissions. These radiofrequency bands have some significant special transmission characteristics which ensure broader signal transmission, while the transmission power remains in very low levels. Moreover, the number of unused channels in these bands is expected to increase as analog television is giving its place to its digital form. The possibility of using the television frequency bands is permitted for wireless devices of limited range. There are a lot of questions, though, concerning the quality of transmissions of primary users of these bands (the actual television emissions) when long range emissions of secondary devices are taking place.

Cognitive Radio technology is a technology based on Software Radio through which telecommunications can become much more flexible and dynamic. This is due to the fact that Cognitive Radio's transmissions can be adjusted dynamically, as this type of devices have the ability to auto-configure their transmission characteristics according to measures they make on their radiofrequency "ecosystem". This has been possible by combining telecommunications technology with other sectors of computer science and engineering, such as artificial intelligence, and hardware engineering, which have greatly developed in the recent years. Considering the development in the telecommunications sector, in May 2004, the Federal Communications Commission of United States of America took the decision to liberate the use of television bands for long range secondary non-licensed users. There would be only one strict limitation in the use of these radiofrequency bands made by secondary users: they must not interfere with the transmissions of incumbent users and short range users of this frequency band. The reaction of the Institute of Electrical and Electronic Engineers was immediate. Later, in the same year, it promoted the development of a new wireless standard, 802.22, which would be used for WRAN (Wireless Regional Access Networks). By using this type of networks in rural areas, broadband internet access could be provided, something that could be very costly or even impossible if using fiber optics networks or WMAN (Wireless Metropolitan Access Networks).

At the time there was some work done in sectors relative to WRAN as there was already a standard for WMAN, 802.16 – Wimax. But this was not enough, because changes were necessary in order to adapt to the highly dynamic behavior of the new protocol and its long range. As in 802.16, the major network entity of this standard is the base station which can be associated with one or more consumer premise equipment devices. Every single entity in 802.22 networks must assure that their operation will not cause harmful interference to incumbent users of the television bands. In this respect, they must periodically perform sensing operations to find out if primary users are in their in-range area. Moreover, overlapping of 802.22 networks which use the same channel/channels is very often, due to the large coverage area of this kind of networks. As a result, there are some synchronization issues that should be taken under consideration for the harmonious coexistence and resource management of all overlapping networks.

As 802.22 standard is still draft for some of the functions mentioned above, as well as for the general network functions, some proposals have already been made, while other proposals are under investigation from different research teams which deal with protocol's development. Research results concerning the protocol security show that this protocol and some mechanisms proposed for this standard have some security vulnerabilities, relating to resource management of the mechanism that must be used. Research has already been conducted on this sector as well as on the proposals regarding some of these functions which revealed that there are some possible scenarios in which this kind of networks will stop operating properly. The present thesis includes an analysis of the scenarios outlined by other researchers, as well as other proposals in order to face these vulnerabilities more efficiently. The focus is to propose solutions which will cause the minimum overhead at network's functionality.

Beyond the theoretical analysis of attacks which exploit the vulnerabilities of the protocols, it was also essential to check the effectiveness and efficiency of the countermeasures proposed, by studying some measurements. In order to take the measurements needed for this study, the network simulator ns-2 was used, with an extra module to support functionality of 802.22. Ns-2 is a very popular, free and open-source network simulator. Due to his open source, it is used from a wide range of users, especially in an academic context, in order to study network behavior. Moreover, it is possible to anyone to modify the source code or add modules to extend the simulator's functionality in all network levels. However, there was not a module available or published simulating the functionality of 802.22. In the context of this thesis, before covering the issues of security vulnerabilities and countermeasures review, a module should be developed, implementing all the functionality of an 802.22 network in ns-2.

As 802.22 is a Medium Access Control Protocol, the functionality developed mainly concerned this network layer. Thus, it was an issue of major significance to develop the main functionality of an 802.22 network, such as sensing that is taking place for incumbent detection, packets sent and received during a frame period and the way that network entities are reacting during this packet exchange. The development process should be done in a way that would enable the addition of countermeasures and then the review of both the functionality proposed and the countermeasures. The effectiveness and efficiency of the countermeasures was tested by using two criteria. Firstly, the network overhead that these are causing and secondly the robustness they show during the attacks. Both issues are very important for the proper network operation. Some changes have been also made in the physical layer. The main changes concerned the transmission in multiple channels but also the support of the Orthogonal Frequency Division Multiple Access (OFDMA) which is used in 802.22 to support access on the physical layer for multiple users and it is used for greater effectiveness on spectrum usage.

According to what was previously mentioned, this thesis is divided into two main parts. In the first part, details are provided on the theoretical aspects of the 802.22 MAC protocol as well as all the necessary information concerning the ns-2 network simulator used for the implementation issues. In order to develop the 802.22 module for ns-2, a study has been carried out on MAC protocols already implemented in ns-2, such as 802.16, which present many similarities and can be used to improve module development. The second part gives a description of the way that the module actually developed but there is also a description of how attack scenarios have been implemented and their countermeasures along with their review.

Athens, February 2010

ΕΙΣΑΓΩΓΙΚΟ ΣΗΜΕΙΩΜΑ

Σελίδα | vi

Το κείμενο που κρατάτε στα χέρια σας είναι η αναφορά για την διπλωματική εργασία του Μεταπτυχιακού προγράμματος Ειδίκευσης στα Πληροφοριακά Συστήματα της τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών. Η διπλωματική αυτή εργασία έλαβε χώρα το ακαδημαϊκό έτος 2009 – 2010 και συγκεκριμένα στο χειμερινό εξάμηνο, έπειτα από ανάθεση του Λέκτορα του τμήματος Πληροφορικής κ.κ. Ιωάννη Μαριά.

Η εργασία αυτή, σε όλα τα επίπεδα έγινε, με την συνεργασία ενός συναδέλφου μεταπτυχιακού φοιτητή και φίλου, του Κωνσταντίνου Γαλανόπουλου. Τα κείμενα που ακολουθούν περιγράφουν την συνεισφορά του γράφοντος στην εκπόνησή της.

Θα ήθελα να ευχαριστήσω όλους τους καθηγητές του μεταπτυχιακού προγράμματος για την γνώση που προσέφεραν καθ' όλη την διάρκεια του προγράμματος. Θα πρέπει να ευχαριστήσω όμως ιδιαίτερα και τον κ.κ. Μαριά για την εμπιστοσύνη που έδειξε με την ανάθεση αυτού του απαιτητικού, κατά γενική ομολογία, θέματος και για τις κατευθύνσεις που έδωσε καθ' όλη την διάρκεια της εκπόνησης της διπλωματικής εργασίας.

Φώτης Σπαθαράκης

ΑΚΡΩΝΥΜΙΑ

BE	Best Effort - Υπηρεσία χωρίς απαιτήσεις
BS	Base Station - Σταθμός Βάσης
CPE	Consumer Premise Equipment - Συσκευή Πελάτη
DCD	Downlink Channel Descriptor - Περιγραφέας Downlink Καναλιού
DL	Downlink
EIRP	Equivalent Isotropically Radiated Power - Ενεργή Ισοτροπική Ακτινοβολούμενη Ισχύς
ERP	Equivalent Radiated Power - Ενεργή Ακτινοβολούμενη Ισχύς
FCH	Frame Control Header - Επικεφαλίδα Ελέγχου του frame
FDD	Frequency Division Duplex - Αμφίδρομη Λειτουργία Διαίρεσης Συχνότητας
FEC	Forward Error Correction - Κώδικας εκ των Προτέρων Διόρθωσης Σφαλμάτων
FFC	Federal Communications Commission - Ομοσπονδιακή Επιτροπή Επικοινωνιών
FFT	Fast Fourier Transformation - Ταχύς Μετασχηματισμός Fourier
FTP	File Transfer Protocol - Πρωτόκολλο Μεταφοράς Αρχείων
LOS	Line of Sight - Οπτική Επαφή
MAC	Medium Access Control - Επίπεδο Πρόσβασης στο Φυσικό Μέσο
MN	Mobile Node - Κινητός Κόμβος
NLOS	Non-Line of Sight - Μη Οπτική Επαφή
ODSC	On-demand Spectrum Contention - Δέσμευση Φάσματος κατόπιν Αίτησης
OFDM	Orthogonal Frequency Division Multiplexing - Ορθογώνια Πολυπλεξία Διαίρεσης Συχνότητας
OFDMA	Orthogonal Frequency Division Multiple Access - Ορθογώνια Διαίρεση Συχνότητας Πολλαπλής Πρόσβασης
PMP	Point to Multipoint - Σημείο προς Πολλαπλά Σημεία
PT	Report - Παράδοση Αναφοράς
PU	Primary User - Πρωτεύων Χρήστης
QAM	Quadrature Amplitude Modulation - Τετραγωνική Διαμόρφωση Πλάτους
QP	Quiet Periods - Περίοδοι Ελέγχου του Καναλιού
QoS	Quality of Service - Ποιότητα Υπηρεσιών
RC	Receive - Λήψη
SCH	Superframe Control Header - Επικεφαλίδα Ελέγχου του superframe
SNR	Signal to Noise Ratio - Λόγος Σήματος Θορύβου
TCP	Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μετάδοσης
TDD	Time Division Duplex - Αμφίδρομη Λειτουργία Διαίρεσης Χρόνου
TTG	Transmission Time Gap - Χρονικό Κενό Μετάδοσης
UCD	Uplink Channel Descriptor - Περιγραφέας Uplink Καναλιού
UDP	User Datagram Protocol
UGS	Unsolicited Grant Service - Υπηρεσίες Σταθερού Ρυθμού Εκπομπής
UL	Uplink
WRAN	Wireless Regional Area Network - Ασύρματα Δίκτυα Μεγάλης Εμβέλειας
ertPS	extended real – time Polling Service

nrtPS	non real-time Polling Service - Υπηρεσία μη Πραγματικού Χρόνου με Μεταβλητό Χρόνο Εκπομπής
rtPS	real-time Polling Service - Υπηρεσία Πραγματικού Χρόνου με Μεταβλητό Χρόνο Εκπομπής

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περίληψη.....	1
Summary	4
Εισαγωγικό Σημείωμα	6
Πίνακας Περιεχομένων	9
Ευρετήριο Εικόνων	11
Ευρετήριο Πινάκων	13

Σελίδα | ix

Η Έννοια Του Cognitive Radio Και Το Πρωτόκολλο IEEE 802.22	1
1.1 Το Cognitive Radio	1
1.2 Το Πρωτόκολλο IEEE 802.22	3
1.2.1 Κίνητρα για την ανάπτυξη του πρωτοκόλλου	5
1.2.2 Κανονιστικό πλαίσιο.....	5
1.3 Χαρακτηριστικά Του 802.22	6
1.3.1 Οντότητες του 802.22.....	6
1.3.2 Κάλυψη.....	7
1.3.3 Δυνατότητες υπηρεσιών	7
1.3.4 Εξασφάλιση ποιότητας υπηρεσιών	8
1.3.5 Το φυσικό επίπεδο και το επίπεδο πρόσβασης στο μέσο του 802.22	8
1.4 Προοπτικές Εφαρμογής του 802.22	19

Ο Προσομοιωτής Δικτύων ns-2.....	21
2.1 Εισαγωγή.....	21
2.2 Εγκατάσταση του ns-2.....	23
2.3 Το μοντέλο της ασύρματης δικτύωσης στον ns-2.....	23
2.3.1 Προγραμματισμός γεγονότων	24
2.3.2 Βασικά συστατικά ενός κινητού κόμβου.....	24
2.3.3 Περιγραφή της τοπογραφίας μιας προσομοίωσης	28
2.3.4 Ορισμός του αντικειμένου GOD	28
2.3.5 Καταγραφή των στοιχείων της προσομοίωσης σε αρχεία	29

Διαδικασία Ανάπτυξης Της Επέκτασης Για Το Πρωτόκολλο IEEE 802.22 Στον ns-2.....	30
3.1 Η Επέκταση του IEEE 802.16	30
3.1.1 Διαχωρισμός δικτυακών οντοτήτων	30
3.1.2 Διατήρηση στοιχείων για τις συσκευές πελατών.....	32
3.1.3 Η έννοια της ροής δεδομένων	33

3.1.4 Συναρτήσεις που καλούνται μόνο από το σταθμό βάσης.....	38
Έλεγχος Του Καναλιού Μετάδοσης - Αλλαγή Καναλιού Μετάδοσης.....	43
4.1 Η Περίοδος Γρήγορου Ελέγχου (Fast Sensing)	43
4.1.1 Η περίοδος γρήγορου ελέγχου στο επίπεδο MAC.....	43
4.1.2 Η περίοδος γρήγορου ελέγχου στο επίπεδο διεπαφής με το φυσικό μέσο.	44
4.1.3 Σύνδεση των πληροφοριών των δυο επιπέδων.....	45
4.2 Η Περίοδος Λεπτομερούς Ελέγχου (Fine Sensing)	47
4.3 Διακοπή Των Μεταδόσεων Κατά Την Διάρκεια Του Fast Και Του Fine Sensing	48
4.4 Δομή Του Υλοποιημένου Module.....	51
4.5 Διαδικασία Ενημέρωσης Σχετικά Με Την αλλαγή Του Καναλιού	53
4.6 Περιγραφή Ενός Αρχείου Tcl.....	55
4.6.1 Ορισμός του σταθμού βάσης.....	55
4.6.2 Ορισμός της συσκευής πελάτη.....	55
4.6.3 Κεραίες εκπομπής σήματος.....	56
4.6.4 Δήλωση των ροών δεδομένων.....	56
4.7 Περιγραφή Ενός Σεναρίου Δοκιμής Της Επέκτασης	57
4.8 Επίπτωση sensing στο ρυθμό μετάδοσης/λήψης δεδομένων	60
Σενάρια Επίθεσης Σε Δίκτυα IEEE 802.22 Και Ανάπτυξη Αντιμέτρων Αντιμετώπισής Τους	62
5.1 Υλοποίηση Του Επιτιθέμενου Στον ns-2.....	62
5.2 Πραγματοποίηση Ελέγχων Από Ανενεργές Συσκευές Πελατών.....	63
5.2.1 Θεωρητική εκτίμηση της κατανάλωσης ενέργειας.....	65
5.2.2 Λειτουργία του επιτιθέμενου.....	70
5.2.3 Περιγραφή του αλγορίθμου	70
5.2.4 Υλοποίηση στον ns-2	71
5.3 Σύγκριση Αλγορίθμων Με Βάση Τις Απώλειες Δεδομένων.....	73
5.3.1 Σχολιασμός αποτελεσμάτων	77
5.4 Εξάρτηση Του Αλγορίθμου Από Την Απόσταση	78
5.4.1 Σχολιασμός γραφικών παραστάσεων.....	79
5.5 Βελτίωση Του Κανόνα Απόφασης.....	80
5.5.1 Υλοποίηση του βελτιωμένου κανόνα απόφασης στον ns-2.....	81
5.5.2 Αξιολόγηση του βελτιωμένου κανόνα απόφασης	83
Βιβλιογραφία	85
Συνοδευτικό Υλικό	89

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

Εικόνα 1: Χρήση συχνοτήτων 30-2900MHz όπως αυτή έχει μετρηθεί σε 6 σημεία ^[33]	2
Εικόνα 2: Συσκευές cognitive radio που λειτουργούν στο πεδίο των τηλεοπτικών συχνοτήτων. Σε διαφορετικές τοποθεσίες, οι συσκευές εντοπίζουν και διαφορετικές μη χρησιμοποιημένες συχνότητες	4
Εικόνα 3: Εμβέλεις διαθέσιμων πρωτοκόλλων ασύρματων δικτύων	5
Εικόνα 4: Πιθανό σενάριο ανάπτυξης ενός δικτύου 802.22.....	6
Εικόνα 5: Εμφάνιση κενών διαστημάτων μετάδοσης στο φάσμα.....	8
Εικόνα 6: Διαφορές μεταξύ ενός συμβόλου OFDM (α) – OFDMA (β).....	10
Εικόνα 7: Κωδικοποιήσεις ανάλογα με την απόσταση.....	11
Εικόνα 8: Γενική δομή του superframe.....	13
Εικόνα 9: Γενική δομή του frame	14
Εικόνα 10: Τα δυο στάδια πραγματοποίησης ελέγχου για εντοπισμό πρωτεύοντων χρηστών	16
Εικόνα 11: Συγχρονισμός επικαλυπτόμενων κυψελών.....	18
Εικόνα 12: Η βασική αρχιτεκτονική του ns-2	22
Εικόνα 13: Αναπαράσταση δυο ασύρματων κόμβων, όπως αυτή παρουσιάζεται από το εργαλείο προσομοίωσης EXAMS. Οι κόκκινοι κύκλοι αντιστοιχούν στην εμβέλεια κάθε κόμβου	22
Εικόνα 14: Αντιστοίχιση μεταξύ κλάσεων της C++ και της OTcl.....	23
Εικόνα 15: Παράδειγμα ενός δρομολογητή γεγονότων	24
Εικόνα 16: Δομή ενός κινητού κόμβου – mobile node.....	25
Εικόνα 17: Ορισμοί του RXThreshold και του CSThreshold	26
Εικόνα 18: Η δομή ενός 802.22 frame και ενός 802.22 superframe, όπως αυτό διαμορφώνεται με βάση τους timers που έχουν προστεθεί. Η δομή βασίζεται στο wimax module που έχει μελετηθεί. Με τη χρήση των timers στέλνονται και τα πακέτα την κατάλληλη χρονική στιγμή, όπως τα superframe και frame control header, τα DCD και UDC και τα DLMAP και ULMAP, με τρόπο παρόμοιο με αυτόν που έχει οριστεί στο 802.22 πρότυπο.....	52
Εικόνα 19: Παρεμβολές σε συνάρτηση με το χρόνο για τους σταθμούς βάσης.....	57
Εικόνα 20: Χρήση καναλιών κατά την διάρκεια της προσομοίωσης.....	58
Εικόνα 21: Παρεμβολές σε συνάρτηση με το χρόνο για τις συσκευές των χρηστών (CPEs) .	59
Εικόνα 22: Τρόπος λειτουργίας sensing από ανενεργές συσκευές. Στα slots που είναι σημειωμένα με κόκκινο είναι τα slots στα οποία οι υπόλοιπες συσκευές πελατών της κυψέλης θα πραγματοποιούν sensing μέχρι να ληφθεί η απόφαση από το σταθμό βάσης. Έπειτα από την αλλαγή του καναλιού δεν παρουσιάζονται παρεμβολές.....	64

Εικόνα 23: Μέγιστος αριθμός sensing λ με βάση τη διάρκεια k της παρεμβολής για διαφορετικό αριθμό n CPEs που πραγματοποιούν sensing. Για τις υπόλοιπες παραμέτρους ισχύει $a=3$ και $i=2$	68
Εικόνα 24: Μέγιστος αριθμός sensing λ με βάση τη διάρκεια k της παρεμβολής για διαφορετικό αριθμό slots στα οποία προκαλείται collision (3 και 5 αντίστοιχα) collision. Για τις υπόλοιπες παραμέτρους ισχύει $n=3$ και $i=2$	69
Εικόνα 25: Μέγιστος αριθμός sensing λ με βάση τη διάρκεια k της παρεμβολής για διαφορετικό αριθμό slots με τις παραμέτρους n , a και i να έχουν τις τιμές 3,1 και 2 αντίστοιχα	69
Εικόνα 26: Κατανάλωση ενέργειας του συστήματος σε συνάρτηση με το μέγιστο αριθμό των frames που πραγματοποιείται sensing για διαφορετικό αριθμό συσκευών πελατών σε ένα κελί. Για τις υπόλοιπες παραμέτρους ισχύει $a=3$ και $i=2$	70
Εικόνα 27: Τοπολογία με την οποία πραγματοποιούνται οι προσομοιώσεις	75
Εικόνα 28: Απώλεια δεδομένων σε bits όπως μετρήθηκε με την εκτέλεση του πρώτου σεναρίου προσομοίωσης	76
Εικόνα 29: Απώλεια δεδομένων σε bits, όπως μετρήθηκε με την εκτέλεση του δεύτερου σεναρίου προσομοίωσης. Παρατηρείται πως το σχήμα της γραφικής παράστασης διαφέρει ελάχιστα από την προηγούμενη.....	76
Εικόνα 30: Απώλεια δεδομένων σε bits, όπως μετρήθηκε με την εκτέλεση του τρίτου σεναρίου προσομοίωσης.	77
Εικόνα 31: Απώλεια δεδομένων σε bits, όπως μετρήθηκε με την εκτέλεση του τέταρτου σεναρίου προσομοίωσης	77
Εικόνα 32: Απώλειες δεδομένων σε bits κατά την διάρκεια των προσομοιώσεων, με την απόσταση του επιτιθέμενου από την μακρινότερη συσκευή πελάτη να αλλάζει συνεχώς. Οι σημειωμένοι χρόνοι αφορούν τις χρονικές στιγμές στις οποίες εντοπίζεται η παρεμβολή, εκκινώντας τις διαδικασίες αλλαγής του καναλιού.....	79
Εικόνα 33: Συνολικές απώλειες δεδομένων με βάση την απόσταση	79
Εικόνα 34: Τοπολογία προσομοίωσης.....	83
Εικόνα 35: Απώλειες δεδομένων στο χρόνο ανάλογα με την απόσταση με χρήση του βελτιωμένου κανόνα απόφασης.....	84

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

Πίνακας I: Αριθμός FFT ανάλογα με τα κανάλια	11
Πίνακας II: Χαρακτηριστικά του φυσικού επιπέδου του 802.22	12
Πίνακας III: Μέτρηση του ρυθμού ροής δεδομένων με την παρουσία sensing και χωρίς την παρουσία sensing και υπολογισμός της αποδοτικότητας. Το αποτέλεσμα που προκύπτει συγκλίνει με το θεωρητικό.	61

Κεφάλαιο 1

Η ΈΝΝΟΙΑ ΤΟΥ COGNITIVE RADIO ΚΑΙ ΤΟ ΠΡΩΤΟΚΟΛΛΟ IEEE 802.22

1.1 Το COGNITIVE RADIO

Το cognitive radio είναι μια μορφή τηλεπικοινωνιών στην οποία ο ίδιος ο δέκτης έχει **επίγνωση της κατάστασης του και των συνθηκών του περιβάλλοντός του**. Έχοντας αυτά ως δεδομένα, παρέχει τη δυνατότητα προσαρμογής σε συνεχώς εναλλασσόμενες καταστάσεις. Παραδείγματα για την επίγνωση της κατάστασής του μπορούν να αποτελούν οι ανάγκες του χρήστη που χρησιμοποιεί τον εκάστοτε δέκτη. Επιπλέον, μπορεί να γνωρίζει και τα **κανάλια του περιβάλλοντος** του και το **καθεστώς χρήσης** τους έτσι ώστε να χρησιμοποιεί τα ελεύθερα και να αποφεύγει τα κατειλημμένα, κάνοντας αποτελεσματική διαχείριση του φάσματος. Τέτοιου είδους συνθήκες αφορούν το περιβάλλον του πομπού με το οποίο αλληλεπιδρά ο δέκτης. Το σημαντικό είναι όμως πως και τα δυο είδη συνθηκών που προαναφέρθηκαν μπορεί να αφορούν και τον πομπό, έτσι ώστε ο δέκτης, μέσα από μηχανισμούς μηχανικής μάθησης, να μπορεί να αυτοπροσαρμόζεται με έξυπνο τρόπο.

Πιθανές επιπρόσθετες δυνατότητες που έχει το cognitive radio σχετίζονται με ακόμα ευρύτερους επιστημονικούς τομείς, όπως για παράδειγμα **τον τομέα των συστημάτων επίγνωσης θέσης**. Ειδικότερα, είναι πιθανό κάποιος από τους δέκτες cognitive radio να έχει τη δυνατότητα να εντοπίζει τη θέση στην οποία βρίσκεται κάθε χρονική στιγμή και να του παρέχονται υπηρεσίες ανάλογα με αυτή (*location-based services*). Επιπλέον, οι δέκτες μπορούν να έχουν τη δυνατότητα κρυπτογράφησης και αποκρυπτογράφησης σημάτων, εντοπισμού άλλων γειτονικών ασύρματων συσκευών, εξακρίβωσης της ταυτότητας και εξουσιοδότησης των χρηστών τους ^{[2][4]}.

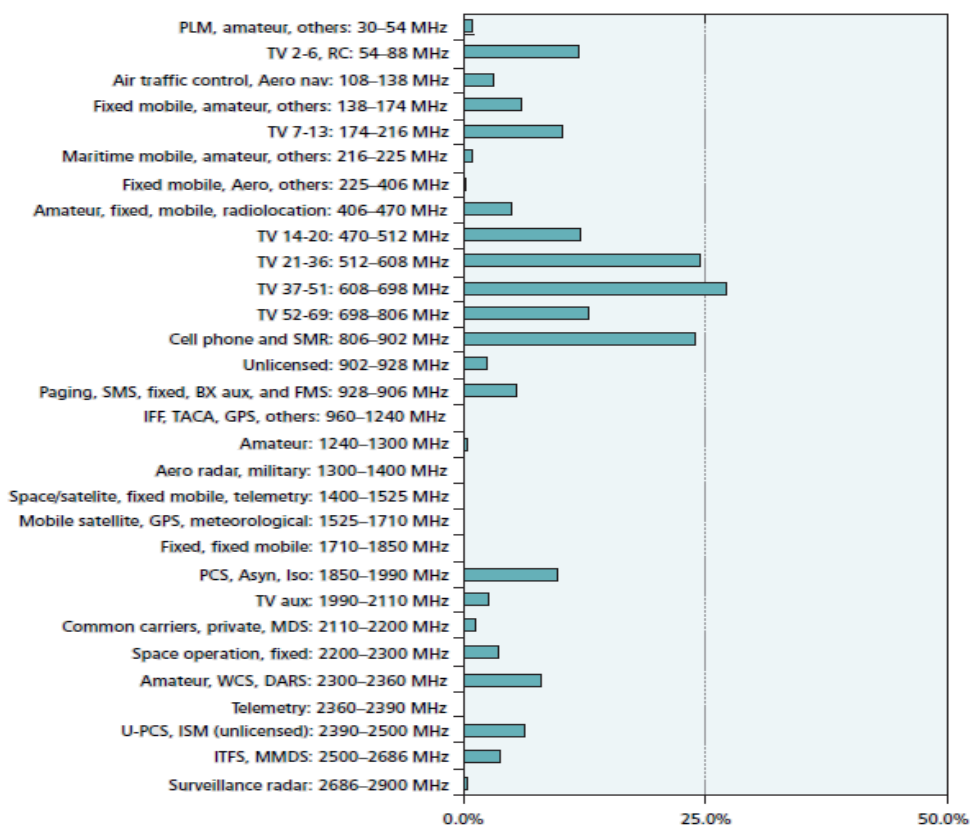
Προπομπός του cognitive radio θεωρείται το **software radio**, μια έννοια που χρησιμοποιήθηκε για πρώτη φορά από τον **Joseph Mitola**, το 1991. Ένα Software Radio είναι ένα σύστημα ραδιοεπικοινωνίας στο οποίο τα συστατικά του, τα οποία βρίσκονται σε μορφή υλικού (*hardware*), όπως ο μετατροπέας αναλογικού 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 προγραμματίσιμου (*programmable*) hardware που ελέγχεται από το λογισμικό. Το cognitive radio άρχισε να αναπτύσσεται από τον Joseph Mitola σε συνεργασία με την Υπηρεσία Προηγμένων Προγραμμάτων Αμυντικών Ερευνών των Ηνωμένων Πολιτειών¹, αλλά επεκτάθηκε και σε πανεπιστημιακά ιδρύματα, ενώ παράλληλα ιδρύθηκε και το SDR Forum (*Software Definable Radio Forum*), μια μη κερδοσκοπική βιομηχανική οργάνωση, με σκοπό τη διάδοση αυτής της νέας τεχνολογίας στις ραδιοεπικοινωνίες.

¹ Defense Advanced Research Projects Agency (DARPA)

Ένα ξεχωριστό χαρακτηριστικό που έχουν οι συσκευές cognitive radio είναι ότι έχουν τη δυνατότητα **προσαρμογής των χαρακτηριστικών της μετάδοσής τους**. Χρησιμοποιούν τεχνικές για τον έλεγχο της ενέργειας αλλά και για την προσαρμογή των χαρακτηριστικών διαμόρφωσης της μετάδοσής τους. Επιπλέον γίνεται κατανομή και δέσμευση καναλιών σε πραγματικό χρόνο, αλλά και έλεγχος ευρείας ζώνης φάσματος. Με την έξυπνη προσαρμογή των χαρακτηριστικών της λειτουργίας στις συνθήκες του περιβάλλοντος, θα γίνει δυνατή η αποτελεσματική χρήση του διαθέσιμου φάσματος συχνοτήτων, ενώ οι ίδιες οι συσκευές θα είναι πολύ ευέλικτες. Όλα αυτά έχουν καταστεί δυνατά λόγω της αλματώδους ανάπτυξης της τεχνολογίας των τηλεπικοινωνιών τα τελευταία χρόνια, ανάπτυξη που αποτέλεσε το εφαλτήριο για την αναγνώριση του cognitive radio ως σημαντικού μοχλού για αποδοτικότερη χρήση του φάσματος των ραδιοσυχνοτήτων².

Σελίδα | - 2 -

Από έρευνες που έχουν εκπονηθεί, έχει διαπιστωθεί ότι μεγάλο μέρος των συχνοτήτων από 30 – 2900 MHz παρουσιάζουν πολύ χαμηλά ποσοστά χρήσης (Εικόνα 1), δημιουργώντας με αυτό τον τρόπο «κενά αχρησιμοποίητα διαστήματα» στο διαθέσιμο φάσμα, μια έννοια που ορίστηκε στην αγγλική γλώσσα ως “whitespace”. Το φαινόμενο αυτό παρατηρήθηκε κυρίως στις συχνότητες που χρησιμοποιούνται από τις υπηρεσίες αναλογικής τηλεόρασης, καθώς επίσης και στις συχνότητες που χρησιμοποιούνται ως προστασία για να προληφθούν παρεμβολές μεταξύ των καναλιών.



Εικόνα 1: Χρήση συχνοτήτων 30-2900MHz όπως αυτή έχει μετρηθεί σε 6 σημεία [33]

² Ραδιοσυχνότητες: 300Hz – 3000GHz^[1]

1.2 Το Πρωτόκολλο IEEE 802.22

Η Ομοσπονδιακή Επιτροπή Επικοινωνιών των Ηνωμένων Πολιτειών³, που είναι υπεύθυνη για την δέσμευση των συχνοτήτων στο φάσμα των ραδιοσυχνοτήτων, έχοντας υπόψη όλα τα παραπάνω, προχώρησε το Μάιο του 2004 σε μια 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 δεν 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.

Σελίδα | - 3 -

Η μερική μη αδειοδοτημένη χρήση των συχνοτήτων που χρησιμοποιούνται από τις τηλεοπτικές υπηρεσίες⁴ οφείλεται σε δυο παράγοντες – κλειδιά:

1. Στην πολύ χαμηλή χρήση των συγκεκριμένων συχνοτήτων σε πολλές περιοχές της υφής. 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 μικρότερη⁵. Συγκεκριμένα, στις Ηνωμένες Πολιτείες αναμένεται να ελευθερωθούν 108MHz φάσματος από αυτή την «συμπίεση» των τηλεοπτικών καναλιών, ενώ στο Βερολίνο, που έχει ήδη συμβεί, ελευθερώθηκαν 35MHz, 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 1.2MHz, ενώ όλα τα τοπικά ασύρματα δίκτυα που χρησιμοποιούν τα πρωτόκολλα IEEE 802.11 b/g απασχολούν 83.5 MHz.
2. Ένα άλλο πολύ σημαντικό χαρακτηριστικό που έχουν οι συγκεκριμένες συχνότητες είναι τα ιδιαίτερα χαρακτηριστικά διάδοσής τους. Τα σήματα αυτών 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^{[5][6]}.

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

³ Federal Communications Commission (FCC)

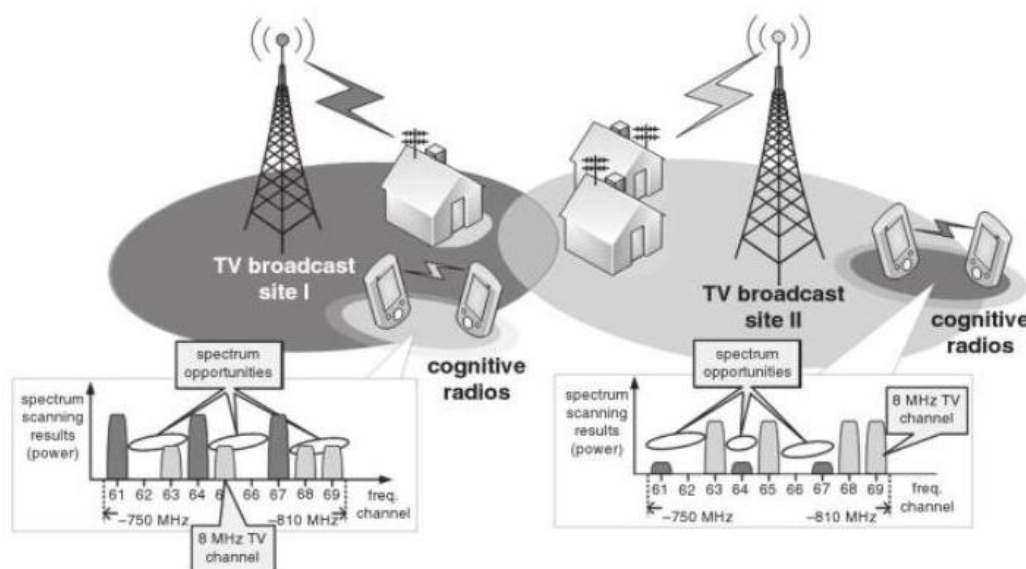
⁴ Οι συχνότητες μεταξύ 54 και 698 MHz

⁵ Δεν ισχύει το ίδιο για μεταδόσεις υψηλής ευκρίνειας (*High Definition - HD*) καθώς αυτές απαιτούν περισσότερο εύρος ζώνης

τις συχνότητες των τηλεοπτικών υπηρεσιών. Μ' 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.

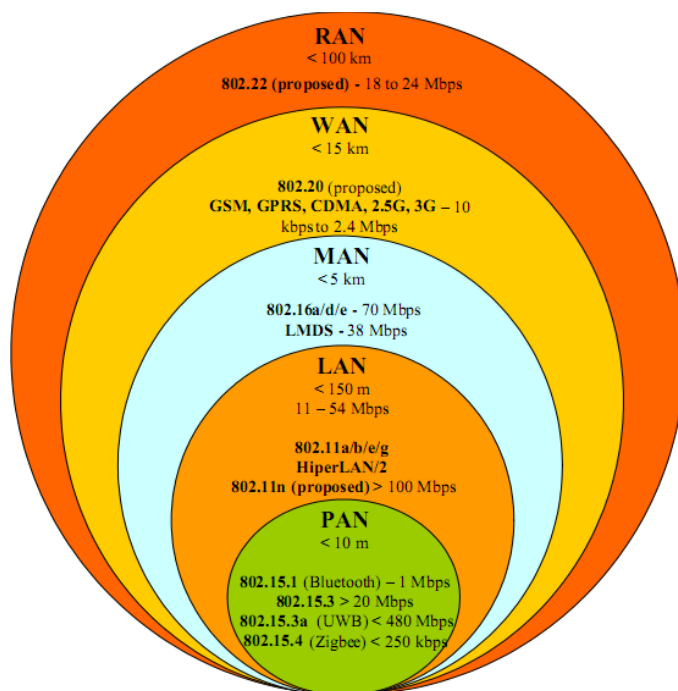
Βάσει των παραπάνω στοιχείων, η ερευνητική ομάδα του 802.22 στοχεύει στην προτυποποίηση της μη αδειοδοτημένης πρόσβασης στις τηλεοπτικές συχνότητες. Χαρακτηριστικό είναι το παράδειγμα της παρακάτω εικόνας, στην οποία παριστάνονται δυο παρακείμενες περιοχές εμβέλειας τηλεοπτικών σημάτων και δυο ζεύγη 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 [16].

Σελίδα | - 4 -



Εικόνα 2: Συσκευές *cognitive radio* που λειτουργούν στο πεδίο των τηλεοπτικών συχνοτήτων. Σε διαφορετικές τοποθεσίες, οι συσκευές εντοπίζουν και διαφορετικές μη χρησιμοποιημένες συχνότητες

1.2.1 Κίνητρα για την ανάπτυξη του πρωτοκόλλου



Εικόνα 3: Εμβέλεις διαθέσιμων πρωτοκόλλων ασύρματων δικτύων

Το κίνητρο για την ανάπτυξη αυτού του πρωτοκόλλου είναι η **κάλυψη με ευρυζωνικά δίκτυα περιοχών που είναι δυσπρόσιτες** και αυτό αφορά κυρίως **μη αστικές περιοχές**, 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.

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 χρειάζονταν (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^[8].

1.2.2 Κανονιστικό πλαίσιο

Το πρωτόκολλο, εφόσον κάνει μη αδειοδοτημένη χρήση των τηλεοπτικών συχνοτήτων για τις μεταδόσεις του, θα πρέπει να υπακούει στον μοναδικό και αυστηρό κανόνα, της μη επιβλαβούς παρενόχλησης των εκπομπών των μεταδόσεων των τηλεοπτικών σταθμών. Πέρα όμως από τις τηλεοπτικούς σταθμούς, υπάρχουν και μια σειρά άλλων συσκευών και υπηρεσιών που χρησιμοποιούν και αυτές χωρίς άδεια τις ελεύθερες τηλεοπτικές συχνότητες.

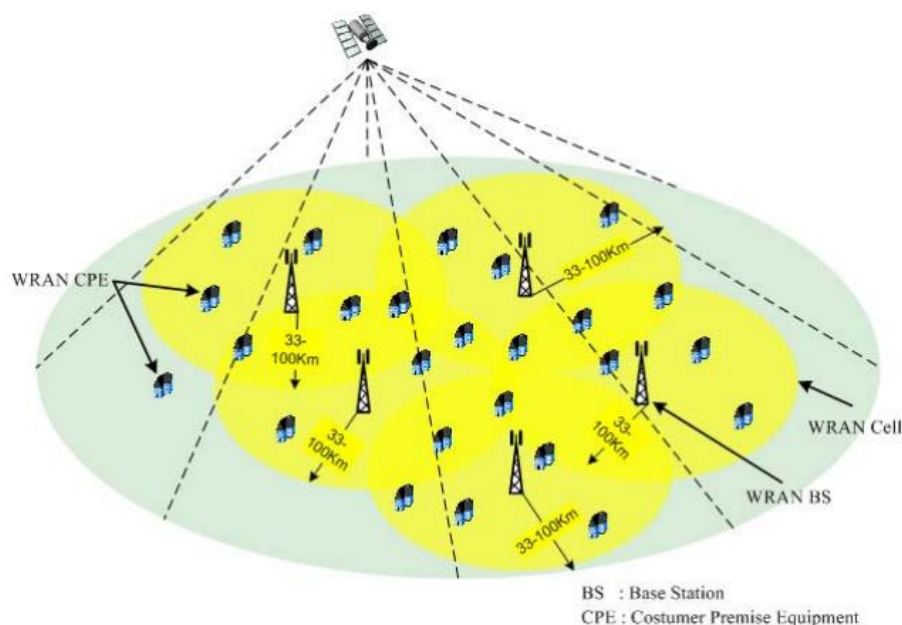
Αυτές είναι τα **ασύρματα μικρόφωνα** αλλά και **υπηρεσίες σχετικές με την δημόσια ασφάλεια** αλλά και εφαρμογές μικρής εμβέλειας όπως η **ασύρματη ενδοεπικοινωνία** μέσα σε κάποια επιχείρηση⁶. Σε κάθε περίπτωση όμως το σύνολο των υπηρεσιών που προαναφέρθηκαν αποτελούν τον πρωτεύον χρήστη αυτών των συχνοτήτων, 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.

Σελίδα | - 6 -

1.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ 802.22

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 μια ή περισσότερες συσκευές πελατών οι οποίες είναι συσχετισμένες με αυτόν (*Consumer Premise Equipments – CPE*).



Εικόνα 4: Πιθανό σενάριο ανάπτυξης ενός δικτύου 802.22

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 αυτόν 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.

⁶ Στις Ηνωμένες Πολιτείες αυτές οι υπηρεσίες αναφέρονται ως Private Land and Commercial Mobile Radio (PLMRS/CMRS)^[7]

Οι συσκευές των πελατών, πέρα από την αποστολή των δεδομένων, «βοηθούν» τους σταθμούς βάσης να κάνουν ελέγχους (*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 και αφορούν τη χρήση καναλιών στην περιοχή που βρίσκεται ο εκάστοτε σταθμός βάσης. Αυτή η διαδικασία εντοπισμού θα αναλυθεί εκτενέστερα αργότερα. Συνοψίζοντας όλα τα παραπάνω, μπορεί να ειπωθεί ότι η σχέση του σταθμού βάσης με τις συσκευές των πελατών είναι μια σχέση αφέντη – σκλάβου (*master – slave*). Όλες οι οντότητες που περιγράφηκαν προηγουμένως παριστάνονται σχηματικά στην Εικόνα 4.

Σελίδα | - 7 -

Μια ιδιαίτερη διαφορά που έχουν οι συσκευές των πελατών με το σταθμό βάσης είναι το **είδος** και ο **αριθμός των κεραιών** που έχουν. Συγκεκριμένα, οι σταθμοί βάσης διαθέτουν μόνο μια κεραία, πανδιευθυντική (*Omni - directional*). Αντίθετα, οι συσκευές των πελατών διαθέτουν δυο είδη κεραιάς. 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 κεραιάς 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 την μεταξύ τους επικοινωνία.

1.3.2 Κάλυψη

Όπως αναφέρθηκε και προηγουμένως, το πρωτόκολλο 802.22 προορίζεται να καλύπτει μεγάλες περιοχές. Η κάλυψη, όπως φαίνεται στην Εικόνα 4, μπορεί να φτάσει στα 33 km με ενέργεια εκπομπής τα 4 Watt EIRP⁷. Η κάλυψη αυτή μπορεί να επεκταθεί μέχρι τα 100 km αν δεν τίθενται περιορισμοί, είτε όσον αφορά την κατανάλωση ενέργειας (καθώς θα είναι αυξημένη), είτε από παρεμβολές, λόγω της αυξημένης ενέργειας εκπομπής. Ζητήματα σχετικά με την αρμονική συνύπαρξη μεταξύ των δικτύων του 802.22 (*self – coexistence*) αλλά και μεταξύ των δικτύων 802.22 και των πρωτευόντων χρηστών των συχνοτήτων θα αναλυθούν περισσότερο στην συνέχεια.

1.3.3 Δυνατότητες υπηρεσιών

Στο 802.22, η απόδοση του φάσματος (*spectral efficiency*) προσδιορίζεται στο εύρος 0.5 – 5 bit/(s/Hz). Βάσει του εύρους 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 στα 18Mbps. Ο ρυθμός αυτός μπορεί να αυξηθεί ακόμα περισσότερο αν χρησιμοποιηθούν μεγαλύτερου εύρους κανάλια, των 7 ή 8 MHz, φτάνοντας στη μέγιστη τιμή των 24 Mbps. Συνεπώς, αν υπάρχουν 12 συσκευών πελατών συνδεδεμένες με ένα σταθμό βάσης, η ελάχιστη δυνατή κάλυψη μπορεί να επιτευχθεί με ένα ρυθμό μετάδοσης δεδομένων της τάξης των 1.5Mbps / 384Kbps 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.

⁷ Equivalent isotropically radiated power. Ο ελληνικός όρος είναι Ενεργή Ισοτροπική Ακτινοβολούμενη Ισχύς.

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:

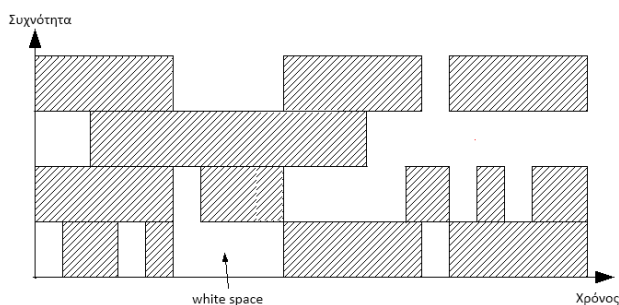
Σελίδα | - 8 -

1. *UGS (Unsolicited Grant Service)*: Για υπηρεσίες σταθερού ρυθμού εκπομπής. Τέτοιες υπηρεσίες είναι οι τηλεδιασκέψεις, διασκέψεις μέσω τηλεφώνου (χωρίς silence suppression⁸) 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 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)^[11].

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

1.3.5.1 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 για να καθοριστεί για να καθοριστεί ο χρόνος εμφάνισης αυτών των διαστημάτων. Στην Εικόνα 5 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 και του επιπέδου πρόσβασης στο μέσο^[9].



Εικόνα 5: 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

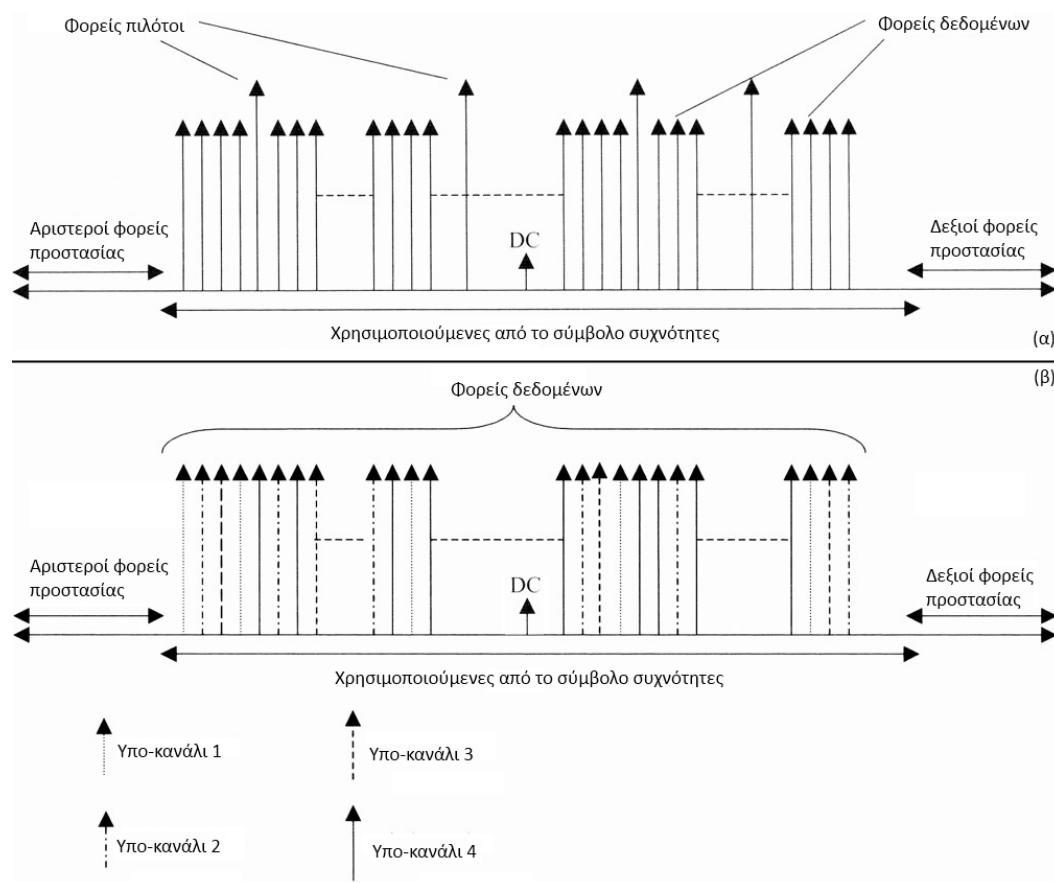
⁸ Σε αυτού του είδους την επικοινωνία φωνής μέσω IP δεν εκπέμπονται δεδομένα όταν εντοπιστεί ότι κάποιο από τα δυο μέλη που συμμετέχουν στην συνομιλία έχει σιγήσει, με αποτέλεσμα να μειώνεται η χρήση του δικτύου.^[15]

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 ^[10].

Με αυτό τον τρόπο εξασφαλίζεται ένας ευέλικτος και δυναμικός τρόπος για την 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). Σε αυτή 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 την 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 στο άξονα της συχνότητας.
4. Ένας ειδικός κενός φορέας είναι ο *φορέας DC (Direct Current)*. Ο φορέας DC έχει συχνότητα ίδια με τη 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 στην παρακάτω εικόνα (Εικόνα 6) ^{[11][12]}.

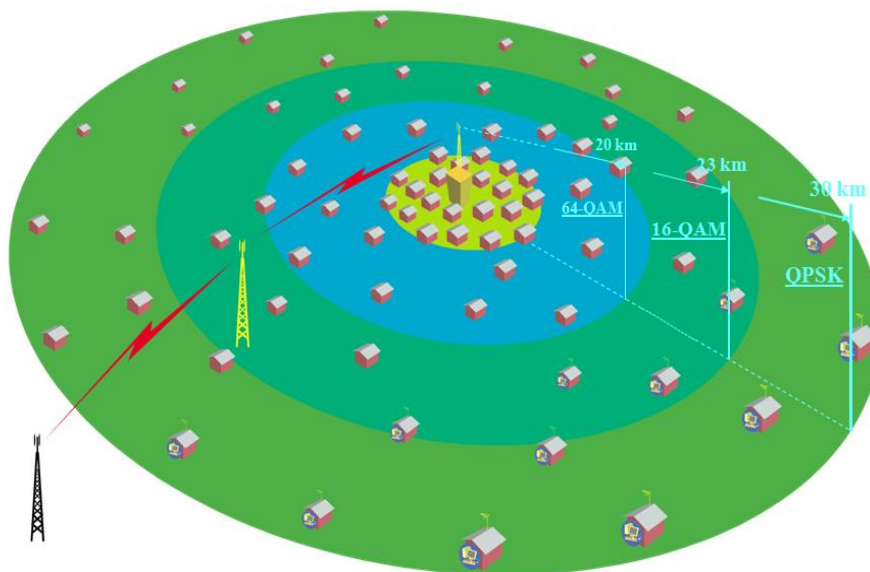


Εικόνα 6: Διαφορές μεταξύ ενός συμβόλου OFDM (α) – OFDMA (β)

Μια ακόμη παράμετρος που παίζει σημαντικό ρόλο στην υψηλή αποδοτικότητα του φάσματος είναι ο αριθμός των μετασχηματισμών Fourier (*Fast Fourier Transformations* – FFT) που γίνονται σε κάθε σύμβολο. Όσο αυξάνεται ο αριθμός των μετασχηματισμών Fourier, τόσο μειώνονται οι απαιτούμενοι φορείς 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 χρησιμοποίηση 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 στην Εικόνα 7, 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 οι διαφοροποιήσεις 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 περίσωση (*multi-path*), έχοντας με αυτό 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*).



Σελίδα | - 11 -

Εικόνα 7: 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 δεν χρησιμοποιείται συνένωση καναλιών, το ένα από τα τρία κανάλια χρησιμοποιείται για τις μεταδόσεις των δεδομένων ενώ τα άλλα δυο για προστασία των τηλεοπτικών καναλιών. Όταν χρησιμοποιείται η συνένωση, τότε χρησιμοποιούνται δυο 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 μ' αυτό φαίνονται στον παρακάτω πίνακα:

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

Πίνακας Ι: Αριθμός FFT ανάλογα με τα κανάλια

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. Για 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 την 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 την 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 εμφανίζονται συνοπτικά και συγκεντρωμένα τα χαρακτηριστικά που θα έχει το φυσικό επίπεδο του πρωτοκόλλου όπως αναφέρθηκαν παραπάνω.

Σελίδα | - 12 -

Συχνότητες	54-862MHz
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 II: Χαρακτηριστικά του φυσικού επιπέδου του 802.22

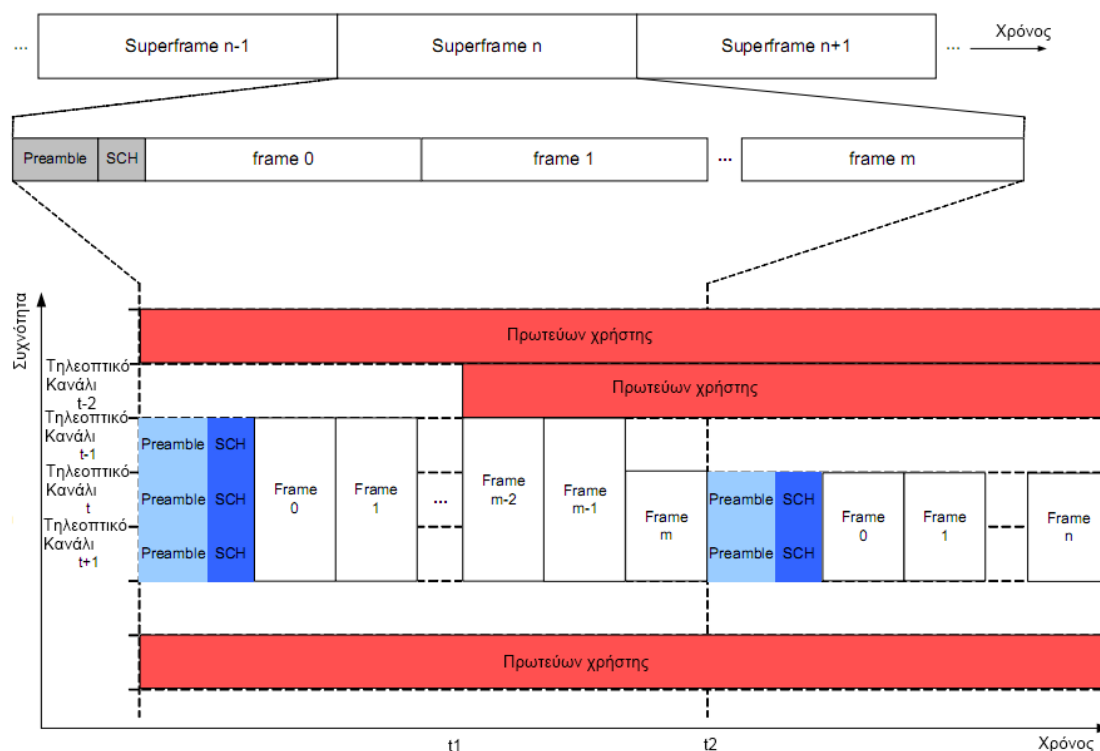
1.3.5.2 Επίπεδο πρόσβασης στο μέσο (MAC)

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 πρωτοκόλλα και συγκεκριμένα στην οικογένεια πρωτοκόλλων του 802.16^[40]. 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 superframes 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 την διαχείριση του φάσματος. Επιπλέον χαρακτηριστικά αυτού του επιπέδου περιλαμβάνονται για την υποστήριξη διαφόρων τύπων κυκλοφορίας με διαφορετικές απαιτήσεις ποιότητας υπηρεσιών (Quality of Service - QoS)^[42].

1.3.5.2.1 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 διάρκειά του είναι 160ms. Στην αρχή κάθε superframe υπάρχει το τμήμα (preamble), το οποίο προαναγγέλλει την αρχή του superframe και χρησιμοποιείται για τον 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 θα πρέπει να λάβουν οι συσκευές του πελάτη για να αρχίσει η διαδικασία συσχετισμού μεταξύ αυτού και του σταθμού βάσης και εκπέμπεται, όπως γίνεται αντιληπτό, από τον σταθμό βάσης και μόνο. Μετά από την επικεφαλίδα ελέγχου του superframe ακολουθούν τα δεκαέξι frames που απαρτίζουν το κάθε superframe.

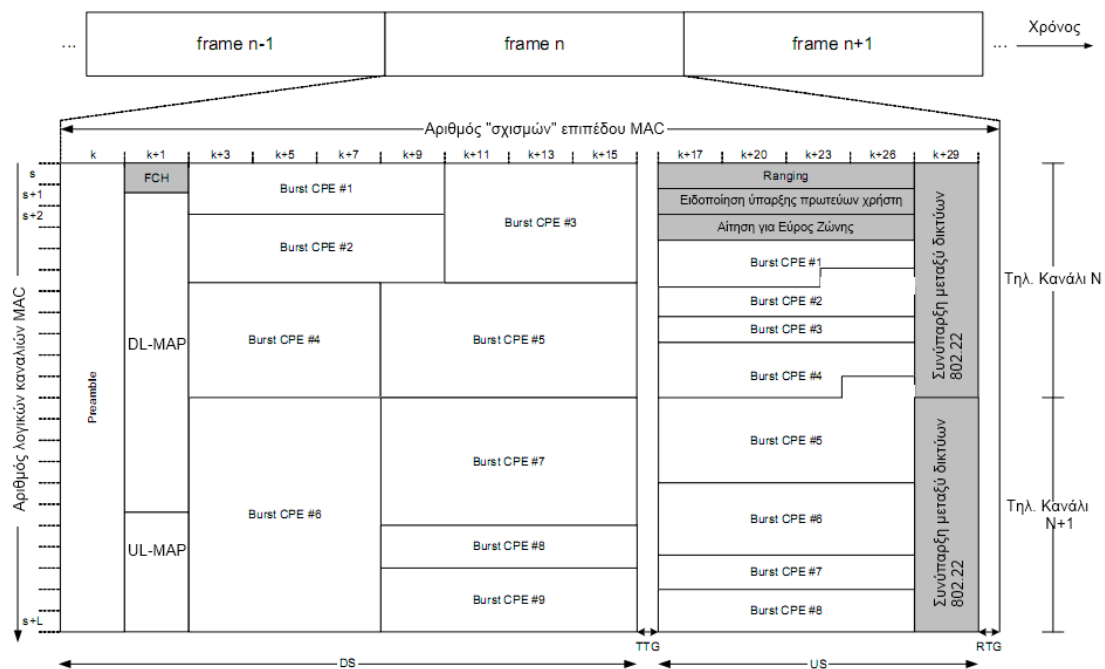


Σελίδα | - 13 -

Εικόνα 8: Γενική δομή του superframe

Στην Εικόνα 8 φαίνεται η δομή του superframe όπως παρουσιάστηκε σε αυτή την παράγραφο, σε συνδυασμό με τις μεταδόσεις των πρωτεύοντων χρηστών. Στην ίδια εικόνα παριστάνεται και η συνένωση των καναλιών, καθώς και μια αντίδραση του συστήματος. Όπως παρατηρείται, την χρονική στιγμή t_1 κάποιος πρωτεύων χρήστης αρχίζει μεταδόσεις στο τηλεοπτικό κανάλι $t-2$, που χρησιμοποιείται, όπως προαναφέρθηκε νωρίτερα, ως συχνότητα προστασίας. Έτσι από την 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 στην Εικόνα 9. Σε αυτή τη δομή εντοπίζονται δυο 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 τον σταθμό βάσης (*Upstream Subframe*). Αυτά τα δυο τμήματα αυτά 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.



Εικόνα 9: 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 Upstream 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, τότε θα γίνουν οι μεταδόσεις προς τις συσκευές πελατών που υπάρχουν στο δίκτυο, όσο και τότε θα μεταδώσουν αυτές προς τον σταθμό βάσης.

Το επόμενο βήμα είναι οι αποστολές των δεδομένων από το σταθμό βάσης προς τις συσκευές των πελατών, που γίνονται με την μορφή ριπών (*bursts*). Κάθε ριπή είναι μια 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 ^[13].

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 την μεριά των συσκευών των πελατών για κάποια από τις ροές δεδομένων⁹ τους με το σταθμό βάσης. Ο σταθμός βάσης λαμβάνοντας υπόψη τις αιτήσεις για αύξηση του εύρους ζώνης σε διάφορες συνδέσεις,

⁹ Οι ροές δεδομένων είναι συνδέσεις με κάποια χαρακτηριστικά, όπως ταχύτητα μετάδοσης δεδομένων, κατεύθυνση, που ορίζονται από το σταθμό βάσης και τις συσκευές των πελατών για την ανταλλαγή των δεδομένων μεταξύ τους.

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 θα μετατοπίσει 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, θα πράξει ανάλογα. Για λόγους μεγαλύτερης ευελιξίας, στο επίπεδο πρόσβασης στο μέσο οι σταθμοί βάσης έχουν την δυνατότητα να υποστηρίξουν συσκευές πελατών που λειτουργούν σε ένα ή περισσότερα κανάλια^{[13][41]}.

1.3.5.2.2 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 σε άλλα κανάλια.

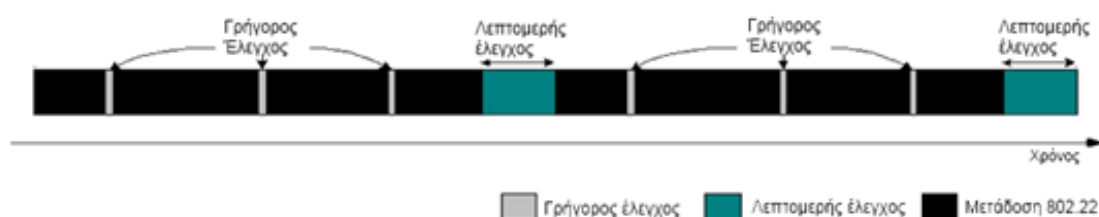
Η διαδικασία αυτή του ελέγχου γίνεται σε δυο φάσεις, κατά τις οποίες διακόπτονται τόσο οι μεταδόσεις του σταθμού βάσης προς τις συσκευές και αντίστροφα:

- *Γρήγορος έλεγχος (fast – sensing)*: Ο γρήγορος έλεγχος γίνεται σε μια 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 κατώφλι¹⁰ (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

¹⁰ Ενδεικτικά παρατίθεται πως το κατώφλι που έχει οριστεί για τον εντοπισμό των ψηφιακών τηλεοπτικών σημάτων είναι -116dBm

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 την 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 καμιά 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*¹¹) που είναι 15.75 kHz στις Ηνωμένες Πολιτείες και 15.625 kHz στην Ευρώπη [18].

Στην Εικόνα 10 φαίνονται οι φάσεις αυτές που περιγράφηκαν παραπάνω σε σχέση με τις μεταδόσεις του πρωτοκόλλου^[9].



Εικόνα 10: Τα δυο 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 δυο 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 την διάρκεια κάποιας περιόδου σιγής προς το σταθμό βάσης, ο οποίος θα πρέπει με την σειρά του να στέλνει και το ανάλογο πακέτο για να επιβεβαιώσει τη λήψη αυτού του πακέτου.

Παρόλα αυτά, επισημαίνεται ότι μεμονωμένη χρήση των δυο αυτών λύσεων δεν είναι τόσο αποτελεσματική. Ο συνδυασμός αυτών των δυο λύσεων θεωρείται προτιμότερος^[14].

¹¹ *Horizontal line – scan rate*: ο ρυθμός με τον οποίο η τηλεοπτική εικόνα ανανεώνεται από τα αριστερά προς τα δεξιά και ξανά προς τα αριστερά. Αντιστοιχεί στον αριθμό των οριζόντιων γραμμών που απεικονίζονται σε ένα δευτερόλεπτο.

1.3.5.2.3 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 δυο είδη:

Σελίδα | - 17 -

- 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 [17].

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 **συνύπαρξη** τους, είτε κάποια από τις δυο (ή περισσότερες) να **αλλάζουν κανάλι λειτουργίας**. Η συμπεριφορά αυτή είναι μείζονος σημασίας για την 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 δεν 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 και έτσι τα συστήματα να καταστούν άχρηστα. Αυτό οφείλεται και στην ευκαιριακή χρήση του φάσματος από αυτά τα συστήματα.

1.3.5.2.4 Συγχρονισμός μεταξύ των κυψελών

Ένας τρόπος έτσι ώστε να γίνει πιο εύκολος ο εντοπισμός πρωτευόντων χρηστών του δικτύου είναι ο συγχρονισμός των δυο φάσεων ελέγχου για πρωτεύοντες χρήστες, της γρήγορης αλλά και της λεπτομερούς φάσης, μεταξύ γειτονικών σταθμών βάσης. Με τον 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.

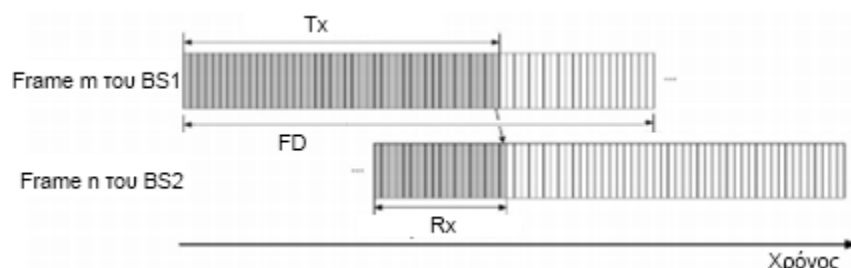
Ας υποθεθεί ότι υπάρχουν δυο επικαλυπτόμενες κυψέλες στις οποίες βρίσκονται δυο σταθμοί βάσης, ο BS_1 και BS_2 , που επιθυμούν να συγχρονίσουν τις μεταδόσεις τους. Ο συγχρονισμός μεταξύ τους θα επιτευχθεί με τη χρήση ειδικών πακέτων – *φάρων* (*inter – cell beacons*). Όταν το BS_1 αποστέλλει ένα beacon πακέτο, καταγράφει σε αυτό και το χρόνο που έχει μεσολαβήσει από την αρχή του frame μέχρι και τη στιγμή που άρχισε την μετάδοση του beacon, έστω T_x (γνωστό και ως *transmission offset*). Το BS_2 , αφού λάβει το beacon από το BS_1 , υπολογίζει το χρόνο που μεσολάβησε από την αρχή του δικού του frame μέχρι και τη στιγμή λήψης του πακέτου, έστω R_x (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 $(FD - T_X + R_X) \leq \left\lceil \frac{FD}{2} \right\rceil$, 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, T_x, R_x με την εφαρμογή του προαναφερθέντος κανόνα.

Σελίδα | - 18 -



Εικόνα 11: Συγχρονισμός επικαλυπτόμενων κυψελών

1.3.5.2.5 Δυναμικός διαμοιρασμός πόρων μεταξύ κυψελών

Υπάρχει τρόπος να διαμοιραστούν το/-α κανάλι/-α λειτουργίας των κυψελών. Γνώμονας για αυτό το διαμοιρασμό των καναλιών αποτελεί η εξασφάλιση της ποιότητας των υπηρεσιών που προσφέρουν οι κυψέλες. Για αυτό το λόγο στο 802.22 ορίζονται δυο 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 *λόγος 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 δυο 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, η βιβλιογραφία περιλαμβάνει αρκετές προτεινόμενες μεθόδους. 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 την 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 επιλεγεί τυχαία από το διάστημα $[0, W]$. Με την αποχώρησή του σταθμού βάσης από το κανάλι, εξασφαλίζεται μεγαλύτερος λόγος σήματος προς παρεμβολές τόσο για αυτόν όσο και για τις υπόλοιπες κυψέλες, αυξάνοντας την δυνατότητα προσφοράς υπηρεσιών^[14]. Παρόλο που η συγκεκριμένη μέθοδος θεωρείται αρκετά δημοφιλής, θεωρείται αρκετά επιρρεπής σε επιθέσεις στις οποίες κάποιος κακόβουλο, αναλαμβάνοντας το ρόλο ενός «πειραγμένου» BS, θα μπορούσε να επιλέγει έναν αριθμό (όχι τυχαία), κερδίζοντας συνεχώς τις διεκδικήσεις του χρησιμοποιημένου καναλιού.

1.4 ΠΡΟΟΠΤΙΚΕΣ ΕΦΑΡΜΟΓΗΣ ΤΟΥ 802.22

Ενδιαφέρον παρουσιάζει και η μελέτη ερευνητικής ομάδας σχετικά με τις προοπτικές εφαρμογής του προτύπου 802.22 στην Ιαπωνία^[8]. 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:

Σελίδα | - 19 -

- 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 τη 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 χάρσμα (15%), όσον αφορά την ευρυζωνικότητα μεταξύ των αστικών και των μη αστικών περιοχών^[19].
- 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 ακόμα 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 τη ψηφιακή μετάδοση αντίστοιχα, στην Ιαπωνία έχει υιοθετηθεί το σύστημα ISDB-T¹² για το οποίο δεν έχει υλοποιηθεί κάποιο 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

¹² Terrestrial Integrated Services Digital Broadcasting

αδειοδοτημένων καναλιών, η επέκταση των τεχνικών εντοπισμού¹³, φαντάζει η πιο ευέλικτη λύση.

¹³ Ειδικότερα επισημαίνεται η ανάγκη επέκτασης των τεχνικών εντοπισμού των κυκλοστατικών χαρακτηριστικών ενός σήματος. Συνεπώς, αναμένεται να βελτιωθεί η λειτουργία του fine sensing, λαμβάνοντας υπόψη και άλλους τύπους σημάτων.

Κεφάλαιο 2

Ο ΠΡΟΣΟΜΟΙΩΤΗΣ ΔΙΚΤΥΩΝ NS-2

2.1 ΕΙΣΑΓΩΓΗ

Για την προσομοίωση της λειτουργίας των δικτύων, όπως ορίζει το πρότυπο 802.22, χρησιμοποιείται ο ns-2. Ο ns-2 αναπτύχθηκε από το Πανεπιστήμιο του Berkeley και αποτελεί έναν από τους πιο δημοφιλείς προσομοιωτές δικτύων, παρέχοντας τη δυνατότητα προσομοίωσης διαφόρων τύπων IP δικτύων. Ένα από τα βασικά στοιχεία που τον καθιστούν ευρέως διαδεδομένο στην ερευνητική κοινότητα αποτελεί και η «ανοιχτή» φιλοσοφία που υιοθετεί: είναι ανοιχτού κώδικα, δίνοντας τη δυνατότητα σε οποιονδήποτε χρήστη να αλλάξει τον κώδικα για να υλοποιήσει διάφορες λειτουργίες ή και ακόμα να επεκτείνει τη λειτουργικότητά του, όπως ισχύει και στην παρούσα διπλωματική εργασία. Δεν είναι τυχαίο πως αρκετές ερευνητικές ομάδες έχουν αναπτύξει επιπλέον τμήματα κώδικα (*modules*) με συγκεκριμένες λειτουργίες οι οποίες ενσωματώνονται σε μεταγενέστερες εκδόσεις του ns-2. Ανήκει στην κατηγορία των προσομοιωτών κατευθυνόμενων από τα γεγονότα (*event-driven simulations*¹⁴)^[20].

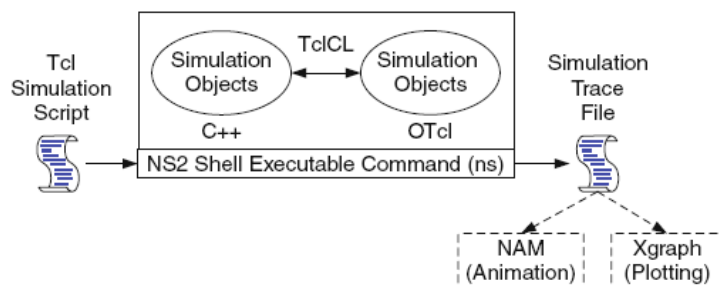
Ανάμεσα στις λειτουργίες του ns-2 περιλαμβάνονται:

- Υλοποίηση πρωτοκόλλων δικτύου, όπως το TCP και το UDP
- Προσομοίωση κυκλοφορίας, όπως FTP, σταθερού ρυθμού δεδομένων, Telnet, κ.α.
- Μηχανισμούς διαχείρισης ουράς (όπως DropTail)

Ο ns-2 έχει υλοποιηθεί σε δυο γλώσσες, τη C++ και την OTcl, μια script γλώσσα που αποτελεί επέκταση της γλώσσας tcl προσδίδοντάς της αντικειμενοστρέφεια. Με τη C++ ορίζονται οι εσωτερικοί μηχανισμοί της προσομοίωσης, όπως οι λειτουργίες των επιπέδων σε ένα δίκτυο (π.χ. το επίπεδο MAC και το φυσικό επίπεδο, όπως θα αναλυθεί στη συνέχεια). Αντίθετα, η γλώσσα OTcl χρησιμοποιείται για την παραμετροποίηση και την εκτέλεση του σεναρίου προσομοίωσης, ορίζοντας τα χαρακτηριστικά του δικτύου, όπως την τοπολογία του, το πρωτόκολλο δρομολόγησης που θα εφαρμοστεί, κ.α. Η αρχιτεκτονική του ns-2 παριστάνεται στην παρακάτω εικόνα. Όπως διαπιστώνεται, ο προσομοιωτής είναι χωρισμένος σε **δύο τμήματα**: το ένα τμήμα που υλοποιεί τη διασύνδεση με το χρήστη και είναι γραμμένο σε OTcl και το υπόλοιπο που είναι γραμμένο σε C++, χαρίζοντας την απαιτούμενη ταχύτητα. Στην εικόνα παρατηρείται η σύνδεση των μεταφρασμένων αντικειμένων της C++ με τα αντικείμενα OTcl μέσω μιας σύνδεσης OTcl (*OTcl linkage* –

¹⁴ Event-driven simulation: Η προσομοίωση εκτελείται με βάση μια ακολουθία γεγονότων, τα οποία ανανεώνονται κατά τη διαδικασία της προσομοίωσης. Ουσιαστικά, κατά την προσομοίωση, γίνεται μετάβαση από το ένα γεγονός στο άλλο, σε αντίθεση με την άλλη μεγάλη κατηγορία προσομοιωτών δικτύου (time-driven simulation) στην οποία πραγματοποιείται μετάβαση από το ένα χρονικό διάστημα στο άλλο.

απεικονίζεται ως *TclCL* στην εικόνα), η οποία αντιστοιχίζει τις συναρτήσεις και τις μεταβλητές που έχουν οριστεί σε C++ αντικείμενα με στιγμιαίες συναρτήσεις και μεταβλητές ενός αντίστοιχου OTcl αντικειμένου. Με αυτόν τον τρόπο, ο χρήστης μπορεί να αποκτήσει τον έλεγχο των C++ αντικειμένων μέσω της OTcl, χωρίς να είναι υποχρεωμένος να γνωρίζει τις εσωτερικές δομές και τις λειτουργίες τους, όπως αυτές έχουν οριστεί στη C++^[21].



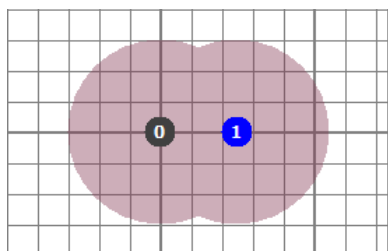
Σελίδα | - 22 -

Εικόνα 12: Η βασική αρχιτεκτονική του ns-2

Για μεγαλύτερη ταχύτητα και ευκολία χρησιμοποιείται η OTcl για την παραμετροποίηση ενός προβλήματος – σεναρίου. Συνεπώς, η περιγραφή της προσομοίωσης γίνεται με την OTcl, με τα αρχεία που είναι γραμμένα σε OTcl να αποτελούν τα Tcl scripts. Αφού έχει δημιουργηθεί το `tcl script`, η **εκκίνηση του ns** γίνεται με την εντολή:

```
ns <tclscript>
```

Αφού ολοκληρωθεί η προσομοίωση, ο ns δημιουργεί αρχεία (trace files) τα οποία παρέχουν τα αποτελέσματα της προσομοίωσης. Τα αποτελέσματα αυτά μπορούν να τεθούν και ως είσοδο σε άλλα εργαλεία για τη γραφική παράστασή τους, όπως το NAM και το XGraph. Για τις ανάγκες της διπλωματικής εργασίας χρησιμοποιείται εκτενώς το NAM (*Network AniMator*). Το NAM παρέχει τη δυνατότητα γραφικής αναπαράστασης πληροφοριών, όπως το throughput, αλλά και της τοπολογίας ενός δικτύου και της ανταλλαγής των μηνυμάτων μεταξύ των κόμβων του δικτύου, ανάλογα με το επίπεδο στο οποίο ανήκουν (π.χ. MAC, δρομολόγησης)^{[21][22][23][24]}. Πέρα από το NAM, έχουν αναπτυχθεί αρκετά εργαλεία από διάφορες ερευνητικές ομάδες. Για την οπτική αναπαράσταση των προσομοιώσεων που πραγματοποιούνται, στην παρούσα εργασία θα χρησιμοποιηθεί επιπλέον και το εργαλείο EXAMS^[25], που είναι ειδικά σχεδιασμένο για αναπαράσταση ασύρματων δικτύων. Η παραπάνω λειτουργία του ns μπορεί να γίνει περισσότερο κατανοητή με ένα **παράδειγμα**. Έστω δυο ασύρματοι κόμβοι οι οποίοι επικοινωνούν μεταξύ τους όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 13: Αναπαράσταση δυο ασύρματων κόμβων, όπως αυτή παρουσιάζεται από το εργαλείο προσομοίωσης EXAMS. Οι κόκκινοι κύκλοι αντιστοιχούν στην εμβέλεια κάθε κόμβου

Οι κόμβοι αυτοί δηλώνονται στο `tcl script` όπως παρακάτω:

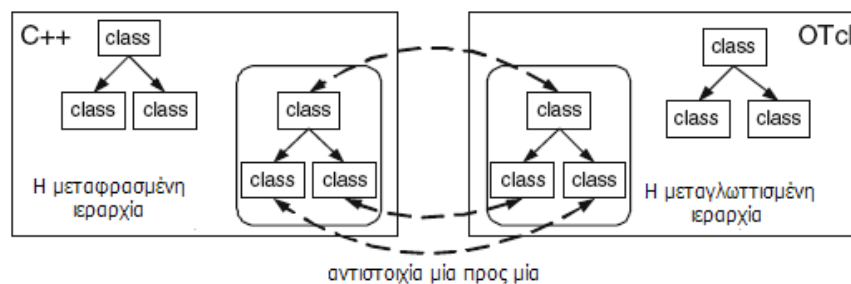
```
set ns [new Simulator]
set node_ (0) [$ns node]
set node_ (1) [$ns node]
```

Αυτομάτως, τα αντικείμενα τύπου `Node` που δημιουργούνται σε OTcl συνδέονται με τα αντίστοιχα μεταφρασμένα (*compiled*) αντικείμενα τύπου `MobileNode` που έχουν υλοποιηθεί σε C++, όπως φαίνεται στο παρακάτω τμήμα κώδικα:

```
class MobileNode : public Node
{
    friend class PositionHandler;
public:
    MobileNode();
    .....
    .....
}
```

Σελίδα | 23

Με αυτόν τον τρόπο ο χρήστης αποκτά πρόσβαση στα αντίστοιχα αντικείμενα της C++ ^[24].



Εικόνα 14: Αντιστοίχιση μεταξύ κλάσεων της C++ και της OTcl

2.2 ΕΓΚΑΤΑΣΤΑΣΗ ΤΟΥ NS-2

Η έκδοση του ns που έχει χρησιμοποιηθεί είναι η 2.29. Παρόλο που η έκδοση αυτή δεν είναι η πιο πρόσφατη, εξασφαλίζει ωστόσο συμβατότητα με ένα από τα επιπλέον modules που θα προστεθούν για τις ανάγκες της διπλωματικής. Η συγκεκριμένη έκδοση έχει εγκατασταθεί και λειτουργεί κανονικά, τόσο σε περιβάλλον Linux, όσο και σε Cygwin ¹⁵.

2.3 ΤΟ ΜΟΝΤΕΛΟ ΤΗΣ ΑΣΥΡΜΑΤΗΣ ΔΙΚΤΥΩΣΗΣ ΣΤΟΝ NS-2

Σε αυτή την παράγραφο θα αναλυθεί το μοντέλο που αφορά τα ασύρματα δίκτυα και το οποίο έχει ενσωματωθεί στον ns-2. Πάνω σε αυτό το μοντέλο θα πραγματοποιηθούν οι απαιτούμενες επεκτάσεις για την υλοποίηση του 802.22. Βασικό στοιχείο του μοντέλου είναι ο ασύρματος κόμβος που αποτελεί αντικείμενο της κλάσης `MobileNode`. Μια μελέτη της ιεραρχίας των κλάσεων στον ns δείχνει πως η κλάση `MobileNode` κληρονομεί τις ιδιότητες της `Node` (του κοινού κόμβου που χρησιμοποιείται στα ενσύρματα δίκτυα). Ωστόσο, λόγω της φύσης της χρήσης ενός κινητού κόμβου, υπάρχουν σημαντικές διαφορές, όπως η δυνατότητα κίνησης του, η δυνατότητα εκπομπής και λήψης σημάτων από και προς ένα ασύρματο κανάλι, αλλά και η απουσία ενός σημαντικού στοιχείου, του `Link`, το οποίο χρησιμοποιείται στα ενσύρματα δίκτυα για τη σύνδεση των κόμβων μεταξύ τους.

Πριν όμως αναλυθούν τα βασικά συστατικά ενός κινητού κόμβου, θεωρείται σκόπιμο να προηγηθεί μια αναφορά στον προγραμματισμό γεγονότων (*event scheduling*) του ns.

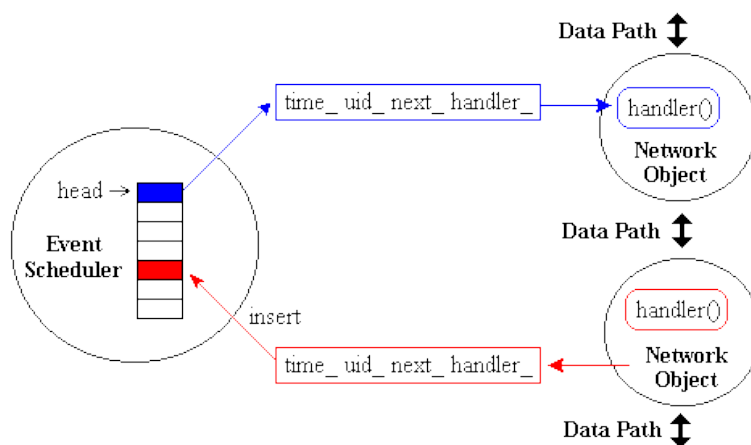
¹⁵ Περιβάλλον προσομοίωσης του UNIX/Linux σε Windows

2.3.1 Προγραμματισμός γεγονότων

Ο προγραμματισμός γεγονότων χρησιμοποιείται κυρίως για την προσομοίωση της μετάδοσης ενός πακέτου (εισάγοντας και την καθυστέρηση), αλλά και για τη χρήση χρονομετρητών (*timers*). Κάθε γεγονός αποτελεί ένα αντικείμενο της κλάσης `Event`. Όπως γίνεται και με τα πραγματικά δίκτυα, έτσι και στον ns-2, τα γεγονότα αποθηκεύονται σε μια ουρά και ταξινομούνται με βάση το χρόνο εκτέλεσής τους¹⁶.

Σελίδα | - 24 -

Ο δρομολογητής γεγονότων δρομολογεί κάθε γεγονός ξεχωριστά, όπως φαίνεται και στην παρακάτω εικόνα. Το γεγονός που βρίσκεται στην κορυφή της ουράς (*head*) δρομολογείται με αποτέλεσμα να εκτελείται ο χειριστή γεγονότος (*handler*) του αντίστοιχου αντικειμένου (*Network Object*) η οποία δείχνει στη συνάρτηση που πρέπει να κληθεί. Τα δεδομένα μεταφέρονται από το ένα αντικείμενο στο άλλο, όπου μπορεί να προστεθεί ένα άλλο γεγονός από κάποιο άλλο αντικείμενο.



Εικόνα 15: Παράδειγμα ενός δρομολογητή γεγονότων

Αφού τα πακέτα είναι και αυτά γεγονότα, όπως αναφέρθηκε, κάθε πακέτο είναι αντικείμενο της κλάσης `Packet` που κληρονομεί με τη σειρά της την `Event`. Έτσι, αν ο κινητός κόμβος A επιθυμεί να στείλει ένα πακέτο, τότε καλεί τη συνάρτηση `send`. Αντίστοιχα, ο B καλεί τη `recv` στην οποία δείχνει η `handle`, αφότου δρομολογηθεί η αποστολή του πακέτου, ύστερα από χρόνο ίσο με τη διάρκεια της αποστολής του πακέτου (`tx_time`).

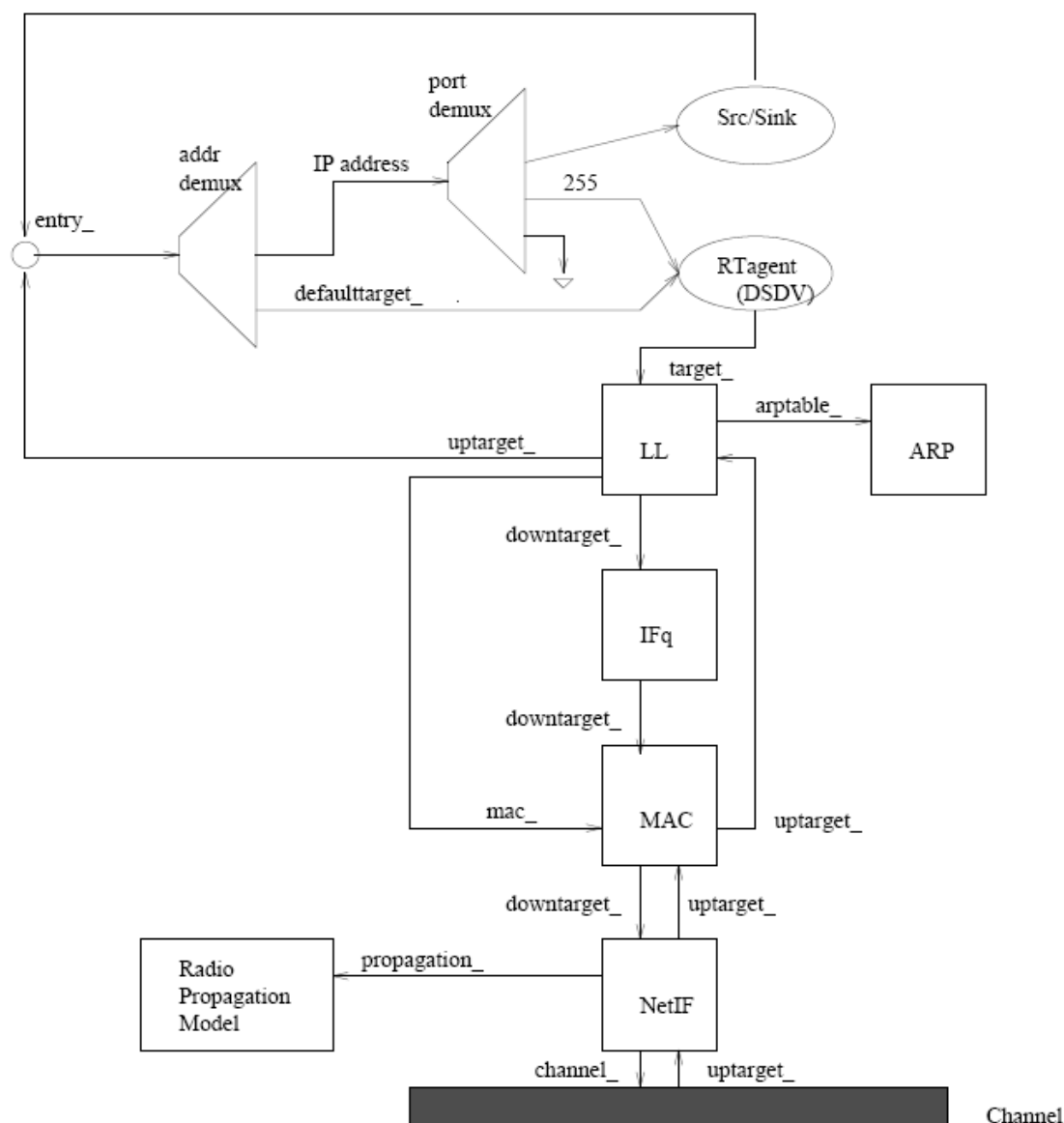
```
A::send (Packet* p) {target_>recv(p)} //target_ is B; call B::recv
B::recv(Packet*, Handler* h = 0) {
    ..
    Scheduler::instance().schedule(target_, p, tx_time)
    //target_ is B;    schedule the packet at the
    // time of (current_time + tx_time)
    ..
}
```

2.3.2 Βασικά συστατικά ενός κινητού κόμβου

Ένας κινητός κόμβος είναι στην ουσία μια στοίβα η οποία περιέχει τα συστατικά που φαίνονται στο παρακάτω σχήμα. Τα συστατικά αυτά είναι το κανάλι (*Channel*), η διεπαφή του δικτύου (*Network Interface*), το μοντέλο διάδοσης του σήματος (*Radio Propagation*)

¹⁶ Υπάρχει ειδικό πεδίο `time_` που αποθηκεύει το χρόνο δρομολόγησης του γεγονότος

Model), τα MAC πρωτόκολλα (MAC protocols), η ουρά (Interface Queue), το επίπεδο σύνδεσης (Link Layer) και το πρωτόκολλο επίλυσης διευθύνσεων (Address Resolution Protocol). Στη συνέχεια, αναπτύσσεται συνοπτικά η λειτουργία κάθε συστατικού.



Εικόνα 16: Δομή ενός κινητού κόμβου – mobile node

2.3.2.1 Channel

Ο ορισμός της κλάσης `Channel` βρίσκεται στο αρχείο `channel.cc`. Ο ρόλος του `Channel` είναι η παράδοση όλων των πακέτων που στέλνονται από έναν κινητό κόμβο σε όλους τους γειτονικούς κόμβους που βρίσκονται εντός της εμβέλειας λειτουργίας του. Για αυτό το λόγο έχει τεθεί ένα ειδικό πεδίο στα πακέτα, το `txinfo` που περιέχει πληροφορίες που αφορούν το πακέτο, προκειμένου να διαπιστώσει ο παραλήπτης αν λαμβάνει σωστά το πακέτο. Η εισαγωγή των πληροφοριών γίνεται με την παρακάτω δήλωση κώδικα:

```
p->txinfo_.stamp((MobileNode *)node(), ant->copy(), Pt_, lambda_),
όπου
```

- `node()`: δείχνει στον κόμβο – αποστολέα

- `ant->copy()`: παράμετροι που αφορούν την κεραία
- `Pt_`: η ισχύς εκπομπής
- `lambda_`: το μήκος κύματος

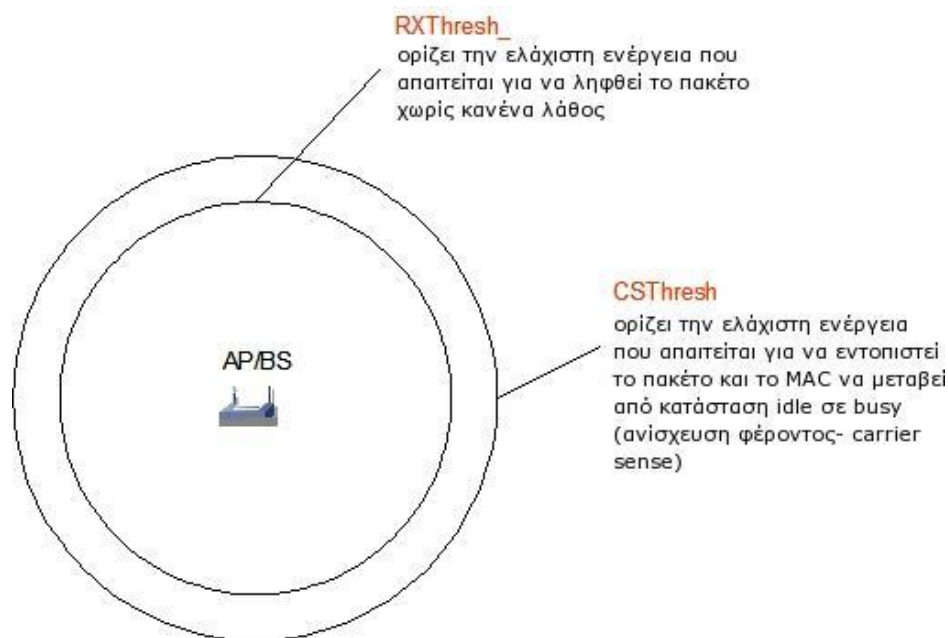
Βάσει των παραπάνω πληροφοριών, ο κόμβος – παραλήπτης υπολογίζει τη λαμβανόμενη ισχύ.

Σελίδα | - 26 -

Ο υπολογισμός του εύρους λειτουργίας του αποστολέα γίνεται με τη συνάρτηση `getDist`, λαμβάνοντας υπόψη το μήκος κύματος, την ισχύ εκπομπής, το κατώφλι εντοπισμού (*Carrier Sense Threshold*), το ύψος της κεραίας, κ.α. Το εύρος αποθηκεύεται στη μεταβλητή `distCST_`. Από την κλάση `Channel` προέρχεται η `WirelessChannel`, που προσομοιώνει τη λειτουργία του ασύρματου καναλιού.

2.3.2.2 NetIF

Το τμήμα `NetIF` (*Network Interface*) προσομοιώνει τη λειτουργία του υλικού (*hardware*) που χρησιμοποιείται από έναν κόμβο για να αποκτήσει πρόσβαση στο κανάλι. Υλοποιεί ουσιαστικά το φυσικό επίπεδο. Το τμήμα αυτό υλοποιείται με την κλάση `WirelessPhy` (αρχεία `phy.cc` και `wireless_phy.cc`). Κάθε κόμβος – παραλήπτης λαμβάνει τα πακέτα που μεταδίδονται από τα `network interfaces` των κόμβων – αποστολέων στο κανάλι. Όπως φαίνεται και στη δομή του `mobile node`, η αποστολή ενός πακέτου από αυτό το τμήμα γίνεται καλώντας τη συνάρτηση `recv` του αμέσως επόμενου επιπέδου, δηλαδή του `channel` (`channel_->recv(p, this)`). Αντίθετα, η λήψη έχει πιο σύνθετη λειτουργία. Όπως και με το `Channel`, έτσι και σε αυτό το τμήμα, το πακέτο περιέχει πληροφορίες οι οποίες χρησιμοποιούνται από το `network interface` του παραλήπτη για να διαπιστώσει αν το πακέτο έχει την ελάχιστη ενέργεια για να ανιχνευθεί (`CSThreshold_`) ή την ελάχιστη ενέργεια για να ληφθεί κανονικά (`RXThresh_`)^[31].



Εικόνα 17: Ορισμοί του `RXThreshold` και του `CSThreshold`

Όπως φαίνεται και στην παραπάνω εικόνα, η ενέργεια του πακέτου που λαμβάνεται¹⁷ είναι μικρότερη από το `CSThresh_`, τότε δεν ανιχνεύεται από τον κόμβο παραλήπτη. Αν η ενέργεια του όμως ξεπερνά την ελάχιστη δυνατή για τη λήψη του πακέτου, τότε το πακέτο λαμβάνεται κανονικά χωρίς λάθη. Αντίθετα, αν για την ενέργεια `Pr` ισχύει $\text{CSThresh_} \leq \text{Pr} < \text{RxThresh_}$, τότε το πακέτο μπορεί να εντοπιστεί, αλλά η ενέργειά του δεν είναι αρκετή για να ληφθεί κανονικά. Οι παραπάνω συνθήκες αποτελούν κομμάτι της συνάρτησης `recv` της κλάσης `WirelessPhy`.

2.3.2.3 Επίπεδο MAC

Προσομοιώνει το MAC επίπεδο του μοντέλου OSI. Σε αυτό το επίπεδο θα υλοποιηθεί και το μεγαλύτερο τμήμα της λειτουργίας του 802.22. Ανάλογα με τον τύπο του φυσικού επιπέδου, το επίπεδο MAC θα πρέπει να ενσωματώνει ένα σύνολο λειτουργιών, όπως έλεγχος συγκρούσεων (*collision*), ακρόαση φέροντος (*carrier sense*), κ.α. Για την αποστολή το MAC θα πρέπει να έχει ακολουθήσει προηγουμένως ένα συγκεκριμένο πρωτόκολλο πρόσβασης στο μέσο, ενώ για τη λήψη το πακέτο μεταφέρεται στο `link layer` επίπεδο.

2.3.2.4 Επίπεδο Link Layer

Το επίπεδο αυτό ενσωματώνει αρκετές λειτουργίες, όπως η δημιουργία ουράς. Το `Link Layer` στον `ns` διαχωρίζεται σε δυο τμήματα: το `Queue` και το `LL`. Το `Queue` διαχειρίζεται την ουρά με τον πιο συνηθισμένο τύπο ουράς να είναι ο `PriQueue`, στον οποίο δίνεται προτεραιότητα σε πακέτο πρωτοκόλλου δρομολόγησης. Το `LL` υλοποιεί κάποιο συγκεκριμένο πρωτόκολλο μεταγωγής δεδομένων (*data link*), όπως το `ARQ`.

2.3.2.5 Μοντέλο Διάδοσης Σήματος

Στον `ns-2` υλοποιούνται αρκετά μοντέλα διάδοσης (*propagation model*), όπως το μοντέλο ελεύθερης διάδοσης στο χώρο (*Free Space*) και το μοντέλο διάδοσης εδάφους δυο ακτινών (*Two – Ray Ground*). Το `Free Space` μοντέλο χρησιμοποιείται για να προσομοιώσει την εξασθένιση του σήματος όταν υπάρχει οπτική επαφή (*line-of-sight*) μεταξύ του αποστολέα και του παραλήπτη, ενώ το `Two Ray Ground` προσομοιώνει επιπρόσθετα και τις ανακλάσεις από το έδαφος. Στην παρούσα εργασία θα χρησιμοποιηθεί το `Two – Ray Ground` μοντέλο [26][27][28][29][30].

Με βάση τις παραπάνω περιγραφές, στις προσομοιώσεις που πραγματοποιούνται ο κινητός κόμβος παραμετροποιείται όπως παρακάτω:

¹⁷ Υπολογίζεται με την εντολή `Pr = propagation_->Pr(&p->txinfo_, &s, this)`

```

set val(chan) Channel/WirelessChannel ;# channel type
set val(netif) Phy/WirelessPhy ;# network interface type
set val(mac) Mac/802_22 ;# MAC type
set val(ifq) Queue/DropTail/PriQueue ;# interface queue type
set val(ifqlen) 50 ;# max packet in ifq
set val(ll) LL ;# link layer type
set val(ant) Antenna/OmniAntenna ;# antenna model
set val(rp) AODV ;# routing protocol

```

Σελίδα | - 28 -

```

set ns [new Simulator]
set chan0 [new $val(chan)]

```

```

$ns node-config -adhocRouting $val(rp) \
                -llType $val(ll) \
                -macType $val(mac) \
                -ifqType $val(ifq) \
                -ifqLen $val(ifqlen) \
                -antType $val(ant) \
                -propType $val(prop) \
                -phyType $val(netif) \
                -channel $chan0 \
                -topoInstance $topo \

```

2.3.3 Περιγραφή της τοπογραφίας μιας προσομοίωσης

Πολύ σημαντικό για την προσομοίωση είναι η τοπογραφία, δηλαδή η προσομοίωση του χώρου στον οποίο είναι διεσπαρμένοι οι κόμβοι ενός δικτύου. Για τις ανάγκες των προσομοιώσεων που έγιναν, θεωρήθηκε ότι όλοι οι κόμβοι του δικτύου είναι διεσπαρμένοι σε έναν επίπεδο χώρο (*flat grid*), απουσία εμποδίων. Ο ορισμός αυτής της τοπογραφίας, που προϋπήρχε στον ns-2 και απλά χρησιμοποιήθηκε, έγινε με την χρήση της παρακάτω δήλωσης στο αρχείο tcl. Λεπτομέρειες που αφορούν την θέση των κόμβων στο χώρο θα δοθούν αργότερα στην περιγραφή των σεναρίων.

Το σύνολο των δηλώσεων που χρειάζονται για τον ορισμό της τοπογραφίας στο αρχείο tcl

```

set val(x) 25000; ;# X dimension of topography
set val(y) 25000; ;# Y dimension of topography
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)

```

Στο παραπάνω παράδειγμα ορίζεται ένας τετράγωνος επίπεδος χώρος πλευράς 25 χιλιομέτρων.

2.3.4 Ορισμός του αντικειμένου GOD

Θα πρέπει να σημειωθεί ότι η χρήση ασύρματης επικοινωνίας σε ένα δίκτυο στην προσομοίωση απαιτεί τον ορισμό ενός αντικειμένου, τύπου GOD (*General Operations Director*). Για να οριστεί αυτού το είδος το αντικείμενο παίρνει σαν όρισμα τον αριθμό των κόμβων που υπάρχουν στο δίκτυο ενώ χρησιμοποιείται για την αποθήκευση πληροφοριών σχετικά με την συνδεσιμότητα στην τοπολογία. Ο ορισμός του φαίνεται παρακάτω.

Ορισμός του αντικειμένου GOD

```

set val(nn) 3 ;# number of nodes in the simulation
create-god $val(nn)

```

2.3.5 Καταγραφή των στοιχείων της προσομοίωσης σε αρχεία

Πολύ χρήσιμο για την διαπίστωση της σωστής λειτουργίας και την γενικότερης συμπεριφοράς των κόμβων κατά την προσομοίωση παίζει η δυνατότητα που έχει ο ns-2 για να καταγράφει το σύνολο ή επιλεγμένα γεγονότα που συμβαίνουν στο δίκτυο κατά την διάρκεια της προσομοίωσης. Ένα από αυτά τα αρχεία, την δημιουργία των οποίων την κάνει ο ns-2 έπειτα από κάποιες δηλώσεις που θα περιγραφούν παρακάτω, χρησιμοποιείται για την οπτικοποίηση της προσομοίωσης με χρήση του εργαλείου *nam* (*Network Animator*). Αυτή η δυνατότητα ενεργοποιείται έπειτα από τις κατάλληλες δηλώσεις που γίνονται στο αρχείο *tcl*. Αυτό γίνεται σε τρεις φάσεις. Αρχικά θα πρέπει να δηλωθεί το αρχείο που θα χρησιμοποιηθεί για την αποθήκευση των πληροφοριών και με ποια δικαιώματα θα ανοιχθεί αυτό. Στη συνέχεια θα πρέπει να γίνει δήλωση για το ποια γεγονότα θα αποθηκεύονται σε αυτό το αρχείο και τέλος θα πρέπει να κλείσουν αυτά τα αρχεία. Στο τμήμα κώδικα παρακάτω φαίνονται οι 3 φάσεις που προαναφέρθηκαν.

Σελίδα | 29

Καταγραφή δεδομένων σε αρχεία από τον ns-2.

```
set tracefd [open simple.tr w]
set namtrace [open simple.nam w] (α)

$ns trace-all $tracefd
$ns namtrace-all-wireless $namtrace $val(x) $val(y) (β)

$ns at $val(stop) "stop"

proc stop {} {
    global ns tracefd namtrace
    $ns flush-trace
    close $tracefd
    close $namtrace
} (γ)
```

Στο τμήμα (α) του παραπάνω τμήματος κώδικα γίνεται ορισμός των αρχείων που θα χρησιμοποιηθούν, και συγκεκριμένα το *namtrace* θα χρησιμοποιηθεί για χρήση με το εργαλείο *nam*. Στο τμήμα (β) ορίζεται ότι στα αρχεία αυτά θα καταγράφονται όλα τα γεγονότα. Πιο συγκεκριμένα στο αρχείο που θα χρησιμοποιηθεί από το εργαλείο *nam* γίνεται η συγκεκριμένη δήλωση αφού χρησιμοποιείται ασύρματη επικοινωνία. Τέλος στο τμήμα (γ) δηλώνεται ότι όταν τελειώσει η προσομοίωση θα εκτελεστεί η συνάρτηση *stop*. Η δήλωση της συνάρτησης αυτής υποδηλώνει ότι ο ns-2 θα αποθηκεύσει στα αρχεία αυτά όλες τις πληροφορίες που έχει σχετικά με την ανίχνευση των γεγονότων, με χρήση της εντολής *\$ns flush-trace*, και στην συνέχεια τα κλείνει.

Τέλος θα πρέπει να σημειωθεί ότι για να είναι δυνατή η απεικόνιση του κάθε κόμβου στο εργαλείο *nam* θα πρέπει να γίνει και μια επιπλέον δήλωση κατά τον ορισμό του. Αυτή είναι η εξής: “*\$ns initial_node_pos \$node 20*”.

Κεφάλαιο 3

ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΠΤΥΞΗΣ ΤΗΣ ΕΠΕΚΤΑΣΗΣ ΓΙΑ ΤΟ ΠΡΩΤΟΚΟΛΛΟ IEEE 802.22 ΣΤΟΝ NS-2

Ένας από τους στόχους που είχε η διπλωματική εργασία ήταν η ανάπτυξη μιας επέκτασης για τον ns-2 για την υποστήριξη του πρωτοκόλλου IEEE 802.22. Αυτή η επέκταση στην συνέχεια θα ήταν η βάση για να γίνει η αξιολόγηση, σε επίπεδο ασφάλειας, των προτάσεων που έχουν γίνει για μια σειρά λειτουργιών του ενώ θα γινόταν και κάποια επέκταση ή τροποποίηση αυτών των λειτουργιών για την δημιουργία αντιμέτρων για τις ευπάθειες που έχουν εντοπιστεί.

3.1 Η ΕΠΕΚΤΑΣΗ ΤΟΥ IEEE 802.16

Όπως έχει αναφερθεί και προηγουμένως υπάρχουν μεγάλες ομοιότητες μεταξύ του πρωτοκόλλου IEEE 802.16 και του 802.22. Τόσο στο 802.16 όσο και στο 802.22 δύο είναι τα διαφορετικά είδη των οντοτήτων που εντοπίζονται σε ένα δίκτυο, ο σταθμός βάσης και οι συσκευές των πελατών¹⁸, ενώ οι δομές του frame και του superframe παρουσιάζουν μεγάλη ομοιότητα. Επιπλέον χαρακτηριστική είναι και η ομοιότητα στον τρόπο με τον οποίο οργανώνεται η κίνηση στο δίκτυο. Όσον αφορά το τελευταίο και στα δυο αυτά πρωτόκολλα υπάρχουν ίδιες κατηγορίες υπηρεσιών και ίδιος τρόπος οργάνωσης της ροής των δεδομένων μεταξύ σταθμού βάσης και συσκευών πελατών. Γι' αυτό το λόγο και για να μειωθεί ο απαιτούμενος χρόνος ανάπτυξης του module χρησιμοποιήθηκε ένα ήδη υπάρχον για το WiMax^[43], το οποίο τροποποιήθηκε κατάλληλα, κυρίως για να προστεθούν λειτουργίες που δεν υπήρχαν στο 802.16. Σκοπός αυτού του κεφαλαίου είναι η περιγραφή των βασικών δομών του module που χρησιμοποιήθηκαν και κάποιες αλλαγές που έγιναν σε αυτό.

3.1.1 Διαχωρισμός δικτυακών οντοτήτων

Ο διαχωρισμός των δικτυακών οντοτήτων, σταθμός βάσης ή συσκευή πελάτη, είναι πολύ σημαντικός για την προσομοίωση, καθώς θα πρέπει μέσα από τον κώδικα να διαχωριστούν οι λειτουργίες και οι μεταβλητές που θα πρέπει να χρησιμοποιηθούν από αυτές. Συχνά άλλωστε οι οντότητες αυτές κάνουν διαφορετικές ενέργειες λαμβάνοντας το ίδιο σήμα. Αυτό που διαχωρίζει τις οντότητες στο module του 802.16 που χρησιμοποιήθηκε ως βάση και το οποίο θα έπρεπε να τροποποιηθεί, είναι ο αριθμός – διεύθυνση MAC που παίρνει κάθε κόμβος στο δίκτυο. Δεδομένου ότι σε δίκτυα 802.16 δεν είναι συχνό να υπάρχουν περιοχές που να καλύπτονται από περισσότερους από έναν σταθμούς βάσης και χάριν απλούστευσης, στο module του 802.16 υπήρχε μόνο μια τέτοια ορισμένη διεύθυνση. Στο 802.22 όμως είναι συχνό να υπάρχουν επικαλύψεις μεταξύ κυνηλών, λόγω και της μεγάλης ακτίνας αποστολής

¹⁸ Στο 802.16 αναφέρονται ως συσκευές συνδρομητών (*Subscriber Station – SS*)^[40]

μηνυμάτων που έχει το πρωτόκολλο, και γι' αυτό άλλαξε ο τρόπος με τον οποίο γινόταν ο διαχωρισμός αυτός.

Ο δημιουργός πλέον δημιουργεί μια οντότητα 802.22 ενώ αργότερα από τις εντολές που υπάρχουν στο αρχείο tcl συγκεκριμενοποιείται ο τύπος της οντότητας, με κλήση επιπλέον συναρτήσεων που αρχικοποιούν και τις μεταβλητές που χρησιμοποιεί καθεμιά από αυτές. Πλέον ο τρόπος με τον οποίο διαχωρίζονται οι οντότητες μεταξύ τους είναι μια μεταβλητή στην οποία αποθηκεύεται η διεύθυνση του σταθμού βάσης με τον οποίο είναι συσχετισμένη κάποια συσκευή πελάτη. Στην περίπτωση κάθε σταθμού βάσης, σε αυτή την μεταβλητή αυτή αποθηκεύεται η ίδια η διεύθυνση του. Έτσι, **ο διαχωρισμός** γίνεται μέσα από τον έλεγχο αν η διεύθυνση του κάθε κόμβου είναι ίδια με την μεταβλητή αυτή. Ο ορισμός των δικτυακών οντοτήτων τόσο στο αρχείο tcl όσο και στον κώδικα του πρωτοκόλλου φαίνονται παρακάτω.

Σελίδα | 31

Περιγραφή του σταθμού βάσης και της συσκευής πελάτη σε TCL αλλά και οι αντίστοιχες συναρτήσεις που καλούνται στο αρχείο mac-802_22.cc του ns-2

```
set bstation [$ns node]
set bstationMac [$bstation getMac 0]
set AP_ADDR_0 [$bstationMac id]
$bstationMac bss_id $AP_ADDR_0

set node_(1) [$ns node]
$node_(1) base-station $AP_ADDR;
$sstationMac is_SS_0
```

```
Mac802_22::Mac802_22() :Mac()
{
    //Δημιουργός οντότητας
}

int
Mac802_22::command(int argc, const char*const* argv)
{
    if (argc == 3)
    {
        if (strcmp(argv[1], "bss_id") == 0) {
            createBS(atoi(argv[2]));
            return TCL_OK;
        }
    }
    if (argc == 2)
    {
        if (strcmp(argv[1], "is_SS") == 0) {
            createSS();
            return TCL_OK;
        }
    }
}

void
Mac802_22::createBS()
{
    //Συνάρτηση αρχικοποίησης μεταβλητών σταθμού βάσης
}

void
Mac802_22::createCPE()
{
    //Συνάρτηση αρχικοποίησης μεταβλητών συσκευής πελάτη
}
```

Σελίδα | - 32 -

3.1.2 Διατήρηση στοιχείων για τις συσκευές πελατών

Κατά την αρχική συσχέτιση της συσκευής πελάτη με το σταθμό βάσης, διαδικασία απαραίτητη για να μπορεί αυτή να στείλει δεδομένα, ο σταθμός βάσης δημιουργεί μια συνδεδεμένη λίστα με πληροφορίες γι' αυτές με τις οποίες είναι συσχετισμένος. Οι πληροφορίες που κρατά κάθε σταθμός βάσης για κάθε συσκευή πελάτη, σε κάθε κόμβο αυτή της λίστας, είναι η διεύθυνση MAC που έχει αυτή, το εύρος ζώνης που ζητάει για την επικοινωνία με το σταθμό βάσης καθώς και το σχήμα διαμόρφωσης που χρησιμοποιείται σε αυτή. Στο παρακάτω τμήμα κώδικα φαίνεται η δομή `BsCpeInfo`.

Η δομή BsCPEInfo

```

struct BsCPEInfo {
    BsCPEInfo () {next = NULL; BasicCID = -1; PrimaryCID = -1;}
    int MacAddr;
    int BasicCID;
    int PrimaryCID;
    int UplinkBandwidth;
    int DownlinkBandwidth;
    bool PollingStatus;
    ModulCodingType ModulCoding;
    BsCPEInfo *next;
};

```

Σελίδα | 33

Επιπρόσθετα, για να είναι δυνατή η εξεύρεση αυτών των πληροφοριών που υπάρχουν σ' αυτή τη συνδεδεμένη λίστα. Αυτό γίνεται με χρήση της συνάρτησης `BsSearchCpeInfo`.

Η συνάρτηση BsSearchCpeInfo

```

BsCpeInfo* Mac802_22::BsSearchCpeInfo(int MacAddr, int CID)

```

Η συνάρτηση αυτή παίρνει δυο ορίσματα. Η αναζήτηση μπορεί να γίνει με οποιοδήποτε από αυτά τα δυο. Πρώτη προτεραιότητα όμως έχει το αναγνωριστικό σύνδεσης. Αν αυτό έχει κάποια έγκυρη τιμή, μια τιμή δηλαδή διαφορετική από "-1", τότε γίνεται αναζήτηση με βάση αυτό, σε διαφορετική περίπτωση η αναζήτηση γίνεται με χρήση της διεύθυνσης MAC.

3.1.3 Η έννοια της ροής δεδομένων

Η κίνηση των δεδομένων στο δίκτυο που έχει σαν βάση το πρωτόκολλο 802.22 οργανώνεται, όπως και στο 802.16, σε ροές. Υπεύθυνοι για την παραγωγή αυτών των ροών είναι οι agents που αντί να κατατάσσουν κίνηση, όπως για παράδειγμα TCP ή UDP, σε κατηγορίες υπηρεσιών παράγουν απευθείας προσαρμοσμένα πακέτα τα οποία έχουν ήδη καταταχθεί σε κάποια από αυτές του πρωτοκόλλου IEEE 802.22 (UGS, rtPS, nrtPS, ertPS, BE). Όλες οι απαραίτητες δηλώσεις σχετικά με το τύπο της κίνησης που παράγεται στο module υπάρχουν στον υποφάκελο "traffic" του module. Θα πρέπει να σημειωθεί το γεγονός ότι αυτά τα είδη των πακέτων αλλά και όλα τα υπόλοιπα που χρησιμοποιούνται από το IEEE 802.22 έχουν δηλωθεί μαζί με τα υπόλοιπα πακέτα που χρησιμοποιούνται από τον ns-2, στο αρχείο `packet.h` του φακέλου "common" αυτού.

Με βάση τον τύπο των υπηρεσιών καθορίζεται και η ανάλογη προτεραιότητα για τα πακέτα που παράγονται, όπως αυτό φαίνεται στο αρχείο `priority.cc` του φακέλου `traffic` του module. Τα πακέτα rtPS, ertPS και UGS παράγονται μέσα από κλάσεις που υλοποιούν την διεπαφή `TrafficGenerator` του ns-2, ενώ οι υπόλοιπες από κλάσεις που υλοποιούν την διεπαφή `Application`. Οι δηλώσεις τους φαίνονται παρακάτω.

Ο ορισμός των agents που είναι υπεύθυνοι για την κίνηση των δεδομένων στο δίκτυο

```

class rtPS_Traffic : public TrafficGenerator

class ertPS_Traffic : public TrafficGenerator

class UGS_Traffic : public TrafficGenerator

class BEApp : public Application

class nrtPSApp : public Application

```

3.1.3.1 Οντότητες MAC και ροές δεδομένων

Στο module κάθε οντότητα MAC διαθέτει μια συνδεδεμένη λίστα με όλες τις ροές δεδομένων με τις οποίες έχει σχέση, όντως το ένα από τα δυο άκρα της επικοινωνίας. Κάθε στοιχείο αυτής της λίστας περιέχει πληροφορίες που αφορούν τις ροές αυτές όπως το αναγνωριστικό της, την κατεύθυνση της, το αναγνωριστικό της σύνδεσης που δημιουργείται για την καθεμιά από αυτές, την κατάσταση της, καθώς και τις ουρές SDU¹⁹ και PDU²⁰ που δημιουργούνται γι' αυτή την ροή. Ανάλογα με το ποια οντότητα του δικτύου αιτείται την δημιουργία της ροής, υπάρχει και η αντίστοιχη ροή. Ο ορισμός αυτών των δομών, για το σταθμό βάσης και την συσκευή πελάτη αντίστοιχα, φαίνεται παρακάτω.

Σελίδα | - 34 -

Δομές για την ροή των δεδομένων μεταξύ σταθμού βάσης και συσκευών πελατών

```
struct BsServiceFlow {
    BsServiceFlow() {next = NULL; TransportCID = -1;}
    int TransportCID;
    int SFID;
    SfStatus Status;
    PacketQueue SduQueue;
    PacketQueue PduQueue;
    SfDirection Direction;
    BsServiceFlow *next;
};

struct CPEServiceFlow {
    CPEServiceFlow() {next = NULL; TransportCID = -1;}
    int TransportCID;
    int SFID;
    SfStatus Status;
    PacketQueue SduQueue;
    PacketQueue PduQueue;
    CPEServiceFlow *next;
};
```

Για να είναι δυνατή η αποστολή οποιοδήποτε είδους δεδομένων μέσω των ροών μεταξύ του σταθμού βάσης και της συσκευής πελάτη θα πρέπει να έχουν γίνει πρώτα δυο διαδικασίες. Πρώτα θα πρέπει να γίνει η σύνδεση – συσχέτιση της συσκευής πελάτη με το σταθμό βάσης (*ranging*). Αυτή γίνεται με την αποστολή ενός RNG-REQ μηνύματος από την συσκευή πελάτη προς το σταθμό βάσης στο οποίο απαντάει ο σταθμός βάσης με ένα RNG-RSP μήνυμα. Αυτό γίνεται την πρώτη φορά που κάποια συσκευή πελάτη προσπαθήσει να κάνει προγραμματισμό των όποιων μεταδόσεων έχει να κάνει, στην συνάρτηση *CpeScheduler*, η λειτουργία της οποίας θα συζητηθεί στη συνέχεια.

Επιπλέον βασικό για να δημιουργηθεί η ροή των δεδομένων είναι να υπάρξει η αίτηση για την δημιουργία αυτής. Αυτή είναι η DSA-REQ (*Dynamic Service Addition Request*) η οποία στέλνεται τόσο από το σταθμό βάσης όσο και από τη συσκευή πελάτη. Η ακολουθία των πακέτων που στέλνονται διαφέρει ανάλογα με το ποια οντότητα είναι αυτή που εκκινεί την διαδικασία. Έτσι αν αυτή την εκκινεί κάποια συσκευή πελάτη η ακολουθία των μηνυμάτων είναι DSA-REQ – DSA-RXD/DSA-RSP – DSA-ACK, ενώ αν αυτή την εκκινήσει ο σταθμός βάσης είναι DSA-REQ – DSA-RSP – DSA-ACK, καθώς η συσκευή πελάτη δεν αποστέλλει το μήνυμα DSA-RXD. Αντίστοιχες συναρτήσεις για την αποστολή και την λήψη αυτών των μηνυμάτων υπάρχουν στον κώδικα του module. Θα πρέπει να σημειωθεί ότι οι ροές των δεδομένων δημιουργούνται με χρήση της αντίστοιχης συνάρτησης, ανάλογα με το αν είναι

¹⁹ SDU: Service Data Unit

²⁰ PDU: Protocol Data Unit

BSServiceFlow ή CPEServiceFlow, και από την αντίστοιχη οντότητα πριν την αποστολή του μηνύματος DSA-RSP. Αυτό γίνεται με τις συναρτήσεις BsCreateServiceFlow και CpeCreateServiceFlow, ο ορισμός των οποίων φαίνεται παρακάτω.

Ο ορισμός των βοηθητικών συναρτήσεων BsCreateServiceFlow και CpeCreateServiceFlow

BSServiceFlow*

Mac802_22::BsCreateServiceFlow(Packet *p, SfDirection Direction)

Σελίδα | 35

CpeServiceFlow*

Mac802_22::CpeCreateServiceFlow(Packet* p, SfDirection Direction)

Το πακέτο που λαμβάνει ως όρισμα οι συναρτήσεις αυτές, όπως φαίνεται στον ορισμό τους, είναι το DSA-REQ που έχει λάβει η κάθε οντότητα προηγουμένως και χρησιμοποιεί τα στοιχεία που υπάρχουν σε αυτό για να συμπληρωθούν τα απαραίτητα στοιχεία για την ροή των δεδομένων.

Επιπλέον στο module υπάρχουν συναρτήσεις που σχετίζονται με τις ροές δεδομένων και έχουν βοηθητικό χαρακτήρα. Καθώς η αποστολή και η λήψη δεδομένων γίνεται με βάση τις ροές δεδομένων που δημιουργούνται από τις οντότητες MAC, θα πρέπει να τους δίνεται η δυνατότητα να βρίσκουν ποια συγκεκριμένη ροή αφορά τα δεδομένα που λαμβάνουν ή αποστέλλουν²¹. Γι' αυτό το λόγο υπάρχουν οι αντίστοιχες συναρτήσεις με την βοήθεια των οποίων οι σταθμοί βάσης και οι συσκευές πελατών μπορούν να ψάξουν με βάση κάποια κριτήρια τις ροές δεδομένων, για να γίνει σωστή αντιστοίχιση πακέτων δεδομένων – ροών δεδομένων για την σωστή αποστολή και λήψη δεδομένων από τις οντότητες μιας κυψέλης. Οι συναρτήσεις για τις οποίες γίνεται λόγος είναι οι BSSearchServiceFlow και CPESearchServiceFlow, οι οποίες καλούνται στις συναρτήσεις send() και recv() του αρχείου mac-802_22.cc.

Οι συναρτήσεις αυτές επιστρέφουν την ροή δεδομένων που έχει βρεθεί με βάση τα ορίσματα που της έχουν δοθεί. Ανάλογα με το σημείο που κρίνεται απαραίτητη η κλήση των συναρτήσεων συμπληρώνονται και με διαφορετικό τρόπο τα ορίσματα αυτά. Το σύνολο των ορισμάτων που μπορούν να πάρουν αυτές οι συναρτήσεις φαίνονται στον ορισμό τους παρακάτω.

Ο ορισμός των βοηθητικών συναρτήσεων BSSearchServiceFlow και CPESearchServiceFlow

BSServiceFlow*

Mac802_22::BSSearchServiceFlow(int SrcMacAddr, int DstMacAddr, packet_t ptype, SfDirection Direction, int TransactionID, int CID)

CpeServiceFlow*

Mac802_22::CpeSearchServiceFlow(int DstMacAddr, packet_t ptype, SfDirection Direction, int TransactionID, int CID)

Κατά την λήψη δεδομένων η αναζήτηση των ροών και από τις δυο οντότητες γίνεται με βάση το αναγνωριστικό της σύνδεσης (CID), ενώ κατά την αποστολή με βάση τις διευθύνσεις MAC και τον τύπο των πακέτων που αποστέλλονται.

3.1.3.2 Αποστολή δεδομένων

Για την αποστολή των πακέτων στο δίκτυο εμπλέκονται μια σειρά από συναρτήσεις, προσομοιώνοντας με πολύ καλό τρόπο τις αντίστοιχες λειτουργίες του πρωτοκόλλου. Το

²¹ Γενικότερα στο πρωτόκολλο IEEE 802.22 όπως και στο IEEE 802.16 είναι πρωτόκολλα προσανατολισμένα στην σύνδεση.

πρώτο βήμα είναι να δημιουργηθεί μια ροή δεδομένων, είτε από τον σταθμό βάσης είτε από κάποια συσκευή πελάτη, κάτι που γίνεται με τις συναρτήσεις `send/recvdSAREQ`, `send/recvdSARSP`, `send/recvdSAACK` και `send/recvdSARVD`. Το επόμενο βήμα είναι να τοποθετηθούν στην ουρά SDU της κάθε ροής πακέτα, κάτι που γίνεται στην συνάρτηση `send`. Όλα αυτές οι διαδικασίες έχουν αναλυθεί παραπάνω.

Αφού τα πακέτα έχουν τοποθετηθεί στην ουρά SDU της ροής θα πρέπει να γίνει ο απαραίτητος προγραμματισμός για την αποστολή των δεδομένων αυτών. Ο προγραμματισμός αυτός, όπως μπορεί να γίνει αντιληπτό, γίνεται ξεχωριστά για κάθε κόμβο της κυψέλης και ανάλογα με τον τύπο της δικτυακής οντότητας. Γι' αυτό το λόγο υπάρχουν δυο συναρτήσεις, η `BsScheduler` και η `CpeScheduler`. Η πρώτη καλείται μετά την λήξη του `timer`²² που σηματοδοτεί την αρχή του τμήματος του Downlink Subframe μετά το ULMAP. Η λειτουργία της μπορεί να συνοψιστεί ως εξής: Αρχικά υπολογίζει, με βάση την κωδικοποίηση που χρησιμοποιείται για την επικοινωνία μεταξύ σταθμού βάσης και καθεμιάς συσκευής πελάτη, το διαθέσιμο εύρος ζώνης για την μεταξύ τους επικοινωνία. Έπειτα για κάθε συσκευή πελάτη με την οποία σχετίζεται και για κάθε διαφορετική ροή δεδομένων που υπάρχει μεταξύ τους μεταφέρονται δεδομένα από την ουρά SDU προς την ουρά PDU με τη συνάρτηση `BsFragOrPack`, η λειτουργία της οποίας θα περιγραφεί στη συνέχεια, χωρίς όμως να ξεπεραστεί το διαθέσιμο εύρος ζώνης. Το τελευταίο βήμα είναι να γίνει η αποστολή των πακέτων με χρήση της συνάρτησης `BsBurstTransmit` που θα περιγραφεί και αυτή στη συνέχεια.

Σελίδα | - 36 -

Αντίστοιχη είναι και η λειτουργία της `CpeScheduler`. Οι όποιες διαφορές υπάρχουν εστιάζονται στα τρία ακόλουθα σημεία:

1. Όπως είναι λογικό αυτή η συνάρτηση αυτή καλείται σε διαφορετική χρονική στιγμή. Καλείται με το τέλος του Downlink Subframe, που σηματοδοτεί την έναρξη του Uplink Subframe.
2. Στην αρχή της συνάρτησης αυτής γίνεται ένας έλεγχος με τον οποίο ελέγχεται αν η συσκευή πελάτη είναι συσχετισμένη με κάποιο σταθμό βάσης. Αν έχει γίνει η κατάλληλη δήλωση στο αρχείο `tel` και αν δεν έχει γίνει ακόμα στέλνεται το πακέτο ελέγχου για την αίτηση συσχέτισης (`RNG-REQ`) που αναφέρθηκε και παραπάνω.
3. Καλεί τις συναρτήσεις `CpeFragOrPack` και `CpeBurstTransmit` που θα περιγραφούν και αυτές στην συνέχεια.

3.1.3.3 Λειτουργία των συναρτήσεων `BsFragOrPack` και `CpeFragOrPack`

Αφού τα πακέτα πλέον βρίσκονται στην ουρά SDU και έχει προγραμματιστεί η αποστολή τους, κάτι το οποίο περιγράφηκε παραπάνω, θα πρέπει αυτά τα πακέτα να κατανεμηθούν κατάλληλα στην ουρά PDU της κάθε ροής. Για να μουν όμως τα πακέτα στην ουρά αυτή θα πρέπει να έχουν ένα καθορισμένο μέγεθος. Αν έχει μέγεθος πέρα ενός καθορισμένου ορίου θα πρέπει να κατατμηθεί έτσι ώστε να είναι δυνατή η αποστολή του. Αυτή την διαδικασία την πραγματοποιεί για το σταθμό βάσης η συνάρτηση `BsFragOrPack` ενώ για τη συσκευή πελάτη η `CpeFragOrPack`. Η γενική λειτουργία που επιτελούν αυτές οι συναρτήσεις μπορεί να συνοψιστεί ως εξής: Κάθε πακέτο της ουράς SDU βγαίνει από την ουρά και ελέγχεται το μέγεθος του. Αν αυτό είναι μικρότερο από το μέγεθος που απαιτείται για την ουρά PDU τότε αυτό μπαίνει κατευθείαν σ' αυτή. Σε διαφορετική περίπτωση τοποθετείται

²² Αυτή, όπως και όλες οι κλάσεις των `timers` με τα μέλη τους και τις συναρτήσεις τους, ορίζονται στα αρχεία `timers-802_22.h/cc`

ένα μέρος αυτού στην ουρά PDU αφού πριν έχει τοποθετηθεί σε αυτό η κεφαλίδα κατάτμησης, που περιέχει και τον αύξοντα αριθμό κατάτμησης²³, για να μπορεί να γίνει επανασύνθεσή του κατά την λήψη του. Η δήλωση των συναρτήσεων που αναφέρθηκαν σ' αυτή την παράγραφο φαίνεται παρακάτω. Η μόνη διαφορά τους είναι η πρώτη δέχεται ροή δεδομένων BsServiceFlow σαν όρισμα ενώ η άλλη CpeServiceFlow. Το άλλο όρισμα είναι το μέγεθος της ουράς σε bytes.

Σελίδα | 37

Ο ορισμός των συναρτήσεων BsFragOrPack και CpeFragOrPack

```
void Mac802_22::BsFragOrPack(BsServiceFlow *BsSF, int Size)

void Mac802_22::CpeFragOrPack(CpeServiceFlow *BsSF, int Size)
```

3.1.3.4 Λειτουργία των συναρτήσεων BsBurstTransmit και CpeBurstTransmit

Το τελικό στάδιο για την αποστολή κάποιου πακέτου δεδομένων είναι η προώθηση του προς τη διεπαφή φυσικού μέσου, κατά την χρονική στιγμή που ο σταθμός βάσης έχει προγραμματίσει τόσο για τον εαυτό του όσο και για τις συσκευές πελατών με τις οποίες έχει συσχετιστεί, κάτι που αναφέρθηκε και προηγουμένως. Υπεύθυνη γι' αυτή την λειτουργία είναι η συνάρτηση BsBurstTransmit για τον σταθμό βάσης ενώ για η αντίστοιχη για τις συσκευές πελατών είναι η συνάρτηση CpeBurstTransmit.

Η συνάρτηση BsBurstTransmit παίρνει σαν όρισμα μια ροή BsServiceFlow. Αυτή ξεκινώντας από την ροή που παίρνει σαν όρισμα ή την πρώτη του σταθμού βάσης, αν το όρισμα είναι ίσο με null, βγάζει ένα-ένα τα πακέτα που υπάρχουν στην ουρά PDU που δημιούργησε προηγουμένως η συνάρτηση BsFragOrPack. Έπειτα σύμφωνα με τον χάρτη αποστολής πληροφοριών που έχει δημιουργήσει βρίσκει τότε έχει υπολογίσει ότι θα κάνει τις μεταδόσεις προς κάποια συγκεκριμένη συσκευή πελάτη και κάθε πότε θα πρέπει να στέλνει τα πακέτα με δεδομένο το μέγεθος και την διάρκεια κάθε συμβόλου του φυσικού μέσου. Η αποστολή σε τακτά χρονικά διαστήματα γίνεται με την χρήση ενός timer, που ανήκει στην κλάση ResumeBsBurst. Κάθε φορά που ο timer λήγει αποστέλλεται ένα πακέτο, ενώ προγραμματίζεται και η αποστολή του επόμενου, στη συνάρτηση ResumeBsBurstHandler. Όλη αυτή η διαδικασία επαναλαμβάνεται για όλες τις ροές δεδομένων που έχει αποθηκευμένες ο σταθμός βάσης για κάποια συσκευή πελάτη και στην συνέχεια για όλες τις συσκευές πελάτη με τις οποίες είναι συσχετισμένος αυτός.

Η αντίστοιχη λειτουργία για τις συσκευές πελάτη γίνεται από την συνάρτηση CpeBurstTransmit. Η λειτουργία αυτής της συνάρτησης είναι παρόμοια με την αντίστοιχη του σταθμού βάσης. Η μόνη διαφορά τους εντοπίζεται στον υπολογισμό του διαστήματος που μεσολαβεί για την αποστολή των πακέτων. Σ' αυτή την περίπτωση η συσκευή υπολογίζει το μεσοδιάστημα αυτό με βάση τον αριθμό των συμβόλων που έχει στην διάθεσή του. Και σε αυτή την περίπτωση η διαδοχική αποστολή των πακέτων γίνεται με χρήση ενός timer, της κλάσης ResumeCpeBurst αντίστοιχης λειτουργίας με αυτή του σταθμού βάσης.

Θα πρέπει να σημειωθεί στο σημείο αυτό ότι οι διαδικασίες για την αποστολή που περιγράφηκαν παραπάνω δεν αφορούν τα μηνύματα ελέγχου για πρωτόκολλο, αλλά μόνο τις μεταφορές δεδομένων με χρήση αυτού του πρωτοκόλλου. Τα μηνύματα ελέγχου του πρωτοκόλλου αποστέλλονται με χρήση timers στις κατάλληλες χρονικές στιγμές.

²³ Fragmentation Sequence Number - FSN

3.1.3.5 Λήψη δεδομένων

Κατά την λήψη των δεδομένων οι διαδικασίες που ακολουθούνται είναι πιο απλές. Πρωτού γίνει οποιαδήποτε ενέργεια θα πρέπει να ελεγχθεί κάθε πακέτο που λαμβάνεται αν έχει ληφθεί σωστά. Αυτό γίνεται με τον έλεγχο που φαίνεται παρακάτω.

Έλεγχος για ορθή λήψη πακέτου

Σελίδα | - 38 -

```
if( hdr->error() ) {
    Packet::free(p);
    goto done;
}
```

Όπως φαίνεται σ' αυτό το τμήμα κώδικα ελέγχεται το πεδίο της κεφαλίδας ελέγχου που αφορά τα λάθη και το οποίο μπορεί να αλλάξει μόνο από το προηγούμενο επίπεδο, το επίπεδο της διεπαφής με το φυσικό μέσο. Σε περίπτωση που το πεδίο αυτό έχει την τιμή true, πράγμα το οποίο υποδεικνύει ύπαρξη λάθους, τότε σταματάει η επεξεργασία του πακέτου, ενώ η μνήμη που καταλαμβάνει το πακέτο απελευθερώνεται.

Το επόμενο βήμα που πρέπει να γίνει είναι να ελεγχθεί η διεύθυνση προορισμού κάθε πακέτου. Έτσι κάθε κόμβος όταν δέχεται ένα πακέτο ελέγχει αν η διεύθυνση προορισμού είναι η διεύθυνση του ή το μήνυμα απευθύνεται προς όλους τους κόμβους της κυψέλης. Σε διαφορετική περίπτωση η επεξεργασία του πακέτου διακόπτεται και η μνήμη που καταλαμβάνει απελευθερώνεται. Αυτό φαίνεται στο τμήμα κώδικα που φαίνεται παρακάτω.

Έλεγχος διεύθυνσης προορισμού

```
if(dst != (u_int32_t)index_ && dst != MAC_BROADCAST) {
    Packet::free(p);
    goto done;
}
```

Από την στιγμή που το πακέτο περάσει αυτούς τους δυο ελέγχους, αρχίζει η επεξεργασία του. Σε κάθε περίπτωση οι ενέργειες που θα πρέπει να γίνουν καθορίζονται από τον τύπο του πακέτου, που υπάρχει στο πεδίο type της κεφαλίδας του πακέτου. Όταν πρόκειται για κάποιο πακέτο ελέγχου του πρωτοκόλλου όλες οι ενέργειες γίνονται σε αυτό το επίπεδο. Όταν όμως πρόκειται για πακέτο δεδομένων τότε θα πρέπει να η επεξεργασία να συνεχιστεί σε επίπεδα ανώτερα του MAC, έτσι το πακέτο αποστέλλεται στο επόμενο επίπεδο, το επίπεδο δικτύου. Παρακάτω φαίνεται ένα παράδειγμα λήψης πακέτου τύπου UGS.

Αποστολή UGS πακέτου στο επίπεδο δικτύου για περαιτέρω επεξεργασία.

```
if (hdr->ptype() == PT_UGS) {
    if (BsSearchServiceFlow(-1, -1, PT_NTYPE, UL, -1, mac22->generic_hdr.CID)) {
        uptarget_>recv(p, this);
    }
}
```

3.1.4 Συναρτήσεις που καλούνται μόνο από το σταθμό βάσης

Ο σταθμός βάσης σε μια κυψέλη, όπως έχει προαναφερθεί, είναι η οντότητα που καθορίζει όλα τα χαρακτηριστικά της επικοινωνίας. Γι' αυτό το λόγο και ο σταθμός βάσης είναι η οντότητα που στέλνει την πλειοψηφία των μηνυμάτων ελέγχου στο module, με τις συσκευές πελατών να περιορίζουν την συμβολή τους στην σηματοδότηση ελέγχου σε απαντήσεις σε κάποια από αυτά. Ως εκ τούτου ο σταθμός βάσης είναι αυτός που γνωρίζει και τους χρονισμούς της σηματοδότησης. Γι' αυτό το λόγο στο module, προσομοιώνοντας αυτή τη λειτουργία, ο σταθμός βάσης είναι ο μόνος που μπορεί να καλέσει μια σειρά συναρτήσεων:

1. Την συνάρτηση που είναι υπεύθυνη για τον καθορισμό των ορίων του κάθε frame και του timer που χρησιμοποιείται για την κλήση της, καθώς καλείται περιοδικά (FrameTimerHandler και FrameTimer αντίστοιχα).
2. Την συνάρτηση που είναι υπεύθυνη για τον καθορισμό του preamble κάθε frame και του timer που χρησιμοποιείται για την κλήση της (PreambleTimerHandler και PreambleTimer αντίστοιχα). Θα πρέπει να τονιστεί ότι το preamble στο συγκεκριμένο module μοντελοποιείται ως ένα χρονικό διάστημα κατά το οποίο δεν υπάρχει κίνηση σε μια κυσέλη. Αυτός ο τρόπος δεν είναι ο καλύτερος δυνατός, καθώς στην πραγματικότητα είναι μια ακολουθία δεδομένων που σηματοδοτεί την έναρξη του frame. Για λόγους απλούστευσης όμως και μόνο και λόγω του ότι ο ns-2 χρησιμοποιεί timers για τους απαραίτητους χρονισμούς αυτή η λύση κρίνεται ικανοποιητική και δε δημιουργεί προβλήματα στην λειτουργία του module.
3. Την συνάρτηση που προσομοιώνει την όλη διαδικασία της διαχείριση του εύρους ζώνης (BandwidthManagement).

Η FrameTimerHandler, η συνάρτηση που καλείται με την λήξη ενός στιγμιότυπου timer της κλάσης FrameTimer και που ουσιαστικά εκκινεί όλους τους μηχανισμούς για την προσομοίωση του πρωτοκόλλου. Ο timer αυτός ξεκινά στην συνάρτηση createBS που αναφέρθηκε και παραπάνω. Αυτό φαίνεται στο παρακάτω τμήμα κώδικα.

Εκκίνηση του στιγμιότυπου του FrameTimer που ανήκει στο σταθμό βάσης μέσα στην συνάρτηση createBS.

```
void Mac802_22::createBS(int id)
{
    //...
    frameTimer.start(0);
    //...
}
```

Όταν ο χρόνος που ορίζεται στην συνάρτηση start τελειώσει γίνεται κλήση της συνάρτησης FrameTimerHandler. Αυτή αρχικά διαγράφει όλα τα επιμέρους στοιχεία που έχουν καταχωρηθεί στους χάρτες αποστολής και λήψης δεδομένων (ULMAPies και DLMAPies) από την διαδικασία δημιουργίας του χάρτη σε προηγούμενα frame. Αυτό άλλωστε αναμένεται καθώς η κίνηση διαφοροποιείται ανάμεσα στα frames. Τα ULMAPies και τα DLMAPies είναι οργανωμένα σε συνδεδεμένες λίστες, ενώ θα πρέπει να σημειωθεί ότι το πρώτο στοιχείο της λίστας με τα DLMAPies την ξέρει μόνο ο σταθμός βάσης καθώς μόνο αυτός την χρησιμοποιεί ενώ το αντίστοιχο στοιχείο για τα ULMAPies είναι γνωστό τόσο στο σταθμό βάσης όσο και στις συσκευές πελατών. Για να είναι αυτό εφικτό αυτό αποτελεί μέρος μιας δομής δεδομένων που μπορούν να προσπελάσουν τόσο ο σταθμός βάσης όσο και οι συσκευές πελάτη της κυσέλης. Τέλος, μια ακόμα σημαντική λειτουργία που επιτελεί αυτή η συνάρτηση είναι η **εκκίνηση του timer για το preamble του frame**, που ανήκει στην κλάση PreambleTimer. Όλα όσο αναφέρονται σε αυτή την παράγραφο φαίνονται στο τμήμα κώδικα που παρουσιάζεται παρακάτω. Εύκολα παρατηρείται και ο έλεγχος που υπάρχει για να γίνει εκτέλεση του τμήματος κώδικα μόνο από τον εκάστοτε σταθμό βάσης που υπάρχει στην πρώτη γραμμή.

Διαγραφή των DLMAPies και ULMAPies στη συνάρτηση FrameTimerHandler

```
if (NodeID == bss_id_) {
    preambleTimer.start(SymbolLength);

    ULMAPie *ULMAPie_tmp, *ULMAPie_backup;
    DLMAPie *DLMAPie_tmp, *DLMAPie_backup;
    ULMAPie_tmp = actualNetCell->ULMAPie_head;
    while (ULMAPie_tmp) {
        ULMAPie_backup = ULMAPie_tmp->next;
```

```

        delete UMapIe_tmp;
        UMapIe_tmp = UMapIe_backup;
    }

    actualNetCell->UMapIe_head = NULL;
    actualNetCell->UMapIe_tail = NULL;

    DlMapIe_tmp = DlMapIe_head;
    while (DlMapIe_tmp) {
        DlMapIe_backup = DlMapIe_tmp->next;
        delete DlMapIe_tmp;
        DlMapIe_tmp = DlMapIe_backup;
    }

    DlMapIe_head = NULL;
    DlMapIe_tail = NULL;
}

```

Σελίδα | - 40 -

Επιπλέον με την αρχή του κάθε superframe, που στο IEEE 802.22 διαρκεί 16 frames, θα πρέπει να γίνει η ίδια διαδικασία για τα προφίλ αποστολής και λήψης δεδομένων (DownlinkBurstProfiles και UplinkBurstProfiles). Η διαδικασία που ακολουθείται είναι παρόμοια με αυτή που περιγράφεται παραπάνω. Αυτό όμως που θα τονιστεί σ' αυτό το σημείο είναι ο τρόπος με τον οποίο γίνεται η αναγνώριση του πρώτου frame κάθε superframe.

Καθορισμός του πότε θα γίνει η επαναφορά των Downlink/Uplink Burst Profiles

```

#define FRAMES_PER_SUPERFRAME    16
//...
if (NodeID == bss_id_) {
    if (FrameNumber_Counter%FRAMES_PER_SUPERFRAME == 0) {
        //...
    }
}

```

Όπως γίνεται αντιληπτό από τα ονόματα των μεταβλητών, κάθε φορά που αρχίζει ένα frame, η μεταβλητή `FrameNumber_Counter` αυξάνεται, ενώ το μετά το πέρας του πρώτου superframe θα γίνει ορισμός νέων προφίλ αποστολής και λήψης δεδομένων.

Η συνάρτηση που καλείται όταν ξεκινάει το preamble είναι η `PreambleTimerHandler`. Αυτή καθορίζει πότε θα ξεκινήσει το επόμενο frame ενώ εδώ γίνεται και η αύξηση του μετρητή των πακέτων, που αναφέρθηκε στην προηγούμενη παράγραφο.

Η συνάρτηση `PreambleTimerHandler`

```

void Mac802_22::PreambleTimerHandler()
{
    if (NodeID == bss_id_) {
        frameTimer.start(DlSymbolNum*SymbolLength + TtgLength +
            UlsymbolNum*SymbolLength + RtgLength);
        BandwidthManagement();
        FrameNumber_Counter++;
    }
}

```

Μια από τις εργασίες που αναλαμβάνει εξ ολοκλήρου ο σταθμός βάσης είναι η διαχείριση του εύρους ζώνης. Προσομοιώνοντας αυτή την λειτουργία του σταθμού βάσης στο module υπάρχει και η αντίστοιχη συνάρτηση, η `BandwidthManagement`, η κλήση της οποίας γίνεται στο τμήμα κώδικα που παρουσιάστηκε αμέσως προηγούμενα.

Αυτή με δεδομένο τον αριθμό των διαθέσιμων συμβόλων του φυσικού μέσου που υπάρχουν για αποστολή δεδομένων προς τις συσκευές πελατών αλλά και των αντίστοιχων για λήψη από αυτούς, προσπελαίνει όλες τις διαθέσιμες ροές δεδομένων του για να ελέγξει αν κάποια από αυτές, ανάλογα και με το είδος της υπηρεσίας που αυτές παρέχουν, χρειάζεται επιπλέον

εύρος ζώνης. Έπειτα για κάθε συσκευή πελάτη στην οποία πρέπει να στείλει δεδομένα, δημιουργεί μια εγγραφή στο DLMAP για να στείλει σε αυτή κάποια ποσότητα δεδομένων, ανάλογα με το είδος της υπηρεσίας που της παρέχει και αφαιρεί αυτή την ποσότητα από το σύνολο των διαθέσιμων συμβόλων. Η διαδικασία αυτή επαναλαμβάνεται μέχρι να τελειώσουν τα διαθέσιμα σύμβολα.

Αφού γίνει αυτό, θα πρέπει να γίνουν οι ανάλογες ενέργειες για το καθορισμό των μεταδόσεων των συσκευών των πελατών. Έτσι με το πέρας αυτών των διαδικασιών, έχει κατασκευαστεί όλος ο χάρτης αποστολών και λήψεων της κυψέλης και το επόμενο βήμα είναι αυτός να κοινοποιηθεί. Το μέγεθος των δυο χαρτών χρειάζεται επιπλέον και στην αποστολή της κεφαλίδας έλεγχου του frame²⁴. Θα πρέπει επίσης να αποσταλεί και το πακέτο που περιγράφει τα κανάλια που χρησιμοποιούνται για την αποστολή και λήψη των πληροφοριών²⁵. Τέλος εκκινεί και ο timer, η λήξη του οποίου σηματοδοτεί την έναρξη του Downlink Subframe.

Σελίδα | 41

(α) Το τελευταίο τμήμα της συνάρτησης BandwidthManagement, (β) Η συνάρτηση sendULMAP που εκκινεί τον timer την αποστολή του ULMAP, (γ) Η συνάρτηση sendDLMAP που εκκινεί τον timer την αποστολή του DLMAP, (δ),(ε) Οι συναρτήσεις που καλούνται για την αποστολή του DLMAP και ULMAP αντίστοιχα.

```
void Mac802_22::BandwidthManagement () {
    //...
    dl = DLMAPLength();
    ul = ULMAPLength();
    struct hdr_cmh *dlhdr = HDR_CMH(dl);
    struct hdr_cmh *ulhdr = HDR_CMH(ul);
    sendFCH(ulhdr->size(), dlhdr->size());
    DCD_Counter++;
    sendDCD();
    UCD_Counter++;
    sendUCD();
    sendDLMAP(dl);
    sendULMAP(ul);
    dlmapTimer.start(3*SymbolLength);
    return;
} (α)
```

```
void Mac802_22::sendULMAP(Packet *p) {
    UlMapMsg *ulmap = (UlMapMsg*) p->accessdata();
    sendULMAPT.start(2*SymbolLength, p);
    return;
} (β)
```

```
void Mac802_22::sendDLMAP(Packet *p) {
    DlMapMsg *dlmap = (DlMapMsg*) p->accessdata();
    sendDLMAPT.start(SymbolLength, p);
    return;
} (γ)
```

```
void Mac802_22::SendDLMAPTimerHandler(Packet* p) {
    NetworkCell *actualNetCell;
    actualNetCell = findCellByBSID(bss_id_);
    downtarget_>recv(p, this);
    return;
} (δ)
```

```
void Mac802_22::SendULMAPTimerHandler(Packet* p) {
    NetworkCell *actualNetCell;
    actualNetCell = findCellByBSID(bss_id_);
```

²⁴ Frame Control Header - FCH

²⁵ Uplink και Downlink Channel Descriptors – UCD/DCD

```
    downtarget_ ->recv(p, this);  
    return;  
}(ε)
```

Κεφάλαιο 4

Έλεγχος ΤΟΥ ΚΑΝΑΛΙΟΥ ΜΕΤΑΔΟΣΗΣ - ΑΛΛΑΓΗ ΚΑΝΑΛΙΟΥ ΜΕΤΑΔΟΣΗΣ

Στην θεωρητική περιγραφή του πρωτοκόλλου IEEE 802.22, στο πρώτο κεφάλαιο, αναφέρθηκε ότι έχουν προβλεφθεί κάποιες περιόδοι σιγής για τον εντοπισμό των πρωτευόντων χρηστών, αν αυτοί φυσικά υπάρχουν, στο ή στα κανάλια που χρησιμοποιούνται από μια κυψέλη 802.22. Αυτό μπορεί να επεκταθεί για να εντοπιστούν και άλλες κυψέλες που χρησιμοποιούν το ίδιο κανάλι αν δεν υπάρχει δυνατότητα αυτές να συγχρονιστούν. Οι περιόδοι αυτές της σιγής είναι ο **γρήγορος** και ο **λεπτομερής έλεγχος** (*fast* και *fine sensing*). Σ' αυτό το κεφάλαιο θα παρουσιαστεί ο τρόπος με τον οποίο έγινε η προσομοίωση αυτών των περιόδων στον ns-2.

4.1 Η ΠΕΡΙΟΔΟΣ ΓΡΗΓΟΡΟΥ ΕΛΕΓΧΟΥ (FAST SENSING)

Στην περίπτωση του γρήγορου ελέγχου πραγματοποιείται **εντοπισμός ενέργειας** στο κανάλι. Παρόλο που αυτή η περίοδος ελέγχου ενεργοποιείται στο επίπεδο MAC, ο εντοπισμός της ενέργειας γίνεται σε επίπεδα χαμηλότερα του MAC και ειδικότερα στο **επίπεδο της διεπαφής με το φυσικό μέσο**, το οποίο προσομοιώνεται στον ns-2 από την κλάση `WirelessPhy` (αρχεία `wireless-phy.{cc,h}`). Συνεπώς, για την αποτελεσματική προσομοίωση της συγκεκριμένης λειτουργίας απαιτούνται τροποποιήσεις τόσο στην κλάση `WirelessPhy` όσο και στην κλάση `Mac802_22`.

Αρχικά οι δυο φάσεις αυτές του ελέγχου ορίστηκαν σε μια απαριθμητή μεταβλητή (`ScanningPhase`), όπως φαίνεται και στο παρακάτω τμήμα κώδικα του αρχείου `mac-802_22.h`.

Ο ορισμός της απαριθμητής μεταβλητής `scanningPhase` όπως αυτή έχει οριστεί στο αρχείο `mac-802_22.h`

```
enum ScanningPhase {
    IDLE = 0,
    FAST_SENSING = 1,
    FINE_SENSING = 2,
};
```

4.1.1 Η περίοδος γρήγορου ελέγχου στο επίπεδο MAC

Όπως έχει προαναφερθεί, η περίοδος του γρήγορου ελέγχου είναι μια περίοδος που ξεκινάει όταν τελειώνει κάθε **frame**. Γι' αυτό και η κυψέλη εισέρχεται σε αυτή την περίοδο ελέγχου

με εντολή του σταθμού βάσης όταν τελειώσει η περίοδος του frame, με τη χρήση του στιγμιότυπου timer (frameTimer) της κλάσης FrameTimer²⁶ με τον οποίο είναι συσχετισμένος ο σταθμός βάσης. Ειδικότερα, όταν εκπνεύσει η περίοδος που έχει οριστεί στην συνάρτηση start του frametimer, καλείται η συνάρτηση FrameTimerHandler όπου εκκινεί η διαδικασία του fast sensing. Όταν η κυψέλη εισέρχεται σ' αυτή τη φάση ελέγχου ενημερώνονται όλες οι συσκευές πελατών, μέσω μιας δομής, της NetworkCell, που μπορεί να προσπελαστεί τόσο από το σταθμό βάσης όσο και από τις συσκευές πελατών. Η έναρξη αυτής της φάσης ελέγχου πυροδοτείται με τη κλήση ενός άλλου timer του fastSensing, ο οποίος ξεκινά με διάρκεια ίση με αυτή που έχει οριστεί στις προδιαγραφές του προτύπου 802.22 (0.001 sec). Στο παρακάτω τμήμα κώδικα παρουσιάζεται η χρονική στιγμή που τελειώνει το frame, οπότε και εκκινεί η διαδικασία fast sensing. Το δίκτυο αλλάζει κατάσταση, μεταβαίνοντας από την κατάσταση IDLE σε κατάσταση FAST_SENSING, όπως φαίνεται και από την αλλαγή τιμής στη μεταβλητή scanningPhase.

Η εκκίνηση του timer fastSensing στην συνάρτηση FrameTimerHandler. Η κυψέλη εισέρχεται σε φάση γρήγορου ελέγχου.

```
#define FAST_SENSING_DURATION 0.001
//...
void Mac802_22::FrameTimerHandler()
{
    //...
    fastSensing.start(FAST_SENSING_DURATION);
    NetworkCell * actualNetCell;
    actualNetCell = findCellByBSID(bss_id);
    actualNetCell->scanningPhase = FAST_SENSING;
}
```

4.1.2 Η περίοδος γρήγορου ελέγχου στο επίπεδο διεπαφής με το φυσικό μέσο.

Για να ολοκληρωθεί η δυνατότητα πραγματοποίησης fast sensing από ένα 802.22 δίκτυο, απαιτούνται τροποποιήσεις και στη λειτουργία της διεπαφής με το φυσικό μέσο. Γι' αυτό το λόγο στο αρχείο wireless-phy.h έχουν οριστεί δυο επιπλέον μεταβλητές:

- phase: αποθηκεύει την κατάσταση στην οποία βρίσκεται το mac επίπεδο, όπως για παράδειγμα αν βρίσκεται σε κατάσταση γρήγορου ελέγχου (*fast sensing*). Ουσιαστικά, η phase έχει ίδια τιμή με τη scanningPhase του επιπέδου MAC.
- response: χρησιμοποιείται για να δηλώσει αν εντοπίστηκε ενέργεια κατά την διάρκεια του ελέγχου. Η τιμή true αντιστοιχεί σε εντοπισμό ενέργειας κατά τη διάρκεια του fast sensing.

Σε πλήρη αντιστοιχία με τις παραπάνω μεταβλητές, έχουν οριστεί και τρεις συναρτήσεις²⁷ για την επιστροφή των τιμών αυτών των μεταβλητών αλλά και για τον ορισμό συγκεκριμένων τιμών στις μεταβλητές αυτές.

²⁶ Ο ορισμός αυτού του timer όπως και των υπολοίπων timers υπάρχουν στο αρχείο timers-802_22.h/cc

²⁷ setPhase(), rsp() και setResponse()

Οι επιπλέον δηλώσεις μεταβλητών και συναρτήσεων που έγιναν στο αρχείο wireless-phy.h

```
class WirelessPhy : public Phy {
public:
    //...
    inline void setPhase(int value) { phase = value; }
    inline bool rsp() { return response; }
    inline void setResponse(bool val) { response = val; }
    //...
private:
    //...
    int phase;
    bool response;
    //...
};
```

Σελίδα | 45

Η συνάρτηση `sendUp` της `WirelessPhy`, αφού μετρήσει το ποσό της λαμβανόμενης ενέργειας και διαπιστώσει πως ξεπερνά το καθορισμένο κατώφλι, προωθεί το πακέτο στο ανώτερο επίπεδο που είναι το επίπεδο MAC. Συνεπώς, αν το επίπεδο διεπαφής στο φυσικό μέσο είναι ενήμερο πως πραγματοποιείται `fast sensing`, τότε ουσιαστικά εντοπίζεται ενέργεια, κάθε φορά που λαμβάνεται οποιαδήποτε ποσότητα ενέργειας μέσω της κλήσης της συνάρτησης `sendUp()`. Επομένως, κάθε φορά που κάποια συσκευή πελάτη λάβει κατά τη φάση γρήγορου ελέγχου ένα **ποσό ενέργειας που είναι μεγαλύτερο από το κατώφλι εντοπισμού**, τότε εντοπίζεται ενέργεια που θα πρέπει να αναφερθεί στο επίπεδο `mac`, λειτουργία που υλοποιείται στη συνάρτηση `sendUp`, όπως φαίνεται και στον παρακάτω κώδικα:

Έλεγχος για εντοπισμό ενέργειας κατά την διάρκεια της φάσης γρήγορου ελέγχου στο αρχείο `wireless-phy.cc`

```
#define FAST_SENSING 1

int WirelessPhy::sendUp(Packet *p){
    //...
    if(propagation_) {
        s.stamp((MobileNode*)node(), ant_, 0, lambda_);
        Pr = propagation_->Pr(&p->txinfo_, &s, this);
        if (Pr < CStresh_) {
            pkt_recvd = 0;
            goto DONE;
        }
        if(phase == FAST_SENSING){
            if (Pr >= CStresh_){
                response = true;
            }
        }
    }
}
```

Όπως παρατηρείται, όταν εντοπιστεί ενέργεια κατά τη διάρκεια της φάσης γρήγορου εντοπισμού (όταν η `phase` δηλαδή έχει την τιμή `FAST_SENSING`), τότε η `response` αποκτά την τιμή `true`.

4.1.3 Σύνδεση των πληροφοριών των δυο επιπέδων

Με βάση τα προαναφερθέντα, ο μηχανισμός του γρήγορου εντοπισμού υλοποιείται τόσο στο επίπεδο `mac` όσο και στο επίπεδο διεπαφής με το φυσικό μέσο. Η πολυεπίπεδη υλοποίησή του ωστόσο απαιτεί την **επικοινωνία μεταξύ των δυο επιπέδων** και ειδικότερα:

- το επίπεδο phy θα πρέπει να ενημερώνεται συνεχώς από το επίπεδο mac για την κατάσταση στην οποία βρίσκεται και ειδικότερα για τις στιγμές στις οποίες πραγματοποιείται fast sensing
- το επίπεδο mac θα πρέπει να ενημερωθεί από το phy, για τον εντοπισμό ή μη επαρκούς επιπέδου ενέργειας μετά το πέρας του fast sensing

Το fast sensing **πραγματοποιείται μόνο από τις συσκευές πελατών** και όχι από το σταθμό βάσης. Συνεπώς, οι συσκευές πελατών με βάση το περιεχόμενο της scanningPhase, θα πρέπει να ενημερώσουν τη μεταβλητή phase του κατώτερου επιπέδου (phy). Η λειτουργία αυτή μπορεί να επιτευχθεί με τη μέθοδο της δειγματοληψίας, όπου χρησιμοποιείται ένας timer της κλάσης sendTimer που καλείται σε πολύ σύντομα χρονικά διαστήματα (κάθε 0.00001s). Με βάση αυτή την προσέγγιση, κάθε συσκευή πελάτη μπορεί να ενημερωθεί γρήγορα για οποιαδήποτε αλλαγή που πραγματοποιείται στο δίκτυο. Κάθε φορά που αυτός ο timer τερματίζει, καλείται η συνάρτηση SendTimerHandler του αρχείου mac-802_22.cc μέσω της οποίας πραγματοποιείται η αμφίδρομη επικοινωνία μεταξύ των δυο επιπέδων, καθώς το MAC ενημερώνει το επίπεδο της διαπαφής για το στάδιο στο οποίο βρίσκεται ο έλεγχος, αλλά ενημερώνεται κιόλας από αυτό για το αν κατά την διάρκεια του ελέγχου εντοπίστηκε ενέργεια. Η λειτουργία της SendTimerHandler φαίνεται στο παρακάτω τμήμα κώδικα:

Σελίδα | - 46 -

Η συνάρτηση SendTimerHandler που είναι αυτή που τροποποιεί τις μεταβλητές του επιπέδου της διαπαφής με το φυσικό μέσο.

```
void Mac802_22::SendTimerHandler()
{
    if(NodeID != bss_id){
        //...
        if(((WirelessPhy*)netif_)->rsp())
            actualNetCell->fast_response = true;
        if(actualNetCell->scanningPhase == FAST_SENSING){
            ((WirelessPhy*)netif_)->setPhase(FAST_SENSING);
        }
        else if(actualNetCell->scanningPhase == IDLE){
            ((WirelessPhy*)netif_)->setPhase(IDLE);
            ((WirelessPhy*)netif_)->setResponse(false);
        }
        sendTimer.start(PAUSE_CHECK);
    }
}
```

Όπως αποδεικνύεται και από τον παραπάνω κώδικα, η setPhase αρχικοποιεί τη μεταβλητή phase του επιπέδου phy με βάση το περιεχόμενο της scanningPhase. Επιπλέον, η response μέσω της rsp, σε περίπτωση που έχει την τιμή true αρχικοποιεί αντίστοιχα το μέλος fast_response της δομής NetworkCell.

Αφού πραγματοποιηθεί η επικοινωνία μεταξύ των δυο επιπέδων, ο τερματισμός της περιόδου του γρήγορου ελέγχου συνοδεύεται από την κλήση της συνάρτησης FastSensingHandler όπου ο σταθμός βάσης ενημερώνεται για τα αποτελέσματα του ελέγχου, ελέγχοντας το περιεχόμενο της μεταβλητής fast_response. Αν **δεν εντοπιστεί ενέργεια**, τότε η κυψέλη επανέρχεται στην κατάσταση μη ελέγχου (IDLE), συνεχίζοντας κανονικά τη λειτουργία της, χωρίς να προκύπτει η ανάγκη λήψης μέτρων. Σε διαφορετική περίπτωση όμως ενεργοποιείται **η κατάσταση του λεπτομερούς ελέγχου (fine sensing)**.

Η ενεργοποίηση του fine sensing πραγματοποιείται θέτοντας τη μεταβλητή isUsed ίση με true. Η τιμή της isUsed καθορίζει αν στο τέλος κάθε frame θα πραγματοποιηθεί fast ή fine sensing. Σε κάθε περίπτωση όμως γίνεται επαναρχικοποίηση των όποιων τιμών είχαν οι

υπόλοιπες μεταβλητές που χρησιμοποιήθηκαν και στα δυο επίπεδα (MAC, διεπαφή φυσικού μέσου), με τις τιμές που είχαν πριν τον έλεγχο.

Η συνάρτηση `FastSensingHandler` που καθορίζει τι γίνεται μετά το τέλος της περιόδου του γρήγορου ελέγχου.

```
void Mac802_22::FastSensingHandler() {
    //...
    if (actualNetCell->scanningPhase == FAST_SENSING) {
        if (actualNetCell->fast_response) {
            actualNetCell->fast_response=false;
            isUsed = true;
        }
        else{
        }
        actualNetCell->scanningPhase = IDLE;
    }
}
```

Σελίδα | 47

4.2 Η ΠΕΡΙΟΔΟΣ ΛΕΠΤΟΜΕΡΟΥΣ ΕΛΕΓΧΟΥ (FINE SENSING)

Όπως έχει προαναφερθεί, η περίοδος fine sensing διαρκεί περισσότερο από την περίοδο του γρήγορου ελέγχου και ενεργοποιείται από την στιγμή που εντοπιστεί. Ωστόσο υπάρχει και μια ακόμα σημαντική διαφορά, με τον έλεγχο αυτή τη φορά να πραγματοποιείται **αποκλειστικά στο επίπεδο MAC**, καθώς απαιτείται **ανάγνωση της πηγής των πακέτων**, λειτουργία που δεν είναι εφικτή σε κατώτερα επίπεδα. Η κυψέλη μεταβαίνει σε κατάσταση fine sensing (η `scanningPhase` θα έχει την τιμή `FINE_SENSING`) στο επόμενο frame από αυτό που θα εντοπιστεί η ενέργεια. Όπως και στην περίπτωση του fast sensing, έτσι και στο fine sensing, η έναρξη του ελέγχου πραγματοποιείται στο τέλος του frame, με την κλήση της συνάρτησης `FrameTimerHandler`. Η περίοδος fine sensing εκκινεί με τη χρήση ενός timer της κλάσης `FineSensing`, όπως φαίνεται και στον παρακάτω κώδικα:

Η εκκίνηση του timer `fineSensing` στην συνάρτηση `FrameTimerHandler`. Η κυψέλη εισέρχεται σε φάση λεπτομερούς ελέγχου

```
#define FINE_SENSING_DURATION 0.025

void Mac802_22::FrameTimerHandler() {
    if (!isUsed) {
        //...
    }
    else {
        isUsed = false;
        fineSensing.start(FINE_SENSING_DURATION);
        NetworkCell * actualNetCell;
        actualNetCell = findCellByBSID(bss_id_);
        actualNetCell->scanningPhase = FINE_SENSING;
    }
    //...
}
```

Κατά τη διάρκεια του fine sensing (που όπως φαίνεται και στον παραπάνω κώδικα διαρκεί 0.025 sec, διάρκεια που συνάδει με τις προδιαγραφές που έχουν τεθεί κατά την περιγραφή του 802.22), ελέγχεται η πηγή των πακέτων που λαμβάνονται μέσω της συνάρτησης `recv`. Συγκεκριμένα, όλες οι συσκευές πελατών που συμμετέχουν στο fine sensing, ελέγχουν αν το πακέτο που λαμβάνουν **αποστέλλεται από κάποιον άλλο κόμβο πέρα από τον σταθμό βάσης**. Αυτό υλοποιείται προγραμματιστικά, ελέγχοντας αν η πηγή του πακέτου είναι διαφορετική από το σταθμό βάσης με τον οποίο είναι συνδεδεμένη η συσκευή πελάτη. Το αναγνωριστικό του σταθμού βάσης προσπελαύνεται με την κλήση της συνάρτησης

base_stn() της κλάσης MobileNode η οποία επιστρέφει το περιεχόμενο της μεταβλητής base_stn, όπως δηλώνεται στο αρχείο mobilenode.h. Η σύνδεση της συσκευής πελάτη με τον σταθμό βάσης πραγματοποιείται μέσω του tcl αρχείου με την παρακάτω δήλωση:

```
set bstation [$ns node]
...
set bstationMac [$bstation getMac 0]
set AP_ADDR_0 [$bstationMac id]
$bstationMac bss_id $AP_ADDR_0
...
set node_(1) [$ns node]
$node_(1) base-station $AP_ADDR_0 ; #attach mn to basestation
```

Σελίδα | - 48 -

Η κλήση της εντολής base-station πυροδοτεί με τη σειρά της την εκτέλεση της αντίστοιχης συνθήκης της συνάρτησης command της κλάσης MobileNode, όπως φαίνεται στον παρακάτω κώδικα:

Εκτέλεση της αντίστοιχης συνθήκης της συνάρτησης command στο αρχείο mobilenode.cc

```
else if (strcmp(argv[1], "base-station") == 0) {
    base_stn_ = atoi(argv[2]);
    if(base_stn_ == -1)
        return TCL_ERROR;
    return TCL_OK;
}
```

Αν ο αποστολέας του πακέτου είναι διαφορετικός από τον σταθμό βάσης, θεωρείται πως υπάρχει παρεμβολή που προκαλείται από μια οντότητα που δεν ανήκει στο δίκτυο. Με βάση τα προαναφερθέντα, ο έλεγχος κατά τη διάρκεια του fine sensing υλοποιείται όπως παρακάτω:

Υλοποίηση του fine sensing μέσω της συνάρτησης recv

```
void Mac802_22::recv(Packet* p, Handler* h){
    //...
    if(actualNetCell->scanningPhase == FINE_SENSING){
        src = mac->macSA();
        if( src != ((WirelessPhy*)netif_)->wirelessNode()->base_stn()){
            otherNetCell = findCellByBSID(src);
            if(otherNetCell!=NULL){
                actualNetCell->scan_status_.recvd_response=true;
                //...
                goto done;
            }
        }
    }
}
```

Όταν ολοκληρωθεί και αυτή η περίοδος ελέγχου, καλείται η συνάρτηση FineSensingHandler, όπου εκεί ενεργοποιούνται οι μηχανισμοί που απαιτούνται για τη διασφάλισης της σωστής και απρόσκοπτης λειτουργίας των κυψελών, όπως η αναζήτηση του φάσματος για ελεύθερα κανάλια.

4.3 ΔΙΑΚΟΠΗ ΤΩΝ ΜΕΤΑΔΟΣΕΩΝ ΚΑΤΑ ΤΗΝ ΔΙΑΡΚΕΙΑ ΤΟΥ FAST ΚΑΙ ΤΟΥ FINE SENSING

Η υλοποίηση του fast και του fine sensing δεν περιορίζεται μόνο στον εντοπισμό ενέργειας ή πακέτων από τις συσκευές πελατών, αλλά περιλαμβάνει και τη διακοπή της αποστολής

οποιοδήποτε είδους πακέτου κατά τη διάρκεια των φάσεων ελέγχου, εξασφαλίζοντας με αυτόν τον τρόπο την αξιοπιστία των αποτελεσμάτων. Η διακοπή των μεταδόσεων υλοποιείται όχι μόνο με την προσθήκη κατάλληλων συνθηκών ελέγχου έτσι ώστε **να μην προωθείται το πακέτο στα κατώτερα επίπεδα για αποστολή**, αλλά και με την **αποτροπή δημιουργίας ουράς δεδομένων προς αποστολή**.

Για την διακοπή των μεταδόσεων πρωταγωνιστικό ρόλο λαμβάνει η μεταβλητή `scanningPhase`. Συνεπώς, ελέγχοντας την τιμή της μεταβλητής (η οποία θα πρέπει να είναι διαφορετική από `FAST_SENSING`) διασφαλίζεται πως δεν θα σταλεί κανένα πακέτο κατά τη διάρκεια της μετάδοσης. Οι βασικότερες τροποποιήσεις που θα πραγματοποιηθούν αφορούν την αποστολή της ροής και ειδικότερα τις συναρτήσεις `ResumeSsBurstHandler` και `ResumeBsBurstHandler`, οι οποίες καλούνται σε κάθε slot, αποδεσμεύουν την ουρά στην οποία έχουν αποθηκευτεί τα δεδομένα προς αποστολή (με την εκτέλεση της `PduQueue.deque()`) και στέλνουν τα δεδομένα. Οι συναρτήσεις αυτές μπορούν να τροποποιηθούν, έτσι ώστε να αποδεσμεύεται η ουρά για να μην σταλούν τα δεδομένα ξανά, αλλά να μην πραγματοποιούνται οι ενέργειες που ακολουθούν για την αποστολή των πακέτων δεδομένων που αποδεσμεύτηκαν από την ουρά (αρχικοποίηση πακέτου και μεταφορά του στο κατώτερο επίπεδο) όταν βρίσκεται σε εξέλιξη το fast sensing. Στον παρακάτω κώδικα, παριστάνεται η συνθήκη ελέγχου που έχει προστεθεί για τη συνάρτηση `ResumeSsBurstHandler`. Ανάλογες τροποποιήσεις έχουν πραγματοποιηθεί και για τη `ResumeBsBurstHandler`.

Σελίδα | 49

Έλεγχος της κατάστασης στην οποία βρίσκεται το δίκτυο, έτσι ώστε να μην πραγματοποιείται αποστολή πακέτων ροής κατά τη διάρκεια του fast sensing

```
void Mac802_22::ResumeSsBurstHandler(int No_packets, double nextTime,
SsServiceFlow* last)
{
    ...
    else{
        Packet *p = last->PduQueue.deque();
        // even though packet might not be received, number
should be
        // decreased to prevent dequeing NULL packets
        No_packets--;
        // there is a high possibility that p may be NULL
        if(actualNetCell->scanningPhase != FAST_SENSING &&
actualNetCell->scanningPhase != PRE_FAST_SENSING){
            struct hdr_cmh *hdr = HDR_CMH(p);
            struct hdr_mac *mac = HDR_MAC(p);
            ...
        }
        resumeSs.start(nextTime, No_packets, last);
    }
}
```

Πέρα από τις περιπτώσεις αποστολής δεδομένων, παρόμοιοι έλεγχοι έχουν τοποθετηθεί και κατά την αποστολή και άλλων ειδών πακέτων, όπως για παράδειγμα κατά την αποστολή πακέτων τύπου DCD και UDC²⁸. Ο έλεγχος πραγματοποιείται ακριβώς πριν από τη μετάβαση του πακέτου στο αμέσως κατώτερο επίπεδο, όπως φαίνεται και στον παρακάτω κώδικα:

²⁸ Αντίστοιχα πραγματοποιούνται τροποποιήσεις στις συναρτήσεις `sendDCD` και `sendUCD` αντίστοιχα

Προσθήκη ελέγχου της κατάστασης που βρίσκεται το δίκτυο πριν το πακέτο που έχει δημιουργηθεί μεταβεί στο αμέσως κατώτερο επίπεδο

```
void Mac802_22::sendDCD()
{
    ...
    if(actualNetCell->scanningPhase != FAST_SENSING)
        downtarget->recv(p,this);
    return;
}
```

Σελίδα | - 50 -

Πέρα όμως από τις παραπάνω τροποποιήσεις, απαραίτητη είναι και η διενέργεια ελέγχων **κατά τη δημιουργία της ουράς δεδομένων που προορίζονται για αποστολή**. Όταν στο δίκτυο πραγματοποιείται sensing, τότε αποτρέπεται η προσθήκη επιπρόσθετων δεδομένων στην ουρά. Σε αντίθετη περίπτωση, παρόλο που τα δεδομένα δεν θα αποστέλλονταν κατά τη διάρκεια του fast sensing, θα αποστέλλονταν μετά τον τερματισμό της, καθώς το μέγεθος της ουράς θα έχει παραμείνει αμετάβλητο. Ουσιαστικά, χωρίς την παραπάνω προσθήκη, η πραγματοποίηση fast sensing δεν θα επέφερε καμιά επιβάρυνση στο ρυθμό μετάδοσης των δεδομένων, οδηγώντας σε μη αξιόπιστα αποτελέσματα κατά την προσομοίωση.

Η αρχικοποίηση της ουράς δεδομένων πραγματοποιείται στη συνάρτηση `send`. Με βάση τις παραπάνω διαπιστώσεις, προστίθενται κατάλληλες συναρτήσεις ελέγχου πριν από την εκτέλεση της `SduQueue.enqueue(p)`, με την οποία το πακέτο που βρίσκεται προς αποστολή, εισάγεται στην ουρά. Ειδικότερα, αν το δίκτυο βρίσκεται σε κατάσταση `IDLE` ή πραγματοποιείται `dynamic sensing`²⁹, τότε τα δεδομένα προωθούνται κανονικά στην ουρά. Σε αντίθετη περίπτωση, το πακέτο που έχει δημιουργηθεί δεν προωθείται στην ουρά, με αποτέλεσμα η `send` να τερματίζει τη λειτουργία της και το πακέτο να μην αποστέλλεται τελικά. Ο έλεγχος αυτός πραγματοποιείται για οποιοδήποτε είδος ροής και αφορά τόσο το σταθμό βάσης, όσο και τις συσκευές πελατών. Στον παρακάτω κώδικα παριστάνεται ο έλεγχος που έχει προστεθεί ακριβώς πριν από το `if` για την περίπτωση της `rtPS` ροής.

Τροποποίηση του κώδικα της συνάρτησης `send` αποτρέποντας την εισαγωγή πακέτων ροής στην ουρά κατά τη διάρκεια `fast` και `fine sensing`

```
/* Thesis NOTE: Send function will actually work only
if we are in an idle phase (or performing dynamic sensing).
During fast/fine sensing no packets are sent */

void Mac802_22::send(Packet* p, Handler* h)
{
    ...
    else if (hdr->ptype() == PT_rtPS) {
        ...
        if(actualNetCell->scanningPhase == IDLE || actualNetCell-
>scanningPhase == DYNAMIC_SENSING){
            SsSearchServiceFlow(mac->macDA(), PT_rtPS, UL, -1, -1)-
>SduQueue.enqueue(p);
        }
    }
    ...
}
```

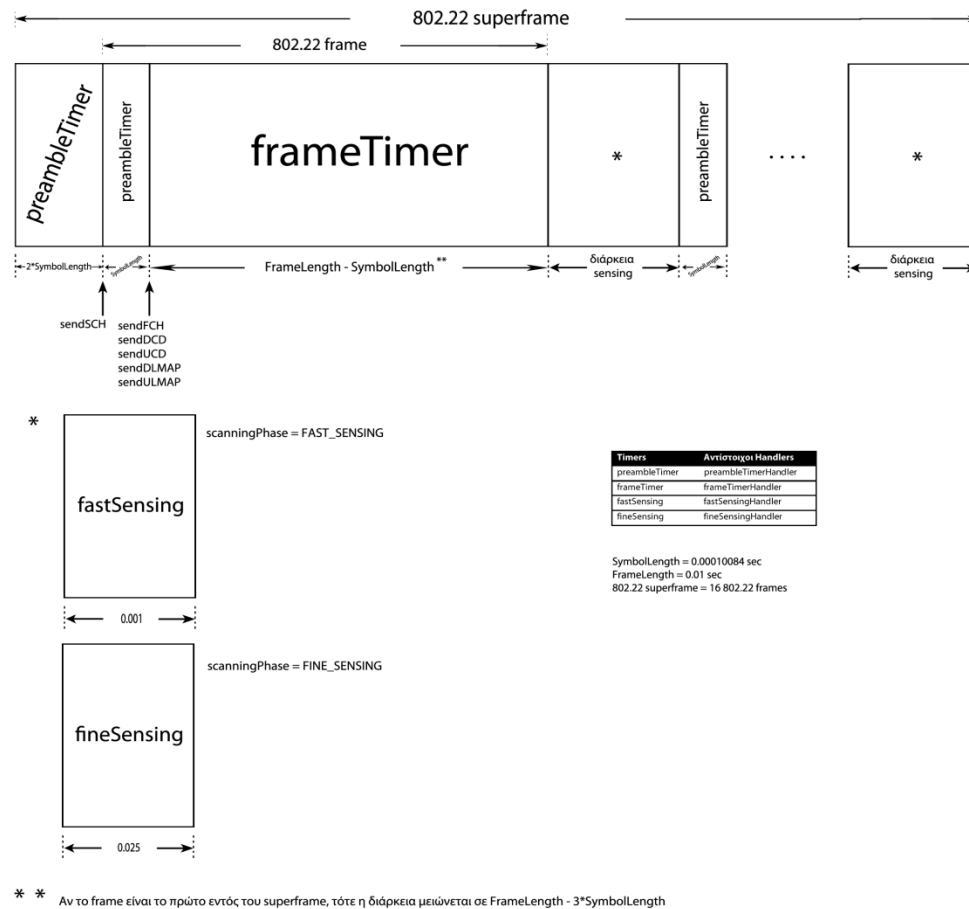
Με τις παραπάνω τροποποιήσεις εξασφαλίζεται πως δεν θα πραγματοποιηθεί καμιά αποστολή δεδομένων κατά τη διάρκεια των ελέγχων. Αντίστοιχα, αφού δεν πραγματοποιούνται αποστολές, δεν θα πραγματοποιηθεί και καμιά λήψη πακέτου κατά τη διάρκεια του sensing που θα μπορούσε να διαταράξει την αξιοπιστία των αποτελεσμάτων

²⁹ Αποτελεί ένα άλλο είδους sensing που υποστηρίζεται από το module και αναλύεται στη συνέχεια

(ειδικότερα του fast sensing). Συνεπώς, θεωρείται πως ενδεχόμενη λήψη ενέργειας ή πακέτου κατά τη διάρκεια των ελέγχων οφείλεται σε παρεμβολές στο ίδιο κανάλι. Η εύρυθμη λειτουργία μιας 802.22 κυψέλης, αποδεικνύεται και στη συνέχεια με την πραγματοποίηση σεναρίων προσομοίωσης στα οποία γίνονται μετρήσεις όσον αφορά το ρυθμό λήψης δεδομένων και την επιβάρυνση που προκαλείται από την πραγματοποίηση fast και fine sensing στο τέλος κάθε frame.

4.4 ΔΟΜΗ ΤΟΥ ΥΛΟΠΟΙΗΜΕΝΟΥ MODULE

Με την ολοκλήρωση και της υλοποίησης του fast και του fine sensing, η δομή του module διαμορφώνεται στην τελική της μορφή, ακολουθώντας τη δομή του 802.22 frame και superframe. Συστατικό στοιχείο της υλοποιημένης δομής αποτελεί η χρήση των timers, όπως φαίνεται και στην παρακάτω εικόνα, στην οποία συγκεντρώνονται συνοπτικά οι βασικές περίοδοι του module. Σε κάθε τμήμα που παριστάνεται, λειτουργούν επιμέρους timers οι οποίοι είναι υπεύθυνοι για την αποστολή και τη λήψη των δεδομένων, όπως ορίζεται από τη δομή ενός 802.22 frame.



Εικόνα 18: Η δομή ενός 802.22 frame και ενός 802.22 superframe, όπως αυτό διαμορφώνεται με βάση τους timers που έχουν προστεθεί. Η δομή βασίζεται στο wimax module που έχει μελετηθεί. Με τη χρήση των timers στέλνονται και τα πακέτα την κατάλληλη χρονική στιγμή, όπως τα superframe και frame control header, τα DCD και UDC και τα DLMAP και ULMAP, με τρόπο παρόμοιο με αυτόν που έχει οριστεί στο 802.22 πρότυπο.

4.5 ΔΙΑΔΙΚΑΣΙΑ ΕΝΗΜΕΡΩΣΗΣ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΑΛΛΑΓΗ ΤΟΥ ΚΑΝΑΛΙΟΥ

Η αλλαγή καναλιού είναι μια αντίδραση που μπορεί να έχει ένα δίκτυο IEEE 802.22 όταν βρεθεί κάποιος πρωτεύων χρήστης του δικτύου ή όταν η ποιότητα υπηρεσιών που παρέχονται από το δίκτυο έχει υποβαθμιστεί λόγω παρεμβολών³⁰. Στο πρότυπο του 802.22 δεν έχει οριστεί ακριβώς ο τρόπος με ποιο θα γίνεται η ενημέρωση του συνόλου του κόμβων του δικτύου για την αλλαγή καναλιού. Γι' αυτό το λόγο αυτό που υλοποιήθηκε στην προσομοίωση του 802.22 στον ns-2 είναι μια προσέγγιση της αντίστοιχης συμπεριφοράς του 802.16.

Σελίδα | 53

Θα πρέπει να σημειωθεί ότι παρόλο που το module που χρησιμοποιήθηκε ως βάση για την ανάπτυξη του module προσομοίωσης του 802.22 ήταν ένα module του 802.16 η συγκεκριμένη λειτουργία δεν είχε υλοποιηθεί. Αυτό, υποθέεται, ότι έγινε αφενός για λόγους απλούστευσης και αφετέρου γιατί δεν είναι συχνό το φαινόμενο ένα δίκτυο 802.16 να αλλάζει κανάλι λειτουργίας διότι πρόκειται για πρωτόκολλο που λειτουργεί σε αδειοδοτημένο φάσμα συχνοτήτων. Σε αντίθεση όμως με το 802.16 και την «στατική» συμπεριφορά που αυτό παρουσιάζει όσον αφορά την χρήση των καναλιών, το 802.22 παρουσιάζει, όπως έχει προαναφερθεί, μια άκρως δυναμική συμπεριφορά σ' αυτόν τον τομέα.

Συγκεκριμένα τώρα, η διαδικασία που ακολουθείται για την αλλαγή καναλιού στο 802.16 είναι να σταλθεί ένα πακέτο DCD (*Downlink Channel Descriptor*). Αυτό το πακέτο είναι ένα πακέτο που σ' αυτό το πρωτόκολλο στέλνεται σε όλους τους κόμβους του δικτύου από το σταθμό βάσης σε τακτά χρονικά διαστήματα και τουλάχιστον ένα κάθε 10 δευτερόλεπτα^[40]. Η διαφορά που υπάρχει σε αυτό το σημείο με το 802.22 είναι ότι αυτό το πακέτο στέλνεται σε κάθε frame. Αυτό δικαιολογείται από το γεγονός ότι στο 802.22 η αλλαγή του καναλιού είναι πολύ συχνή λόγω του ότι αυτό λειτουργεί σε μη αδειοδοτημένο φάσμα και στην δυναμική συμπεριφορά που αυτό έχει ως αποτέλεσμα. Έτσι στο 802.16 ορίζεται ότι κάθε φορά που αλλάζει κανάλι λειτουργίας αυτό ορίζεται στο πεδίο *Channel Nr* του πακέτου αυτού που στέλνει ο σταθμός βάσης. Αν το πεδίο αυτό είναι διαφορετικό από αυτό που γνωρίζουν οι σταθμοί των συνδρομητών, αυτοί αλλάζουν το κανάλι τους σε αυτό.

Αυτό που έχει προσομοιωθεί στο module του 802.22 που αναπτύχθηκε παρουσιάζει κάποιες διαφορές οι οποίες αφορούν στην οντότητα του δικτύου που στέλνει αυτό το μήνυμα. Σε αντίθεση με το 802.16, που το πακέτο αυτό το στέλνει ο σταθμός βάσης, στην προσομοίωση που έγινε αυτό το μήνυμα το στέλνει μια συσκευή πελάτη και συγκεκριμένα αυτή που έκανε τον έλεγχο για την διαθεσιμότητα των καναλιών. Έτσι όλοι οι κόμβοι που υπάρχουν στο κανάλι και είναι στο δίκτυο, συμπεριλαμβανομένου και του σταθμού βάσης, θα πρέπει από την στιγμή που έλαβαν το πακέτο αυτό και μετά να αλλάξουν κανάλι στο καινούριο που τους έχει κοινοποιηθεί.

Η αποστολή του πακέτου αυτού γίνεται από τη συνάρτηση *sendChangeChannelDCD*. Το τμήμα κώδικα που παρουσιάζεται παρακάτω αφορά το τμήμα αυτό που διαφέρει σε λίγα αλλά καίρια σημεία σε σχέση με την συνηθισμένη αποστολή του πακέτου DCD. Οι διαφορές αυτές φαίνονται στο τμήμα κώδικα που φαίνεται παρακάτω. Αρχικά, καθώς το μήνυμα, όπως αναφέρθηκε, το στέλνει μια συσκευή πελάτη το πεδίο *BS_ID.Value* παίρνει την αποθηκευμένη τιμή που έχει κάθε συσκευή πελάτη, την *bss_id_*. Όπως μπορεί εύκολα να

³⁰ Ο λόγος Σήμα/παρεμβολές (*SIR – Signal to Interference*) είναι μικρός. Οι παρεμβολές μπορεί να οφείλονται τόσο σε άλλες κυψέλες που λειτουργούν στο ίδιο κανάλι στην ίδια περιοχή όσο και σε κάποιον κακόβουλο χρήστη.

παρατηρηθεί πέρα από τον αριθμό του καναλιού υπάρχει και η συχνότητα λειτουργίας του συγκεκριμένου καναλιού. Θα πρέπει να τονιστεί επίσης ότι αλλαγή έγινε και στην συνάρτηση sendDCD που στέλνει αυτά τα πακέτα όλες τις υπόλοιπες φορές. Σ' αυτή προστέθηκε, αφού πρώτα προστέθηκε ο ορισμός του συγκεκριμένου πεδίου στο πακέτο DCD στο αρχείο packet-802_22.h, ο ορισμός της τιμής του πεδίου Channel_Nr³¹.

(α) Αποστολή πακέτου DCD, (β)Πεδία που αλλάζουν στην αποστολή ενός πακέτου DCD που έχει ως σκοπό την ενημέρωση για αλλαγή καναλιού, (γ) ο επιπλέον ορισμός του πεδίου του Channel_Nr του πακέτου DCD, όπως αυτό φαίνεται στο αρχείο packet-802_22.h

Σελίδα | - 54 -

```
void Mac802_22::sendDCD() {
    // ...
    dcd->BS_ID.Value = NodeID;
    dcd->Channel_Nr.Value = channel_;
} (α)
```

```
void Mac802_22::sendChangeChannelDCD(int channelToChangeTo) {
    // ...
    dcd->BS_ID.Value = bss_id_;
    dcd->Channel_Nr.Value = channelToChangeTo;
    dcd->Frequency.Value = (u_int32_t)calFreq(channelToChangeTo);
} (β)
```

```
struct DcdMsg {
    //...
    TLV_LEN8 Channel_Nr;
    TLV_LEN32 Frequency;
    TLV_LEN48 BS_ID;
}; (γ)
```

Πέρα όμως από αυτό το σημείο, όπως είναι λογικό, υπάρχει και αντίστοιχη αλλαγή στη συνάρτηση recvDCD που είναι αυτή που είναι υπεύθυνη για την λήψη του πακέτου. Αν το πακέτο DCD είναι από κάποιον στο δίκτυο και ο αριθμός του καναλιού είναι διαφορετικός από αυτόν που έχουν αποθηκευμένες οι συσκευές τότε, είτε πρόκειται για σταθμό βάσης είτε για συσκευή πελάτη οι συσκευές αυτές θα πρέπει να αλλάξουν το κανάλι τους. Αυτό φαίνεται στο παρακάτω τμήμα κώδικα.

Η συνάρτηση recvDCD που είναι υπεύθυνη για τη λήψη του πακέτου DCD

```
void Mac802_22::recvDCD(Packet *p){
    // ...
    DcdMsg *dcd = (DcdMsg*) p->accessdata();
    // ...
    if (NodeID != bss_id_) { // CPE
        if ((int)dcd->BS_ID.Value == bss_id_){
            if((int)dcd->Channel_Nr.Value!=channel_){
                Tcl& tcl = Tcl::instance();
                tcl.evalf ("%s set-freq %f", netif_->name(),
                    calFreq((int)dcd->Channel_Nr.Value));
            }
            // ...
        }
        // ...
    }
    else { // BS
        if ((int)dcd->BS_ID.Value == bss_id_){
            if((int)dcd->Channel_Nr.Value!=channel_){
```

³¹ TLV- Type/Length/Value – Είναι ένα σχήμα μορφοποίησης που προσθέτει μια ετικέτα σε κάθε παράμετρο που διαβιβάζεται και περιέχει σε αυτό τον τύπο της παραμέτρου (και έμμεσα τους κανόνες για την κωδικοποίησή της) και το μήκος της κωδικοποιούμενης παραμέτρου ^[40]

```

        Tcl& tcl = Tcl::instance();
        tcl.evalf ("%s set-freq %f", netif_>name(),
calFreq((int)dcd->Channel_Nr.Value));
    }

    // ...
}

// ...
}
}

```

4.6 ΠΕΡΙΓΡΑΦΗ ΕΝΟΣ ΑΡΧΕΙΟΥ TCL

Σ' αυτή την παράγραφο θα γίνει αναφορά στα βασικά σημεία των αρχείων tcl που χρησιμοποιήθηκαν για τις προσομοιώσεις. Καθώς αναφορά γενικά για τα αρχεία tcl έχει γίνει και σε προηγούμενα κεφάλαια σ' αυτό το τμήμα επιλέχθηκε να αναφερθούν τμήματα του αρχείου που αφορούν αποκλειστικά το πρωτόκολλο 802.22 που υλοποιήθηκε.

4.6.1 Ορισμός του σταθμού βάσης

Κατά τον ορισμό ενός κόμβου που είναι σταθμός βάσης θα πρέπει να καθοριστεί η θέση του στο χώρο που θα χρησιμοποιηθεί για την προσομοίωση, αν αυτός θα κινείται, ενώ γίνονται και κάποιες επιπλέον δηλώσεις που χρησιμοποιούνται για την αρχικοποίηση μεταβλητών που θα χρησιμοποιηθούν για την προσομοίωση του πρωτοκόλλου MAC. Η δήλωση ενός σταθμού βάσης φαίνεται παρακάτω.

Δήλωση ενός κόμβου που είναι σταθμός βάσης

```

set channelAP0 1

set bstation [$ns node]
$bstation random-motion 0
$bstation set X_ 200
$bstation set Y_ 200
$bstation set Z_ 0.0
$ns initial_node_pos $bstation 20
set bstationMac [$bstation getMac 0]
set AP_ADDR_0 [$bstationMac id]
$bstationMac bss_id $AP_ADDR_0
$bstationMac set-channel $channelAP0

```

Η δήλωση «\$bstation random-motion 0» υποδηλώνει ότι ο σταθμός βάσης θα παραμένει ακίνητος, ενώ οι αμέσως παρακάτω, όπως γίνεται εύκολα αντιληπτό, αφορούν την θέση του σταθμού βάσης στο χώρο.

4.6.2 Ορισμός της συσκευής πελάτη

Με παρόμοιο τρόπο γίνεται και ο ορισμός ενός κόμβου που είναι συσκευή πελάτη. Μια διαφορά που παρατηρείται έγκειται στον στην ρητή δήλωση του ως συσκευή πελάτη με την δήλωση «\$cpetationMac is_CPE», έτσι ώστε να είναι δυνατή η αρχικοποίηση των μεταβλητών της προσομοίωσης που σχετίζονται με τις συσκευές πελατών. Μια επιπλέον διαφορά εντοπίζεται στην δήλωση «\$node (1) base-station \$AP_ADDR_0;» σε συνδυασμό με την δήλωση «\$cpetationMac is_CPE» η πρώτη εκ των οποίων αρχικοποιεί μια μεταβλητή που διαχωρίζει τις δικτυακές οντότητες. Η δήλωση μιας συσκευής πελάτη φαίνεται παρακάτω.

Δήλωση ενός κόμβου που είναι συσκευή πελάτη

```
set channelAP0 1

set node_1 [$ns node]
$node_1 base-station $AP_ADDR_0 ;
$node_1 set X_ 5200
$node_1 set Y_ 200
$node_1 set Z_ 0.0
$ns initial_node_pos $node_1 20
set cpetationMac [$node_1 getMac 0]
$cpetationMac is_CPE
$cpetationMac set-channel $channelAP0
```

Σελίδα | - 56 -

4.6.3 Κεραίες εκπομπής σήματος

Όπως περιγράφηκε σε προηγούμενο κεφάλαιο, για την περιγραφή των προσομοιώσεων στα αρχεία tcl είναι απαραίτητος ο ορισμός των κεραιών που θα χρησιμοποιηθούν από τους κόμβους της προσομοίωσης. Η δήλωση αυτή φαίνεται παρακάτω.

Επιλογή κεραίας εκπομπής σήματος

```
set val(ant) Antenna/OmniAntenna ;# antenna model

set ns [new Simulator]
set chan0 [new $val(chan)]

$ns node-config-antType $val(ant)
```

Στις παραπάνω δηλώσεις φαίνεται ο ορισμός μιας μόνο κεραίας, μιας πανδιευθυντικής. Δεδομένου ότι η παραπάνω δήλωση επηρεάζει τις ρυθμίσεις όλων των κόμβων του δικτύου, θα μπορούσε να ειπωθεί ότι δεν υπάρχει πλήρης αντιστοιχία με το πρωτόκολλο 802.22 που ορίζει ότι οι συσκευές πελατών θα πρέπει να έχουν τόσο μια πανδιευθυντική όσο και μια κατευθυντική κεραία. Ωστόσο, μέχρι στιγμής, δεν έχει αναπτυχθεί η δυνατότητα λήψης δεδομένων από δυο κεραίες στο περιβάλλον του ns-2.

4.6.4 Δήλωση των ροών δεδομένων

Κατά την δήλωση των ροών δεδομένων που θα χρησιμοποιηθούν καθορίζεται τόσο ποιος κόμβος θα είναι η πηγή των δεδομένων όσο και ο τύπος δεδομένων που θα μεταδοθούν. Επιπλέον καθορίζεται και αρχή και το τέλος των μεταδόσεων.

Δήλωση μιας ροής δεδομένων

```
set val(start) 0.5 ;# time of simulation start
set val(stop) 3.0 ;# time of simulation end

1.set udp [new Agent/UDP]
2.$ns attach-agent $bstation $udp
3.set null [new Agent/Null]
4.$ns attach-agent $node_1 $null
5.$ns connect $udp $null
6.set cbr [new Application/Traffic/rtPS]
7.$cbr8 attach-agent $udp8
8.$ns at $val(start) "$cbr start"
9.$ns at $val(stop) "$cbr stop"
```

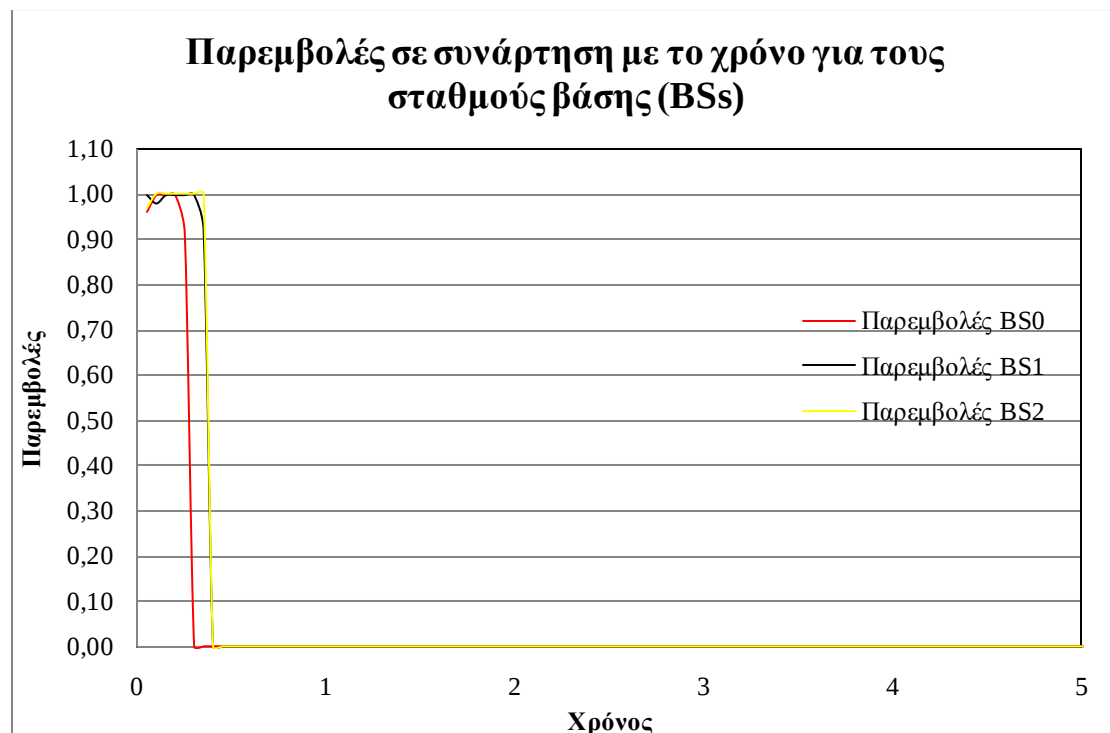
Στην παραπάνω δήλωση στις γραμμές 1 και 2 φαίνεται ο ορισμός ενός agent κυκλοφορίας UDP ο οποίος προσαρτάται σε στον σταθμό βάσης. Αυτός θα είναι η πηγή της επικοινωνίας κάτι που δηλώνεται στη γραμμή 7, ενώ στην γραμμή 6 έχει γίνει ο ορισμός της κίνησης που

θα χρησιμοποιείται (τ_{tPS}). Στις γραμμές 3 και 4 γίνεται ο αντίστοιχος ορισμός του άλλου άκρου της επικοινωνίας των που είναι ένας agent λήψης δεδομένων, ο οποίος προσαρτάται στην συσκευή πελάτη. Στην γραμμή 5 γίνεται η σύνδεση τους, ενώ στις τελευταίες δυο γραμμές καθορίζεται η αρχή και το τέλος των μεταδόσεων.

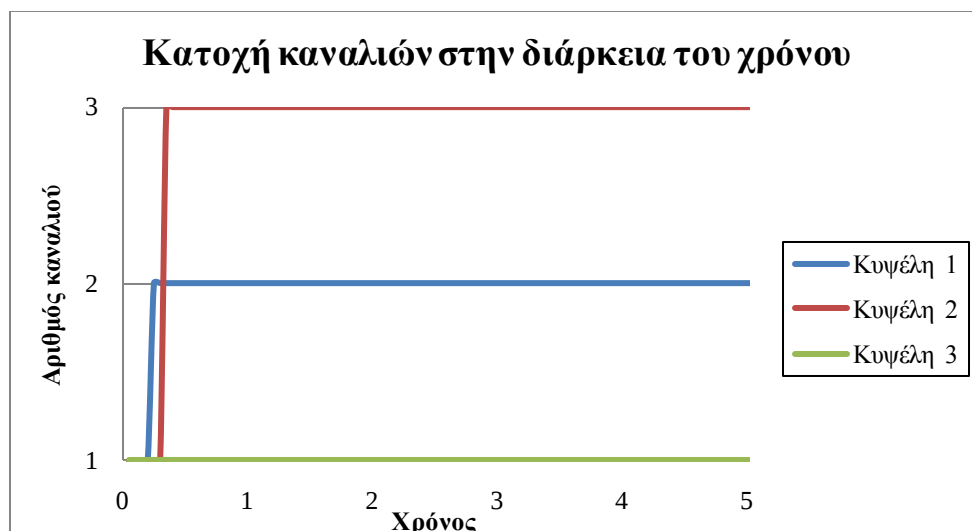
4.7 ΠΕΡΙΓΡΑΦΗ ΕΝΟΣ ΣΕΝΑΡΙΟΥ ΔΟΚΙΜΗΣ ΤΗΣ ΕΠΕΚΤΑΣΗΣ

Σελίδα | 57

Σε αυτή την παράγραφο θα περιγραφεί ένα σενάριο προσομοίωσης στο οποίο επιδεικνύεται ο τρόπος με τον οποίο δίκτυα που **βρίσκονται στο ίδιο κανάλι, αλλάζουν κανάλι**, αποφεύγοντας με αυτόν τον τρόπο τη μεταξύ τους παρεμβολή. Αρχικά θα πρέπει να αναφερθούν κάποια πράγματα σχετικά με την τοπολογία που είχαν οι σταθμοί βάσης (BSs) και οι συσκευές των πελατών (CPEs) στην προσομοίωση. Σε μια περιοχή που ορίζεται από ένα τετράγωνο πλευράς ενός χιλιομέτρου, υπάρχουν τρεις (3) σταθμοί βάσης. Στην ίδια περιοχή βρίσκονται και τρεις (3) συσκευές πελατών, καθεμιά από τις οποίες είναι συσχετισμένη με ένα σταθμό βάσης. Ο αριθμός των καναλιών που είναι διαθέσιμα (είναι δηλαδή ελεύθερα) είναι 3. Αρχικά και οι τρεις σταθμοί βάσης λειτουργούν στο ίδιο κανάλι. Σκοπός του σεναρίου είναι η λειτουργία και των τριών σταθμών βάσης σε διαφορετικά κανάλια, έτσι ώστε να μην υπάρχουν παρεμβολές μεταξύ τους.



Εικόνα 19: Παρεμβολές σε συνάρτηση με το χρόνο για τους σταθμούς βάσης



Εικόνα 20: Χρήση καναλιών κατά την διάρκεια της προσομοίωσης

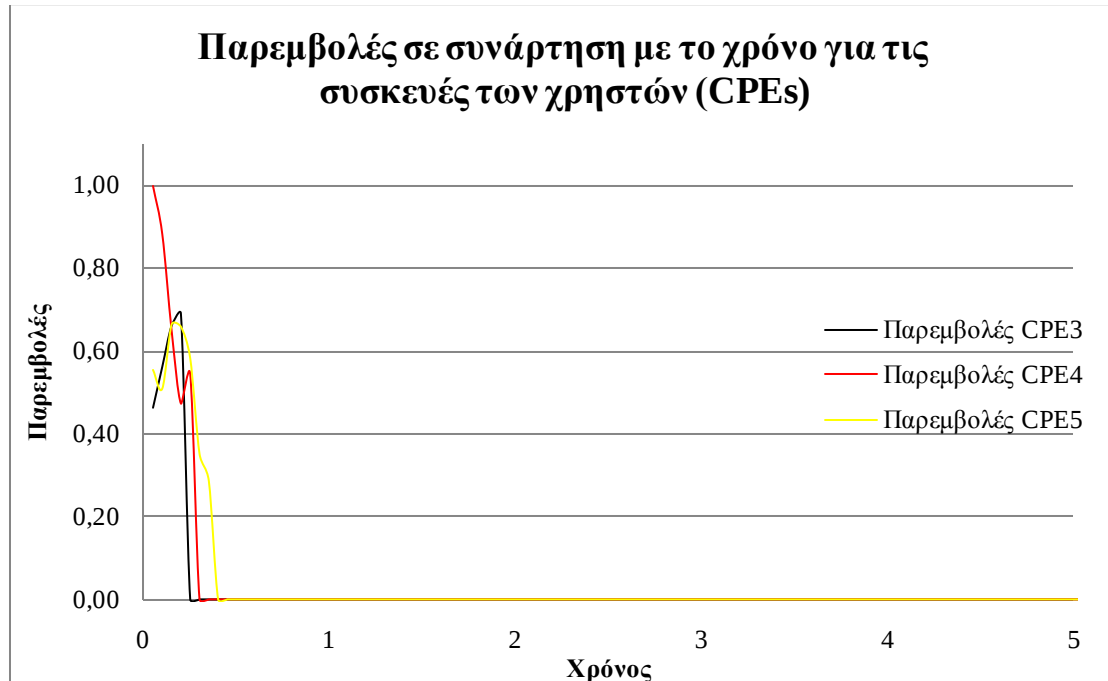
Στην Εικόνα 19 παριστάνονται οι παρεμβολές σε συνάρτηση με το χρόνο. Η παρεμβολή που έχει μετρηθεί είναι αποτέλεσμα των πακέτων που έχουν ληφθεί από άλλα δίκτυα προς τα συνολικά πακέτα που έχουν ληφθεί. Αντίστοιχα, στην Εικόνα 20 παριστάνεται η κατοχή των καναλιών από τις κυψέλες (*cells*) τη χρονική διάρκεια του πειράματος. Κυψέλη (*cell*), όπως αναφέρθηκε και παραπάνω, θεωρείται το δίκτυο που δημιουργείται μεταξύ των σταθμών βάσης και των κινητών τερματικών που είναι συσχετισμένα με αυτό. Θα πρέπει όμως να προσδιοριστεί και η έννοια της παρεμβολής. Θα αναλυθεί η παρεμβολή τόσο όσον αφορά την οντότητα του σταθμού βάσης όσο και όσον αφορά το κινητό τερματικό. Παρεμβολές για τον σταθμό βάσης θεωρούνται αφενός τα πακέτα που δέχεται από κάποια άλλη κυψέλη αλλά και αφετέρου όλες αυτά τα οποία λαμβάνει αλλά δεν προορίζονται για αυτόν (πακέτα τα οποία στη συνέχεια αποδεσμεύονται με τη διαδικασία του *address filtering*). Για την περίπτωση του κινητού τερματικού, παρεμβολές θεωρούνται όλα τα πακέτα που δεν λαμβάνονται από το συσχετισμένο με αυτό σταθμό βάσης, καθώς αυτός είναι ο μόνος κόμβος του δικτύου από τον οποίο λαμβάνει πληροφορίες.

Όπως έχει αναφερθεί, και οι 3 σταθμοί βάσης της προσομοίωσης εκκινούν τη λειτουργία τους σε διαφορετικές χρονικές στιγμές, στο ίδιο αρχικό κανάλι, το κανάλι 1. Πρώτο ξεκινάει το BS0 μετά από **0.00054332s**, δεύτερο το 2 στα **0.265272746s** και τελευταίο στη σειρά το 1 την χρονική στιγμή **0.279940915s**. Με βάση το χρόνο εκκίνησης του κάθε σταθμός βάσης μπορεί να εξηγηθεί και η γραφική παράσταση της Εικόνα 19.

Καθώς το BS0 ξεκινάει πρώτο τις μεταδόσεις του, μέχρι να εκκινήσει τις μεταδόσεις του το BS2, δεν υπάρχει καμιά παρεμβολή. Αυτό άλλωστε φαίνεται και από την παραπάνω γραφική παράσταση, στην οποία η παρεμβολή για το BS0 αρχίζει και αποκτά μη μηδενική τιμή τη στιγμή εκκίνησης του BS2. Από εκείνη τη στιγμή και μετά, τόσο το BS0 όσο και το BS2, αρχίζουν και δέχονται μηνύματα το ένα από το άλλο που θεωρούνται παρεμβολές. Με την εκκίνηση των μεταδόσεων και του BS1 οι παρεμβολές μεγιστοποιούνται, όπως φαίνεται και στην παραπάνω γραφική παράσταση στην οποία η παρεμβολή και των τριών BSs τείνει στη μονάδα. Η αύξηση των παρεμβολών στην περίπτωση των BS εκείνη τη χρονική περίοδο εξηγείται από το γεγονός ότι τα μόνα πακέτα που δέχονται οι σταθμοί βάσης είναι μόνο τα διαχειριστικά μηνύματα από άλλους σταθμούς βάσης, καθώς δεν έχει εκκινήσει ακόμα η ροή δεδομένων μεταξύ των κινητών τερματικών και των σταθμών βάσης³². Στα 0.211054999s η κυψέλη που αποτελείται από το BS0 και το CPE3 έχοντας εντοπίσει τις παρεμβολές αυτές

³² Έχουν οριστεί στην προσομοίωση να ξεκινούν τη χρονική στιγμή 1sec

αλλάζει το κανάλι λειτουργίας, μεταβαίνοντας στο κανάλι 2. Από την χρονική στιγμή αυτή και έπειτα παρατηρείται μείωση στις τιμές των παρεμβολών των BS1 και BS2, ενώ η αντίστοιχη για το BS0 μηδενίζεται. Η χρονική στιγμή που παρατηρείται η μείωση στο 0 των παρεμβολών όλων των σταθμών βάσης είναι η χρονική στιγμή 0,310822339s όπου η κυψέλη που αποτελείται από το BS1 και το CP4 έχοντας εντοπίσει ότι κάποια άλλη κυψέλη λειτουργεί στο ίδιο κανάλι, αλλάζει το κανάλι λειτουργίας του και αρχίζει να λειτουργεί στο κανάλι 3. Από εκεί και μετά, μιας και κάθε κυψέλη λειτουργεί σε διαφορετικό κανάλι, δεν υπάρχει καμία παρεμβολή στην λειτουργία τους.



Εικόνα 21: Παρεμβολές σε συνάρτηση με το χρόνο για τις συσκευές των χρηστών (CPEs)

Στην Εικόνα 21 φαίνεται η αντίστοιχη γραφική παράσταση των παρεμβολών σε συνάρτηση με το χρόνο, αυτή τη φορά για τις συσκευές των πελατών. Παρατηρούνται κάποιες διαφορές στη μορφή της γραφικής παράστασης σε σχέση με την αντίστοιχη των σταθμών βάσης. Αυτό οφείλεται στον ορισμό για τις παρεμβολές που έχει δοθεί παραπάνω όσον αφορά το τι θεωρείται παρεμβολή για τις συσκευές των πελατών. Όσο δεν έχει εκκινήσει τις μεταδόσεις του ο σταθμός βάσης με τον οποίο είναι συσχετισμένη η εκάστοτε συσκευή πελάτη, λαμβάνει πακέτα (διαχειριστικά πακέτα) μόνο από τους σταθμούς βάσης που έχουν εκκινήσει, που γι' αυτό όμως θεωρούνται παρεμβολές. Μια ακόμα διαφορά παρουσιάζεται και στο γεγονός ότι πέρα από το CPE4 του οποίου το BS ξεκινάει τελευταίο τις μεταδόσεις του, κανένα άλλο δεν πλησιάζει το 1, παρόλο που δεν έχουν αρχίσει οι ροές των δεδομένων από επίπεδα ανώτερα του MAC. Αυτό οφείλεται στο γεγονός ότι οι συσκευές πελατών λαμβάνουν πακέτα τόσο από το σταθμό βάσης με το οποίο είναι συσχετισμένο όσο και από τα υπόλοιπα, με αποτέλεσμα ο λόγος του αριθμού των πακέτων που λαμβάνονται και δεν θεωρούνται παρεμβολές να είναι αισθητά μικρότερος από τον συνολικό αριθμό των πακέτων που λαμβάνονται.

Έτσι, για τη χρονική περίοδο 0.00054332 - 0.002272746s, το CPE3, εφόσον ο μόνος σταθμός βάσης που έχει ξεκινήσει τις μεταδόσεις του είναι το συσχετισμένο με αυτό, δεν παρουσιάζει κάποιου είδους παρεμβολή. Για το ίδιο χρονικό διάστημα, τα CPE4 και CPE5 δέχονται μόνο από το BS0 που θεωρούνται όλες παρεμβολές. Με την εκκίνηση του BS2, μειώνονται οι παρεμβολές του CPE5 και αυξάνονται αυτές του CPE3. Οι παρεμβολές αυξάνονται ακόμα περισσότερο με την εκκίνηση των μεταδόσεων του BS1. Η μείωση αρχίζει την χρονική

στιγμή 0.211054999s, όπου η κυψέλη του BS2 αλλάζει κανάλι λειτουργίας, ενώ μηδενίζεται και για τα 3 CPEs, όταν και το BS2 αλλάξει το κανάλι λειτουργίας του στα 0.310822339 sec.

Η ακρίβεια όλων των αποτελεσμάτων που παρουσιάζονται παραπάνω εξαρτώνται από την συχνότητα με την οποία λαμβάνονται οι μετρήσεις. Οι συγκεκριμένες μετρήσεις λαμβάνονται κάθε 0.05sec.

Σελίδα | - 60 -

4.8 ΕΠΙΠΤΩΣΗ SENSING ΣΤΟ ΡΥΘΜΟ ΜΕΤΑΔΟΣΗΣ/ΛΗΨΗΣ ΔΕΔΟΜΕΝΩΝ

Ένα αρκετά ενδιαφέρον στοιχείο που εξετάζεται με τη χρήση του συγκεκριμένο module, είναι οι επιπτώσεις του sensing στο ρυθμό μετάδοσης των δεδομένων (*throughput*). Παρόλο, που με την προσθήκη των λειτουργιών του fast και του fine sensing, οι συσκευές των πελατών είναι σε θέση να εντοπίσουν οποιαδήποτε παρεμβολή, είτε αυτή προέρχεται από κάποιο τηλεοπτικό σήμα (*primary users*), είτε αυτή προέρχεται από κάποιον κακόβουλο χρήστη (είτε αυτός είναι σταθμός βάσης είτε συσκευή πελάτη), δεν λείπουν και οι επιβάρυνσεις στη ροή των δεδομένων. Έστω:

- T_{sense} : η διάρκεια του sensing σε κάθε frame και
- T_{frame} : η διάρκεια του frame

Η επιβάρυνση στο throughput ^[18] μπορεί να υπολογιστεί με τη μέτρηση της αποδοτικότητας στη μετάδοση (*transmission efficiency*) a , η οποία είναι ο λόγος του χρόνου στον οποίο πραγματοποιείται η μετάδοση προς τη συνολική περίοδο στην οποία πραγματοποιείται το sensing και μετάδοση δεδομένων, όπως φαίνεται και στην παρακάτω σχέση:

$$a = \frac{T_{\text{frame}}}{T_{\text{frame}} + T_{\text{sense}}} \quad (1)$$

Το T_{sense} θα αντιστοιχεί στη διάρκεια του fast sensing το οποίο πραγματοποιείται σε κάθε frame. Όπως έχει οριστεί στο πρότυπο του 802.22, το fast sensing θα πρέπει να έχει διάρκεια 1 ms (= 0.001 sec), ενώ η διάρκεια του frame είναι 10ms (0.01 sec). Επομένως, η αποδοτικότητα που προκύπτει είναι:

$$a = \frac{0.01 \text{ sec}}{0.01 \text{ sec} + 0.001 \text{ sec}} = \frac{0.01}{0.011} = 0.909090 \dots$$

Με βάση την παραπάνω σχέση, αν το throughput σε κανονικές συνθήκες (χωρίς την παρουσία sensing) είναι T , τότε το throughput με την προσθήκη του sensing μειώνεται, με την τιμή του να είναι aT . Η μείωση του throughput μπορεί να επιβεβαιωθεί και **πειραματικά** με την εκτέλεση του module, όπου θα μετρηθεί η ροή των δεδομένων με (και χωρίς) την παρουσία sensing. Έστω, ένας σταθμός βάσης που ανταλλάσσει δεδομένα με κάποιες συσκευές πελατών σε ένα συγκεκριμένο κανάλι, χωρίς να υπάρχει κάποια άλλη παρεμβολή, εντός της εμβέλειας λειτουργίας τους. Οι μετρήσεις που πραγματοποιήθηκαν παρουσιάζονται στον παρακάτω πίνακα. Ειδικότερα, μετρήθηκε ο ρυθμός λήψης της ροής³³ για μια συσκευή πελάτη στο δίκτυο.

³³ Η ροή που χρησιμοποιήθηκε είναι τύπου *itPS*

Λειτουργία	Ρυθμός ροής δεδομένων (Mbps)	Αποδοτικότητα α
Με παρουσία sensing	0.7219584	0.91063644
Χωρίς παρουσία sensing	0.7928064	

Πίνακας III: Μέτρηση του ρυθμού ροής δεδομένων με την παρουσία sensing και χωρίς την παρουσία sensing και υπολογισμός της αποδοτικότητας. Το αποτέλεσμα που προκύπτει συγκλίνει με το θεωρητικό.

Όπως παρατηρείται, τα παραπάνω αποτελέσματα, επιβεβαιώνουν τη σωστή λειτουργία του module, αλλά και τη συμφωνία με τη θεωρητική σχέση που διατυπώθηκε προηγουμένως.

Κεφάλαιο 5

ΣΕΝΑΡΙΑ ΕΠΙΘΕΣΗΣ ΣΕ ΔΙΚΤΥΑ IEEE 802.22 ΚΑΙ ΑΝΑΠΤΥΞΗ ΑΝΤΙΜΕΤΡΩΝ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥΣ

Στα προηγούμενα κεφάλαια έγινε αναφορά στον τρόπο με τον οποίο υλοποιήθηκε η λειτουργικότητα ενός δικτύου 802.22 σχετικά με τον έλεγχο για πρωτεύοντες χρήστες στα κανάλια που χρησιμοποιούνται για τις μεταδόσεις μιας κυψέλης. Επιπλέον προτάθηκε και ένας τρόπος με τον οποίο αυτός ο έλεγχος μπορεί να γίνει ταχύτερα, εμποδίζοντας ταυτόχρονα και κάποια είδη επιθέσεων από κακόβουλους χρήστες. Σ' αυτό το κεφάλαιο θα περιγραφεί ένα εξελιγμένο σενάριο επίθεσης σε δίκτυα 802.22 ενώ θα αναλυθούν αντίμετρα που σχεδιάστηκαν και υλοποιήθηκαν για την αντιμετώπισή του.

5.1 ΥΛΟΠΟΙΗΣΗ ΤΟΥ ΕΠΙΤΙΘΕΜΕΝΟΥ ΣΤΟΝ NS-2

Ο επιτιθέμενος αποτελεί, όπως και οποιοδήποτε «νόμιμο» BS ή CPE, ένα αντικείμενο της κλάσης `Mac802_22`. Παρακάτω, παρουσιάζεται η δήλωση του επιτιθέμενου σε γλώσσα TCL, γλώσσα που χρησιμοποιήθηκε για τις περιγραφές όλων των σεναρίων λειτουργίας και επίθεσης:

Περιγραφή του επιτιθέμενου σε γλώσσα TCL

```
set attacker [$ns node]
$attacker set X_ 10200
$attacker set Y_ 200
$attacker set Z_ 0.0
$ns initial_node_pos $attacker 20
set sstationMac [$attacker getMac 0]
$sstationMac attacker
$sstationMac set-channel $channelAP1
```

Η διαφορά με τη δημιουργία των νόμιμων κόμβων εντοπίζεται στη δήλωση `$sstationMac attacker`, όπου ενεργοποιείται η αντίστοιχη συνθήκη της συνάρτησης `command` στο αρχείο `mac-802_22.cc`, όπως φαίνεται και στο παρακάτω τμήμα κώδικα:

Δημιουργία της οντότητας του επιτιθέμενου, όπως αυτή ορίζεται στη συνάρτηση `command` στο αρχείο `mac-802_22.cc`. Διαβάζοντας το όρισμα "attacker" που έχει δηλωθεί στο προηγούμενο αρχείο tcl, η εκτέλεση της συνάρτησης πραγματοποιείται στην παρακάτω συνθήκη

```
if (strcmp(argv[1], "attacker") == 0) {
    attacker = true;
    createBS(index_);
    attackTimer.start(0.001);
    return TCL_OK;
}
```

Παρατηρείται πως ο επιτιθέμενος δηλώνεται ως BS, χωρίς αυτό να έχει κάποια πρακτική αξία. Η συμπεριφορά του διαφοροποιείται από τη φυσιολογική με τη χρήση του `flag attacker`, το οποίο έχει την τιμή `true`. Ο `attackerTimer` είναι ένας `timer` που χρησιμοποιεί ο επιτιθέμενος, στην εκπνοή του οποίου αποστέλλεται ένα πακέτο³⁴, για να εκκινήσει ξανά μετά την αποστολή του πακέτου (συνάρτηση `interfere`).

Σε αντίθεση με τους φυσιολογικούς σταθμούς βάσης, ο επιτιθέμενος αγνοεί τυχόν πακέτα που μπορεί να λάβει³⁵, δε δημιουργεί ροή, ούτε και στέλνει κανένα πακέτο οποιουδήποτε άλλου τύπου. Όπως διαπιστώνεται, ο επιτιθέμενος δεν πραγματοποιεί έλεγχο για παρεμβολές στο κανάλι, ούτε και αλλάζει κανάλι λειτουργίας. Ωστόσο, μπορεί να προγραμματίσει πότε θα πραγματοποιηθεί το `fast sensing`, χωρίς να γίνεται στην ουσία έλεγχος του καναλιού, χαρακτηριστικό που θα αποβεί ιδιαίτερο χρήσιμο σε πιο πολύπλοκα σενάρια προσομοίωσης.

Σελίδα | 63

5.2 ΠΡΑΓΜΑΤΟΠΟΙΗΣΗ ΕΛΕΓΧΩΝ ΑΠΟ ΑΝΕΝΕΡΓΕΣ ΣΥΣΚΕΥΕΣ ΠΕΛΑΤΩΝ

Ένας τρόπος που προτείνεται για την αντιμετώπιση κάποιας παρεμβολής που δέχεται κάποια συσκευή πελάτη κατά τη λήψη πακέτων από το σταθμό βάσης με τον οποίο είναι συσχετισμένη είναι η **πραγματοποίηση sensing από τις υπόλοιπες συσκευές πελατών** που βρίσκονται στην ίδια κυψέλη και παραμένουν εκείνη τη χρονική στιγμή **ανενεργές** αναμένοντας την αποστολή πακέτων από το σταθμό βάσης. Ο συγκεκριμένος μηχανισμός ενεργοποιείται, όπως και στην περίπτωση της υλοποίησης `sensing` μέσα στο `frame` που περιγράφηκε σε προηγούμενη παράγραφο, όταν κάποια από αυτές τις συσκευές εντοπίζει κάποια παρεμβολή κατά την λήψη των δεδομένων.

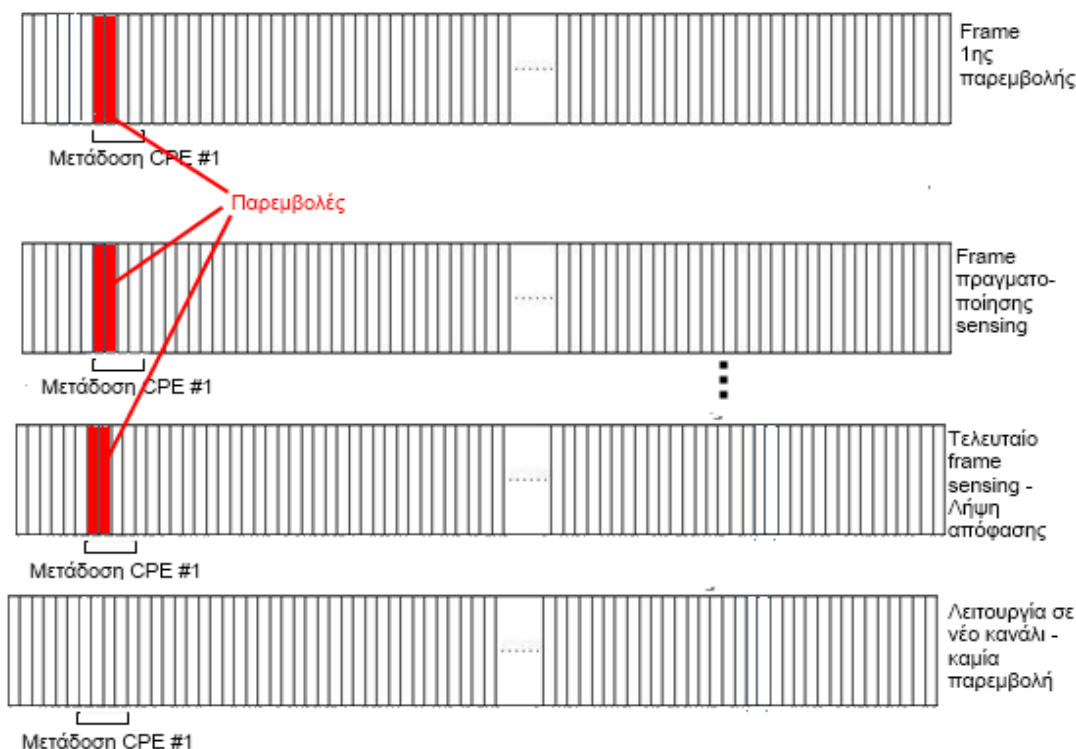
Όταν ενεργοποιηθεί ο συγκεκριμένος μηχανισμός, από το επόμενο `frame` και για **ορισμένο αριθμό frames**, ζητείται από τις υπόλοιπες συσκευές πελατών της κυψέλης να εντοπίσουν αν λαμβάνουν δεδομένα από άλλες πηγές πέρα από το σταθμό βάσης με τον οποίο είναι συσχετισμένες³⁶. Μετά το πέρας του ελέγχου, κάθε συσκευή συντάσσει μια αναφορά με τα αποτελέσματα που προκύπτουν, βάσει των οποίων, όπως θα διαπιστωθεί και στη συνέχεια, καθορίζονται οι απαιτούμενες ενέργειες.

Ο σταθμός βάσης είναι υπεύθυνος για τη συγκέντρωση των αναφορών στο τέλος κάθε `frame`. Εφόσον ένας αριθμός συσκευών αναφέρει ότι εντοπίστηκαν παρεμβολές, γεγονός που πιστοποιεί την ύπαρξη κάποιου επιτιθέμενου ο οποίος προσπαθεί να μειώσει την ποιότητα υπηρεσιών που προσφέρει η κυψέλη, η συσκευή που παρατήρησε πρώτη τις παρεμβολές παίρνει εντολή από το σταθμό βάσης να αναζητήσει για άλλο διαθέσιμο κανάλι στο οποίο θα συνεχιστεί η λειτουργία της κυψέλης χωρίς παρεμβολές. Θα πρέπει να τονιστεί ότι ο τύπος συσκευής που κάνει τις παρεμβολές δεν έχει κάποια σημασία, δεν χρησιμοποιείται ως κριτήριο για τον εντοπισμό της. Σχηματικά, ο τρόπος λειτουργίας αυτού του είδους `sensing` παριστάνεται στην παρακάτω εικόνα.

³⁴ Το πακέτο που αποστέλλεται είναι τύπου `Superframe Control Header (SCH)`, χωρίς να έχει ιδιαίτερη σημασία ο συγκεκριμένος τύπος πακέτου

³⁵ Υπάρχει ειδική συνθήκη ελέγχου στη συνάρτηση `recv` στο `mac-802_22.cc`

³⁶ Οι συσκευές πελατών όπως έχει προαναφερθεί επικοινωνεί μόνο με το σταθμό βάσης με τον οποίο είναι συσχετισμένες.



Εικόνα 22: Τρόπος λειτουργίας sensing από ανενεργές συσκευές. Στα slots που είναι σημειωμένα με κόκκινο είναι τα slots στα οποία οι υπόλοιπες συσκευές πελατών της κυψέλης θα πραγματοποιούν sensing μέχρι να ληφθεί η απόφαση από το σταθμό βάσης. Έπειτα από την αλλαγή του καναλιού δεν παρουσιάζονται παρεμβολές.

Πέρα από τη γενική προσέγγιση της λειτουργίας του αλγορίθμου, σημαντικό ενδιαφέρον παρουσιάζουν ορισμένα τεχνικά χαρακτηριστικά του αλγορίθμου που τον καταστούν ιδιαίτερα αποτελεσματικό:

- Ο συγκεκριμένος τρόπος πραγματοποίησης sensing, σε αντίθεση με αυτούς που προαναφέρθηκαν, παρουσιάζει το εξής σημαντικό πλεονέκτημα: Δεν επηρεάζει το throughput του δικτύου. Στις προαναφερθείσες προσεγγίσεις η μετάδοση δεδομένων μεταξύ των συσκευών πελατών και του σταθμού βάσης διακοπτόταν για να γίνει ο εντοπισμός της παρεμβολής. Τώρα όμως η μετάδοση των δεδομένων στο δίκτυο συνεχίζεται, έστω και αν οι παρεμβολές στις λήψεις πακέτων κάποιου ή κάποιων συσκευών πελατών εξακολουθούν να υπάρχουν³⁷. Τον εντοπισμό αναλαμβάνουν να τον κάνουν οι συσκευές πελατών που είναι ήδη ανενεργές, όσο οι υπόλοιπες εξακολουθούν να λαμβάνουν κανονικά δεδομένα. Συνεπώς, δεν προκαλείται επιπρόσθετη επιβάρυνση στη μετάδοση.
- Εφόσον ο εντοπισμός πραγματοποιείται από άλλες συσκευές πελατών της κυψέλης θα πρέπει αυτές με την σειρά τους εθελοντικά να καταναλώσουν περισσότερη ενέργεια για να συμβάλλουν με αυτό τον τρόπο στην εύρυθμη λειτουργία ολόκληρης της κυψέλης. Σημαντικός παράγοντας για την κατανάλωση ενέργειας είναι τόσο ο αριθμός των συσκευών πελατών που θα αναλάβουν να κάνουν sensing, όσο και ο χρόνος που θα χρειαστεί για να ληφθεί με μεγάλο βαθμό βεβαιότητας η απόφαση για την εκκίνηση της διαδικασίας αλλαγής καναλιού λειτουργίας της κυψέλης. Σημαντικό ρολό λαμβάνει και ο αριθμός των slots λήψης που επηρεάζονται από τις παρεμβολές του επιτιθέμενου. Η ενέργεια αποτελεί τον πιο σημαντικό παράγοντα αν συνυπολογιστεί και το γεγονός πως

³⁷ Αυτή είναι η μόνη περίπτωση που παρατηρείται στο throughput και είναι πολύ μικρή και γι' αυτό θεωρείται αμελητέα.

όλες αυτές οι λειτουργίες πραγματοποιούνται από κινητές συσκευές στις οποίες η υψηλή ενεργειακή αυτονομία αποτελεί σημαντική προτεραιότητα.

Με βάση την παραπάνω περιγραφή του αλγορίθμου, πραγματοποιείται αρχικά μια θεωρητική εκτίμηση της επιβάρυνσης της ενέργειας που προκαλείται στο σύστημα.

5.2.1 Θεωρητική εκτίμηση της κατανάλωσης ενέργειας

Σελίδα | 65

Έστω πως **δεν πραγματοποιείται καθόλου sensing** από τις υπόλοιπες συσκευές πελατών για τον εντοπισμό της παρεμβολής. Τότε, σε αυτή την περίπτωση, ο επιτιθέμενος συνεχίζει ανενόχλητος να παρεμβάλλεται και η επηρεαζόμενη συσκευή πελάτη να χάνει σταθερά δεδομένα καθ' όλη την διάρκεια της επίθεσης. Έστω:

- k : ο αριθμός των frames στα οποία παρεμβάλλεται ο επιτιθέμενος
- P_{RC} : η ενέργεια που αντιστοιχεί στη λήψη ενός πακέτου για ένα slot.

Όπως προαναφέρθηκε, καθώς ο επιτιθέμενος παρεμβάλλεται, δημιουργούνται συγκρούσεις (*collisions*) από τη μεριά της λήψης δεδομένων, προκαλώντας προβλήματα στη λήψη από τον σταθμό βάσης. Η απώλεια αυτή (που αποτελεί ουσιαστικά απώλεια πακέτων) προκαλεί και επιπλέον επιβάρυνση ενέργειας, που αντιστοιχεί όχι μόνο

- στην ενέργεια που χάνεται λόγω του collision, αλλά και
- στην επιπλέον ενέργεια που θα πρέπει να δαπανηθεί για την εκ νέου λήψη των χαμένων πακέτων.

Ειδικότερα, στο πρώτο frame (από τα k στα οποία θα διαρκεί η παρεμβολή), θα χάνεται ενέργεια που αντιστοιχεί στη διάρκεια του collision, που είναι πολλαπλάσια της διάρκειας ενός slot. Αντίθετα, από το επόμενο frame μέχρι και το τέλος της παρεμβολής, η ενέργεια που χάνεται θα είναι διπλάσια (ενέργεια collision και ενέργεια για την λήψη των χαμένων πακέτων). Με βάση τα παραπάνω, έστω:

- a : ο αριθμός των slots σε κάθε frame στα οποία προκαλείται παρεμβολή,
- τότε, για k frames, **η ενέργεια που χάνεται σε όλο το σύστημα είναι ίση με την ενέργεια που χάνει η συγκεκριμένη συσκευή πελάτη**, απώλεια που περιγράφεται από την παρακάτω σχέση:

$$aP_{RC} + 2(k-1)aP_{RC} = (2k-1)aP_{RC} \quad (1)$$

Έστω τώρα πως **πραγματοποιείται sensing από τις υπόλοιπες συσκευές πελατών** του δικτύου. Τα slots στα οποία γίνεται το sensing είναι και τα slots στα οποία διαπιστώνεται το collision από τη μεριά της συσκευής πελάτη – θύματος. Αν:

- P_{SENSE} : η ενέργεια που καταναλώνεται από μια συσκευή πελάτη για το sensing για ένα slot
- n : ο αριθμός των συσκευών πελατών που πραγματοποιούν sensing,

τότε, το κόστος για κάθε frame που δαπανείται για το sensing είναι $n \cdot a \cdot P_{SENSE}$. Επιπλέον, δαπανείται επιπρόσθετο κόστος σε κάθε frame για την ενημέρωση του σταθμού βάσης από τις συσκευές πελατών σχετικά με τα αποτελέσματα του sensing (διαδικασία αναφοράς - reporting). Θεωρώντας πως η διαδικασία της αναφοράς σε κάθε frame διαρκεί όσο ένα slot, τότε αν:

- P_{RT} : η ενέργεια που καταναλώνεται από μια συσκευή πελάτη για την αναφορά των αποτελεσμάτων σε κάθε frame

Το κόστος του reporting σε κάθε frame είναι $n \cdot P_{RT}$. Αν θεωρηθεί πως η διαδικασία του sensing διαρκεί λ frames (όπου $\lambda < k$), τότε οι συσκευές πελατών που κάνουν sensing καταναλώνουν συνολικά ενέργεια ίση με $n \cdot \lambda \cdot P_{SENSE} \cdot a + n \cdot \lambda \cdot P_{RT}$. Κατά τη διάρκεια του sensing, εξακολουθεί να χάνεται ενέργεια και από τη συσκευή πελάτη – θύματος λόγω του collision. Επομένως, σε αυτή την περίπτωση, η συνολική **ενέργεια που καταναλώνεται από το σύστημα** είναι:

Σελίδα | - 66 -

$$(2\lambda + 1)aP_{RC} + n\lambda(aP_{SENSE} + P_{RT})$$

Το sensing όμως που πραγματοποιείται στην ουσία είναι fine sensing, καθώς πρέπει να ταυτοποιηθεί αυτός που προκαλεί τις παρεμβολές. Συνεπώς, η ενέργεια που δαπανείται ισοδυναμεί με την ενέργεια που δαπανείται για τη λήψη ενός πακέτου κατά τη διάρκεια του sensing. Τα πακέτα που λαμβάνονται θα είναι τα πακέτα που στέλνει ο επιτιθέμενος, βάσει των οποίων εντοπίζεται η παρεμβολή. Επομένως $P_{SENSE} = P_{RC}$ και η σχέση ενέργειας αποκτά την **παρακάτω μορφή**:

$$(2\lambda + 1)aP_{RC} + n\lambda(aP_{RC} + P_{RT})(2)$$

Βάσει της παραπάνω σχέσης, θεωρείται πως το sensing εκκινεί στο επόμενο frame από την πρώτη φορά που γίνεται το collision. Επομένως, η απώλεια ενέργειας λόγω collision θα είναι $2\lambda aP_{RC} + aP_{RC} = (2\lambda + 1)P_{RC}$. Μετά από την πραγματοποίηση sensing για λ frames στα οποία εντοπίζεται η παρεμβολή, το δίκτυο αλλάζει κανάλι, με αποτέλεσμα να παύει να εμφανίζεται το collision. Για να είναι ωστόσο αποδεκτή η πραγματοποίηση του sensing, θα πρέπει η ενέργεια βάσει της (2) να είναι μικρότερη από την ενέργεια που προβλέπει η (1). Επομένως:

$$(2) < (1) \Rightarrow (2\lambda + 1)aP_{RC} + n\lambda(aP_{RC} + P_{RT}) < (2k - 1)aP_{RC} \Rightarrow$$

$$2\lambda aP_{RC} + aP_{RC} + n\lambda aP_{RC} + n\lambda P_{RT} < (2k - 1)aP_{RC} \Rightarrow$$

$$\lambda(2aP_{RC} + naP_{RC} + nP_{RT}) + aP_{RC} < (2k - 1)aP_{RC} \Rightarrow$$

$$\lambda(2aP_{RC} + naP_{RC} + nP_{RT}) < (2k - 2)aP_{RC} \xrightarrow{P_{RT} = iP_{RC}}$$

$$\lambda(2aP_{RC} + naP_{RC} + niP_{RC}) < (2k - 2)aP_{RC} \Rightarrow \lambda(2a + na + ni) < (2k - 2)a \Rightarrow$$

$$\lambda < \frac{(2k - 2)a}{a(2 + n) + ni} \quad (3)$$

Η αντικατάσταση του όρου P_{RT} με το iP_{RC} υποδηλώνει την κατανάλωση περισσότερης ενέργειας για την αναφορά των αποτελεσμάτων, παρά για τη λήψη ενός πακέτου. Με βάση την παραπάνω σχέση, για να υπάρχει κέρδος, το λ θα πρέπει να είναι μικρότερο από την τιμή που ορίζει η (3). Αν για παράδειγμα:

- προκαλείται collision λόγω παρεμβολών του επιτιθέμενου για 15 frames ($k=15$)
- η ενέργεια P_{RT} είναι διπλάσια από την ενέργεια P_{RC} ($i = 2$)
- μια συσκευή πελάτη του δικτύου πραγματοποιεί sensing ($n = 1$)
- γίνεται collision σε 3 slots σε κάθε frame ($a = 3$),

τότε ο μέγιστος αριθμός sensing λ (ή αλλιώς ο αριθμός των frames στα οποία οι υπόλοιπες συσκευές πελατών θα πραγματοποιούν sensing) θα είναι:

$$\lambda < \frac{(2 * 15 - 2) * 3}{3(2 + 1) + 1 * 2} \Rightarrow \lambda < \frac{84}{11} \Rightarrow \lambda_{\max} = 7$$

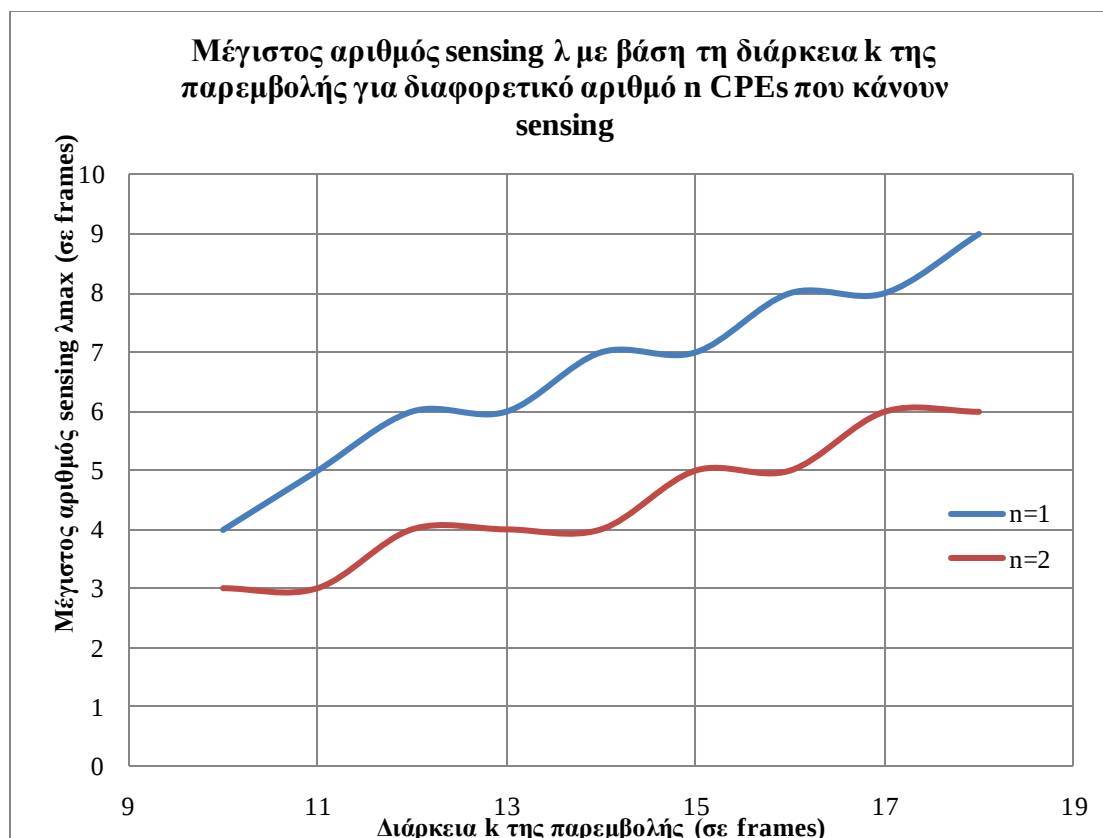
Επομένως, αν στο 7^ο frame δεν εντοπιστεί η παρεμβολή, τότε το sensing **δε χρειάζεται να πραγματοποιηθεί στο επόμενο frame**, καθώς θα προκληθεί ασύμφορα υψηλή απώλεια ενέργειας.

Σελίδα | 67

Βάσει της παραπάνω σχέσης, αλλάζοντας τις τιμές που καθορίζουν τις συνθήκες προσομοίωσης, υπολογίζεται **ο μέγιστος αριθμός των frames (λ)** στα οποία θα πρέπει να διαρκεί το sense για δεδομένη διάρκεια παρεμβολής. Τα αποτελέσματα που υπολογίστηκαν παριστάνονται στον παρακάτω πίνακα:

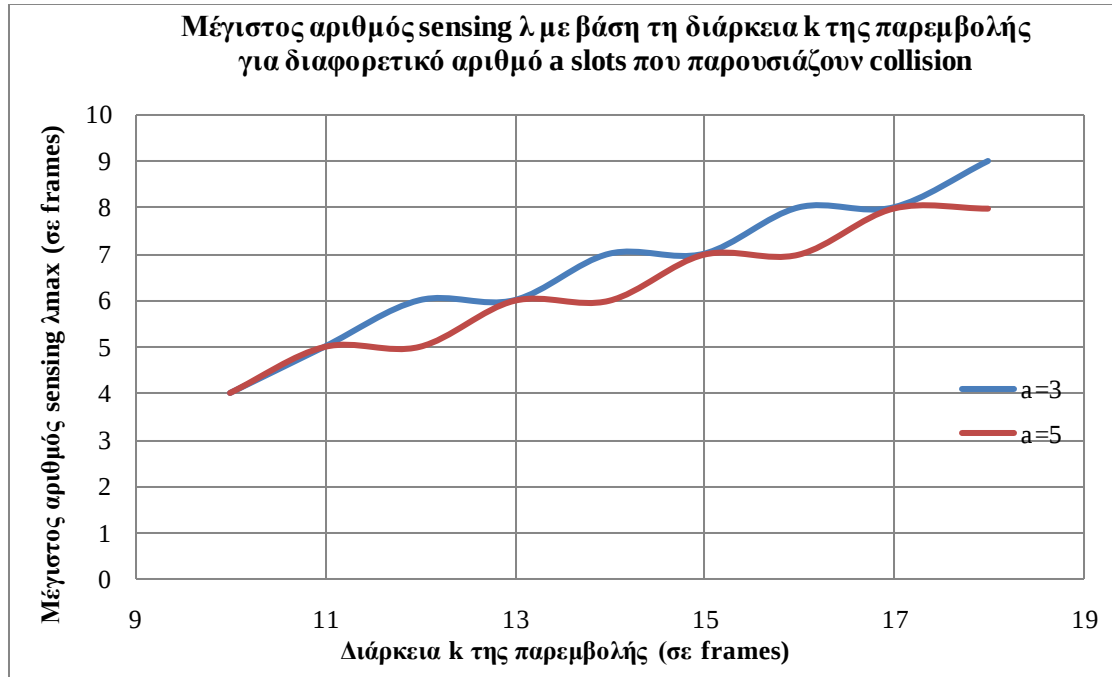
k	(i, n, a) = (2, 1, 3) $\lambda_{\max}$	(i, n, a) = (2, 2, 3) $\lambda_{\max}$	(i, n, a) = (2, 1, 5) $\lambda_{\max}$
10	4	3	4
11	5	3	5
12	6	4	5
13	6	4	6
14	7	4	6
15	7	5	7
16	8	5	7
17	8	6	8
18	9	6	8

Ενδιαφέρον παρουσιάζει η διακύμανση του λ για διαφορετικό αριθμό συσκευών πελατών που πραγματοποιούν sensing. Παρακάτω παρουσιάζεται η γραφική παράσταση του μέγιστου επιτρεπόμενου αριθμού sensing (σε frames), όπως έχει υπολογιστεί βάσει της (3), θεωρώντας πως ο επιτιθέμενος προκαλεί collision σε 3 slots κάθε frame ($a=3$) και πως η ενέργεια για το reporting είναι διπλάσια από την ενέργεια για τη λήψη ενός πακέτου ($i=2$). Στη μία περίπτωση (μπλε γραμμή), μια συσκευή πελάτη του δικτύου πραγματοποιεί sensing, ενώ η κόκκινη γραμμή αντιστοιχεί στην περίπτωση που το sensing πραγματοποιείται από δύο συσκευές πελατών του δικτύου. Μεγαλύτερος αριθμός των συσκευών πελατών που κάνουν sensing, συνεπάγεται και αυξημένη κατανάλωση ενέργειας, γεγονός που διαπιστώνεται και από τη χαμηλότερη επιτρεπόμενη τιμή του λ για $n=2$. Ωστόσο, η πραγματοποίηση sensing από περισσότερες συσκευές πελατών συνεπάγεται και αυξημένη ακρίβεια στον εντοπισμό της παρεμβολής, καθώς ορισμένες συσκευές πελατών λόγω της θέσης τους και της μικρότερης απόστασης από τον επιτιθέμενο είναι σε θέση να εντοπίσουν την παρεμβολή, κάτι που δεν θα ήταν δυνατό από συσκευές πελατών που βρίσκονται σε μεγαλύτερη απόσταση. Συνεπώς, θα πρέπει να εξασφαλιστεί μια **ισορροπία ανάμεσα στην κατανάλωση ενέργειας και στην ακρίβεια εντοπισμού της παρεμβολής**.



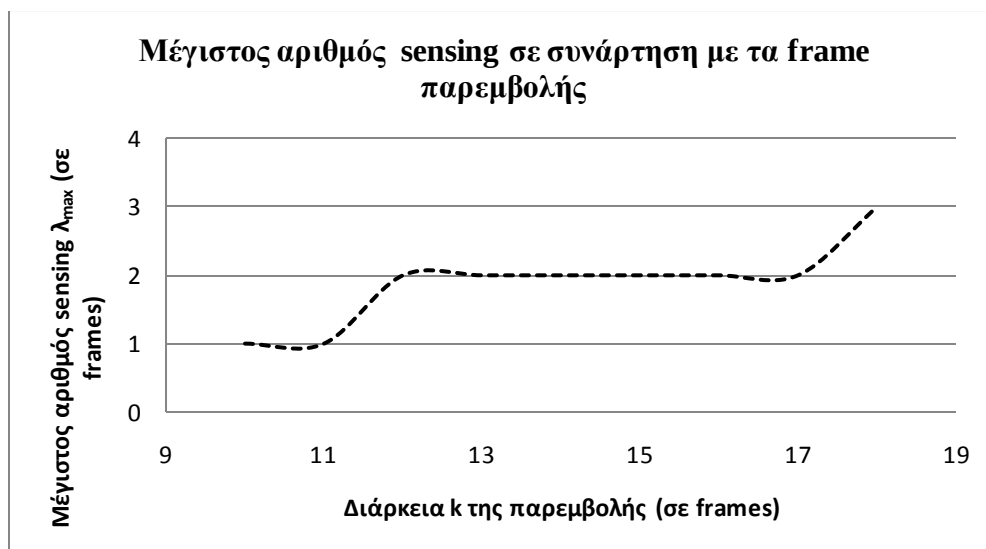
Εικόνα 23: Μέγιστος αριθμός sensing λ με βάση τη διάρκεια k της παρεμβολής για διαφορετικό αριθμό n CPEs που πραγματοποιούν sensing. Για τις υπόλοιπες παραμέτρους ισχύει $a=3$ και $i=2$

Αντίστοιχα, με βάση τα αποτελέσματα του παραπάνω πίνακα, προκύπτει και η παρακάτω γραφική παράσταση (Εικόνα 24) στην οποία παρουσιάζεται συγκριτικά η διακύμανση του λ στην περίπτωση που ο επιτιθέμενος προκαλεί collision σε 3 slots και σε 5 slots κάθε frame αντίστοιχα. Οι διαφορές που παρατηρούνται είναι σαφώς μικρότερες σε σχέση με την προηγούμενη γραφική παράσταση. Ωστόσο, διαπιστώνεται πως η **αύξηση της διάρκειας του collision** που προκαλεί ο επιτιθέμενος (με βάση των αριθμό των πακέτων που στέλνει σε κάθε frame) συνεπάγεται και ανάλογες **αυξημένες απαιτήσεις για γρηγορότερο εντοπισμό** της παρεμβολής από τις συσκευές πελατών.



Εικόνα 24: Μέγιστος αριθμός sensing λ με βάση τη διάρκεια k της παρεμβολής για διαφορετικό αριθμό slots στα οποία προκαλείται collision (3 και 5 αντίστοιχα) collision. Για τις υπόλοιπες παραμέτρους ισχύει $n=3$ και $i=2$

Τροποποιώντας κατάλληλα τις παραμέτρους k , λ , a και i , εξάγονται επιπλέον γραφικές παραστάσεις που απεικονίζουν τις απαιτήσεις για γρήγορο εντοπισμό της παρεμβολής σε περιπτώσεις που υπάρχουν **περισσότερες από 2 συσκευές πελατών στο δίκτυο**. Ειδικότερα, παρακάτω απεικονίζεται η γραφική παράσταση του μέγιστου αριθμού λ, βάσει της σχέσης (3), ο επιτιθέμενος πραγματοποιεί παρεμβολές σε ένα slot σε κάθε frame.



Εικόνα 25: Μέγιστος αριθμός sensing λ με βάση τη διάρκεια k της παρεμβολής για διαφορετικό αριθμό slots με τις παραμέτρους n , a και i να έχουν τις τιμές 3,1 και 2 αντίστοιχα

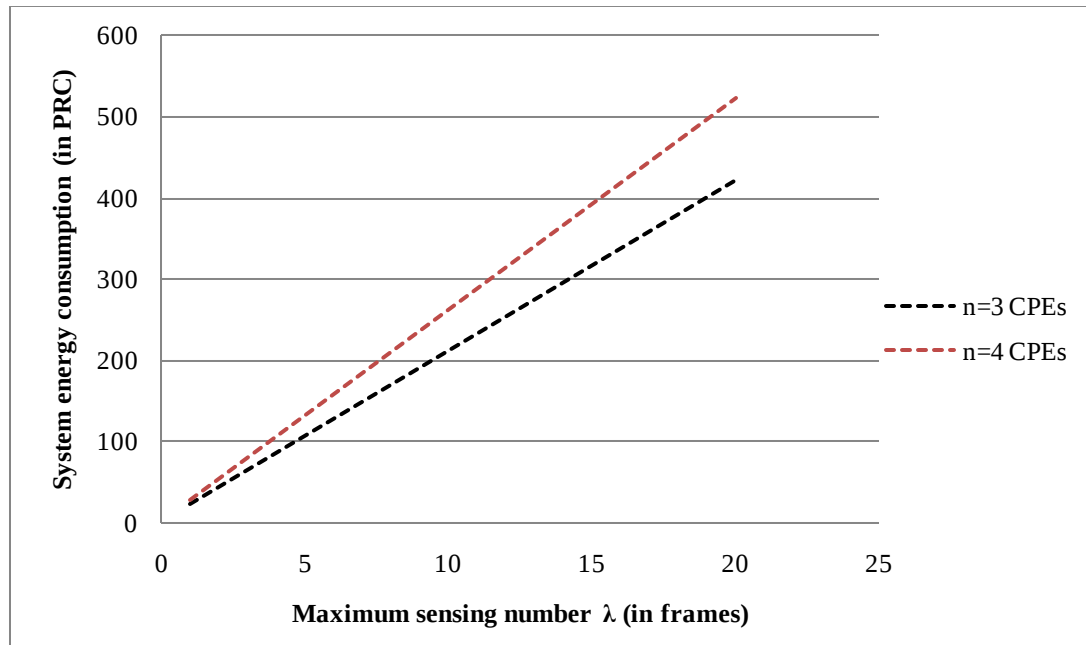
- Λόγω της αυξημένης κατανάλωσης ενέργειας με την παρουσία περισσότερων CPEs εντός δικτύου, απαιτείται να εντοπιστεί η παρεμβολή σε πολύ μικρότερο αριθμό σε σχέση με την περίπτωση της Εικόνα 23. Πέρα όμως από τη θεωρητική εκτίμηση του μέγιστου επιτρεπόμενου αριθμού sensing, ενδιαφέρον παρουσιάζει και η εκτίμηση της ενέργειας που καταναλώνει το σύστημα για διαφορετικό $\lambda_{\max}$ και για διαφορετικό αριθμό CPEs

εντός του κελιού. Αντικαθιστώντας στη σχέση (2) τον όρο PRT με το iPRC, προκύπτει η παρακάτω σχέση για τη θεωρητική εκτίμηση της ενέργειας E, σε πολλαπλάσια του PRC.

$$E = [n(a + 1) + a(2\lambda + 1)]P_{RC}$$

Αρχικοποιώντας τις παραμέτρους με τις ίδιες τιμές όπως και στην περίπτωση της Εικόνα 25 (a=3 και i=2), προκύπτει η παρακάτω γραφική παράσταση:

Σελίδα | - 70 -



Εικόνα 26: Κατανάλωση ενέργειας του συστήματος σε συνάρτηση με το μέγιστο αριθμό των frames που πραγματοποιείται sensing για διαφορετικό αριθμό συσκευών πελατών σε ένα κελί. Για τις υπόλοιπες παραμέτρους ισχύει a=3 και i=2

5.2.2 Λειτουργία του επιτιθέμενου

Έχοντας αναλύσει την πλευρά των έννομων χρηστών της κυψέλης θα πρέπει να παρουσιαστεί και ο τρόπος λειτουργίας του επιτιθέμενου. Ο επιτιθέμενος προκαλεί παρεμβολές κατά τη διάρκεια λήψης δεδομένων μέσω μιας ή περισσότερων συσκευών πελατών. Οι παρεμβολές αυτές προκαλούνται από πακέτα χωρίς σημαντική αξία, των οποίων σκοπός είναι η δημιουργία προβλημάτων σε κάποια συσκευή όσον αφορά την αποτελεσματική λήψη των πακέτων που αποστέλλονται από τον συσχετιζόμενο ένομο σταθμό βάσης. Σημειώνεται ότι ο επιτιθέμενος και σε αυτή την περίπτωση **δεν αποστέλλει πακέτα κατά την διάρκεια του fast sensing** που πραγματοποιείται στο τέλος κάθε frame.

5.2.3 Περιγραφή του αλγορίθμου

Παρακάτω φαίνεται η περιγραφή του αλγορίθμου για τις έννομες οντότητες της κυψέλης με μορφή ψευδοκώδικα:

Περιγραφή λειτουργίας Αλγορίθμου C (adaptive sensing). Ο αλγόριθμος περιγράφεται ξεχωριστά για τον σταθμό βάσης και για τη συσκευή πελάτη.

```
BS{
//n: ο αριθμός των συσκευών πελατών που κάνουν sensing
//b: η συσκευή πελάτη που εντόπισε πρώτη την παρεμβολή
//λ: αριθμός frame που γίνεται έλεγχος μέχρι να παρθεί απόφαση
Αν (τύπος_sensing == adaptive){
    foreach frame_end{
        m = Αριθμός_συσκευών_πελατών_που_ανέφεραν_παρεμβολή();
```

```

        Av ( m == n){
            μετρητής_frame_ελέγχου++;
        }
        Av (μετρητής_frame_ελέγχου == λ){
            καινούριο_κανάλι = Εύρεση_ελεύθερου_καναλιού(b);
            Αλλαγή_καναλιού(καινούριο_κανάλι);
        }
    }
}
}

CPE{
    Av (τύπος_sensing == adaptive){
        Av (is_idle == true){
            Πραγματοποίηση_sensing(slots_ελέγχου);
            Δημιουργία_αναφοράς();
        }
        Αλλιώς
            συνέχισε;
    }
    Αλλιώς{
        Av (λήψη_πακέτων_χωρίς_παρεμβολές == true)
            συνέχισε;
        Αλλιώς{
            τύπος_sensing = adaptive;
            slots_ελέγχου = Αρχικοποίηση_slots_ελέγχου();
            μετρητής_frame_ελέγχου = 0;
            b = MAC_ADDR;
        }
    }
}
}

```

5.2.4 Υλοποίηση στον ns-2

Για να οριστεί η χρήση αυτού του είδους sensing στο αρχείο TCL που θα χρησιμοποιηθεί για την εξομοίωση θα πρέπει να γίνει η ακόλουθη δήλωση:

```
Mac/802_22 set sensing_type_ 3
```

όπου η τιμή «3» δηλώνει το είδος sensing, σε συνδυασμό με την δήλωση που υπάρχει στο αρχείο “mac-802_22.cc”:

```
bind("sensing_type_", &sensing_type_);
```

που ουσιαστικά αντιστοιχίζει τις δυο αυτές μεταβλητές. Έτσι η απαριθμητή μεταβλητή sensingType που ορίζεται στο αρχείο mac-802_22.h παίρνει την τιμή που αντιστοιχεί στο «3» που είναι ADAPTIVE.

Για τον **εντοπισμό της παρεμβολής** που δημιουργεί ο επιτιθέμενος στην κυσέλη κατά την λήψη των πακέτων των συσκευών των πελατών από το σταθμό βάσης χρησιμοποιείται ο ίδιος μηχανισμός που αναλύθηκε προηγουμένως για το in-frame sensing, δηλαδή **ο μηχανισμός της ταυτοποίησης της πηγής αποστολής του πακέτου**. Έτσι, αν κάποια συσκευή πελάτη λάβει κάποιο πακέτο από πηγή εκτός κυσέλης τίθεται η boolean μεταβλητή receive αποκτά την τιμή true. Αν ληφθεί κάποιο πακέτο από τον σταθμό βάσης με τον οποίο είναι συσχετισμένη αυτή τη συσκευή όσο αυτή η μεταβλητή είναι true, δημιουργείται συμφόρηση (congestion), με αποτέλεσμα να απορριφθεί το πακέτο που θα έπρεπε να λάβει

κανονικά η συσκευή πελάτη από τον σταθμό βάσης. Η εμφάνιση συμφόρησης πυροδοτεί το μηχανισμό για το adaptive sensing, ενημερώνοντας τις υπόλοιπες συσκευές πελατών της κυψέλης να πραγματοποιήσουν sensing έτσι ώστε να εντοπιστεί ο επιτιθέμενος. Οι υπόλοιπες συσκευές πελατών μόλις ειδοποιηθούν προγραμματίζουν, με τη βοήθεια ενός timer, την εκκίνηση του sensing στο επόμενο frame. Το sensing ωστόσο, όπως έχει αναφερθεί, δεν πραγματοποιείται σε όλο το μήκος του frame, αλλά για τα slots στα οποία έχει παρατηρηθεί η παρεμβολή. Επομένως, για να εντοπιστεί η παρεμβολή, κάθε συσκευή πελάτη που έχει ενημερωθεί, εκκινεί το sensing στο αμέσως προηγούμενο slot από εκείνο στο οποίο διαπιστώθηκε η παρεμβολή στα προηγούμενα frames. Ο καθορισμός της χρονικής στιγμής που θα πραγματοποιηθεί το sensing από τις συσκευές πελατών, έτσι ώστε να πραγματοποιείται στα slots στα οποία παρατηρήθηκε η συμφόρηση αποτελεί σημαντικό χαρακτηριστικό του αλγορίθμου, αυξάνοντας τις πιθανότητες εντοπισμού της παρεμβολής. Αντίστοιχα, αν ο επιτιθέμενος προκαλέσει παρεμβολές σε περισσότερα από ένα πακέτα, τότε προγραμματίζονται πολλαπλοί timers, χρησιμοποιώντας έναν πίνακα από timers. Όσα περιγράφονται σε αυτή την παράγραφο φαίνονται στο παρακάτω τμήμα κώδικα.

Πυροδότηση της λειτουργίας του adaptive sensing όπως έχει οριστεί στην συνάρτηση `recv()` του αρχείου `mac-802_22.cc`

```
if(received && actualNetCell->collided < attacks_per_frame_ ) {
    if((actualNetCell->scanningPhase == IDLE || actualNetCell-
>scanningPhase == DYNAMIC_SENSING)){
        drop(p, DROP_MAC_COLLISION);
        actualNetCell->collided++;
        if(sensingType == ADAPTIVE){
            dynamicSensingStart[actualNetCell->collided-1]-
>resched(FrameLength + FAST_SENSING_DURATION - slot_size);
        }
    }
}
```

Όπως αναφέρθηκε στη θεωρητική περιγραφή του αλγορίθμου, όταν εντοπιστεί κάποια παρεμβολή, αλλάζει η φάση sensing, μεταβαίνοντας στη φάση που πραγματοποιείται ο δυναμικός αυτός τρόπος sensing (*adaptive sensing*). Η μετάβαση αυτή πραγματοποιείται όταν λήξει ο timer που φαίνεται στο παραπάνω τμήμα κώδικα. Η συνάρτηση `startDynamicSensing` είναι ο handler του συγκεκριμένου timer που πυροδοτείται όταν φτάσει στη λήξη.

Αλλαγή φάσης sensing μέσα στην συνάρτηση `startDynamicSensing` του αρχείου `mac-802_22.cc`

```
void Mac802_22::startDynamicSensing()
{
    if((actualNetCell->scanningPhase == IDLE || actualNetCell-
>scanningPhase == DYNAMIC_SENSING)){
        actualNetCell->scanningPhase = DYNAMIC_SENSING;
    }
}
```

Από την στιγμή που η κυψέλη έχει εισέλθει σε αυτή την φάση sensing, όλες οι συσκευές πελατών, πέρα από αυτή που λαμβάνει (και είναι αποθηκευμένη στην μεταβλητή `actualNetCell->CPE_Sensor`), ελέγχουν την πηγή των πακέτων που δέχονται στα slots που έχουν οριστεί από τις συσκευές πελατών που εντόπισαν συμφόρηση κατά τη λήψη δεδομένων. Έτσι, κάθε φορά που δέχονται κάποιο πακέτο ενώ βρίσκονται σε αυτή την φάση, αφού ελέγξουν την πηγή, μπορούν να αποφανθούν αν πρόκειται ή όχι για παρεμβολή. Σημαντική είναι και η ενημέρωση για τα αποτελέσματα του sensing που πραγματοποιήθηκε. Αυτό γίνεται μέσω μιας δομής τύπου `CpeInfo` που έχει δημιουργηθεί προηγουμένως από το σταθμό βάσης, και η οποία, όπως μαρτυρά και η ονομασία της, περιέχει πληροφορίες που αφορούν μόνο τις συσκευές πελατών, όπως:

- η γεωγραφική θέση της κάθε συσκευής
- η MAC διεύθυνσή της
- η πληροφορία που συμπληρώνει καθεμιά από αυτές σχετικά με την τα αποτελέσματα του sensing

Η δομή αυτή συμπληρώνεται μια φορά από κάθε συσκευή πελάτη για κάθε περίοδο sensing. Αν κάποια από τις συσκευές πελατών που κάνουν sensing εντοπίσει κάποια παρεμβολή, τότε θέτουν την boolean μεταβλητή `recv_response` με την τιμή `true`.

Σελίδα | 73

Συμπεριφορά των συσκευών πελατών που πραγματοποιούν sensing. (τμήμα της συνάρτησης `recv()` του αρχείου `mac-802_22.cc`

```

if(actualNetCell->scanningPhase == DYNAMIC_SENSING ){
    if(NodeID != actualNetCell->CPE_Sensor) {
        src = mac->macSA();
        if( src != ((WirelessPhy*)netif_)->wirelessNode()-
>base_stn()){
            actualNetCell->scan_status_.recvd_response=true;
            if(!gotResponse){
                gotResponse = true;
                cpeinfo = actualNetCell->SsInfo_head;
                while (cpeinfo) {
                    if(cpeinfo->MacAddr == NodeID)
                        cpeinfo->recv_response = true;
                    cpeinfo = cpeinfo->next;
                }
            }
        }
    }
}

```

Στο τέλος κάθε frame ο σταθμός βάσης θα πρέπει, εξετάζοντας τις πληροφορίες που θα έχουν συγκεντρωθεί από τις συσκευές των πελατών, να βγάλει το συμπέρασμα αν υπάρχουν όντως παρεμβολές από κάποιον επιτιθέμενο ή όχι. Ο **κανόνας απόφασης** σύμφωνα με τον οποίο θα πρέπει να βγάλει αυτό το συμπέρασμα είναι ο ακόλουθος: «*Αν όλες οι συσκευές πελατών της κυψέλης ανέφεραν ότι εντόπισαν παρεμβολές τότε όντως πρόκειται για κάποιο επιτιθέμενο*». Βέβαια θα πρέπει να τονιστεί δεν αρκεί να διαπιστωθεί αυτό μόνο μια φορά έτσι ώστε να υπάρχει βεβαιότητα ότι πρόκειται για κάποιον επιτιθέμενο. Ο έλεγχος θα πρέπει να επαναληφθεί κάποιες φορές (συγκεκριμένα λ φορές, σύμφωνα με αυτά που αναφέρθηκαν στην προηγούμενη παράγραφο) έτσι ώστε να υπάρχει μεγαλύτερη σιγουριά αλλά χωρίς να ξεπεραστεί το όριο κατανάλωσης ενέργειας. Εφόσον επαληθευτεί αυτό για λ φορές τότε ο σταθμός βάσης δίνει εντολή στη συσκευή πελάτη που εντόπισε πρώτη παρεμβολή κατά τη λήψη πακέτων να ψάξει για ελεύθερο κανάλι έτσι ώστε η λειτουργία όλης της κυψέλης να συνεχιστεί σε αυτό χωρίς παρεμβολές. Σημειώνεται ότι ο αριθμός λ ορίζεται στο αρχείο `TCL` με την δήλωση:

- `Mac/802_22 set l_ 3`

και μέσω της αντιστοίχισης αυτής με την μεταβλητή `l_` του αρχείου `mac-802_22.cc` που γίνεται με δήλωση παρόμοια με τον ορισμό του `sensing_type_` που αναφέρθηκε παραπάνω.

5.3 ΣΥΓΚΡΙΣΗ ΑΛΓΟΡΙΘΜΩΝ ΜΕ ΒΑΣΗ ΤΙΣ ΑΠΩΛΕΙΕΣ ΔΕΔΟΜΕΝΩΝ

Έχοντας περιγράψει όλους τους τρόπους εντοπισμού επιτιθέμενων επιλέχθηκε να γίνει μια συγκριτική μελέτη αυτών που θα έχει ως σκοπό να κρίνει την αποτελεσματικότητά κάθε

αλγόριθμοι βάσει των απωλειών σε δεδομένα που παρουσιάζονται. Για αυτό το λόγο οργανώθηκε μια σειρά προσομοιώσεων όπου χρησιμοποιούνται και οι τρεις αλγόριθμοι εντοπισμού. Αυτά τα **σενάρια** διαφοροποιούνται ως προς τον τρόπο με τον οποίο δρα ο επιτιθέμενος. Συγκεκριμένα:

1. Στο πρώτο σενάριο ο επιτιθέμενος επηρεάζει τρία συνεχόμενα slots λήψεων μιας μόνο συσκευής πελάτη.
2. Στο δεύτερο η μόνη διαφορά σε σχέση με το πρώτο είναι ότι τα slots αυτά είναι τυχαία.
3. Στο τρίτο χάνονται πέντε συνεχόμενα slots λήψεων που ανήκουν σε δυο συσκευές πελατών.
4. Στο τέταρτο χάνονται τυχαία slots από δυο συσκευές πελατών.

Σελίδα | - 74 -

Σε αυτό το σημείο αξίζει να γίνει μια αναφορά στον **τρόπο με τον οποίο υλοποιείται η επίθεση** στα σενάρια αυτά στον ns-2. Τόσο στην περίπτωση των τυχαίων επιθέσεων (*σενάρια 2 και 4*), όσο και στην περίπτωση των συνεχόμενων (*σενάρια 1 και 3*), η επίθεση γίνεται με τον προγραμματισμό `timers` πριν αρχίσει το κάθε frame (με την εκπνοή του preamble μέσω της συνάρτησης `PreambleTimerHandler`). Η μόνη διαφοροποίηση των επιμέρους σεναρίων εντοπίζεται στον τρόπο με τον οποίο προγραμματίζονται κάθε φορά αυτοί οι `timers`. Επειδή οι παρεμβολές είναι περισσότερες από μια σε κάθε frame προγραμματίζεται ένας πίνακας από `timers`. Έτσι στα σενάρια των συνεχόμενων επιθέσεων του πρώτου σεναρίου οι `timers` αυτοί εκκινούν σε χρόνο πολλαπλάσιο της διάρκειας ενός συμβόλου (`SymbolLength`), αλλά μετά το πέρας όμως της μετάδοσης των ULMAP και DLMP που μεταδίδονται στα δυο πρώτα σύμβολα του κάθε frame. Η μόνη διαφοροποίηση μεταξύ των σεναρίων 1 και 3 τη στιγμή εκκίνησης της παρεμβολής, η οποία, στην περίπτωση του σεναρίου 3, τοποθετείται στο τέλος των λήψεων της πρώτης συσκευής πελάτη και ειδικότερα στα 2-3 τελευταία πακέτα που λαμβάνει η πρώτη συσκευή για να συνεχιστεί στην αρχή των λήψεων της δεύτερης συσκευής πελάτη που ακολουθεί. Η περιγραφόμενη λειτουργία παριστάνεται στο παρακάτω τμήμα κώδικα:

Προγραμματισμός επίθεσης του επιτιθέμενου σε συνεχόμενα slots, όπως έχει οριστεί στην συνάρτηση `PreambleTimerHandler` του αρχείου `mac-802_22.cc`

```
if(CPEs_to_attack_ == 1)
    rnd = i+1;
else if(CPEs_to_attack_ == 2)
    rnd = i+8;
attackTimer[i]->resched(2*SymbolLength + rnd*slot_size);
i++;
```

Αξίζει να σημειωθεί ότι η μεταβλητή `i` μετράει τον αριθμό των επιθέσεων που θα κάνει ο επιτιθέμενος, ενώ η `rnd` ορίζει το slot στο οποίο θα πραγματοποιείται η επίθεση. Όπως φαίνεται και στον κώδικα, η `rnd` αποκτά την τιμή της `i` αυξανόμενη κατά μια ακέραια τιμή, ικανοποιώντας τις απαιτήσεις των σεναρίων 1 και 3 περί επιθέσεων σε διαδοχικά slots. Η μεταβλητή `CPEs_to_attack_` ορίζεται στο αρχείο TCL, που αντιστοιχίζεται με την αντίστοιχη μεταβλητή στο αρχείο `mac-802_22.cc`, και όπως μαρτυρά το όνομα της ορίζει τον πλήθος των συσκευών πελατών που θα επηρεαστούν από την επίθεση του επιτιθέμενου.

Στην περίπτωση που οι επιθέσεις είναι τυχαίες, τα slots στα οποία θα γίνει η επίθεση επιλέγονται τυχαία μέσω μιας κανονικής κατανομής. Στο δεύτερο σενάριο, όπου ο επιτιθέμενος παρεμβάλλεται στη λήψη μιας συσκευής πελάτη οι θέσεις των slots επιλέγονται τυχαία από το διάστημα [1, 9] ενώ στην περίπτωση του τέταρτου σεναρίου όπου οι συσκευές πελατών που επηρεάζονται είναι δυο, το εύρος από το οποίο επιλέγονται οι αριθμοί είναι το [1, 17].

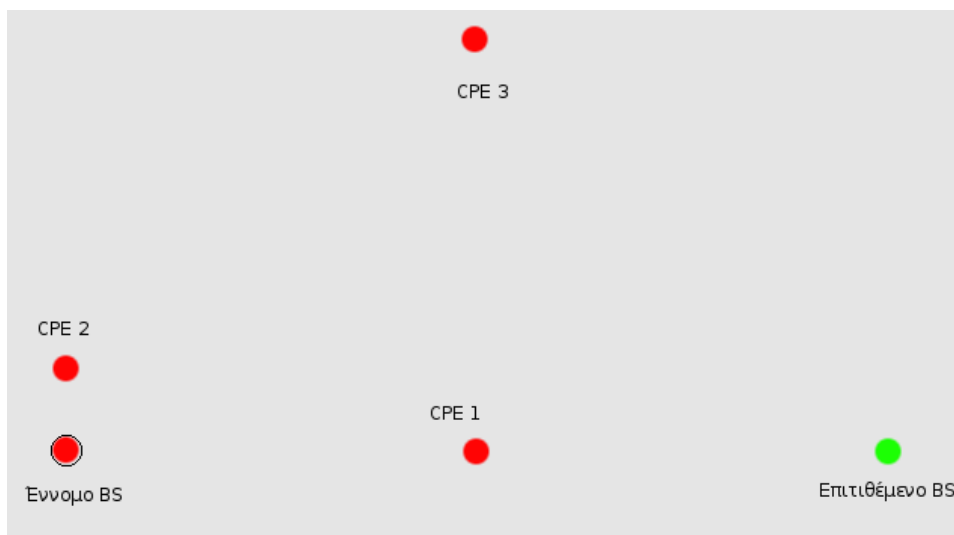
Προγραμματισμός επίθεσης του επιτιθέμενου σε τυχαία slots, όπως έχει οριστεί στην συνάρτηση PreambleTimerHandler του αρχείου mac-802_22.cc

```
while (i<attacks_per_frame_){
    if(random_attack_ == 1){
        if(CPEs_to_attack_ == 1)
            rnd = Random::uniform(1, 9);
        else if(CPEs_to_attack_ == 2)
            rnd = Random::uniform(1, 17);
        fprintf(fp, "Random1: %d\n", rnd);
    }
    attackTimer[i]->resched(2*SymbolLength + rnd*slot_size);
    i++;
}
```

Σελίδα | 75

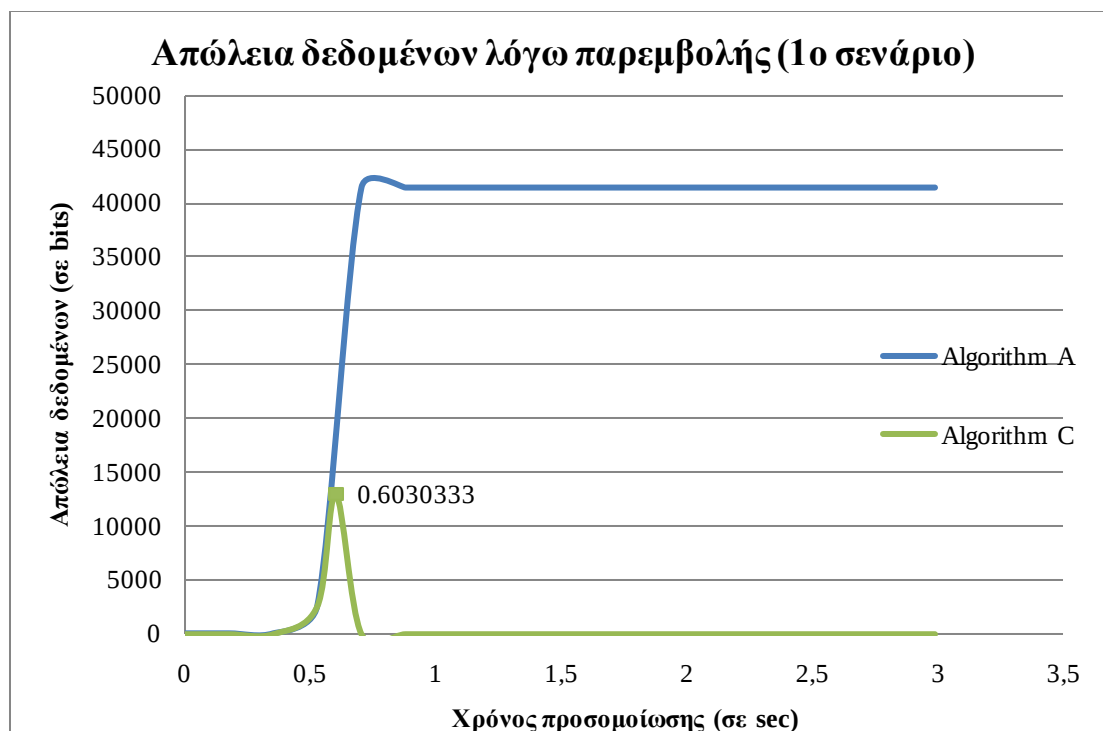
Όπως και στο προηγούμενο τμήμα κώδικα, η μεταβλητή `rnd` αποθηκεύει το slot στο οποίο γίνεται η παρεμβολή, η οποία σε αυτή την περίπτωση δεν είναι γραμμική του `i`, αλλά τυχαία. Η μεταβλητή `random_attack_` ορίζει κάθε φορά ποια από τις δυο ομάδες σεναρίων θα εκτελεστεί με την προσομοίωση, με την τιμή `true` να αντιστοιχεί στα σενάρια 2 και 4 και τη `false` στα σενάρια 1 και 3, όπου γίνονται επιθέσεις σε διαδοχικά slots και όχι τυχαία.

Για το σύνολο των προσομοιώσεων **χρησιμοποιήθηκε η ίδια τοπολογία**, έτσι ώστε να είναι αντικειμενική η κρίση των τριών αλγορίθμων. Η τοπολογία αυτή φαίνεται στην παρακάτω εικόνα. Η τοπολογία αυτή προσομοιώνει μια περιοχή 25 τετραγωνικών χιλιομέτρων.



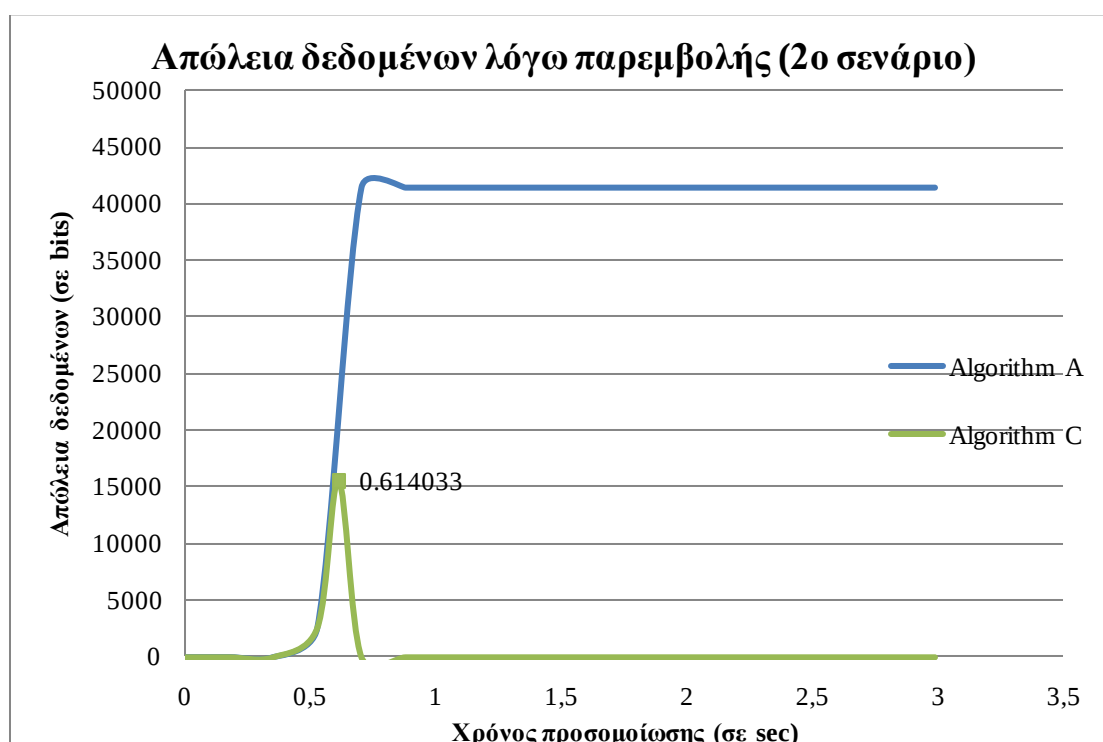
Εικόνα 27: Τοπολογία με την οποία πραγματοποιούνται οι προσομοιώσεις

Τα **αποτελέσματα των προσομοιώσεων** παρουσιάζονται στις παρακάτω γραφικές παραστάσεις. Οι αριθμοί που σημειώνονται πάνω στις γραφικές παραστάσεις είναι οι χρόνοι στους οποίους γίνεται αλλαγή του καναλιού λειτουργίας της κυψέλης.

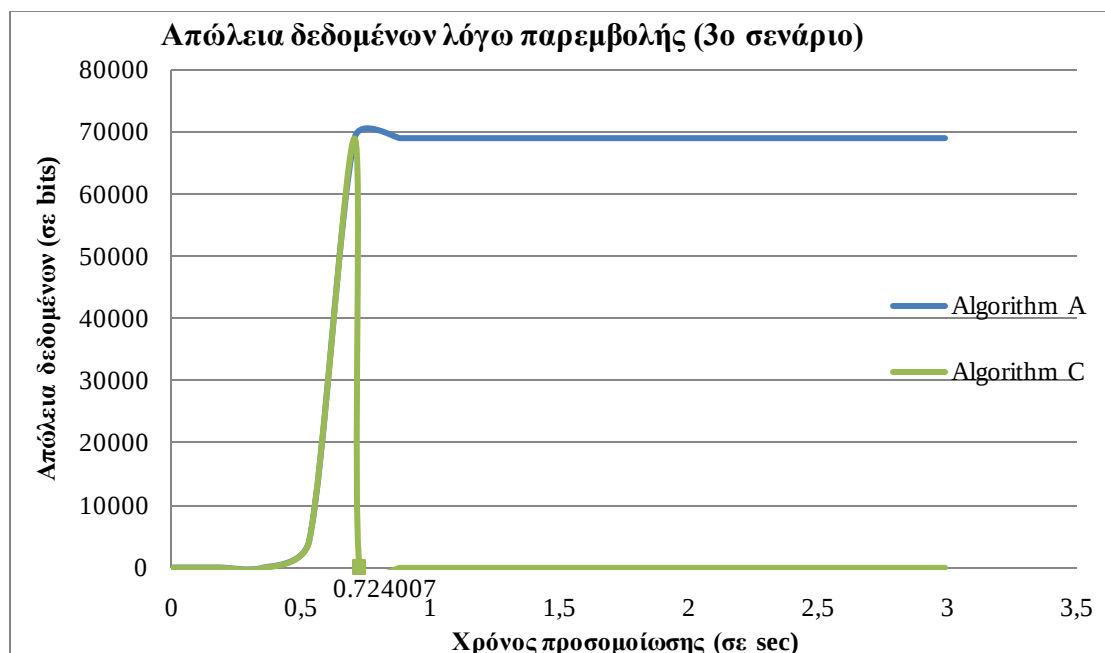


Σελίδα | - 76 -

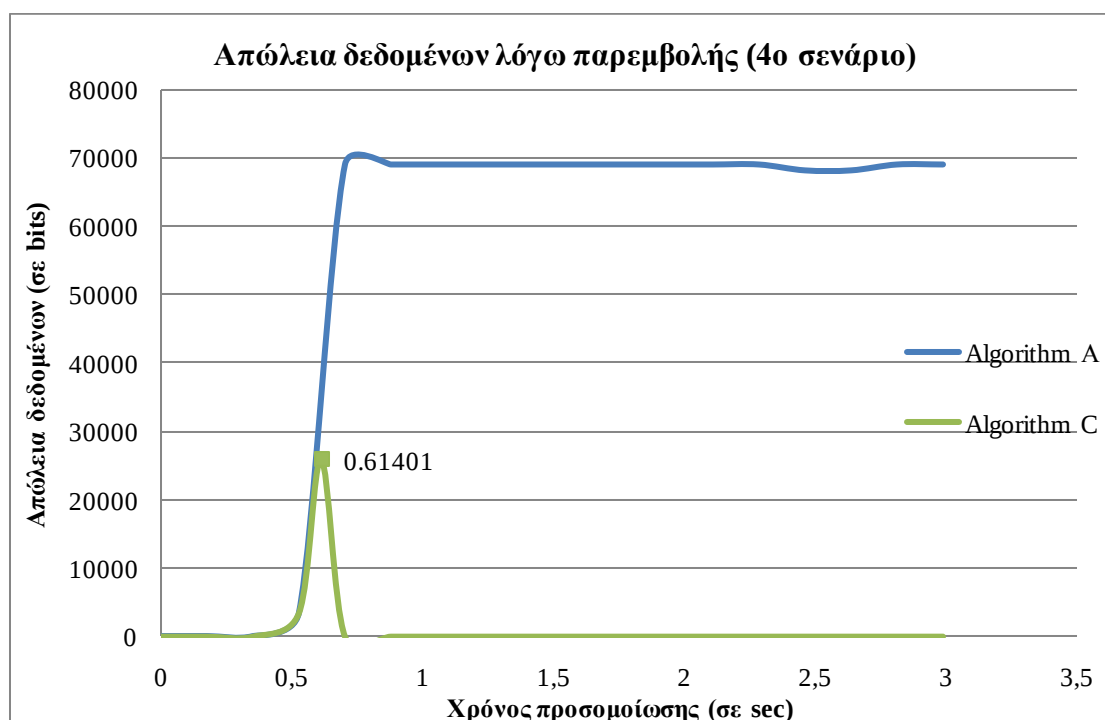
Εικόνα 28: Απώλεια δεδομένων σε bits όπως μετρήθηκε με την εκτέλεση του πρώτου σεναρίου προσομοίωσης



Εικόνα 29: Απώλεια δεδομένων σε bits, όπως μετρήθηκε με την εκτέλεση του δεύτερου σεναρίου προσομοίωσης. Παρατηρείται πως το σχήμα της γραφικής παράστασης διαφέρει ελάχιστα από την προηγούμενη



Εικόνα 30: Απώλεια δεδομένων σε bits, όπως μετρήθηκε με την εκτέλεση του τρίτου σεναρίου προσομοίωσης.



Εικόνα 31: Απώλεια δεδομένων σε bits, όπως μετρήθηκε με την εκτέλεση του τέταρτου σεναρίου προσομοίωσης.

5.3.1 Σχολιασμός αποτελεσμάτων

Παρατηρώντας τις γραφικές παραστάσεις διαπιστώνεται ότι στον πρώτο αλγόριθμο υπάρχει **μια σταθερή απώλεια δεδομένων** καθ' όλη τη διάρκεια και των τεσσάρων σεναρίων. Αυτό οφείλεται στον έξυπνο τρόπο με τον οποίο λειτουργεί ο επιτιθέμενος καθιστώντας αδύνατο τον εντοπισμό του με τη συγκεκριμένη υλοποίηση του αλγορίθμου. Ο επιτιθέμενος δεν αποστέλλει πακέτα κατά την διάρκεια του fast και του fine sensing που είναι οι μόνοι μηχανισμοί που χρησιμοποιούνται σε αυτή την περίπτωση για τον εντοπισμό των παρεμβολών. Αυτό έχει ως αποτέλεσμα το δίκτυο να αδυνατεί να εντοπίσει την παρουσία του

επιτιθέμενου, έτσι ώστε να ξεκινήσει ο μηχανισμός αλλαγής του καναλιού, χάνοντας με αυτόν τον τρόπο σταθερό αριθμό πακέτων σε κάθε frame, όπως φαίνεται και στο τμήμα των γραφικών παραστάσεων με την ευθεία γραμμή (μπλε χρώμα).

Ο άλλος αλγόριθμος όμως, λόγω του δυναμικού τρόπου πυροδότησης των ελέγχων για τον εντοπισμό επιτιθέμενων, **καταφέρνει να εντοπίσει τον επιτιθέμενο**. Όπως φαίνεται και από τις γραφικές παραστάσεις, με την εφαρμογή του adaptive sensing σε χρόνο μικρότερο από ένα δευτερόλεπτο, η επίθεση όχι μόνο έχει εντοπιστεί, αλλά η κυνέλη έχει αλλάξει και κανάλι λειτουργίας, έτσι ώστε να μην υπάρχουν πλέον παρεμβολές από τον επιτιθέμενο. Επιπλέον, με τη χρήση του adaptive sensing, στο σύνολο των περιπτώσεων, οι απώλειες δεδομένων παραμένουν σε πολύ μικρά επίπεδα.

Σελίδα | - 78 -

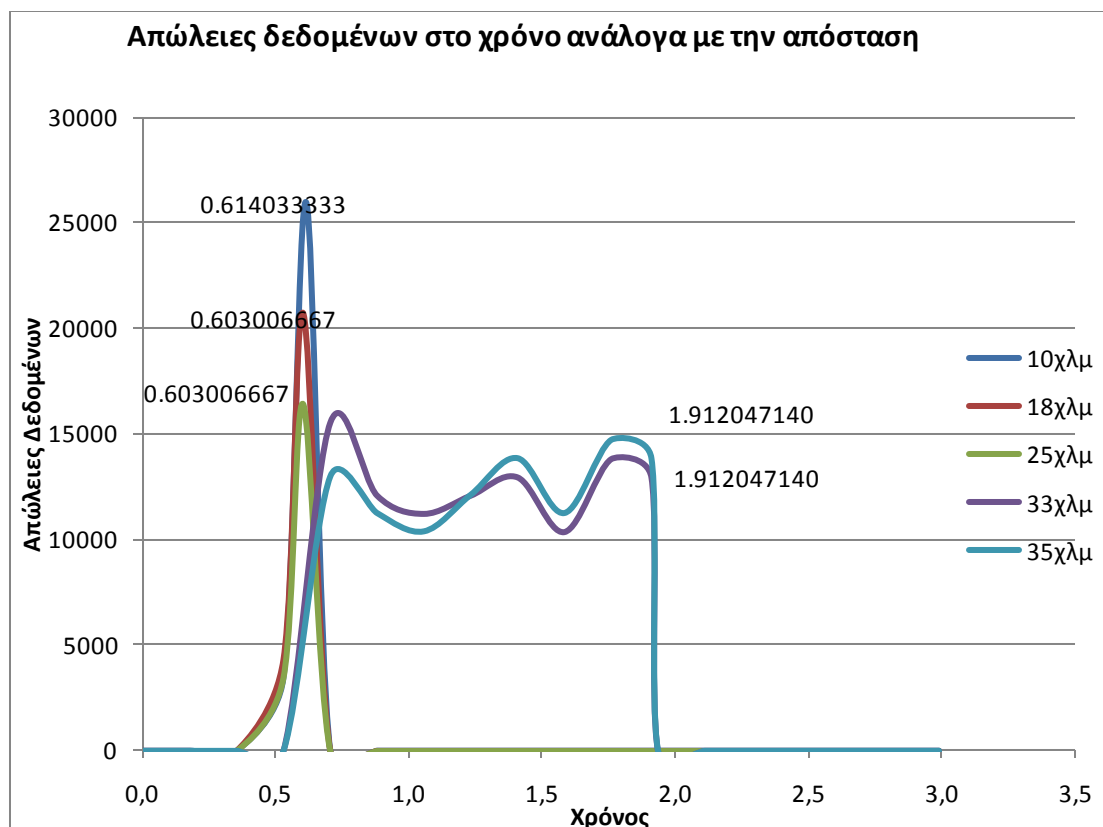
5.4 ΕΞΑΡΤΗΣΗ ΤΟΥ ΑΛΓΟΡΙΘΜΟΥ ΑΠΟ ΤΗΝ ΑΠΟΣΤΑΣΗ

Σε αυτή την παράγραφο αναλύεται η αποτελεσματικότητα που έχει ο συγκεκριμένος αλγόριθμος ανάλογα με την απόσταση και συγκεκριμένα **με την απόσταση του επιτιθέμενου από την πιο μακρινή συσκευή πελάτη**, καθώς οι συσκευές πελατών είναι αυτές που πραγματοποιούν το sensing. Σε αυτή την περίπτωση θεωρείται πως ο επιτιθέμενος βρίσκεται εντός εμβέλειας όλων των συσκευών του κελιού.

Ιδιαίτερα σημαντικό ρόλο για να ληφθεί ένα πακέτο από κάποια συσκευή λαμβάνει η ενέργεια που θα πρέπει να έχει το πακέτο. Όπως έχει αναφερθεί και στην ανάλυση του ns-2, το ποσό ενέργειας του πακέτου θα πρέπει να είναι τέτοιο έτσι ώστε να μπορεί να εντοπιστεί (*Carrier Sense Threshold*) αλλά και να ληφθεί με επιτυχία (*Receive Threshold*). Ειδικότερα, αν κάποιο πακέτο έχει ενέργεια μικρότερη από το Carrier Sense Threshold δεν γίνεται να εντοπιστεί, αν έχει ενέργεια ανάμεσα στο Carrier Sense Threshold και το Receive Threshold λαμβάνεται αλλά όχι με επιτυχία, καθώς εντοπίζεται μόνο η ενέργεια, ενώ αν έχει ενέργεια μεγαλύτερη από το Receive Threshold, τότε το πακέτο λαμβάνεται και μπορεί να μεταβεί από το επίπεδο του φυσικού μέσου στο αμέσως επόμενο επίπεδο, το MAC.

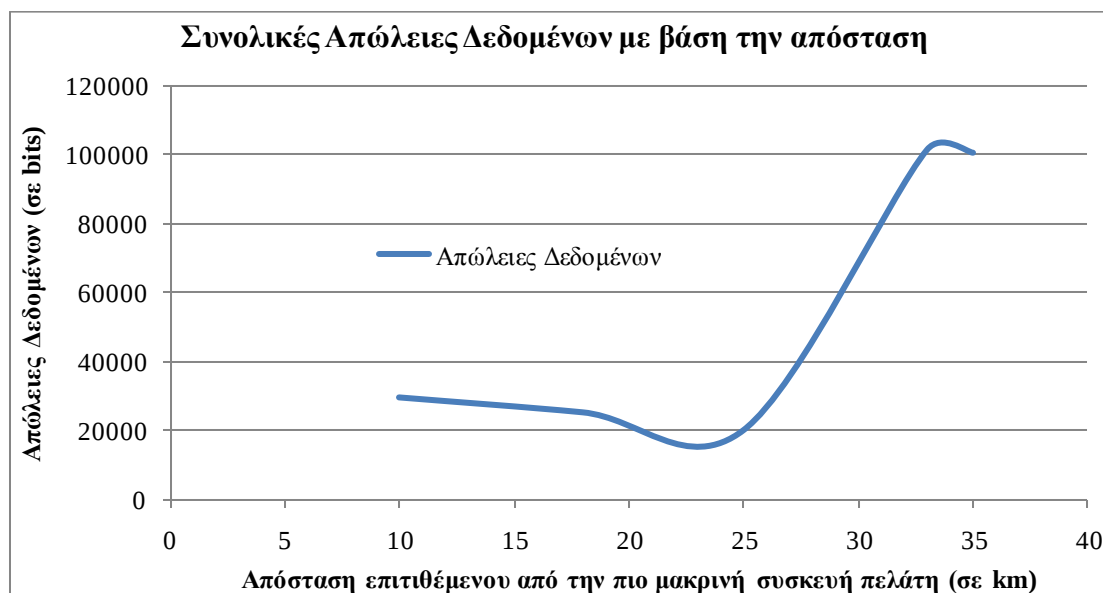
Ο μηχανισμός αυτός παίζει σημαντικό ρόλο στη λειτουργία και αποτελεσματικότητα του αλγορίθμου. Και αυτό γιατί με τον συγκεκριμένο αλγόριθμο ελέγχεται η ταυτότητα του αποστολέα των παρεμβολών, έλεγχος που είναι εφικτός μόνο στο επίπεδο MAC. Έτσι αν η ενέργεια των παρεμβολών δεν επαρκεί για να περάσει η πληροφορία στο επίπεδο MAC, η ταυτοποίηση δεν μπορεί να γίνει.

Για να ελεγχθεί ο βαθμός με τον οποίο η απόσταση επηρεάζει την αποτελεσματικότητα του αλγορίθμου χρησιμοποιείται η ίδια τοπολογία με την παραπάνω, μόνο που σε κάθε προσομοίωση **αλλάζει η θέση που είχε ο επιτιθέμενος σταθμός βάσης**, ο οποίος **απομακρύνεται όλο και περισσότερο** από τις συσκευές πελατών του δικτύου. Το μέγεθος της τοπολογίας αλλάζει και αυτό, καλύπτοντας μια περιοχή **100 τετραγωνικών χιλιομέτρων**. Τα αποτελέσματα που προκύπτουν απεικονίζονται στις ακόλουθες γραφικές παραστάσεις.



Σελίδα | 79

Εικόνα 32: Απώλειες δεδομένων σε bits κατά την διάρκεια των προσομοιώσεων, με την απόσταση του επιτιθέμενου από την μακρινότερη συσκευή πελάτη να αλλάζει συνεχώς. Οι σημειωμένοι χρόνοι αφορούν τις χρονικές στιγμές στις οποίες εντοπίζεται η παρεμβολή, εκκινώντας τις διαδικασίες αλλαγής του καναλιού



Εικόνα 33: Συνολικές απώλειες δεδομένων με βάση την απόσταση

5.4.1 Σχολιασμός γραφικών παραστάσεων

Παρατηρώντας την πρώτη από τις γραφικές παραστάσεις είναι φανερό ότι για απόσταση, μεταξύ επιτιθέμενου και της πιο μακρινής συσκευής πελάτη του δικτύου, που **βρίσκεται εντός των 33 χιλιομέτρων** που είναι δυνατή η αποστολή και λήψη δεδομένων ο εντοπισμός

γίνεται αρκετά άμεσα. Ο άμεσος εντοπισμός οφείλεται και στο γεγονός πως εντός των 33 χιλιομέτρων η ενέργεια του λαμβανόμενου πακέτου είναι πάντοτε μεγαλύτερη από το Receive Threshold. Επιπλέον, παρατηρείται ότι όσο αυτή η απόσταση μεγαλώνει οι απώλειες δεδομένων μικραίνουν, καθώς χάνονται περισσότερα πακέτα παρεμβολής.

Καθώς όμως μεγαλώνει η απόσταση και τείνει να **ξεπεράσει τα 33 χιλιόμετρα**, τότε οι απώλειες δεδομένων αυξάνονται. Αυτό οφείλεται στο γεγονός ότι για να αποφανθεί ο σταθμός βάσης ότι όντως γίνεται κάποια προσπάθεια επίθεσης προς το δίκτυο, εφόσον η τρίτη συσκευή πελάτη βρίσκεται σε μεγάλη απόσταση και δεν μπορεί να λάβει χωρίς λάθη το πακέτο, την απόφαση για τον εντοπισμό της επίθεσης θα πρέπει να την πάρουν οι συσκευές πελάτη που βρίσκονται σε εμβέλεια λήψης. Αυτές όμως καθυστερούν να αναφέρουν καθώς δέχονται ταυτόχρονα τις επιδράσεις του επιτιθέμενου.

Σελίδα | - 80 -

Αξίζει να σημειωθεί ότι η αντίδραση αυτή θα μπορούσε να γίνει **πιο άμεση** αν διαφοροποιούνταν **ο κανόνας απόφασης και γινόταν πιο ελαστικός**. Καθώς ο εντοπισμός αργεί αυξάνεται η κατανάλωση ενέργειας από το σύστημα που έχει σκοπό τον εντοπισμό του επιτιθέμενου, ξεπερνώντας το θεωρητικό μέγιστο που πρέπει να καταναλωθεί. Αλλά φαίνεται ότι έστω και αυτή η μεγαλύτερη κατανάλωση ενέργειας για κάποιο σύντομο χρονικό διάστημα μπορεί να έχει μεγαλύτερη αξία καθώς σε βάθος χρόνου μπορεί να φανεί σχετικά μικρή, αν συνυπολογιστεί και το γεγονός πως ο επιτιθέμενος μπορεί να παύσει να παρεμβάλλεται στο δίκτυο.

5.5 ΒΕΛΤΙΩΣΗ ΤΟΥ ΚΑΝΟΝΑ ΑΠΟΦΑΣΗΣ

Όπως αναφέρθηκε παραπάνω όταν αναφερθεί από κάποια συσκευή πελάτη ότι εντόπισε κάποια παρεμβολή κατά την λήψη δεδομένων από το σταθμό βάσης, αυτή πραγματοποιεί δυο ενέργειες.

1. Ενεργοποιεί την φάση ελέγχου.
2. Ενημερώνει τις **όλες** τις υπόλοιπες συσκευές πελατών που είναι συσχετισμένες με το σταθμό βάσης να αρχίσουν την αναζήτηση όσο θα είναι ανενεργές, για να διαπιστωθεί αν όντως υπάρχει παρεμβολή.

Στην συνέχεια αν **όλες οι συσκευές πελάτη που πραγματοποιούν τον έλεγχο** αναφέρουν ότι εντόπισαν παρεμβολές και εφόσον υπάρχει ομοφωνία, αλλάζουν κανάλι έτσι ώστε να αποφύγουν τις παρεμβολές.

Το γεγονός όμως ότι όλες οι υπόλοιπες συσκευές πελατών αναζητούν παρεμβολές έχει αντίκτυπο τόσο στην **κατανάλωση ενέργειας** όσο και στην **ποιότητα της απόφασης** που θα ληφθεί. Αρχικά η κατανάλωση της ενέργειας του συστήματος είναι μεγαλύτερη καθώς η φάση του ελέγχου γίνεται από πολλές συσκευές πελατών. Επιπλέον, όσον αφορά την ποιότητα της απόφασης, η ισορροπία είναι λεπτή. Αυτό οφείλεται στο γεγονός ότι όλες οι συσκευές πελατών θα πρέπει να συμφωνήσουν ότι όντως υπάρχει κάποια παρεμβολή λόγω κάποιου επιτιθέμενου. Μπορεί όμως όντως να υπάρχει παρεμβολή από επιτιθέμενο αλλά κάποιες συσκευές να είναι αδύνατον να την εντοπίσουν λόγω απόστασης από αυτόν.

Για να βελτιωθεί αυτό θα μπορούσαν να ακολουθηθούν δυο λύσεις:

- Να μην χρειάζεται να συμφωνήσουν όλοι κατά την λήψη της απόφασης, παρά μόνο μια πλειοψηφία
- Να αλλάξει ο τρόπος με τον οποίο αποφασίζεται ποιες συσκευές θα πραγματοποιήσουν έλεγχο. Η όποια απόφαση από εκεί και μετά θα πρέπει να ληφθεί από αυτές.

Από τις δυο αυτές λύσεις η δεύτερη είναι η πιο αποδοτική καθώς δεν γίνεται σπατάλη ενέργειας από το σύστημα. Στην πρώτη περίπτωση η ενέργεια καταναλώνεται από όλες τις συσκευές του δικτύου αλλά υπάρχει περίπτωση κάποια συσκευή να καταναλώσει ενέργεια και η αναφορά που θα δώσει να μην ληφθεί υπ' όψιν, αφού υπάρχει κανόνας πλειοψηφίας. Γι' αυτό το λόγο κρίθηκε σκόπιμο να ακολουθηθεί η δεύτερη λύση, από την στιγμή που υπάρχουν και επιπλέον πληροφορίες σχετικά με την θέση των συσκευών και μπορούν να αξιοποιηθούν. Συγκεκριμένα, οι συσκευές πελατών που θα πραγματοποιήσουν έλεγχο θα είναι αυτές που θα βρίσκονται πιο κοντά στην συσκευή πελάτη που εντόπισε την παρεμβολή. Αυτό γίνεται γιατί κάποια συσκευή που βρίσκεται κοντά στην παρεμβαλλόμενη, μπορεί αφενός να επηρεαστεί και αυτή αργότερα από τις παρεμβολές του επιτιθέμενου και αφετέρου έχει καλύτερη εικόνα για την περιοχή σε σχέση με κάποια άλλη που βρίσκεται πιο μακριά. Έτσι, για να ληφθεί η απόφαση, θα είναι απαραίτητο να συμφωνήσουν μόνο οι συσκευές αυτές που θα κάνουν τον έλεγχο.

Σ' αυτό το σημείο θα πρέπει να επισημανθεί ότι πέρα από αυτά θα πρέπει να υπάρχει μια συμφωνία μεταξύ όλων των συσκευών πελατών και του σταθμού βάσης σχετικά με το μέγιστο αριθμό των συσκευών που θα πρέπει να κάνουν έλεγχο. Η επιλογή των συσκευών γίνεται με βάση ακτίνες απόστασης από την συσκευή που έχει παρεμβολές. Πρώτα ελέγχονται αν υπάρχουν συσκευές που βρίσκονται σε ακτίνα 10χλμ από την συσκευή και αν δεν συμπληρωθεί ο μέγιστος αριθμός η ακτίνα μεγαλώνει στα 20χλμ κ.ο.κ. Βέβαια γίνεται και μια επιπλέον υπόθεση, ότι με το τέλος της όλης διαδικασίας θα υπάρχει τουλάχιστον μια συσκευή για να πραγματοποιήσει έλεγχο, ενώ μια γενικότερη υπόθεση γίνεται σχετικά με τον τρόπο που είναι παρατεταγμένες όλες οι συσκευές πελατών στην τοπολογία, καθώς θα πρέπει να βρίσκονται σε σχετικά κοντινές αποστάσεις η μια με την άλλη.

5.5.1 Υλοποίηση του βελτιωμένου κανόνα απόφασης στον ns-2

Για να υλοποιηθεί αυτός ο κανόνας απόφασης στον ns-2 θα έπρεπε να γίνουν κάποιες αλλαγές στην ήδη υπάρχουσα λύση. Καταρχάς για να αποθηκεύονται οι κόμβοι που θα κάνουν έλεγχο ορίστηκε μια δομή, η CPEsToSense, η οποία θα δημιουργούσε μια λίστα από τις συσκευές που θα πραγματοποιούν τον έλεγχο. Σε κάθε μέλος της λίστας αυτής αποθηκεύονται πληροφορίες σχετικά με μια συσκευή πελάτη, όπως η διεύθυνση MAC που έχει και πληροφορίες σχετικά με την απόσταση της από την συσκευής πελάτη που δέχεται τις παρεμβολές. Ο ορισμός της γίνεται στο αρχείο "mac-802_22.h". Τις πληροφορίες για την αρχή και το τέλος αυτή της λίστας τις γνωρίζουν όλοι οι κόμβοι του δικτύου και αρχικοποιούνται στην δομή του τύπου NetworkCell.

Ορισμός της δομής CPEsToSense στο αρχείο mac-802_22.h

```
struct CPEsToSense{
    CPEsToSense() {
        next = NULL;
        MacAddress = -1;
        distanceFromVictim = 0.0;
    }
    CPEsToSense *next;
    int MacAddress;
    int whenFound;
    double distanceFromVictim;
};
```

Η αρχικοποίηση των στοιχείων αυτής της λίστας γίνεται στην συνάρτηση που είναι υπεύθυνη για την έναρξη αυτής της φάσης ελέγχου, της startDynamicSensing. Καθώς η αρχικοποίηση των στοιχείων αυτής της λίστας θα πρέπει να γίνει μια φορά για κάθε frame χρησιμοποιείται μια boolean μεταβλητή για να σημειωθεί αυτό, την CPEsForSensingSet. Από τις πληροφορίες που υπάρχουν στην δομή CpeInfo σχετικά με την θέση των συσκευών των πελατών υπολογίζεται η απόσταση και τοποθετούνται τα στοιχεία στην λίστα.

Αρχικοποίηση των στοιχείων της λίστας στην συνάρτηση startDynamicSensing του αρχείου mac-802_22.cc

```
void Mac802_22::startDynamicSensing() {
//...
    if(!CPesForSensingSet){
        CPesForSensingSet = true;
        int actualX = CalMod->search(NodeID)->x;
        int actualY = CalMod->search(NodeID)->y;
        int found = 0;
        int distanceMode = 1;
        int noOfCpesToSense = 2;
        SsInfo *cpesByPosition = actualNetCell->SsInfo_head;
        while(cpesByPosition != NULL){
            if(cpesByPosition->MacAddr != NodeID){
                double distance =
sqrt(pow((double)(abs((actualX - cpesByPosition->exactX))),2) +
pow((double)(abs((actualY -cpesByPosition->exactY))),2));
                if(distance<(double)10000 && distanceMode ==
1){
                    found++;
                    if(found == noOfCpesToSense){
                        break;
                    }
                }
                else if(distance>(double)10000 &&
distance<(double)20000 && distanceMode == 2){
                    found++;
                    if(found == noOfCpesToSense){
                        break;
                    }
                }
            }
            cpesByPosition = cpesByPosition->next;
        }
    }
// ...
}
```

Σελίδα | - 82 -

Αντίστοιχα έγιναν και αλλαγές στο τμήμα που γίνεται η συλλογή των πληροφοριών από το σταθμό βάσης, στην συνάρτηση FrameTimerHandler.

Αλλαγή στη συνάρτηση FrameTimerHandler του αρχείου mac-802_22.cc

```

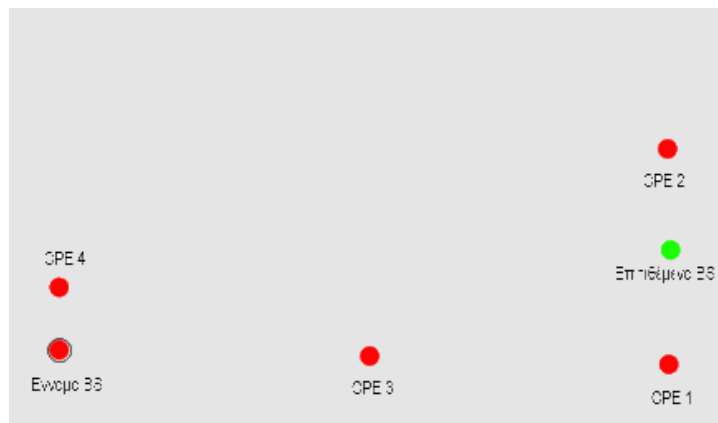
void Mac802_22:: FrameTimerHandler() {
// ...
    CPESForSensing = actualNetCell->CpesToSense_head;
    while(CPESForSensing){
        cpeinfo = actualNetCell->SsInfo_head;
        while (cpeinfo) {
            if(cpeinfo->MacAddr == CPESForSensing->
>MacAddress){
                if(cpeinfo->recv_response){
                    no_detections++;
                    cpeinfo->recv_response = false;
                }
                cpeinfo = cpeinfo->next;
            }
            no_CPES++;
            CPESForSensing = CPESForSensing->next;
        }
    }
// ...
}

```

Σελίδα | 83

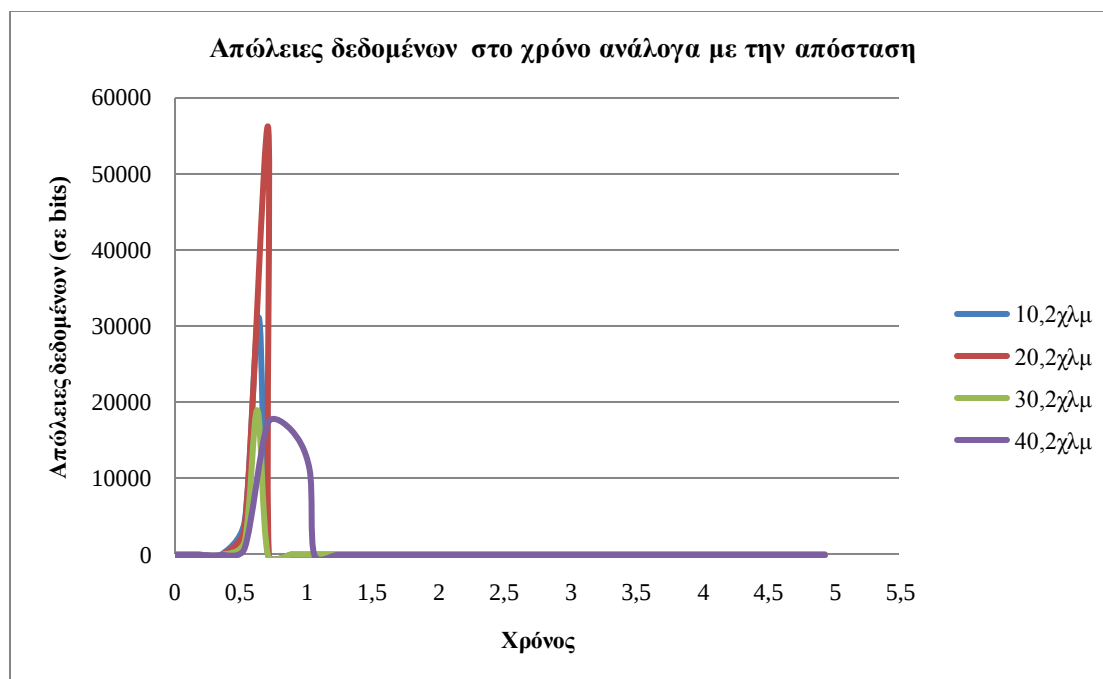
5.5.2 Αξιολόγηση του βελτιωμένου κανόνα απόφασης

Για να γίνει αξιολόγηση αυτού του βελτιωμένου κανόνα απόφασης δημιουργήθηκε μια καινούρια τοπολογία σεναρίου, παρόμοια με την προηγούμενη όμως. Αυτή φαίνεται παρακάτω. Σ' αυτή την τοπολογία για τις προσομοιώσεις που έγιναν μετατοπιζόταν ο επιτιθέμενος άξονα των χ δεξιά, απομακρύνοντάς τον από το πιο απομακρυσμένο κόμβο που είναι, όπως φαίνεται στην εικόνα, το CPE 4. Ο μέγιστος αριθμός συσκευών πελατών που θα πραγματοποιούσαν έλεγχο για παρεμβολές ήταν 2 ενώ ο επιτιθέμενος παρεμβαλλόταν στις λήψεις δεδομένων των CPE 1 και 3. Η διάρκεια των προσομοιώσεων ήταν 5s.



Εικόνα 34: Τοπολογία προσομοίωσης

Οι απώλειες δεδομένων που παρουσιάστηκαν με τα παραπάνω δεδομένα φαίνονται στην παρακάτω γραφική παράσταση.



Εικόνα 35: Απώλειες δεδομένων στο χρόνο ανάλογα με την απόσταση με χρήση του βελτιωμένου κανόνα απόφασης

Όπως παρατηρείται η αντίδραση του αλγορίθμου είναι βελτιωμένη καθώς οι απώλειες δεδομένων είναι μικρές ακόμα και σε μεγαλύτερες αποστάσεις από τα 33 χλμ από τον πιο απομακρυσμένο κόμβο καθώς δεν λαμβάνεται υπ' όψιν στην διαδικασία του ελέγχου. Άρα με αυτό τον τρόπο πιστοποιείται ότι ο νέος κανόνας απόφασης σχετικά με τις συσκευές πελατών που θα πραγματοποιήσουν έλεγχο έχει καλύτερη συμπεριφορά στις μεγάλες αποστάσεις.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] Stimac T. Definition of frequency bands. Retrieved December 10, 2009:
<http://www.vlf.it/frequency/bands.html>
- [2] SearchNetworking Definitions: Cognitive Radio definition, 2008. Retrieved December 10, 2009:http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci1186990,00.html
- [3] Whatis.com Target Search: White space definition, 2008. Retrieved December 10, 2009:http://whatistechtarget.com/definition/0,,sid9_gci1189510,00.html
- [4] Penasco Valley Telecommunications: Glossary of telecommunication terms, (N.D). Retrieved December 8, 2009: <http://www.pvt.com/oth/glossary.htm>
- [5] 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>
- [6] 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.
- [7] FCC rules for Part 90 services, Overview, 2008. Retrieved December 7, 2009, from Federal Communications Commission:
http://wireless.fcc.gov/services/index.htm?job=service_home&id=industrial_business
- [8] Kimtho Po, Jun-ichi Takada, Study of Applicability of IEEE 802.22 in Japan. Technical Report of IEICE, July 2006.
- [9] 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.
- [10] Time Division Duplex (TDD) Vs Frequency Division Duplex (FDD) in Wireless Backhauls, (N.D). Retrieved November 27, 2009 from Netkrom Technologies:
http://www.netkrom.com/support/whitepapers/TDD_vs_FDD_in_wireless_backhaul_white_paper.pdf.
- [11] Loutfi Nuyami, WiMax : Technology for Broadband Wireless Access, John Wiley & Sons, 2007.

- [12] 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.
- [13] 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.
- [14] 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.
- [15] International Engineering Consortium - “Voice Quality in Converging telephony an internet protocol networks”: http://www.iec.org/online/tutorials/voice_qual/topic07.asp
- [16] Berlemann L., Mangold S. *Cognitive Radio for Dynamic Spectrum Access*, John Wiley and Sons Ltd., 2009
- [17] Kwang-Cheng Chen, Ramjee Prasad. *Cognitive Radio Networks*, John Wiley and Sons Ltd. 2009
- [18] Yang Xiao, Fei Hu, *Cognitive Radio Networks*, Taylor & Francis Group. 2009
- [19] Meinrath S., Calabrese M. Unlicensed Broadband Device Technologies: “White Space Device” Operations on the TV Band and the Myth of Harmful Interference, 2007. Retrieved October 10, 2009 from New America Foundation: http://wirelessfuture.newamerica.net/publications/policy/unlicensed_broadband_device_technologies
- [20] The Network Simulator Wiki, Retrieved June 20, 2009, http://nsnam.isi.edu/nsnam/index.php/Main_Page
- [21] Issariyakul T., Hossain E., *Introduction to Network Simulator NS2*, Springer Science & Business Media, 2009
- [22] Greis M. Tutorial for the UCB/LBNL/VINT Network Simulator "ns", (N.D). Retrieved June 20, 2009 from Information Science Institute: <http://www.isi.edu/nsnam/ns/tutorial/>

- [23] Chung J., Claypool M. NS by Example, (N.D). Retrieved July 3, 2009 from Computer Science – Worcester Polytechnic Institute: <http://nile.wpi.edu/NS/>
- [24] J. Wang, Ns-2 Tutorial, Multimedia Networking Group, The Department of Computer Science, UVA
- [25] EXAMS: Overview, 2009. Retrieved December 3, 2009: http://www.livathinos.gr/EXAMS_overview.aspx
- [26] Fall K., Varadhan K. The ns Manual (formerly ns Notes and Documentation), 2009. Retrieved June 20, 2009 from Information Science Institute: <http://www.isi.edu/nsnam/ns/doc/>
- [27] NS-2 Tutorial, (N.D). Retrieved June 30, 2009 from Demokritos University of Thrace, <http://utopia.duth.gr/~skontog/work/wlesson.pdf>
- [28] Wang Y. A Tutorial of 802.11 implementation in ns-2, 2009. Retrieved June 21, 2009 from MobiTec Lab: http://www.winlab.rutgers.edu/~zhibinwu/pdf/tr_ns802_11.pdf.
- [29] Liu K., Understanding the implementation of IEEE MAC 802.11 standard in NS-2, (N.D.). Retrieved June 25, 2009 from Binghamton State University of New York: <http://www.cs.binghamton.edu/~kliu/research/ns2code/>
- [30] Xiuchao W. Simulate 802.11b Channel within NS2, (N.D.). Retrieved November 12, 2009 from National University of Singapore – School of computing.
- [31] The Network Simulator NS-2 NIST add-on for Mac 802.11, Draft 1.0, 2009. Retrieved September 19, 2009 from National Institute of Standards and Technology.
- [32] Soo – Young Chang, Wendong Hu, Khalona R., Sofer E. IEEE 802.22 WRAN Standard PHYMAC Proposal, 2006. Retrieved November 5, 2009 from docstoc: <http://www.docstoc.com/docs/16782659/IEEE-80222-WRAN-Standard-PHYMAC-Proposal>
- [33] A. Ghasemi, E. S. Sousa, Spectrum Sensing in Cognitive Radio Networks: Requirements, Challenges and Design Trade-offs, Cognitive Radio Communications and Networks, IEEE Communications Magazine, April 2008
- [34] J. Zhong, J. Li. Cognitive Radio Cognitive Network Simulator. Retrieved October 1, 2009, from Michigan Technology University: <http://stuweb.ee.mtu.edu/~ljialian/>

- [35] EMNTG Seamless and Secure Mobility - Publications and tools, Retrieved October 2009 from National Institute of Standards and Technology – Advanced Network Technologies Division, <http://w3.antd.nist.gov/seamlessandsecure/pubtool.shtml>,
- [36] The Network Simulator NS-2 - NIST add-on - Mac 802.11. Retrieved October , 2009 from National Institute of Standards and Technology:
http://w3.antd.nist.gov/seamlessandsecure/files/mobility/doc/MAC802_11.pdf
- [37] Svenson C. R., Cordeiro C., Sofer E., Chouinard G. Functional requirements for the 802.22 WRAN Standard, 2005. Retrieved November 23, 2009 from mentor-IEEE:
<https://mentor.ieee.org/802.22/dcn/05/22-05-0007-45-0000-draft-wran-rqmts-doc.doc>
- [38] J. Robinson, 802.11 mac code in ns-2 (version 2.28), Retrieved June 26, 2009 from:
http://www.joshuarobinson.net/docs/802_11.html
- [39] C. Ke, Setting Communication Radius in wireless nodes, Retrieved November 28 2009 from Department of Electrical Engineering of National Cheng Kung University of China: http://hpds.ee.ncku.edu.tw/~smallko/ns2/range_en.htm
- [40] 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.
- [41] 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.
- [42] J. Thiel, Metropolitan and Regional Wireless Networking: 802.16, 802.20 and 802.22, Retrieved October 20, 2009 for Department of Computer Science and Engineering of Washington University in St. Louis:
<http://www.cse.wustl.edu/~jain/cse574-06/ftp/wimax/index.html>
- [43] Chen, J., Wang, C., Tsai, F. C., Chang, C., Liu, S., Guo, J., Lien, W., Sum, J., and Hung, C. 2006. The design and implementation of WiMAX module for ns-2 simulator. In Proceeding From the 2006 Workshop on Ns-2: the IP Network Simulator (Pisa, Italy, October 10 - 10, 2006). WNS2 '06, vol. 202. ACM, New York, NY, 5. DOI=
<http://doi.acm.org/10.1145/1190455.1190458>

ΣΥΝΟΔΕΥΤΙΚΟ ΥΛΙΚΟ

Στο συνοδευτικό CD-ROM περιλαμβάνονται τα απαραίτητα αρχεία για την επιτυχή εγκατάσταση του module στον ns-2:

- `channel.cc`
- `mobilenode.cc`
- `packet.h`
- `queue.h`
- `wireless-phy.{cc, h}`
- `mac-802_22`: Στον φάκελο αυτό περιέχονται όλα τα αρχεία που έχουν δημιουργηθεί και αφορούν αποκλειστικά την προσομοίωση του 802.22. Ενώ τα παραπάνω αρχεία αποτελούν τροποποιήσεις των υπάρχοντων, ο φάκελος περιέχει όλες τις νέες υλοποιήσεις, σε επίπεδο mac, φυσικού μέσου, ροής δεδομένων, κτλ
 - `distance.h`
 - `geographic.h`
 - `mac-802_22.{cc, h}`
 - `packet-802_22.{cc, h}`
 - `timer-802_22.{cc, h}`
 - `traffic/BE_traffic.{cc, h}`: προσομοίωση ροής τύπου BE
 - `traffic/ertPS_traffic.cc`: προσομοίωση ροής τύπου ertPS
 - `traffic/nrtPS_traffic.{cc, h}`: προσομοίωση ροής τύπου nrtPS
 - `traffic/priority.{cc, h}`
 - `traffic/rtPS_traffic.cc`: προσομοίωση ροής τύπου rtPS
 - `traffic/UGS_traffic.cc`: προσομοίωση ροής τύπου UGS
- `properties.tcl`
- `scenario.tcl`: Είναι το tcl αρχείο που περιέχει το βασικό σενάριο προσομοίωσης με τη λειτουργία ενός κελιού που αποτελείται από 3 CPEs και δέχεται παρεμβολές από έναν επιτιθέμενο
 - `INSTALL_README.txt`

Οδηγίες για την εγκατάσταση του module περιέχονται στο αρχείο `INSTALL_README.txt`. Προϋποθέτει την εγκατάσταση του ns-2. Για την εξάλειψη προβλημάτων ασυμβατότητας, συνίσταται η εγκατάσταση του ns-allinone-2.29.3.