ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΗΤΙΚΟΤΗΤΑΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΠΡΟΣΒΑΣΗΣ 5ης ΓΕΝΙΑΣ

ΝΤΑΡΑΡΑΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΑΓΓΕΛΟΣ ΜΙΧΑΛΑΣ

ΘΕΣΣΑΛΟΝΙΚΗ,2021

Περίληψη

Η παρούσα διπλωματική εργασία έχει ως θέμα μελέτης την διαχείριση κινητικότητας σε ασύρματα δίκτυα πρόσβασης 5ης γενιάς. Αρχικά μελετάμε τα δίκτυα οχηματικών επικοινωνιών (V2X) καθώς και τις κατηγορίες εφαρμογών τους. Επίσης παρουσιάζονται οι απαιτήσεις που εισάγουν τα V2X στα δίκτυα πρόσβασης.

Στην συνεχεία παρουσιάζουμε τις τεχνολογίες δικτύων από τις οποίες απαρτίζονται τα V2X και τα πρωτόκολλα που χρησιμοποιούνται κατά την διαδικασία της διαπομπής. Επίσης παρουσιάζουμε μελέτες που αναλύουν μοντέλα για την διαπομπή κινητών τερματικών.

Η ανάγκη για ερεύνα στο συγκεκριμένο αντικείμενο είναι σημαντική στην εποχή που τα έξυπνα οχήματα πληθαίνουν, η αυτόνομη οδήγηση επεκτείνεται και δημιουργούνται καινούριές εφαρμογές με μεγάλες απαιτήσεις από το δίκτυο. Ιδιαίτερη προσοχή δίνεται στην διαχείριση της διαπομπής και τους μηχανισμούς που μπορούν να βελτιώσουν την διαδικασία.

Κύριος στόχος είναι η παρουσίαση ενός βελτιωμένου μοντέλου διαπομπής με σκοπό την μείωση της καθυστέρηση και της απώλειας πακέτων κατά την διαδικασία της διαπομπής. Τέλος, αναλύουμε τις βελτιστοποιήσεις σε σχέση με το βασικό μοντέλο διαπομπής και εξετάζουμε το προτεινόμενο μοντέλο με την βοήθεια μαθηματικών σχέσεων, ώστε να συγκριθεί η απόδοση του με το βασικό μοντέλο και να εξάγουμε αποτελέσματα.

Abstract

The topic of this thesis is the study of mobility management in 5th generation wireless access networks. In the beginning we study vehicular communications (V2X) as well as their categories of applications. Also, presented are the requirements that V2X introduce to access networks.

Next presented are the network technologies which V2X are composed of and the protocols used for the handover. Also presented are studies that analyze models for mobile handovers.

The need for research in this area is important in the era where the number of smart vehicles is growing, autonomous driving is expanding and new applications are created that introduce high demands to the network. Particular attention is given to the handover management and the mechanisms that could improve the handover process.

The key objective is to present an improved model for handovers in order to reduce the delay and packet loss of the handover process. Moreover, analyzed are the optimizations employed in relation to the standard handover model. Also the proposed model is examined using mathematical models in order to compare its performance with the standard model and extract results.

Δήλωση Πνευματικών Δικαιωμάτων

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1986 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα Διπλωματική Εργασία με τίτλο:

“ Διαχείριση κινητικότητας ασυρμάτων δικτύων πρόσβασης 5ης γενιάς ”

καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας και αναφέρονται ρητώς μέσα στο κείμενο που συνοδεύουν,
και η οποία έχει εκπονηθεί στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Δυτικής Μακεδονίας, υπό την επίβλεψη του μέλους του Τμήματος κ. Άγγελος Μιχάλας αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή / και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και μόνο.

Νταραράς Κωνσταντίνος, Άγγελος Μιχάλας , 2021 , Κοζάνη

Υπογραφή Φοιτητή:

ΠΙΝΑΚΑΣ ΠΕΡΙΟΧΟΜΈΝΩΝ

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΛΙΣΤΑ ΠΙΝΆΚΩΝ

ΠΙΝΑΚΑΣ ΑΚΡΩΝΎΜΙΩΝ

V2X	Vehicle to Everything
LTE	Long Term Evolution
WAVE	Wireless Access in Vehicular Environments
DSRC	Dedicated Short-Range Communications
RSU	Roadside Unit
IEEE	Institute of Electrical and Electronics Engineers
MAC	Media Access Control
EPC	Evolved Packet Core
MME	Mobility Management Entity
SGW	Service Gateway
PGW	Packet Gateway
IPv6	Internet Protocol V6
MIPv6	Mobile Internet Protocol V6
PMIPv6	Proxy Mobile Internet Protocol V6
FPMIPv6	Fast Handovers for Proxy Mobile Internet Protocol V6
HI	Handover Initiation
HACK	Handover Acknowledgment
PBU	Process Binding Update
PBA	Process Binding Acknowledgment
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
VPMIPv6	Προτεινόμενο Μοντέλο Διαπομπής
MN	Mobile Node
AMF	Access and Mobility Management Function
UPF	User Plane Function
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
NG-RAN	New Generation Radio Access Network
5GC	5G Cores

Κεφάλαιο 1: Εισαγωγή

1.1 Τι είναι η διαχείριση κινητικότητας:

Τα δίκτυα 5ης γενιάς ενσωματώνουν πολλές διαφορετικές τεχνολογίες δικτύων όπως είναι τα δίκτυα κινητής τηλεφωνίας LTE και 5G, δίκτυα Wi-Fi, δίκτυα WAVE αλλά και δορυφορικά δίκτυα. Τα δίκτυα αυτά χρησιμοποιούνται από βασικές υπηρεσίες, όπως η περιήγηση στο διαδίκτυο, αλλά και υπηρεσίες πραγματικού χρόνου όπως η μετάδοση φωνής και βίντεο, εφαρμογές με χρήση τοποθεσίας αλλά και εφαρμογές αυτόνομης οδήγησης. Για την υποστήριξη της λειτουργιάς αυτών των δικτύων και των εφαρμογών τους είναι υπεύθυνη η διαχείριση κινητικότητάς. Οι βασικές λειτουργιές της διαχείρισης κινητικότητας είναι η διαχείριση θέσης και η διαχείριση διαπομπής. Η διαχείριση θέσης επιτρέπει στα ασύρματα δίκτυα τον εντοπισμό και την παρακολούθηση της τοποθεσίας των κινητών τερματικών για να υποστηρίξουν τις υπηρεσίες που απαιτούν. Η διαχείριση διαπομπής έχει ως στόχο να διατηρεί τις συνδέσεις των κινητών τερματικών κατά την μετάβαση τους σε μια καινούρια περιοχή εξυπηρέτησης, η οποία μπορεί να εξυπηρετείται από δίκτυο ιδίου η διαφορετικού τύπου.

1.2 Κίνητρο Υλοποίησης

Τα τελευταία χρόνια υπάρχει μια συνεχής μετάβαση σε μια ψηφιακή εποχή στην οποία τα οχήματα και άλλες γενικότερες συσκευές γίνονται έξυπνες και αποκτούν επιπλέον δυνατότητες ώστε να βελτιώσουν την χρησιμότητα τους και να αναβαθμίσουν τον τρόπο ζωής μας. Τα οχήματα πλέον εφοδιάζονται με μια μεγάλη γκάμα από εφαρμογές και υπηρεσίες, οι οποίες εισάγουν πολλές απαιτήσεις στα δίκτυα όσο αφορά το ρυθμό μετάδοσης και την καθυστέρηση προκειμένου να μην υπάρχει διακοπή των υπηρεσιών. Έτσι οι διαδικασίες της διαχείρισης κινητικότητας των δίκτυών 5ης γενιάς καλούνται να καλύψουν τις νέες απαιτήσεις που παρουσιάζονται. Κατά συνέπεια, υπάρχει ανάγκη για την μελέτη και την βελτίωση των διαδικασιών της διαχείρισης κινητικότητας ώστε ο χρήστης να απολαμβάνει στο έπακρο τις υπηρεσίες και εφαρμογές που προσφέρονται.

1.3 Στόχος διπλωματικής εργασίας

Στόχος της διπλωματικής εργασίας είναι αρχικά η μελέτη και η παρουσίαση των σχηματικών δικτυών και των τεχνολογιών πρόσβασης που χρησιμοποιούνται. Επίσης παρουσιάζονται τα πρωτοκόλλα και οι διαδικασίες για την διαχείριση διαπομπής. Στην συνέχεια έχοντας μελετήσει κάποια μοντέλα διαπομπής από βιβλιογραφία, περιγράφουμε ένα προτεινόμενο μοντέλο διαπομπής. Το προτεινόμενο μοντέλο έχει στόχο να μειώσει την καθυστέρηση και την απώλεια πακέτων κατά την διαπομπή ώστε να αντιμετωπιστούν τυχόν διακοπές που παρουσιάζονται στις συνεδρίες των κινητών τερματικών.

1.4 Επισκόπηση Εργασίας

Στο 2ο κεφάλαιο αρχικά γίνεται μια παρουσίαση των οχηματικών δικτύων και στην συνέχεια κατηγοριοποιούνται οι εφαρμογές που υποστηρίζονται ανάλογα με την λειτουργία και τις απαιτήσεις τους. Στην συνέχεια αναλύονται η αρχιτεκτονική και τα πρωτόκολλα των δικτύων πρόσβασης που απαρτίζουν τα οχηματικα δίκτυα όπως είναι το 802.11p, το 4G LTE και το 5G.

Το 3ο κεφάλαιο ξεκινά με την περιγραφή των διαδικασιών της διαχείρισης θέσης και την διαχείρισης διαπομπής. Στην συνέχεια αναλύουμε τα πρωτοκολλά κινητικότητας, όπως το MIPv6, το PMIPv6, FPMIPv6 και το MIH. Επίσης παραθέτουμε κάποιες μελέτες σχετικά με μοντέλα διαπομπής από βιβλιογραφία.

Το 4ο και 5ο κεφάλαιο αφορά το προτεινόμενο βελτιωμένο μοντέλο διαπομπής. Ξεκινώντας περιγράφουμε τις predictive και reactive λειτουργίες του μοντέλου το όποιο βασίζεται στο FMIPv6, ενώ περιγράφεται και η λειτουργία του μοντέλου σε περιπτώσεις false handover. Αμέσως μετά παρουσιάζουμε τις μαθηματικές εκφράσεις που χρησιμοποιούνται για την ανάλυση του προτεινομένου μοντέλου με τελικό σκοπό την σύγκριση της απόδοσης του σε σχέση με το FPMIPv6 μοντέλο. Συγκεκριμένα συγκρίνουμε την καθυστέρηση διαπομπής, το κόστος σηματοδοσίας και tunneling και την απώλεια δεδομένων. Η σύγκριση των μοντέλων διαπομπής γίνεται μέσω γραφικών παραστάσεων οι οποίες δημιουργήθηκαν στο MATLAB. Τέλος, στο 6ο κεφάλαιο εξάγουμε συμπεράσματα.

Κεφάλαιο 2: Δίκτυα κινητών οχημάτων

2.1 Εισαγωγή στα Δίκτυα κινητών οχημάτων

Τα συστήματα οχηματικών δίκτυών Vehicle to Everything(V2X) υποστηρίζουν την μετάδοση πληροφορίων από οχήματα προς οποιαδήποτε συσκευή σε ένα περιβάλλον κυκλοφορίας.

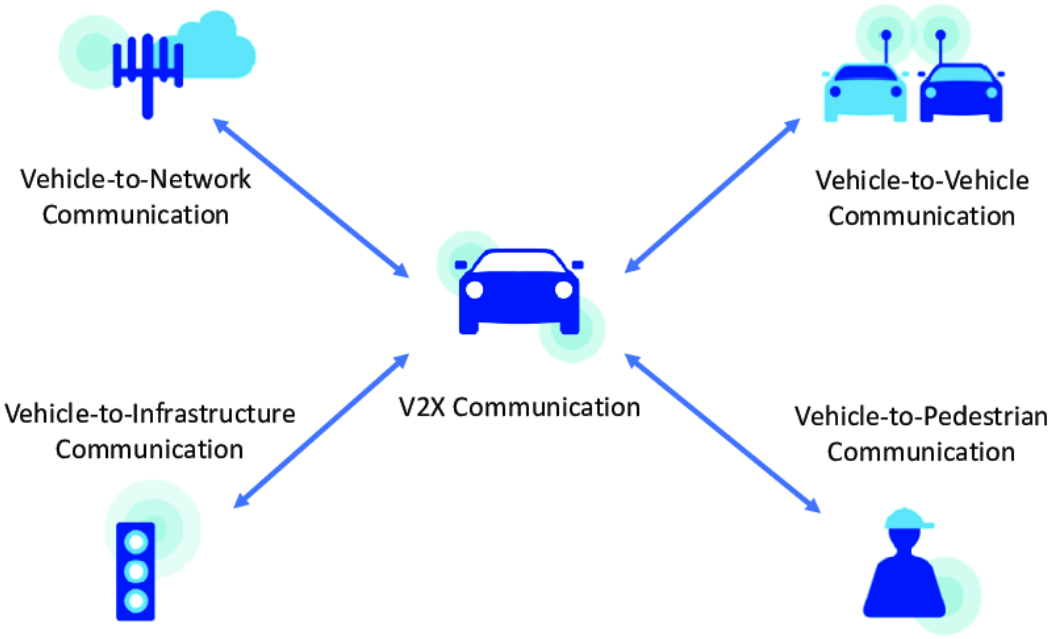

Figure 1. Κατηγορίες V2X επικοινωνιών

Οι βασικές κατηγορίες των οχηματικών δικτύων είναι τα δίκτυα V2V (vehicle to vehicle),τα δίκτυα V2I (vehicle to infrastructure) και τα δίκτυα V2P (vehicle to pedestrian).Τα δίκτυα V2V επιτρέπουν στα οχήματα να επικοινωνούν μεταξύ τους δημιουργώντας τα VANET(Vehicular Ad Hoc Networks), ενώ τα δίκτυα V2I επιτρέπουν την επικοινωνία με τις υπόλοιπες οντότητες του περιβάλλοντος όπως σηματοδότες, χώροι στάθμευσης, κτήρια και συσκευές πεζών και ποδηλατών.

Η σωστή μετάδοση των πληροφοριών σε αυτά τα συστήματα απαιτεί συνδέσεις με υψηλό εύρος ζώνης και μεγάλη αξιοπιστία. Για αυτόν τον λόγο οι αυτοβιομηχανίες σε συνεργασία με τους πάροχους αναπτύσσουν συνέχεια τα συστήματα οχηματικών επικοινωνιών με στόχο να κάνουν πιο εύκολη και ασφαλή την οδήγηση των οχημάτων

ενώ ταυτόχρονα σχεδιάζουν και παρέχουν καινοτόμες εφαρμογές και υπηρεσίες στους οδηγούς για να βελτιώσουν την εμπειρία τους.

Τα δίκτυα οχημάτων χρησιμοποιούν το πρωτόκολλο IPv6 (Internet Protocol version 6) για να υποστηρίξουν την κινητικότητα των χρηστών τους, επιτρέποντας σε κάθε όχημα να διατηρεί τη διεύθυνση IP του ενώ αλλάζει από δίκτυο σε δίκτυο. Αυτή η ιδιότητα είναι ιδιαίτερα σημαντική σε οχηματικα περιβάλλοντα, δεδομένου ότι τα οχήματα χαρακτηρίζονται από πολύ υψηλή κινητικότητα, ενώ ταυτόχρονα η συνεχής σύνδεση τους χωρίς διακοπές είναι απαραίτητη για την σωστή λειτουργία των εφαρμογών που προσφέρουν άλλα και την αποφυγή τροχαίων σε περιπτώσεις αυτόνομης οδήγησης [1],[4].

2.2 Εφαρμογές οχηματικών δικτύων

Οι εφαρμογές των οχηματικών δικτύων μπορούν να κατηγοριοποιηθούν στις εξής κατηγορίες:

- Εφαρμογές ασφάλειας πραγματικού χρόνου και επείγουσας ανάγκης:
  Τα οχήματα με βάση τις πληροφορίες που λαμβάνουν από τις υπόλοιπες συσκευές στο περιβάλλον άλλα και από το διαδίκτυο, μπορούν να προειδοποιήσουν τον οδηγό για ατυχήματα που έχουν συμβεί στο δρόμο αλλά και να εμφανίζουν ζωντανές ενημερώσεις για πιθανές δυσμενείς καιρικές συνθήκες. Επίσης, σε περίπτωση πού ο οδηγός εμφανίσει σημάδια κόπωσης τα οχήματα μπορούν να υποβοηθήσουν την οδήγηση και να ακινητοποιήσουν το όχημα με ασφάλεια. Τέλος στην περίπτωση κάποιου ατυχήματος ή βλάβης του οχήματος, το οχήματα μπορούν να ειδοποιήσουν τις αντίστοιχες υπηρεσίες επείγουσας ανάγκης.
- Εφαρμογές έξυπνης πλοήγησης:
  Τα οχήματα μπορούν να παρέχουν υπηρεσίες αυτόνομης οδήγησης αλλά και να συλλέγουν δεδομένα από το περιβάλλον για την εκπαίδευση της αυτόνομης οδήγησης. Συγκεκριμένα, κατά την πλοήγηση ενός οχήματος σε μια πόλη, τα οχήματα μπορούν να εμφανίσουν διαδρομές ειδικά διαμορφωμένες για τον οδηγό με βάση τα πιο συχνά σημεία ενδιαφέροντος του. Επίσης σε περίπτωση κυκλοφοριακής συμφόρησης υπολογίζουν και εμφανίζουν μια εναλλακτική

ταχύτερη διαδρομή. Ακόμα ανάλογα με την τοποθεσία του οχήματος μπορούν να πληροφορήσουν τον οδηγό για προτεινόμενους χώρους στάθμευσης.

- Εφαρμογές ψυχαγωγίας:
  Κατά την διάρκεια ενός ταξιδιού οι επιβάτες μπορούν να απολαμβάνουν υπηρεσίες μουσική και βίντεο, ενώ ακόμη λόγω της παρεχόμενης σύνδεσης στο διαδίκτυο οι επιβάτες μπορούν να συνεχίσουν να χρησιμοποιούν τις προσωπικές τους εφαρμογές χωρίς διακοπή. Τέλος τα οχήματα έχουν την δυνατότητα να προβάλουν διαφημίσεις για εστιατόρια, καφέ και άλλα σημεία ενδιαφέροντος και αναψυχής κατά την διάρκεια μιας διαδρομής [1],[5].

2.3 Απαιτήσεις εφαρμογών V2X

Οι εφαρμογές των V2X δικτύων καλύπτουν ένα μεγάλο εύρος αναγκών των καταναλωτών. Η κάθε εφαρμογή έχει διαφορετικές απαιτήσεις από το δίκτυο σχετικά με την καθυστέρηση και την Ρυθμοαπόδοση(bandwidth). Προκειμένου το δίκτυο να αποδώσει το απαραίτητο QoS (quality of service) στις εφαρμογές, γίνεται συχνά μια κατηγοριοποίηση των εφαρμογών σε ομάδες, ανάλογα με την λειτουργεία και τις απαιτήσεις τους.

Ψυχαγωγία: Οι εφαρμογές Infotainment όπως ονομάζονται στο τομέα της αυτοβιομηχανίας αποτελούνται ένα πλήθος υπηρεσιών μη σχετιζόμενές με την διαδικασία της οδήγησης αλλά σχετιζόμενες με την ενημέρωση και την ψυχαγωγία. Τέτοιες υπηρεσίες περιλαμβάνουν λειτουργίες όπως είναι η μεταφορά πολυμέσων, η άμεση ανταλλαγή μηνυμάτων μεταξύ των επιβατών και η εμφάνιση διαφημίσεων ανάλογα με την γεωγραφική τοποθεσία. Ένα παράδειγμα είναι η λειτουργία των ενσωματωμένων συστημάτων και οθονών στο ταμπλό του αυτοκινήτου για την ενημέρωση του οδηγού και στην συνέχεια για την ψυχαγωγία των επιβατών. Οι υπηρεσίες ψυχαγωγίας χαρακτηρίζονται από σχετικά μικρές απαιτήσεις σχετικά με την καθυστέρηση της τάξης των 500-1000 ms, ενώ σχετικά με την Ρυθμοαπόδοση οι απαιτήσεις είναι συγκρίσιμες με τις συμβατικές κινητές υπηρεσίες της τάξης των 80 Mpbs.

Απόδοση Κυκλοφορίας: Η κατηγορία αυτή περιέχει ένα ευρύ φάσμα εφαρμογών που αποσκοπούν στη βελτιστοποίηση της ροής της κυκλοφορίας οχημάτων σε ένα οδικό δίκτυο. Μια από τις λειτουργίες των εφαρμογών είναι ο συντονισμός των διασταυρώσεων και των σηματοδοτών σε επίπεδο συστήματος και ο χρονοπρογραμματισμός τους. Μια ακόμη λειτουργία είναι ο συντονισμός της χρήσης του ηλεκτροκινητήρα ενός οχήματος(στην περίπτωση των υβριδικών οχημάτων) για εξοικονόμηση ενέργειας και προστασίας του περιβάλλοντος. Ένα παράδειγμα εφαρμογής απόδοσης κυκλοφορίας είναι ένα ενσωματωμένο σύστημα GPS το οποίο έχει την δυνατότητα να επαναδρομολογεί αυτόματα τα οχήματα με βάση τις συνθήκες κυκλοφορίας. Οι εφαρμογές αυτής της κατηγορίας έχουν μεγαλύτερες απαιτήσεις από ότι οι εφαρμογές ψυχαγωγίας. Η καθυστέρηση θα πρέπει να κυμαίνεται στα 100-500 ms ενώ η Ρυθμοαπόδοση στα 10-45 Mpbs.

Ασφάλεια Κυκλοφορίας: Οι εφαρμογές για την ασφάλεια της κυκλοφορίας στοχεύουν στην μείωση της συχνότητας εμφάνισης των συγκρούσεων οχημάτων, των υλικών ζημιών και των ανθρώπινων απωλειών. Αποτελείται από εφαρμογές που αφορούν τη λήψη κρίσιμων αποφάσεων, όπως είναι η αντιμετώπιση ασυνήθιστων συμπεριφορών οχημάτων, η προστασία των ευάλωτων οδικών χρηστών όπως είναι οι ποδηλάτες και οι πεζοί και η λήψη μέτρων για τη διέλευση των οχημάτων έκτακτης ανάγκης. Η πιο συχνά αναφερόμενη χρήση των εφαρμογών της κατηγορίας είναι η προειδοποίηση του οδηγού για μια ενδεχόμενη σύγκρουση προς αποφυγή της καθώς και την ανίχνευση μιας αναπόφευκτης σύγκρουσης και το συντονισμό του οχήματος ώστε να μετριαστούν επιπλέον συγκρούσεις μεταξύ ενός ή περισσότερων οχημάτων. Ανάλογα με τις υπηρεσίες που παρέχονται σε κάθε όχημα οι απαιτήσεις σε καθυστέρηση είναι 20-100 ms και σε Ρυθμοαπόδοση είναι 1-700 Mpbs.

Συνεργατική οδήγηση: Οι περισσότερες εφαρμογές που ανήκουν σε αυτήν την κατηγορία μπορούν να ενσωματωθούν στην κατηγορία της ασφάλειας κυκλοφορίας καθώς η λειτουργία και οι απαιτήσεις τους είναι παραπλήσιες. Παρόλα αυτά κάποιες εφαρμογές κατηγοριοποιούνται σε αυτήν την ξεχωριστή κατηγορία καθώς εμφανίζουν πολύ αυστηρές απαιτήσεις και η λειτουργία τους είναι ιδιαίτερα σημαντική αφού αφορά την αυτόνομη λειτουργία οχημάτων. Μια εφαρμογή της συνεργατικής οδήγησης είναι το co-operative platooning που είναι η δημιουργία ομάδων από πολύ κοντινά οχήματα κινούμενα προς την ίδια κατεύθυνση σε μια λωρίδα κυκλοφορίας. Επίσης άλλη εφαρμογή είναι το Cooperative Adaptive Cruise Control το όποιο είναι

μια επέκταση του adaptive cruise control με την δυνατότητα ανταλλαγής μηνυμάτων μεταξύ των οχημάτων για την λήψη της ταχύτητάς ενός προπορευόμενου οχήματος. Οι εφαρμογές συνεργατικής οδήγησης έχουν πολύ υψηλές απαιτήσεις από το δίκτυο όσο αφορά την καθυστέρηση της τάξης των 2-10 ms. Ωστόσο, όσο αφορά την Ρυθμοαπόδοση τα 5 Mbps μπορούν να καλύψουν την λειτουργία των εφαρμογών αφού δεν ανταλλάσσονται δεδομένα μεγάλου μεγέθους [2],[3].

2.4 Προκλήσεις και απαιτήσεις ασφάλειας στα V2X

Οι διάφορες εφαρμογές των V2X επιβάλλουν ποίκιλλες απαιτήσεις στο δίκτυο οι οποίες επηρεάζουν άμεσα την ασφάλεια των δίκτυών.

Η τοπολογία των V2X είναι δυναμική λόγο της κινητικότητας των οχημάτων. Τα οχήματα κινούνται με μεγάλη ταχύτητα και οι συνδέσεις που εγκαθιδρύουν έχουν μικρή διάρκεια. Τα χαρακτηριστικά ασφάλειας κατά την δημιουργία των συνδέσεων πρέπει να προσαρμοστούν για να μην εισάγετε επιπλέον καθυστέρηση στις διαδικασίες εγγραφής στο δίκτυο και ως αποτέλεσμα να εμποδίζεται η σύνδεση των οχημάτων.

Τα V2X επίσης χαρακτηρίζονται από μεγάλη ετερογένεια, αφού εφαρμόζονται πολλαπλές τεχνολογίες πρόσβασης σε όλο το κόσμο. Έτσι οι αυτοβιομηχανίες διαλέγουν και εφαρμόζουν στα οχήματα τις τεχνολογίες ανάλογα τις πολιτικές ασφάλειας και προστασίας της κάθε χώρας. Έτσι είναι απαραίτητος ο σωστός συγχρονισμός μεταξύ των διαφορετικών χαρακτηριστικών ασφάλειας που εφαρμόζει ο κάθε κατασκευαστής.

Η καθυστέρηση κατά την επικοινωνία στα V2X οφείλεται σε ζητήματα όπως είναι η συλλογή και το φιλτράρισμα των πληροφοριών και ο διαχωρισμός των δεδομένων σε αυτά προς επεξεργασία και σε αυτά προς μετάδοση. Επομένως είναι απαραίτητο οι παράγοντές που σχετίζονται με την καθυστέρηση να αντιμετωπιστούν έτσι ώστε το δίκτυο να έχει την δυνατότητα να διαχειριστεί πιθανές κρίσιμες καταστάσεις ασφάλειας σε πραγματικό χρόνο όταν εμφανιστούν.

Τα δίκτυα V2X θα πρέπει να έχουν την δυνατότητα να αποδώσουν την κατάλληλη προτεραιότητα στα δεδομένα που λαμβάνονται από τους διάφορους κόμβους. Τα δεδομένα που λαμβάνονται από κρίσιμους τομείς για την ασφάλεια θα πρέπει να

διαχειρίζονται με μεγαλύτερη προτεραιότητα ώστε να αποφευχθούν προβλήματα ασφάλειας που δυνητικά θα προκαλούσαν παράπλευρές ζημίες σε όλο το δίκτυο [2].

2.5 Τεχνολογίες πρόσβασης στα V2X

2.5.1 IEEE 802.11p

Το πιο συχνά μελετημένο δίκτυο πρόσβασης που συναντάμε στα V2X είναι το πρωτόκολλο IEEE 802.11p. Το πρωτόκολλο 802.11p είναι μια τροποποίηση του βασικού πρωτόκολλου 802.11a (Wi-Fi). Στόχος του πρωτοκόλλου είναι να υποστηρίξει τις εφαρμογές ITS(intelligent transportation systems).

Ένα μεγάλο μέρος της ανάπτυξης του πρωτοκόλλου βασίζεται στην πρόοδο των dedicated short-range communications (DSRC), που επιτρέπουν την επικοινωνία μεταξύ των οχημάτων και των οδικών υποδομών. Το DSRC είναι ένα πρότυπο που έχει προταθεί από την ομοσπονδιακή επιτροπή επικοινωνίας (FCC: Federal Communication Commission) το 1999. Το πρότυπο κατοχύρωσε ένα φάσμα 75MHz στην συχνότητα των 5.9GHz για την υποστήριξη των V2I και V2V επικοινωνιών. Η κάλυψη του DSRC είναι μέχρι τα 500 μετρά. Η αρχιτεκτονική του συστήματος DSRC αποτελείται από μια ενσωματωμένη μονάδα (OBU:on board unit) και μια οδική μονάδα (RSU: road side unit). Τα OBU αποτελούν συσκευές ασύρματής επικοινωνίας οι όποιες τοποθετούνται στα κινούμενα οχήματα. Τα RSU λειτουργούν ως σταθμοί βάσης για τα OBU και αποτελούνται από εξοπλισμό που υπάρχει κατά μήκος των οδών, στις διασταυρώσεις κυκλοφορίας και σε άλλες τοποθεσίες που το όχημα θα έχει συνεχής σύνδεση.

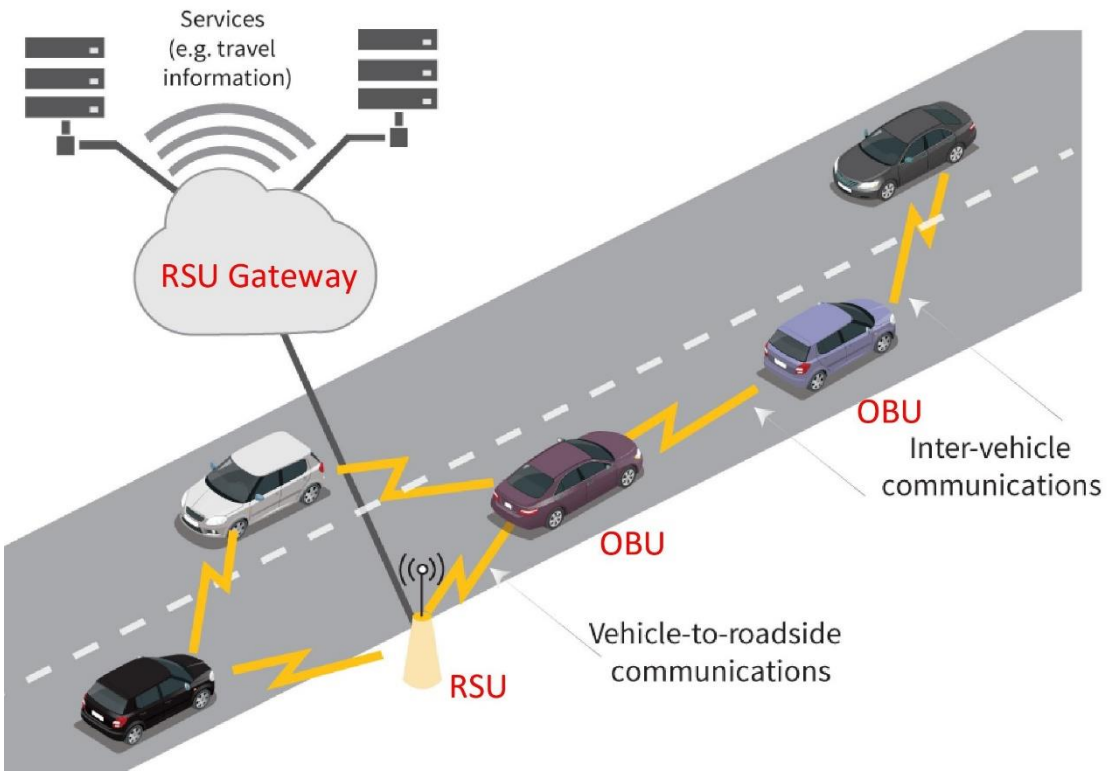

Figure 2. Αρχιτεκτονική 802.11p/DSRC δικτύων [30].

Στο φάσμα των 75 MHz υπάρχει ένα κανάλι κρατημένο για τον έλεγχο του συστήματος και σημαντικά μηνύματα σχετικά με την ασφάλεια του οχήματος, το οποίο ονομάζεται κανάλι ελέγχου(CCH:control channel). Στη συνέχεια υπάρχουν 6 κανάλια για την ανταλλαγή των υπόλοιπων δεδομένων που δεν σχετίζονται με την ασφάλεια τα οποία ονομάζονται κανάλια σηματοδότησης (SCH: signaling channels).

Το 802.11p υιοθετεί την αρχιτεκτονική των DSRC ενώ επίσης διαθέτει ένα ξεχωριστό σχήμα για την πρόσβαση των οχημάτων σε αυτά τα κανάλια. Ο χρόνος των καναλιών μοιράζεται σε ίσα διαστήματα συγχρονισμού των 100ms, τα οποία χωρίζονται σε υπό-διαστήματα εναλλασσόμενα μεταξύ του CCH και των SCH. Κατά το διάστημα που μεταδίδει το CCH κανάλι όλες οι συσκευές των οχημάτων πρέπει να συντονιστούν στη συχνότητα του CCH για την μετάδοση πληροφορίων ελέγχου και ασφάλειας. Κατά το διάστημα που μεταδίδουν τα SCH κανάλια τα οχήματα μπορούν να επιλέξουν σε ποια SCH συχνότητα θέλουν να συνδεθούν. Επομένως το φάσμα του 802.11p χωρίζεται σε εφτά κανάλια των 10MHz και πρόσθετα υπάρχει και μία ζώνης φύλαξης των 5MHz.

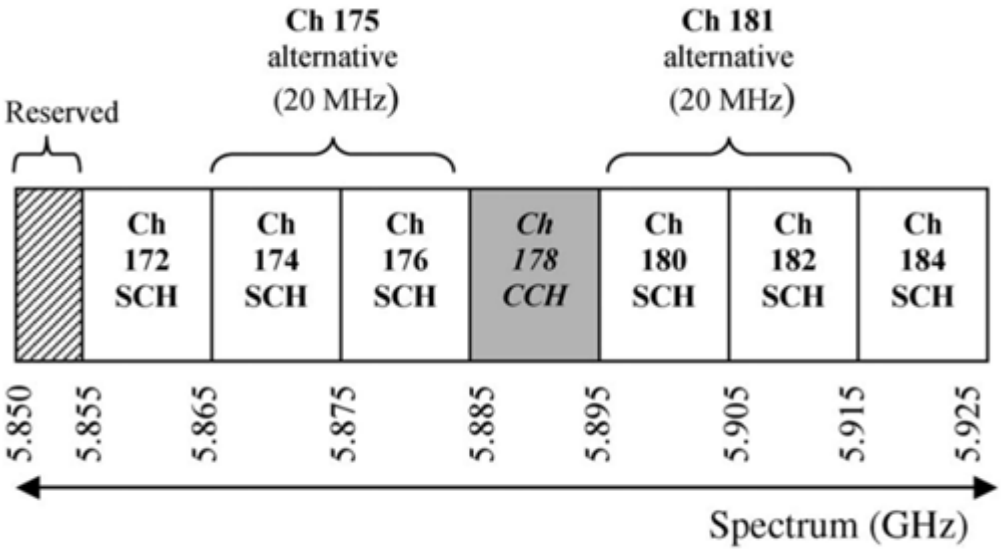

Figure 3. Φάσμα των DSRC επικοινωνιών [29].

Το WAVE(wireless access in vehicular environments) είναι η κατάσταση των 802.11p συσκευών ώστε να λειτουργούν στο φάσμα των DSRC. ΤΟ WAVE περιέχει στα ανώτερα επίπεδα της στοίβας πρωτοκόλλων του, το πρότυπο IEEE 1609. Το IEEE 1609 αποτελείται από το επίπεδο ασφάλειας 1609.2, το επίπεδο δικτύου 1609.3 και το 1609.4 που είναι το ανώτερο MAC επίπεδο. Στη συνέχεια της στοίβας πρωτοκόλλων περιλαμβάνεται το επίπεδο πρόσβασης MAC και το φυσικό επίπεδο όπως ορίζονται στο πρωτόκολλο 802.11p.

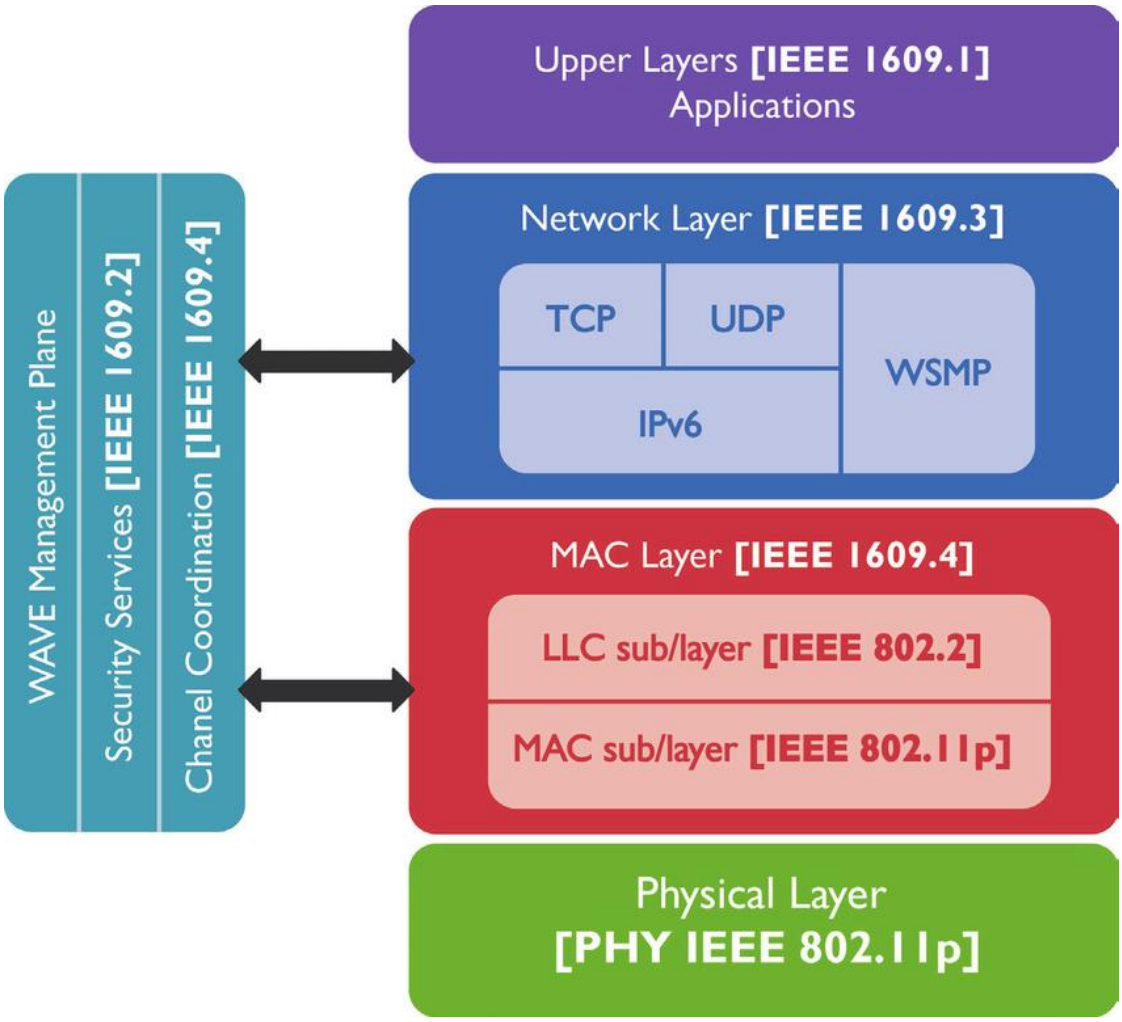

Figure 4. Στοίβα πρωτοκόλλων του WAVE [31].

Στο MAC επίπεδο του 802.11p προτάθηκαν νέες δυνατότητες ώστε να διευκολυνθεί η μεταξύ επικοινωνία των οχημάτων. Το οχήματα μπορούν να ανταλλάσσουν δεδομένα με μειωμένη επιβάρυνση αφού δεν χρειάζονται οι διαδικασίες ταυτοποίησης που είναι απαραίτητές πριν την ανταλλαγή δεδομένων όπως στο 802.11. Για να επιτευχθεί αυτό τα οχήματα υιοθετούν μια BSSID wildcard(μπαλαντέρ) που τους επιτρέπει να μεταδώσουν στα οχήματα που διαθέτουν το ίδιο wildcard ανεξάρτητα του WBSS που ανήκουν. WBSS είναι ένα σύνολο αποτελούμενο από RSU και OBU που λειτουργούν σε WAVE και έχουν το ίδιο BSSID. Αυτό σημαίνει ότι 2 γρήγορα κινούμενα οχήματα που είναι σε απόσταση επικοινωνίας μπορούν να ξεκινήσουν την μετάδοση δεδομένων στο ίδιο κανάλι χρησιμοποιώντας την κοινή BSSID wildcard που διαθέτουν, γλυτώνοντας τις καθυστερήσεις που μπορεί σε άλλη περίπτωση να μην τα επίτρεπε να επικοινωνήσουν. Επίσης το WAVE χρησιμοποιεί την μέθοδο πολυπλεξίας EDCA(802.11e), η οποία βασίζεται στο CSMA/CA. Το CSMA/CA έχει μεγαλύτερη

πιθανότητα απόδοσης καναλιού σε υπηρεσίες με μεγαλύτερη προτεραιότητα χρησιμοποιώντας έναν μηχανισμό αποχής από το μέσο (backoff) ώστε να εξασφαλίσει ότι το κανάλι είναι διαθέσιμο για τον κόμβο που έχει μεγαλύτερη προτεραιότητα για μετάδοση. Τέλος το φυσικό επίπεδο του 802.11p διαφοροποιείται από το φυσικό επίπεδο του 802.11a αφού η συχνότητα λειτουργίας του είναι στα 5.9GHz αντί για 5GHz και έχει εύρος ζώνης 10MHz ενώ το 802.11 έχει 20MHz [6],[7],[9].

2.5.2 4G LTE

Στο άλλο άκρο των τεχνολογιών πρόσβασης στα V2X βρίσκεται το πρότυπο LTE. Το πρότυπο αυτό έχει οριστεί από την 3GPP και προσφέρει πολύ καλές επιδόσεις στο κομμάτι της καθυστέρησης και του ρυθμού μετάδοσης. Το LTE θεωρητικά μπορεί να προσφέρει ρυθμό δεδομένων downlink 150Mbps ενώ για uplink δεδομένα φτάνει τα 50Mbps. Χρησιμοποίει ένα εύρος ζώνης 20MHz και σε συνδυασμό με την χαμηλή καθυστέρηση των 5ms, μπορεί να καλύψει τις περισσότερες απαιτήσεις των εφαρμογών στα οχηματικά δίκτυα. Η αρχιτεκτονική του LTE αποτελείται από το δίκτυο πρόσβασης (E-UTRAN) και το δίκτυο κορμού (EPC).

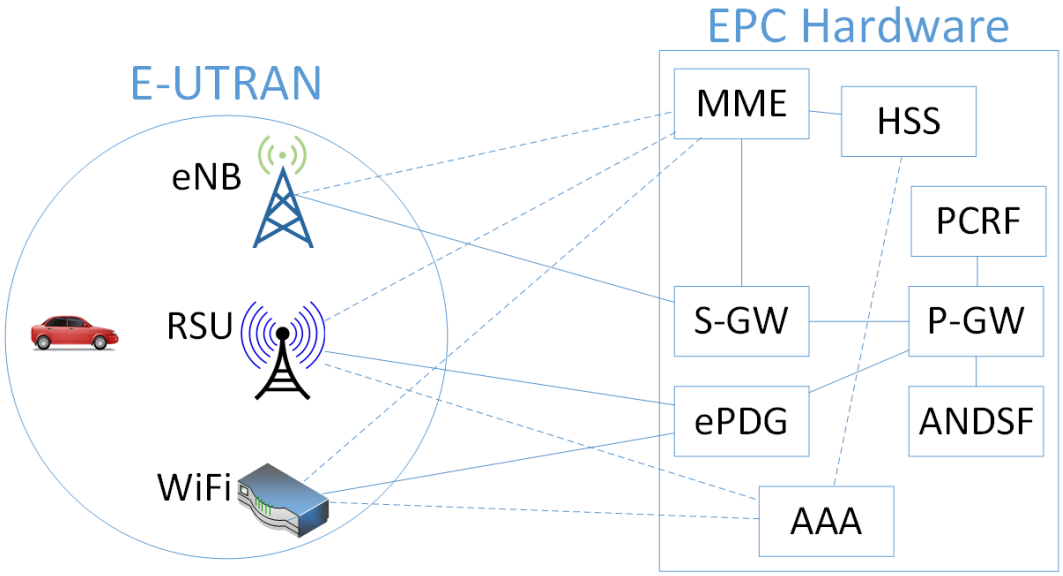

Figure 5. Αρχιτεκτονική LTE δίκτυών.

Το E-UTRAN είναι η διεπαφή σύνδεσης του MN με το σκελετό των δικτυών πρόσβασης ανεξάρτητα της τεχνολογίας του κάθε δικτύου. Είναι μια ασύρματη τεχνολογία πρόσβασής με στόχο να αντικαταστήσει της προηγούμενες τεχνολογίες των UMTS, HSDPA και HSUPA που είχαν καθοριστεί στις προηγούμενες εκδόσεις της

3GPP. Χρησιμοποιεί την OFDMA τεχνολογία πολυπλεξίας για το downlink και την SC-FDMA για το uplink. Το E-UTRAN αποτελείται από έναν μοναδικό κόμβο, το eNobeB που είναι υπεύθυνος για την επικοινωνία με το MN. Αυτή η απλούστευση της αρχιτεκτονικής στοχεύει στην μείωση της καθυστέρησης επικοινωνίας. Επίσης, το E-UTRAN διασυνδέεται με άλλες τεχνολογίες πρόσβασης όπως το Wi-Fi και το 802.11p, ώστε το MN να μπορεί να συνδεθεί σε οποιαδήποτε διαθέσιμο δίκτυο.

Η στοίβα πρωτοκόλλων του E-UTRAN αποτελείται από 3 επίπεδα. Το κατώτερο επίπεδο είναι το φυσικό το όποιο μεταφέρει όλες τις πληροφορίες από τα ανώτερα επίπεδα στο φυσικό μέσο. Υλοποιεί λειτουργίες όπως η μέτρηση της ποιότητας του καναλιού, η ανίχνευση λαθών, η εύρεση κυψελών για συγχρονισμό και διαπομπή και η ρύθμιση της ισχύς των καναλιών. Στην συνέχεια το 2^{ο} επίπεδο είναι το επίπεδο σύνδεσης δεδομένων, το οποίο αποτελείται από τα υπό-επίπεδα MAC, RLC(Radio Link Control), PDPC(Packet Data Convergence) και RRC(Radio Resource Control).

Η λειτουργία του επίπεδου ελέγχου πρόσβασης MAC είναι να συνδέσει το φυσικό επίπεδο με τα ανωτέρα υπό-επίπεδα και να προσφέρει ένα σύνολο λογικών καναλιών στο RLC τα οποία στην συνέχεια πολυπλέκονται σε κανάλια μεταφοράς του φυσικού επιπέδου. Επίσης διαχειρίζεται την διόρθωση σφαλμάτων μέσω HARQ (Hybrid automatic repeat request), καθορίζει την προτεραιότητα μεταξύ των λογικών καναλιών ενός MN καθώς και την προτεραιότητα για μετάδοση μεταξύ του πλήθους των MN.

Στην συνέχεια το επίπεδο RLC μεταφέρει τα PDU(Packet Data Unit) από το PDCP επίπεδο. Έχει 3 τύπους λειτουργίας που σχετίζονται με την αξιοπιστία που αποδίδει. Ανάλογα με τον τύπο λειτουργείας προσφέρει διόρθωση λαθών μέσω ARQ (Automatic repeat request), τμηματοποίηση και συνένωση των PDU, αναδιάταξη των PDU για την παράδοση τους με σωστή ακολουθία και τέλος ανίχνευση των διπλότυπων PDU.

Το επίπεδο PDCP υλοποιεί την μεταφορά των δεδομένων του ανώτερου επιπέδου RRC προσφέροντας υπηρεσίες κρυπτογράφησης και διατήρησης της ακεραιότητας των δεδομένων. Πρόσθετα μεταφέρει τα IP πακέτα που προέρχονται από το IP layer ενώ επιπλέον συμπιέζει της κεφαλίδες των πακέτων με ROHC (Robust Header Compression) και κρυπτογραφεί τα πακέτα.

Το τελευταίο υπό-επίπεδο του επιπέδου σύνδεσης δεδομένων είναι το RRC το οποίο φροντίζει για την μετάδοση των πληροφοριών του συστήματος που σχετίζονται με το επίπεδο πρόσβασης, αλλά και την μεταφορά των μηνυμάτων NAS(Non-Access

Stratum). Τέλος υλοποιεί την σελιδοποίηση, την εγκαθίδρυση και την απελευθέρωση των RRC συνδέσεων. Επίσης διαχειρίζεται τα κλειδιά ασφάλειάς και είναι υπεύθυνο για τις διαδικασίες μετρήσεων στα MN σχετικά με την κινητικότητά τους εντός του δικτύου.

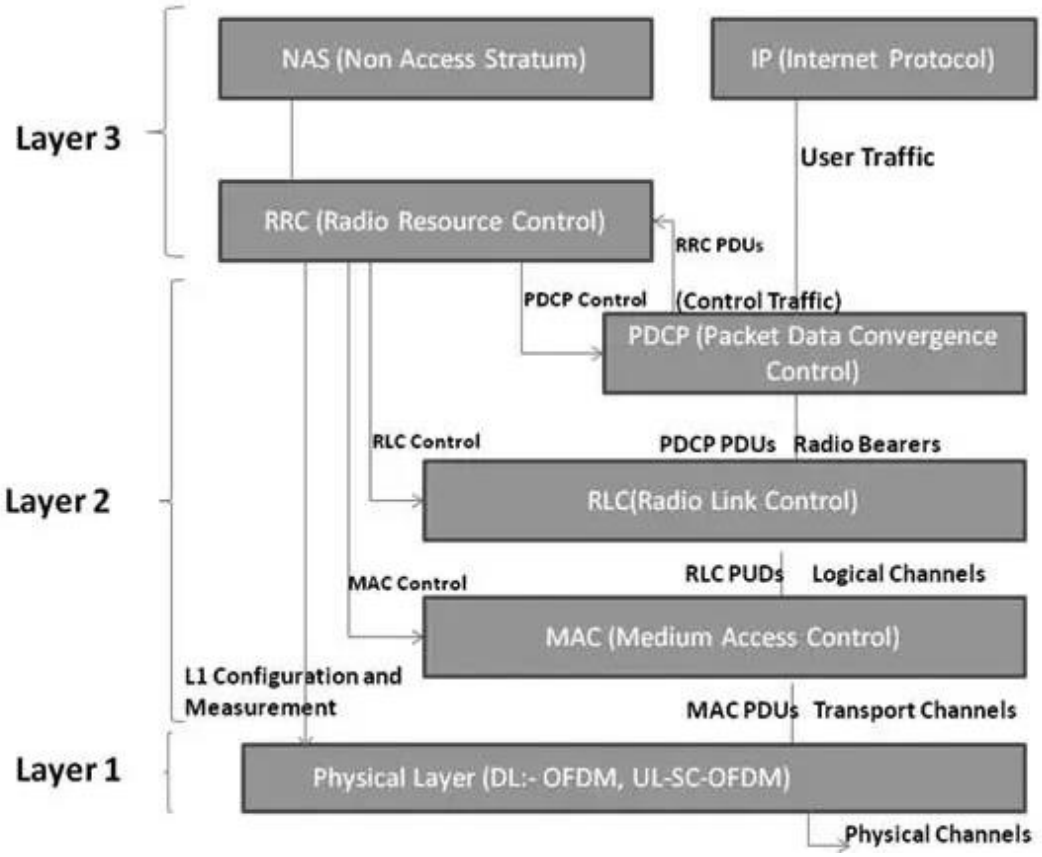

Figure 6. Στοίβα πρωτοκόλλων του E-UTRAN [32].

Το δίκτυο κορμού EPC είναι μια εξέλιξη της packet-switch αρχιτεκτονικής που χρησιμοποιούταν στις GPRS και UMTS τεχνολογίες. Έτσι η μετάδοση της φωνή και η αποστολή των σύντομων μηνυμάτων SMS που χρησιμοποιούσαν packet και circuit switch, θα υλοποιούνται με διαδικασίες βασισμένες στην IP αρχιτεκτονική. Ακόμα, αποφασίστηκε η διαδικασία της μετάδοσης των δεδομένων των χρηστών και η διαδικασία της σηματοδοσίας να ξεχωριστές και υλοποιημένες από διαφορετικές οντότητες ώστε να μπορεί εύκολα να προσαρμοστεί και να αλλάξει το μέγεθος του δικτύου. Οι οντότητες του EPC είναι το S-GW(serving gateway), το PDN-GW(packet data network gateway),το MME(mobility management entity) και το HSS(home subscriber server).

Το S-GW διαχειρίζεται την κίνηση των δεδομένων μεταξύ του MN και των εξωτερικών δικτύων. Είναι το σημείο σύνδεσης του δικτύου πρόσβασης με το δίκτυο κορμού EPC και δρομολογεί το εισερχόμενα και εξερχόμενα IP πακέτα. Επίσης λειτουργεί σαν mobility anchor των MN για τις εσωτερικές διαπομπές μεταξύ των eNobeB αλλά και για τις διαπομπές μεταξύ του LTE και άλλων τεχνολογιών πρόσβασης. Τέλος ενεργοποιεί την διαδικασία paging όταν το MN εισέρχεται σε idle κατάσταση.

Η οντότητα διαχείρισης κινητικότητας MME είναι ο κύριος κόμβος ελέγχου για το δίκτυο πρόσβασης LTE. Είναι υπεύθυνη για τις διαδικασίες paging και παρακολούθησης όταν το MN βρίσκεται σε κατάσταση αναμονής(idle), καθώς και για τις τυχόν αναμεταδόσεις των δεδομένων που θα προκύψουν. Επίσης συμμετέχει στην διαδικασία της ενεργοποίησης και απενεργοποίησης του φορέα. Ακόμα είναι υπεύθυνη για την επιλογή του S-GW το όποιο θα εξυπηρετήσει το MN κατά την αρχική σύνδεση του στο δίκτυο. Επίσης στην περίπτωση της εσωτερικής LTE διαπομπής είναι υπεύθυνη για την επιλογή του κόμβου που θα συνεχίσει να εξυπηρετεί το MN. Οι υπόλοιπες λειτουργίες του είναι η αυθεντικοποίηση του χρήστη και την παραγωγή και κατανομή προσωρινών ταυτοτήτων στα MN. Τέλος η οντότητα MME είναι υπεύθυνη για την κινητικότητα αναμεσά στο LTE και στα 2G/3G δίκτυα πρόσβασης μέσω της διεπαφής S3 που διασυνδέεται με την οντότητα SGSN.

Ο PDN-GW παρέχει την συνδεσιμότητά του MN με τα εξωτερικά δίκτυα πακέτων δεδομένων, αφού είναι ο κόμβος εξόδου και είσοδού της κυκλοφορίας των πακέτων του MN.Το MN συνήθως έχει πολλαπλές συνδέσεις σε διαφορικούς PDN-GW ώστε να έχει πρόσβαση σε πολλαπλά εξωτερικά δίκτυα πακέτων δεδομένων. Οι λειτουργίες του είναι η επιβολή της πολιτικής του πρωτοκόλλου, το φιλτράρισμα και ο έλεγχος των πακέτων του κάθε MN και η παρακολούθηση τους όσο αφορά την νομιμότητα τους.

Ο HSS είναι η κύρια βάση δεδομένων με τα στοιχεία χρήστη, η οποία βρίσκεται σε έναν κεντρικό κόμβο. Επιτρέπει στους πάροχους υπηρεσιών επικοινωνίας να διαχειρίζονται τους πελάτες τους σε πραγματικό χρόνο. Μέσω του HSS οι πάροχοι μπορούν να ορίζουν της υπηρεσίες και λειτουργίες που παρέχονται σε κάθε πελάτη, την ενεργοποίηση και την απενεργοποίηση των SIM, και τον διαχωρισμό των πελατών ανάλογα με την συνδρομή τους. Η λειτουργία του HSS είναι η συλλογή των πληροφορίων σχετικά με το προφίλ του συνδρομητή και ο έλεγχος των ταυτοτήτων τους. Στην συνέχεια μεταφέρει της πληροφορίες αυτές στο υπόλοιπο δίκτυο

επικοινωνώντας με την οντότητα MME μέσω της διεπαφής S6a. Επίσης σε συνδυασμό με έναν AAA(authentication,authorization,accounting) server, ο HSS μπορεί να διασφαλίσει ότι το δίκτυο κορμού μπορεί να διασυνδεθεί με άλλες τεχνολογίες πρόσβασης όπως το 802.11p και το Wi-Fi [8],[9].

2.5.3 5G Δίκτυα

Η σχεδίαση των προηγούμενων συστημάτων κινητών δικτύων ήταν διαμορφωμένη με πυρήνα τον άνθρωπο ως τελικό χρήστη. Οι τελικοί χρήστες θεωρούνταν ως πρώτης τάξης, έτσι οι πάροχοι με την εξέλιξη των κινητών δίκτυών τους στόχευαν να προσφέρουν στους χρήστες όλο και μεγαλύτερη χωρητικότητα και ταχύτητα ώστε να έχουν πάντα διαθέσιμες της υπηρεσίες που επιθυμούν. Η ανανεωμένη αρχιτεκτονική του 5G εισάγει καινούριες κατηγορίες χρηστών πρώτης τάξης, όπως είναι ο τομέας της αυτοκίνησης, της ενέργειας, της διαχείρισης των πόλεων, της φροντίδα υγείας και των έξυπνων συστημάτων μεταφοράς. Ακόμα, το 5G αναμένεται να προσφέρει βελτιώσεις στο κόμματι της ταχύτητας και της καθυστέρησης ώστε να μπορέσει να ικανοποιήσει τις απαιτήσεις που δημιουργούνται από τους νέους χρήστες. Για να επιτύχει τους παραπάνω στόχους, το 5G απομακρύνεται από το περιβάλλον της αρχιτεκτονικής των προηγουμένων τεχνολογιών που απαρτίζεται από ξεχωριστά φυσικά μηχανήματα ως οντότητες για τις λειτουργίες του δικτύου και προσανατολίζεται σε ένα περιβάλλον που βασίζεται στο λογισμικό ως αντικαταστατή των φυσικών μηχανημάτων. Για αυτόν το λόγο η αρχιτεκτονική του 5G είναι σχεδιασμένη να χρησιμοποιεί τεχνολογίες όπως software defined networks(SDN), λειτουργίες virtualization δικτύου (NFV) και υπολογιστικά νέφη(cloud computing).

Η αρχιτεκτονική των 5G δικτύων απαρτίζεται από το δίκτυο πρόσβασης NG-RAN και το δίκτυο κορμού 5GC. Το NG-RAN χρησιμοποιεί την νέα ράδιο-διεπαφή του 5G, καθώς επίσης διασυνδέεται με άλλα δίκτυα πρόσβασης, για να συνδέσει τους χρήστες με το δίκτυο κορμού. Πιο συγκεκριμένα, μπορεί να διασυνδεθεί με δίκτυα πρόσβασης παλαιότερης τεχνολογίας ορισμένα από την 3GPP(LTE) αλλά και με δίκτυα διαφορετικής τεχνολογίας(Wi-Fi, WAVE). Το NG-RAN αποτελείται από τους σταθμούς βάσης gNB, οι οποίοι είναι συνδεδεμένοι μεταξύ τους μέσω φυσικών διεπαφών. Η αρχιτεκτονική του gNB είναι κατανεμημένη και διαμορφώνεται από την κεντρική μονάδα (gNB-CU) που ελέγχει ένα πλήθος από κατανεμημένες μονάδες (gNB-DU). Η gNB-DU συνδέεται σε ένα απομακρυσμένο ραδιοπομπό (RRH:remote

radio head) και έτσι παρέχεται η επικοινωνία με το MN. Η gNB-CU επίσης διαχωρίζεται στην μονάδα λειτουργίας επιπέδου ελέγχου (gNB-CU-CP) και στην μονάδα λειτουργίας επιπέδου χρήστη (gNB-CU-UP) υιοθετώντας τον διαχωρισμό των διαδικασιών ελέγχου και διαδικασιών μετάδοσης δεδομένων του χρήστη που έχει εισαχθεί στο LTE.

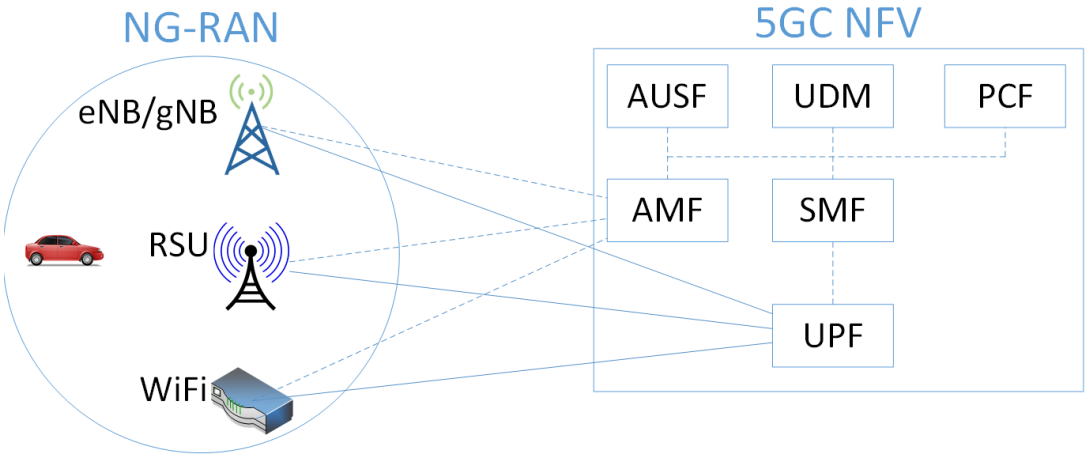

Figure 7. Αρχιτεκτονική 5G δίκτυών.

Τον ίδιο τρόπο διαχωρισμού του gNB-CU, ακολουθεί και η λίστα πρωτοκόλλων του 5G, δηλαδή υπάρχει μια λίστα πρωτόκολλων για την λειτουργιά χρήστη και μια δεύτερη λίστα για την λειτουργιά ελέγχου. Κοινά επίπεδα μεταξύ των 2 λιστών είναι το φυσικό επίπεδο, το επίπεδο ελέγχου πρόσβασης MAC, το πρωτόκολλο radio link control (RLC) και το πρωτόκολλο data convergence protocol (PDCP). Στα λίστα της λειτουργίας του χρήστη προστίθεται το service data adaptation protocol (SDAP), ενώ αντίστοιχα στη λίστα της λειτουργίας ελέγχου προστίθεται το radio resource control (RRC).

Το φυσικό επίπεδο υλοποιεί τις διαδικασίες επεξεργασίας των σημάτων που μεταφέρουν πληροφορίες ανάμεσα στα MN και τους σταθμούς βάσης. Χρησιμοποιεί την OFDMA πολυπλεξία με adaptive carrier spacing(15,30,60,120,240 KHz) και ένα σχήμα προσαρμογής διαμόρφωσης και κωδικοποίησης(π/2 BPSK σε 256QAM).

Το MAC είναι υπεύθυνο για τον βασικό έλεγχο του φυσικό επιπέδου. Κύρια λειτουργία του είναι ο προγραμματισμός των μεταδόσεων μεταξύ του κινητού και των σταθμών βάσεων gNB.

Το RLC εξασφαλίζει την αξιόπιστη μετάδοση των δεδομένων πού πρέπει να φτάσουν άθικτα μέσω του HARQ. Επίσης διαχειρίζεται την τμηματοποίηση των δεδομένων.

Το PDCP υλοποιεί λειτουργίες για την συμπίεση των κεφαλίδων των πακέτων και είναι υπεύθυνο για την ασφάλεια και ακεραιότητα των δεδομένων κατά την μετάδοση.

Το SDAP που περιέχεται στα επίπεδα της λειτουργίας του χρήστη διαχειρίζεται το QoS(quality of service) flow σε όλη την διεπαφή του 5G. Συγκεκριμένα κατά την περίοδο μια συνεδρίας PDU θα αντιστοιχίσει ένα συγκριμένο QoS flow σε ένα data radio bearer(μεταφορείς των δεδομένων πάνω στην ασύρματη διεπαφή) που έχει το καθορισμένο QoS. Επίσης σημειώνει τα πακέτα προς μετάδοση με το σωστό QFI(QoS Flow ID) για να διασφαλίσει την σωστή και γρήγορη προώθηση που απαιτεί το κάθε πακέτο κατά την μετάδοση του.

Τέλος, το RRC που περιέχεται στα επίπεδα της λειτουργίας ελέγχου είναι το πρωτόκολλο υπεύθυνο για την σηματοδοσία πρόσβασης του MN στους σταθμούς βάσης gNB. Οι κύριες λειτουργίες του είναι η εγκαθίδρυση και η απελευθέρωση των συνδέσεων και η μετάδοση των πληροφορίων συστήματος. Επίσης εγκαθιδρύει, αναδιαμορφώνει και απελευθερώνει τις συνδέσεις με τον radio bearer και διαχειρίζεται τις διαδικασίες κινητικότητας των συνδέσεων. Επιπλέον υλοποιεί το paging και ελέγχει την ισχύς των σταθμών βάσεων.

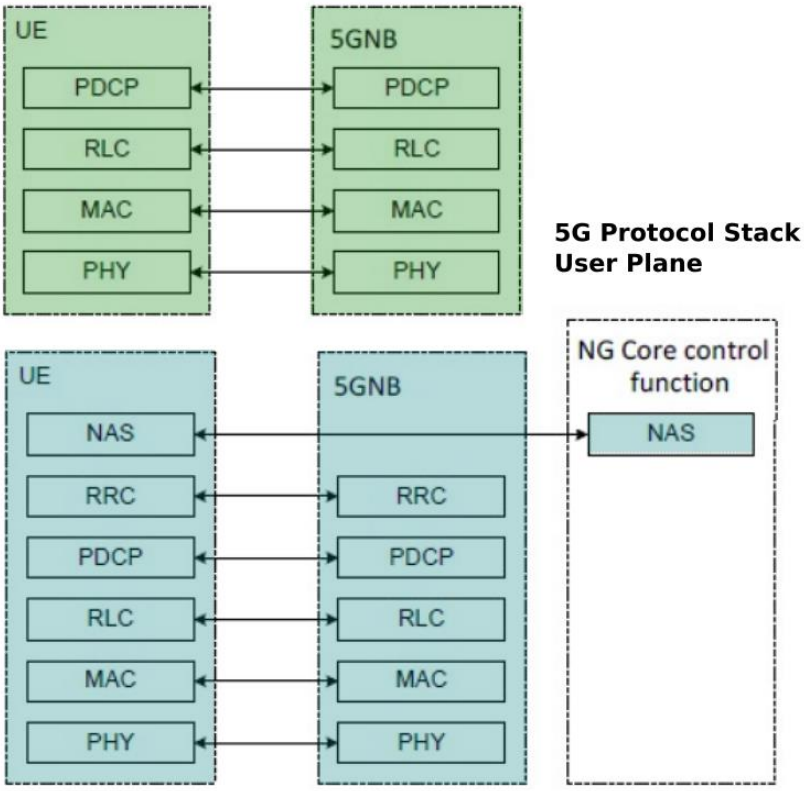

Figure 8. Στοίβα πρωτοκόλλων του NG-RAN [33].

Η αρχιτεκτονική του δικτύου κορμού του 5G(5GC) όπως προαναφέρθηκε βασίζεται στο virtualization. Έτσι, σε αντίθεση με τα προηγούμενα πρωτόκολλά που χρησιμοποιούν συγκεκριμένες φυσικές οντότητες για να επιτελέσουν τις λειτουργίες του δικτύου κορμού, οι λειτουργίες του 5GC ορίζονται από λογισμικό, τα network functions(NF). Το 5GC συνήθως περιέχει πολλαπλά αντίγραφα απο κάθε network function για να μπορεί να εξυπηρετεί το μεγαλύτερο δυνατό πλήθος χρηστών. Επίσης όπως και στο δίκτυο πρόσβασης NG-RAN υπάρχει διαχωρισμός στο user plane και στο control plane. Το user plane αποτελείται από τα UPF (user plane function), ενώ τα υπόλοιπα NFs ανήκουν στο control plane.

Πιο αναλυτικά το UPF περιέχει κομμάτια από τις λειτουργίες των SGW και PDN-GW στο LTE. Είναι υπεύθυνο για την μετάδοση των δεδομένων στις συνδέσεις των MN. Επίσης λειτουργεί ως mobility anchor για την διαδικασία της διαπομπής και επιβάλει τις πολίτικες για το QoS και την δικτυακή κίνηση.

Το SMF(session management function) περιέχει κομμάτια από τις λειτουργίες των MME και PGW στο LTE. Οι λειτουργίες του είναι η διαμόρφωση των συνδέσεων στο δίκτυο πρόσβασης, η έκδοση IP διευθύνσεων βάση του DHCP και η καθοδήγηση της κυκλοφορίας των πακέτων στο δίκτυο.

Το AMF(access and mobility management function) περιέχει κομμάτια από τις λειτουργίες του MME στο LTE. Είναι υπεύθυνο για την σηματοδοσία των τερματικών. Με την βοήθεια άλλων NF υποστηρίζει την πρόσβαση του χρηστών στο δίκτυο και διαχειρίζεται την κινητικότητα τους.

Το AUSF(authentication server function) περιέχει κομμάτια από τις λειτουργίες του MME στο LTE. Υλοποιεί λειτουργίες ελέγχου ταυτότητας για την πρόσβαση στα λοιπά δίκτυα της 3GPP (LTE,3G) αλλά και σε εξωτερικά δίκτυα που δεν ανήκουν στην 3GPP (802.11p,Wi-Fi).

Το UDM(unified data management function) περιέχει κομμάτια από την λειτουργία του HSS στο LTE. Αποτελεί την βάση δεδομένων για τις πληροφορίες των MN, όπως είναι τα διαπιστευτήρια και τα αναγνωριστικά τους καθώς και τις λειτουργίες του SMF που αφορά την συνέδρια του MN.

Το PCF(policy control function) περιέχει κομμάτια από την λειτουργία του PCRF στο LTE. Παρέχει τους κανόνες πολιτικής που πρέπει να ακολουθούνε τα υπόλοιπα network function του control plane.

Το NSSF (network slice selection function) δεν σχετίζεται με τις λειτουργίες του LTE. Η λειτουργία του είναι να επιλέγει το πλήθος των network slices που θα εξυπηρετήσει το MN. Το Network slice ορίζεται ως ένα λογικό δίκτυο επικοινωνίας με καθορισμένη αρχή και τέλος το όποιο βρίσκεται μέσα στο κινητό δίκτυο του 5G και αποτελείται από ένα κομμάτι του 5GC με τα network functions και το 5G-RAN. Η χρήση των Network slices επιτρέπει στους πάροχους διαδικτύου να φιλοξενούν απομονωμένες υπηρεσίες με τον ίδιο τρόπο που οι πάροχοι cloud προσφέρουν τις υπηρεσίες τους. Έτσι αρχικά οι καταναλωτές, ορίζουν τις προδιαγραφές όσο αφορά το εύρος ζώνης, την καθυστέρηση και την χωρητικότητα για την υπηρεσία που επιθυμούν να λειτουργεί στο network slice. Στην συνέχεια οι πάροχοι αφού αναλύσουν τις απαιτήσεις δημιουργούν ένα συμβόλαιο επιπέδου υπηρεσίας και αποδίδουν το network slice στον καταναλωτή. Τέλος το NSSF επιλέγει το καλύτερο AMF για να υποστηρίξει το MN.

Το NEF (network exposure function) σχετίζεται με το SCEF(service capabilities exposure function) στο LTE. Η λειτουργία του είναι να διευκολύνει την ασφαλή και φιλική πρόσβαση των προγραμματιστών στις ανοιχτές υπηρεσίες και δυνατότητες του δικτύου. Η πρόσβαση παρέχεται μέσω ενός συνόλου από RESTful APIs.

Το NRF (network repository function) δεν σχετίζεται με τις λειτουργίες του LTE. Είναι υπεύθυνό για την ανακάλυψη των network function και των πολλαπλών αντιγραφών τους. Όταν το NRF λάβει ένα αίτημα ανακάλυψης από κάποιο network function, παρέχει όλα τα αντίγραφα του αναζητουμένου network function [10],[11],[12].

Κεφάλαιο 3: Διαχείριση κινητικότητας

3.1 Διαχείριση θέσης

Οι διαδικασίες της διαχείρισης θέσεως επιτρέπουν στα δίκτυα την παρακολούθηση της τοποθεσίας των MN κατά την κίνηση τους στο περιβάλλον του δικτύου. Οι δυο βασικές λειτουργίες της διαχείρισης θέσης είναι η ανίχνευση και εγγραφή της τοποθεσίας του MN και στην συνέχεια η παράδοση κλήσεων στο MN. Επίσης παρακολουθεί συνεχώς την θέση των MN (paging) όταν είναι σε κατάσταση αδράνειας (idle). Για να επιτευχθεί η εγγραφή της τοποθεσίας, το MN σε τακτικά περιοδικά διαστήματα εκπέμπει το

συγκεκριμένο σήμα για να ενημερώσει την τρέχουσα θέση του στο δίκτυο. Άμεσα η υπεύθυνη οντότητα ενημερώνει την βάση δεδομένων που περιέχει τις θέσεις του κάθε MN. Μετά την ολοκλήρωση της διαδικασίας εγγραφής της τοποθεσίας, η διαδικασίας της παράδοσης κλήσεων μπορεί να ξεκινήσει. Για να μπορέσει μια εισερχόμενη κλήση να παραδοθεί στο MN, το δίκτυο αναζητεί την θέση του από την βάση δεδομένων και στην συνέχεια η κλήση προωθείται στον σταθμό βάσης που εξυπηρετεί την περιοχή. Κατά τον σχεδιασμό ενός συστήματος διαχείρισης θέση είναι θα πρέπει να ικανοποιούνται κάποιες απαιτήσεις όπως:

- Η ελαχιστοποίηση των διαδικασιών σηματοδοσίας και της καθυστέρησης κατά την παροχή των υπηρεσιών.
- Η ικανοποίηση του απαιτούμενου QoS που ζητάνε οι εφαρμογές και υπηρεσίες.
- Η σχεδίαση ενός αποτελεσματικού αλγορίθμου για την επιλογή του σωστού δίκτυού από το MN κατά την διαδικασία εγγραφής στις περιοχές που υπάρχουν πολλαπλά αλληλεπικαλυπτόμενα δίκτυα [15].

3.2 Διαχείριση διαπομπής

Η διαχείριση της διαπομπής (Handover) είναι υπεύθυνη για την διατήρηση της ενεργής σύνδεσης των MN κατά την μετακίνηση τους από ένα σημείο πρόσβασης σε κάποιο άλλο. Η διαδικασία του handover χωρίζεται σε τρία στάδια:

1. Το MN η κάποια οντότητα του δίκτυού ενεργοποιεί την διαδικασία διότι οι συνθήκες της σύνδεσης του MN αλλάζουν.
2. Η δημιουργία μιας νέας σύνδεσης και η εξασφάλιση των απαραίτητων πόρων για την μεταβίβαση της συνεδρίας του MN.
3. Εξασφάλιση της μεταφοράς των παλιών δεδομένων από τον προηγούμενο δίκτυο εξυπηρέτησης στο νέο, προσφέροντας το απαραίτητο QoS.

Ανάλογο με τον τύπο της κίνηση του τερματικού, η διαπομπή μπορεί να είναι:

- Οριζόντια οπού σε αυτήν την περίπτωση το MN υλοποιεί διαπομπή μεταξύ σημείων πρόσβασης της ίδια τεχνολογίας δικτύου (π.χ. LTE eNodeB -> LTE eNodeB, 802.11p RSU -> 802.11p RSU).
- Κάθετη, δηλαδή το MN υλοποιεί διαπομπή από ένα δίκτυο σε ένα δίκτυο διαφορετικής τεχνολογίας (π.χ 5G->LTE, LTE->802.11p)

Η διαδικασία της διαπομπής μπορεί να ενεργοποιηθεί σε μια από τις ακόλουθες περιπτώσεις:

- Η ισχύς του σήματος στο MN που λαμβάνεται από σταθμό βάσης πέφτει κάτω από το ορισμένο κατώφλι.
- Το MN κατά την κίνηση του στο περιβάλλον εξέρχεται από την περιοχή εξυπηρέτησης του προηγούμενου δικτύου και εισέρχεται στην περιοχή ενός άλλο δικτύου.
- Το MN επιλέγει να συνδεθεί σε ένα επικαλυπτόμενο δίκτυο με καλύτερες συνθήκες σύνδεσης λόγω των απαιτήσεων των υπηρεσιών και την εφαρμογών που χρησιμοποίει.
- Το δίκτυο παρουσιάζει μεγάλο φορτίο και απαιτείται η διανομή των MN στα γειτονικά σημεία πρόσβασης αλλά και σε δίκτυα διαφορετικής τεχνολογίας για να αποφευχθεί η συμφόρηση [15].

3.3 Πρωτόκολλα Διαχείρισης κινητικότητας

3.3.1 Mobile IPv6(MIPv6)

Το Mobile IPv6 παρέχει την υποστήριξη κινητικότητας για το πρωτόκολλο IPv6 μεταξύ ομογενών και ετερογενών τύπων δίκτυών (LTE->802.11p). Το κύριο χαρακτηριστικό του είναι η διατήρηση της ίδιας διεύθυνσης διαδικτύου (IP) του MN σε όλο το κόσμο και επιτρέπει στις υπηρεσίες και εφαρμογές των MN να διατηρούν τη σύνδεση τους κατά την αλλαγή τοποθεσίας του MN.

Στο IPv6 κάθε MN αναγνωρίζεται από δυο IP διευθύνσεις, την home address και την care-of-address. Η home address είναι μια σταθερή IP διεύθυνση που προσδιορίζει το MN ανεξάρτητα της τοποθεσίας του και του ξένου τοπικού δικτύου που είναι συνδεδεμένο. Η care-of-address αλλάζει κάθε φορά που το MN συνδέεται σε κάποιο ξένο δίκτυο και παρέχει πληροφορίες για την τωρινή κατάσταση του. Έτσι, κατά την σύνδεση του MN στο ξένο δίκτυο, το MN πρέπει να αποκτήσει μια care-of-address διεύθυνση, η οποία θα χρησιμοποιείται για όσο διάστημα το MN παραμένει συνδεδεμένο στο συγκεκριμένο δίκτυο.

Έτσι, ορίζονται δυο δίκτυα το home network(HN) και το foreign network(FN). Το HN είναι το τοπικό δίκτυο που συνδέεται το MN κατά την αρχική είσοδο του σε ένα

καινούριο δίκτυο πρόσβασης και λαμβάνει από αυτό την home address διεύθυνση του. Ως FN ορίζεται το ξένο τοπικό δίκτυο που επισκέπτεται το MN όταν είναι απομακρυσμένο από το HN.

Στο HN βρίσκεται ο home agent(HA). Όταν το MN βρίσκεται μακριά από το HN,το MN στέλνει στον HA πληροφορίες σχετικά με την τοποθεσία του και στην συνέχεια έχοντας εγκαθιδρύσει ένα τούνελ με το HN, ο HA μπορεί να προωθήσει τα πακέτα του MN. Επίσης ο HA αναλαμβάνει την αντιστοίχιση της home address διεύθυνσης με την care-of-address, μέσω της διαδικασίας του binding. Το IPv6 παρέχει δυο τρόπους επικοινωνίας όταν το MN βρίσκεται μακριά από το HN.

Ο τρόπος επικοινωνίας Bidirectional Tunnel χρησιμοποίει αποκλειστικά τον HA ως ενδιάμεσο κόμβο ώστε το MN να λάβει και να στείλει τα πακέτα από το corresponding node(CN). Ως CN ορίζεται μια οντότητά που βρίσκεται σε κάποιο 3^{ο} ξένο τοπικό δίκτυο διαφορετικό από αυτό του MN.

Ο τρόπος αυτός απαιτεί από τον HA να υποστηρίζει την δυνατότητα IPv6 neighbor discovery. Το IPv6 neighbor discovery επιτρέπει στους κόμβους να ανακαλύψουν την link-layer διεύθυνση των υπόλοιπων κόμβων που βρίσκονται στο ίδιο δίκτυο.

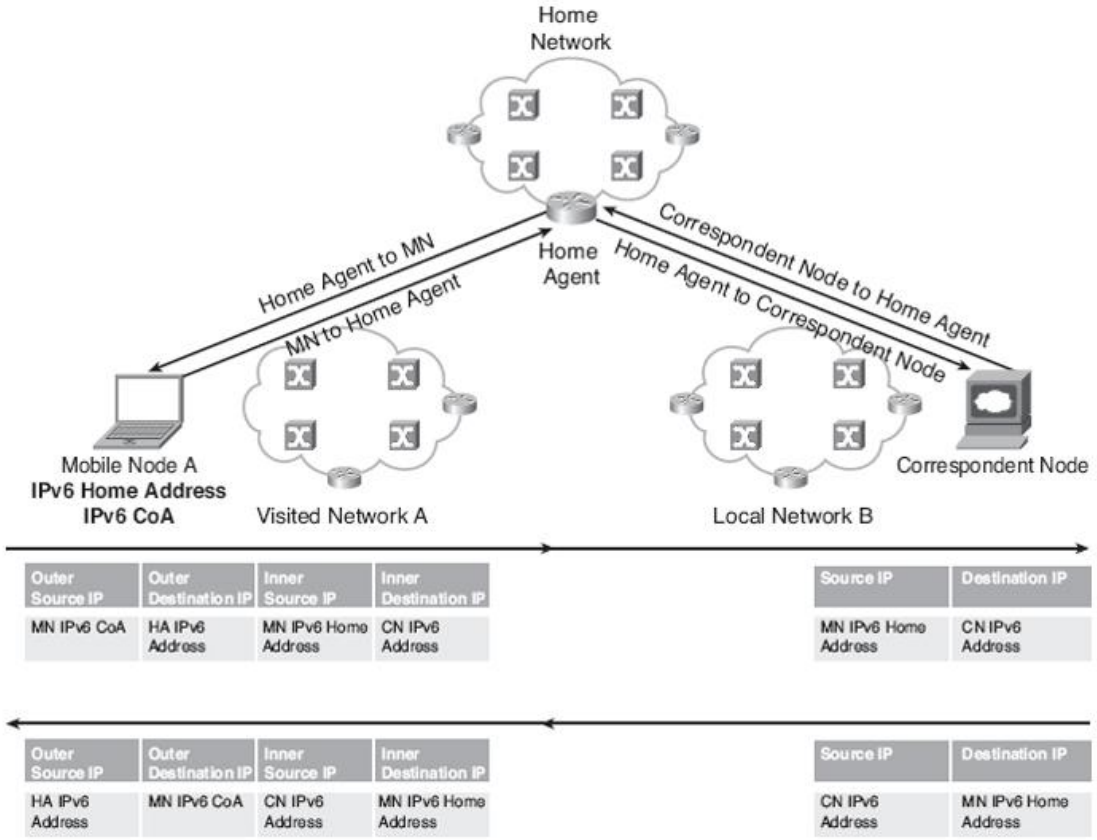

Figure 9. Λειτουργεία Bidirectional Tunnel του MIPv6 [16].

Το Router Optimization είναι ένας αμέσως τρόπος επικοινωνίας του MN με το CN. Σε αυτήν την περίπτωση ο CN απαιτείται να υποστηρίζει το MIPv6 πρωτόκολλο. Μετά την ανταλλαγή των μηνυμάτων συγχρονισμού Binding Update και Binding Acknowledgment, ο CN δηλώνει την care-of-address διεύθυνση του MN στην βάση δεδομένων του και μέσω αυτής επικοινωνεί με το MN χωρίς την παρουσία του HA στην διαδικασία. Ο τρόπος αυτός βοηθάει στην αντιμετώπιση της συμφόρησης που μπορεί να εμφανιστεί λόγο της μεγάλης κίνησης που υπάρχει στον HA [16],[17].

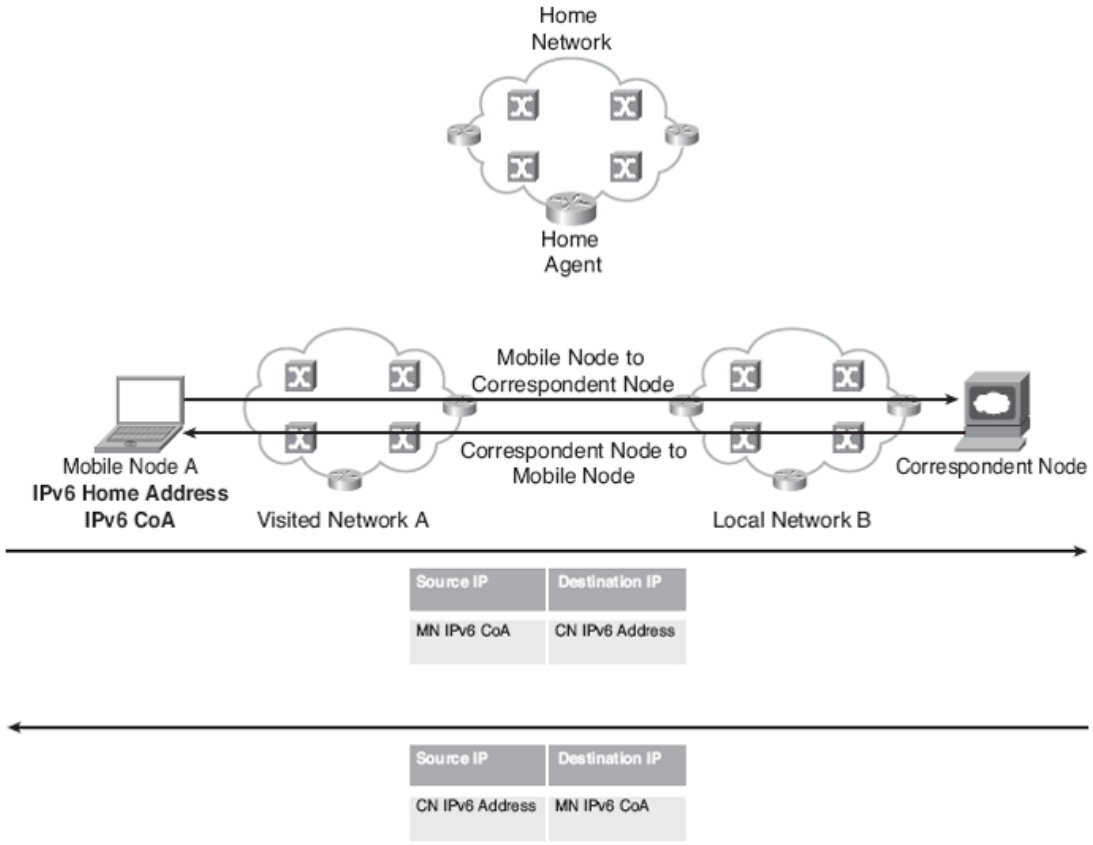

Figure 10. Λειτουργεία Router Optimization του MIPv6 [16].

3.3.2 Proxy Mobile IPv6 (PMIPv6)

Η σχεδίαση του πρωτόκολλου PMIPv6 βασίζεται στο MIPv6, αφού στοχεύει να επεκτείνει τις διαδικασίες σηματοδοσίας που ορίζονται στο MIPv6 και επαναχρησιμοποιεί τις έννοιες που υπάρχουν σε αυτό. Σε αντίθεση με την αρχιτεκτονική του MIPv6, στο PMIPv6 οι λειτουργίες για την διαχείριση κινητικότητας υλοποιούνται εξολοκλήρου από το δίκτυο χωρίς να χρειαστεί κάποια ενέργεια από το MN. Επομένως το MN δεν συμμετέχει σε οποιαδήποτε διαδικασία σηματοδοσίας και ο proxy mobility agent που βρίσκεται στο δίκτυο πρόσβασης είναι υπεύθυνος για να εκτελέσει την σηματοδοσία εκ μέρους του MN.

Όταν το MN εισέλθει σε ένα καινούριο δίκτυο πρόσβασης που χρησιμοποιεί το PMIPv6 είναι απαραίτητο να ολοκληρώσει τον έλεγχο ταυτότητας του. Στην συνέχεια το δίκτυο πρόσβασης είναι υπεύθυνο για την διασφάλιση της συνεχής σύνδεσης του MN στο home network(HN) και την δυνατότητα να αποκτήσει την home address(HoA) από οποιοδήποτε τοπικό δίκτυο. Η home address είναι η διεύθυνση του MN που λαμβάνει από το home network κατά την αρχική είσοδο σε ένα δίκτυο πρόσβασης. Το

τερματικό θα συνεχίσει να χρησιμοποιεί την HoA για όσο περιφέρεται στο δίκτυο πρόσβασης. Επίσης το δίκτυο πρόσβασης είναι υπεύθυνο για την εκχώρηση ενός μοναδικού προθέματος home network στο MN, το οποίο θα το ακολουθεί κατά την πλοήγηση του στο δίκτυο πρόσβασης που λειτουργεί με PMIPv6. Από την προοπτική του MN, ολόκληρο το δίκτυο πρόσβασης εμφανίζεται ως το home network. Έτσι δεν υπάρχει ανάγκη για τον ορισμό της care-of-address του MN, όπως ήταν απαραίτητο στο MIPv6, αλλά ορίζεται η proxy care-of-address με την έννοια της διεύθυνσης των MAG.

Οι καινούριες οντότητες που εμφανίζονται στο PMIPv6 είναι το MAG(mobile access gateway) και το LMA(local mobility anchor). Το MAG είναι η πύλη της επικοινωνίας του MN με το τοπικό δίκτυο και στην συνέχεια με το υπόλοιπο δίκτυο πρόσβασης. Είναι υπεύθυνο για την ανίχνευση της κίνησης του MN και την σηματοδοσία σχετικά με την κινητικότητα του. Επίσης το MAG δημιούργει μια σήραγγα επικοινωνίας (tunnel) με το LMA έτσι ώστε στην συνέχεια να προωθηθούν τα πακέτα του MN στα εξωτερικά δίκτυα. Τέλος μια ακόμη λειτουργεία του είναι να μιμείται το home network.

Το LMA είναι παρόμοιο με το home agent(HA) του MIPv6, με την προσθήκη επιπλέον δυνατοτήτων για την υποστήριξη του PMIPv6. Ο αρμοδιότητα του LMA είναι να διατηρεί την προσβασιμότητα του MN ενώ κινείται στο δίκτυο πρόσβασης, ενώ αποτελεί και την πύλη είσοδού και εξόδου της κίνησης του MN με τα εξωτερικά δίκτυα. Επίσης περιέχει καταχωρήσεις προσωρινής μνήμης για τα στοιχεία του κάθε MN που εξυπηρετεί. Οι καταχωρήσεις του LMA είναι πιο εκτεταμένες από τις αντίστοιχες του HA στο MIPv6 και περιλαμβάνουν το:

- Το αναγνωριστικό του MN(MN-identifier)
- Το πρόθεμα home network του MN.
- Το αναγνωριστικό της αμφίδρομης σήραγγας μεταξύ του LMA και του MAG που εξυπηρετεί το MN.

Έτσι μέσω των παραπάνω καταχωρήσεων το LMA μπορεί να συσχετίσει το κάθε MN με το αντίστοιχο MAG που το εξυπηρετεί.

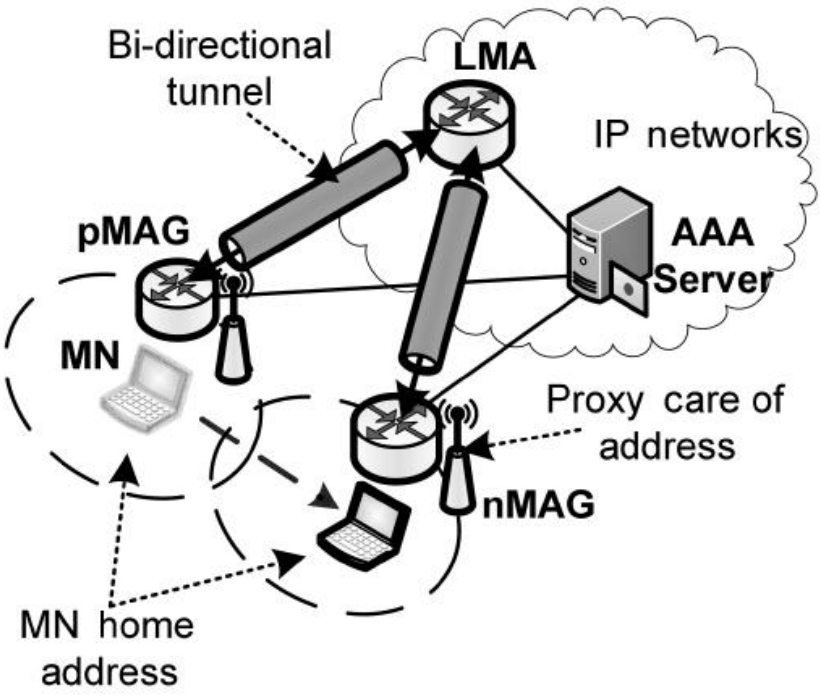

Figure 11. Αρχιτεκτονική Συστήματος PMIPv6 [34].

Στην συνέχεια παρουσιάζονται τα μηνύματα σηματοδοσίας για εγγραφή στο δίκτυο που ανταλλάσσονται κατά την είσοδο του MN σε ένα δίκτυο πρόσβασης που βασίζεται στο PMIPv6:

- Κατά την είσοδο του MN στο δίκτυο πρόσβασης, το MN στέλνει το Router Solicitation μήνυμα στο MAG που έχει συνδεθεί. Μετά την επιτυχή αυθεντικοποίηση του MN, το MAG αποκτά τις πληροφορίες του προφίλ του MN από τον AAA(authentication, authorization,accounting) server. Αυτές οι πληροφορίες μπορεί να είναι το αναγνωριστικό του, το LMA που είναι υπεύθυνο για το MN και την υποστηριζόμενη λειτουργία διαμόρφωσης διεύθυνσης.
- Στην συνέχεια, το MAG στέλνει το PBU(proxy binding update) μήνυμα στο LMA που περιέχει το identifier του MN.
- Το LMA αφού λάβει το PBU, ελέγχει ότι ο αποστολέας είναι εξουσιοδοτημένος να στείλει το μήνυμα. Αν ο αποστολέας είναι ένα έγκυρο MAG, το LMA κάνει δεκτό το PBU. Το LMA απαντάει στέλνοντας ένα PBA μήνυμα. Στο μήνυμα περιλαμβάνεται η επιλογή του home network προθέματος για το MN και επίσης αρχικοποιείται η δημιουργία του αμφίδρομου tunnel με το MAG.

- Μόλις το MAG λάβει το PBA μήνυμα ολοκληρώνεται η δημιουργία του tunnel και το MAG ρυθμίζει την διαδρομή για την προώθηση της κίνησης του MN. Στην συνέχεια το MAG στέλνει το Router Advertisement μήνυμα στο MN με περιεχόμενο το πρόθεμα home network που έχει οριστεί για το MN.
- Τέλος το MN μόλις λάβει το Router Advertisement, διαμορφώνει την διεπαφή του με stateful ή stateless τρόπο, βασισμένο στο τρόπο που επιτρέπεται στην συγκεκριμένη σύνδεση.

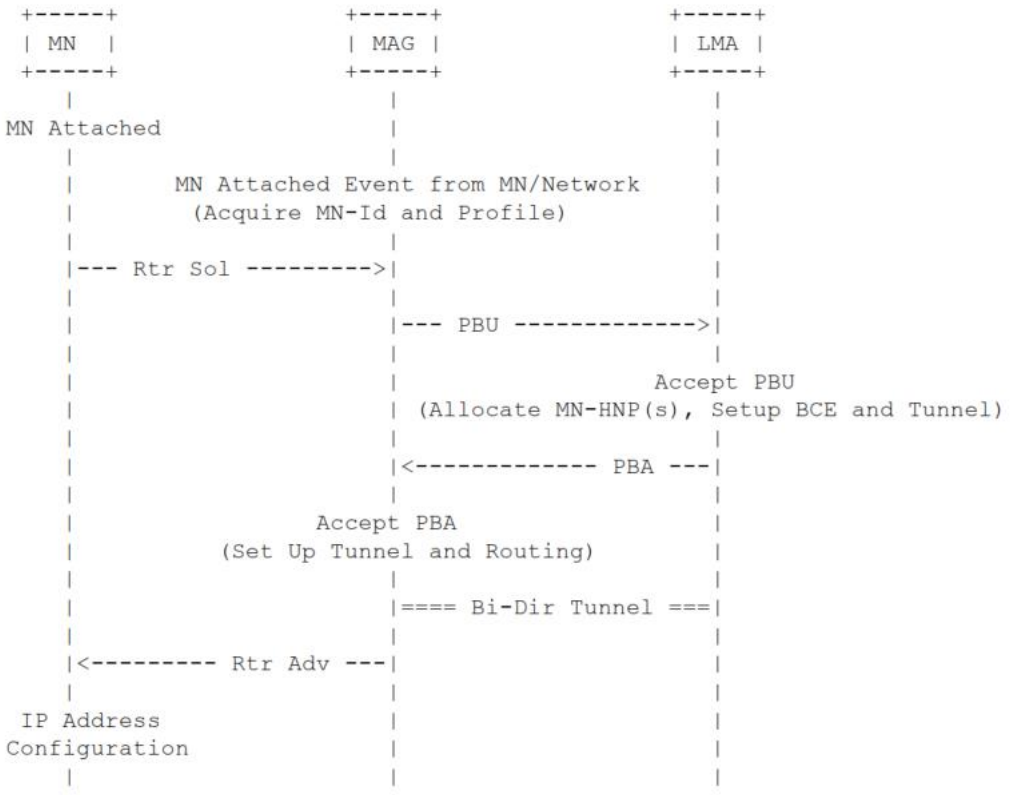

Figure 12. Σηματοδοσία για την εγγραφή του τερματικού στο δίκτυο για το PMIPv6 [18].

Η ανταλλαγή μηνυμάτων στην σηματοδοσία για την διαπομπή μεταξύ των MAG στο PMIPv6 διαμορφώνεται ως εξής:

- Μόλις το MN αποσυνδεθεί από το MAG της προηγούμενης σύνδεση(PMAG), το PMAG θα εντοπίσει την αποσύνδεση και στη συνέχεια θα επικοινωνήσει με το LMA στέλνοντας ένα PBU μήνυμα ως αίτηση αποσυσχέτισης του MN με το PMAG.
- Το LMA αφού λάβει το PBU, εντοπίζει την αντίστοιχη συνεδρία για το MN για την όποια έγινε το αίτημα αποσυσχέτισης και δέχεται το αίτημα.

Στην συνέχεια περιμένει για ένα συγκεκριμένο χρονικό διάστημα, το οποίο χρειάζεται το καινούριο MAG που θα εξυπηρετήσει το MN (NMAG) για να ενημερώσει την νέα συσχέτιση του με το MN στέλνοντας ένα PBU μήνυμα. Στην περίπτωση που δεν λάβει το PBU εντός του προκαθορισμένου χρόνου, διαγράφει την καταχώρηση συσχέτισης από την προσωρινή μνήμη του.

- Το LMA απαντάει στο NMAG με ένα PBA μήνυμα. Η διαδικασία της διαπομπής ολοκληρώνεται με την επανάληψή της διαδικασίας σηματοδοσίας για την αρχική είσοδο του MN στο δίκτυο πρόσβασης όπως περιγράφεται παραπάνω [17],[18].

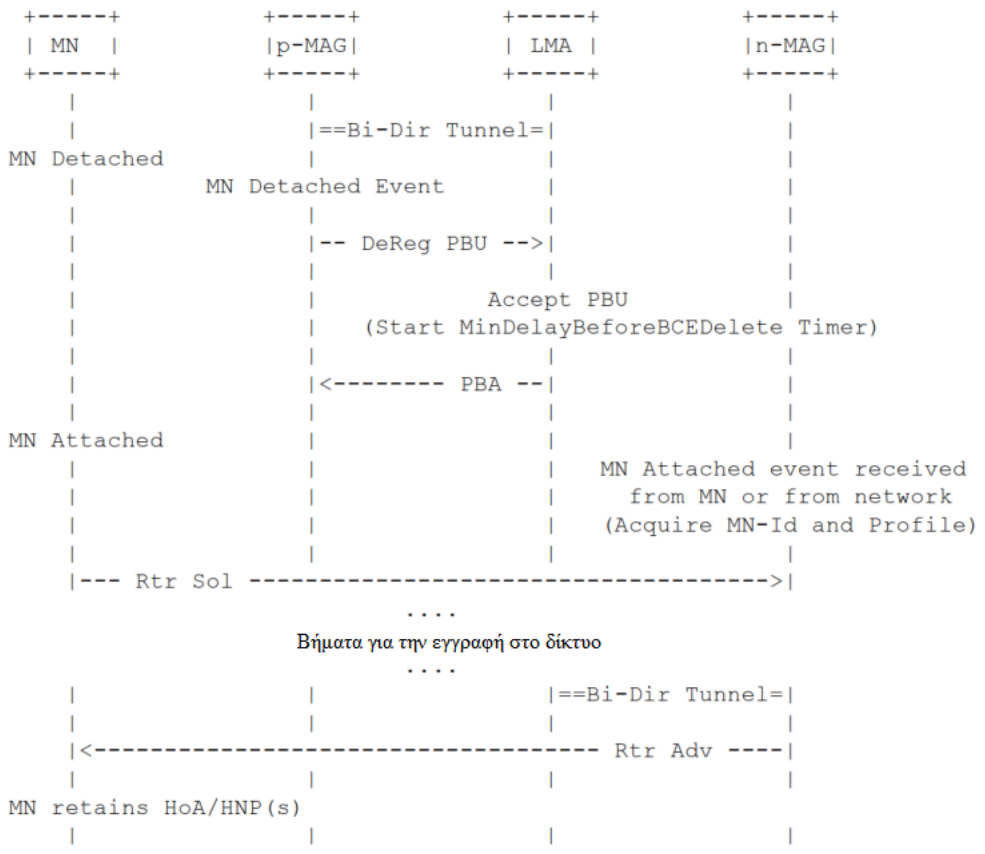

Figure 13. Σηματοδοσία για την διαπομπή στο PMIPv6 [18].

3.3.3 Fast Handovers for Mobile IPv6 (FMIPv6)

Το FMIPv6 επίσης είναι βασισμένο στο MIPv6 και στοχεύει στην μείωση της καθυστέρησης της διαπομπής. Η βασική ιδέα του πρωτοκόλλου είναι η έγκυρη επικοινωνία του MN με το καινούριο σημείο πρόσβασης έτσι ώστε να ρυθμίσει τις υπηρεσίες του για το MN, πριν την σύνδεση του MN στο σημείο πρόσβασης. Αυτές οι ρυθμίσεις μπορούν να είναι η εγκαθίδρυση της νέας care-of-address για το MN και η δημιουργία ένα αμφίδρομου tunnel μεταξύ του σημείου πρόσβασης που εξυπηρετούσε το MN πριν την διαπομπή (PAR:previous access router) και το σημείου πρόσβασης που θα εξυπηρετεί το MN μετά την διαπομπή (NAR:next access router). Στο FMIPv6 ορίζονται τα παρακάτω μηνύματα για την σηματοδοσία κατά την διαπομπή:

- Router Solicitation for Proxy Advertisement (RtSolPr): Ένα μήνυμα που στέλνετε από το MN στο PAR ζητώντας πληροφορίες για μια πιθανή διαπομπή.
- Proxy Router Advertisement (PrRtAdv): Το μήνυμα που στέλνεται από το PAR στο MN που περιέχει τις πληροφορίες σχετικά με γειτονικά σημεία πρόσβασης που λειτουργούν με το FMIPv6.
- Fast Binding Update (FBU): Ένα μήνυμα που αποστέλλεται από το MN ζητώντας από το PAR να ανακατευθύνει την κίνηση των πακέτων στο NAR.
- Fast Binding Acknowledgment (FBack): Ένα μήνυμα που στέλνεται από το PAR ως απάντηση στο FBU.
- Fast Neighbor Advertisement (FNA): Ένα μήνυμα από το MN προς το NAR για να ανακοινώσει την σύνδεση του σε αυτό και να επιβεβαιώσει την χρήση την νέας care-of-address(CoA) του MN, σε περίπτωση που δεν λάβει το μήνυμα FBack.
- Handover Initiate (HI): Ενα μήνυμα που στέλνεται από το PAR στο NAR σχετικά με την διαπομπή του MN.
- Handover Acknowledge (HAck): Ένα μήνυμα από το NAR στο PAR ως απάντηση στο HI.

Η διαδικασία της διαπομπής ξεκινάει με την αποστολή του RtSolPr από το MN στο PAR για να εύρεση των αναγνωριστικών των γειτονικών σημείων πρόσβασης. Στην συνέχεια το PAR ως απάντηση με το μήνυμα PrRtAdv επιστρέφει έναν πίνακα που περιέχει πλειάδες με τις πληροφορίες των γειτονικών σημείων πρόσβασης. Το MN μπορεί να στείλει το RtSolPr οποιαδήποτε στιγμή, για παράδειγμα μπορεί να είναι ως

απάντηση σε κάποιο γεγονός σχετικά με την σύνδεση του (trigger) η μπορεί να είναι μετά την εκτέλεση της εύρεσης γειτονικών σημείων πρόσβασης.

Στην συνέχεια, αφού το MN λάβει τις πληροφορίες για τα γειτονικά AR(σημεία πρόσβασης), το MN κατασκευάζει την καινούρια του πιθανή care-of-address(NCoA) και στέλνει το FBU μήνυμα στην περίπτωση που ένα γεγονός από το υπάρχον δίκτυο το ωθεί σε διαπομπή. Η λειτουργία του FBU είναι να συσχετίσει τις PCoA και NCoA μεταξύ τους, έτσι ώστε τα εισερχόμενα πακέτα για το MN να ανακατευθύνονται προς την νέα τοποθεσία του. Οπότε είναι εφικτό, προτιμάται το FBU μήνυμα να στέλνεται κατά την χρονική περίοδο που το MN είναι συνδεδεμένο στο PAR. Σε περίπτωση που δεν είναι εφικτό, το FBU στέλνεται από την καινούρια σύνδεση του MN.

Αν το MN λάβει το FBack όσο ακόμα έχει σύνδεση με το PAR τότε η διαπομπή συνεχίζει με την predictive λειτουργία. Πρώτου το PAR στείλει το FBack πρέπει να καθορίσει αν το NCoA του MN είναι αποδεκτό στο NAR μέσω της ανταλλαγής των HI και HACK. Στην συνέχεια γίνεται η προώθηση των πακέτων από το PAR στο NAR μέχρι την στιγμή που το MN θα συνδεθεί στο NAR. Τέλος το MN πρέπει άμεσα να στείλει το FNA μήνυμα, ώστε το NAR να προωθήσει τα buffered πακέτα σε αυτό.

Αν το MN δεν λάβει το FBack μήνυμα στην προηγουμένη σύνδεση του, η διαπομπή συνεχίζει με την reactive λειτουργία. Αυτό μπορεί να συμβεί γιατί το MN δεν έστειλε το FBU λόγο της πρόωρης αποσύνδεσης του από το PAR. Έτσι, αρχικά το MN ξαναστέλνει το FBU μόλις συνδεθεί στο NAR. Στην συνέχεια το MN πρέπει να στείλει το FNA ενσωματώνοντας το FBU για επιτρέψει στο NAR να επιβεβαιώσει την NCoA του MN και να προωθήσει σε αυτό το buffered πακέτα.

Επίσης μπορεί να συμβεί το παρακάτω σενάριο κατά την διαπομπή. Το RtSolPr δεν μπορεί να σταλθεί η το PrRtAdv δεν μπορεί να παραληφθεί κατά την περίοδο που το MN είναι ακόμα συνδεδεμένο με το PAR. Το MN δεν έχει καμία πληροφορία για τα γειτονικά σημεία πρόσβασης και η διαπομπή λειτουργεί σύμφωνα με το στάνταρ MIPv6 πρωτόκολλο [19].

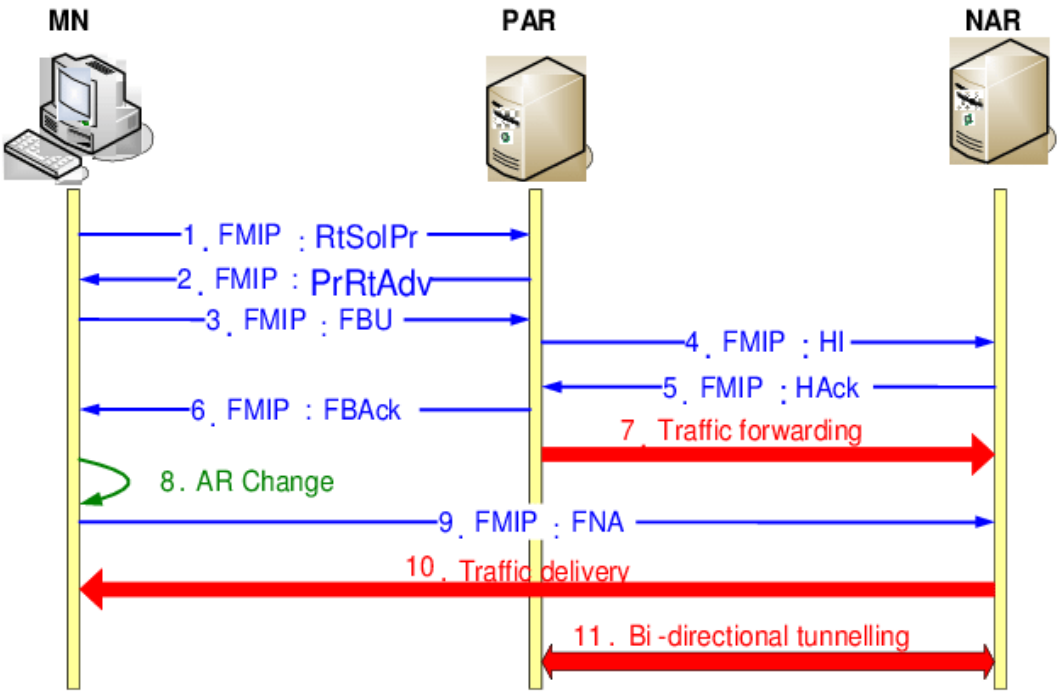

Figure 14. Σηματοδοσία για την διαπομπή στο FMIPv6 [35].

3.3.4 Fast Handovers for Proxy Mobile IPv6 (FPMIPv6)

Το πρωτόκολλο FPMIPv6 είναι μια βελτίωση του PMIPv6 σε συνδυασμό με το FMIPv6 και σχεδιάστηκε με στόχο να μειώσει την καθυστέρηση κατά την διαπομπή όσο αφορά το επίπεδο δικτύου και να ελαχιστοποιήσει την απώλεια των δεδομένων (packet loss). Το FMIPv6 βασίζεται στη ιδέα ότι:

- Η διαπομπή είναι δυνατόν να προβλεφθεί. Ως αποτέλεσμα το MAG το όποιο έχει επιλεχθεί να εξυπηρετήσει το MN μετα την διαπομπή(NMAG) μπορεί να στείλει ένα proxy binding update στο LMA πρόωρα. Στην συνέχεια το LMA μπορεί να ανακατευθύνει την downlink κίνηση του MN στο NMAG, έτσι ώστε τα δεδομένα να είναι άμεσα διαθέσιμα μόλις το MN συνδεθεί στο NMAG.
- Οποιαδήποτε downlink κίνηση που φτάνει στο MAG που προηγουμένως εξυπηρετούσε το MN πριν την διπομπή(PMAG) θα γίνεται buffered και στην συνέχεια θα προωθείται στο NMAG.

Πιο αναλυτικά, στο FPMIPv6 ορίζονται δυο πιθανά σενάρια διαπομπής. Στο predictive σενάριο, η διαδικασία της διαπομπής ξεκινάει με την ανάγκη του MN για διαπομπή, αποστέλλοντας το Handover Indication μήνυμα από το MN προς το προηγούμενο τοπικό δίκτυο (PAN) που εξυπηρετείται από το PMAG. Στην συνέχεια μόλις το PMAG

λάβει το μήνυμα αποθηκεύει (buffering) τα downlink πακέτα του MN και στέλνει το Handover Initiation μήνυμα στο NMAG. Το NMAG απαντάει με το Handover Acknowledgement μήνυμα και έτσι δημιουργείται ένα αμφίδρομο τούνελ επικοινωνίας μεταξύ των δυο MAG. Άμεσα το PMAG προωθεί το αποθηκευμένα πακέτα στο NMAG ώστε να αποθηκευτούν εκεί και να σταλούν στο MN όταν συνδεθεί. Αμέσως μετα το MN συνδέεται στο νέο τοπικό δίκτυο. Το LMA στέλνει τα downlink πακέτα στο PMAG και στην συνέχεια μαζί με τα αποθηκευμένα πακέτα στέλνονται στο MN μέσω του NMAG. Επίσης τα uplink πακέτα στέλνονται από το MN στο NMAG και σε συνέχεια στο LMA μέσω του PMAG. Τέλος το NMAG στέλνει το Proxy Binding Update στο LMA ώστε να ενημερώσει την εγγραφή στο Binding Cache και το LMA απαντάει με το Proxy Binding Acknowledgment. Από αυτό το σημείο τα δεδομένα του MN θα στέλνονται άμεσα μέσω του NMAG χωρίς να χρειάζεται το PMAG στην διαδικασία.

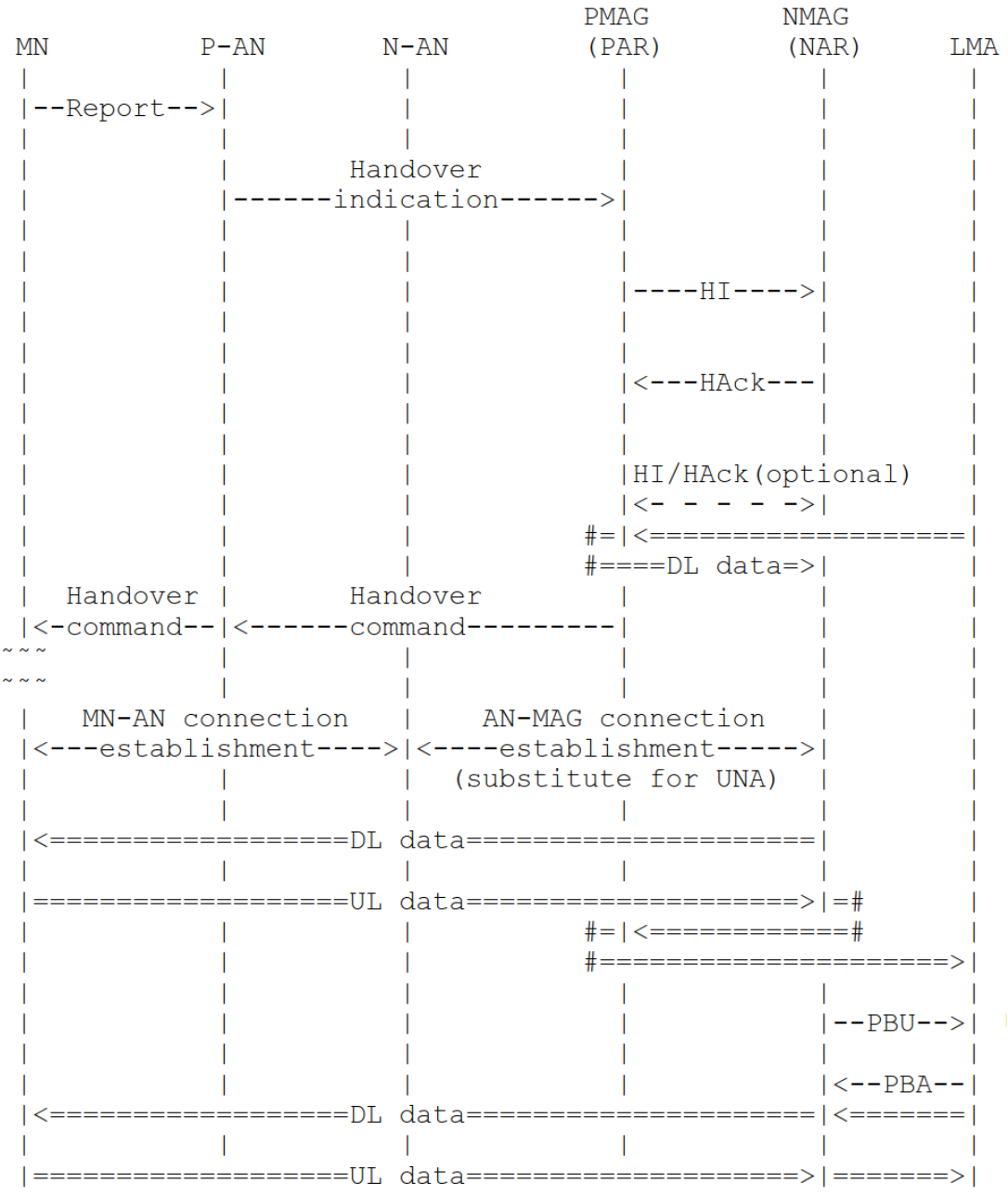

Figure 15. Σηματοδοσία predictive λειτουργίας για διαπομπή στο FPMIPv6 [20].

Το reactive σενάριο ορίζεται ως εξής: Μετά την απότομη αποσύνδεση του MN από το προηγούμενο τοπικό δίκτυο (PAN), συνδέεται άμεσα στο καινούριο τοπικό δίκτυο που εξυπηρετείται από το NMAG. Αρχικά το NMAG στέλνει το Handover Initiation μήνυμα στο PMAG. Το PMAG μόλις λάβει το μήνυμα αρχίζει το buffering των downlink πακέτων για το MN και απαντάει στο NMAG με το Handover Acknowledgement. Ως αποτέλεσμα δημιουργείται ένα αμφίδρομο τούνελ μεταξύ των MAG και το PMAG στέλνει τα buffered πακέτα στο NMAG για να αποθηκευτούν προσωρινά εκεί. Στην συνέχεια το LMA στέλνει τα downlink πακέτα στο PMAG και

στην συνέχεια μαζί με τα αποθηκευμένα πακέτα στέλνονται στο MN μέσω του NMAG. Επίσης τα uplink πακέτα στέλνονται από το MN στο NMAG και σε συνέχεια στο LMA μέσω του PMAG. Τέλος τα μηνύματα Proxy Binding Update και Proxy Binding Acknowledgment ανταλλάσσονται μεταξύ του LMA και του NMAG και το LMA ενημερώνει την εγγραφή στο Binding Cache [20].

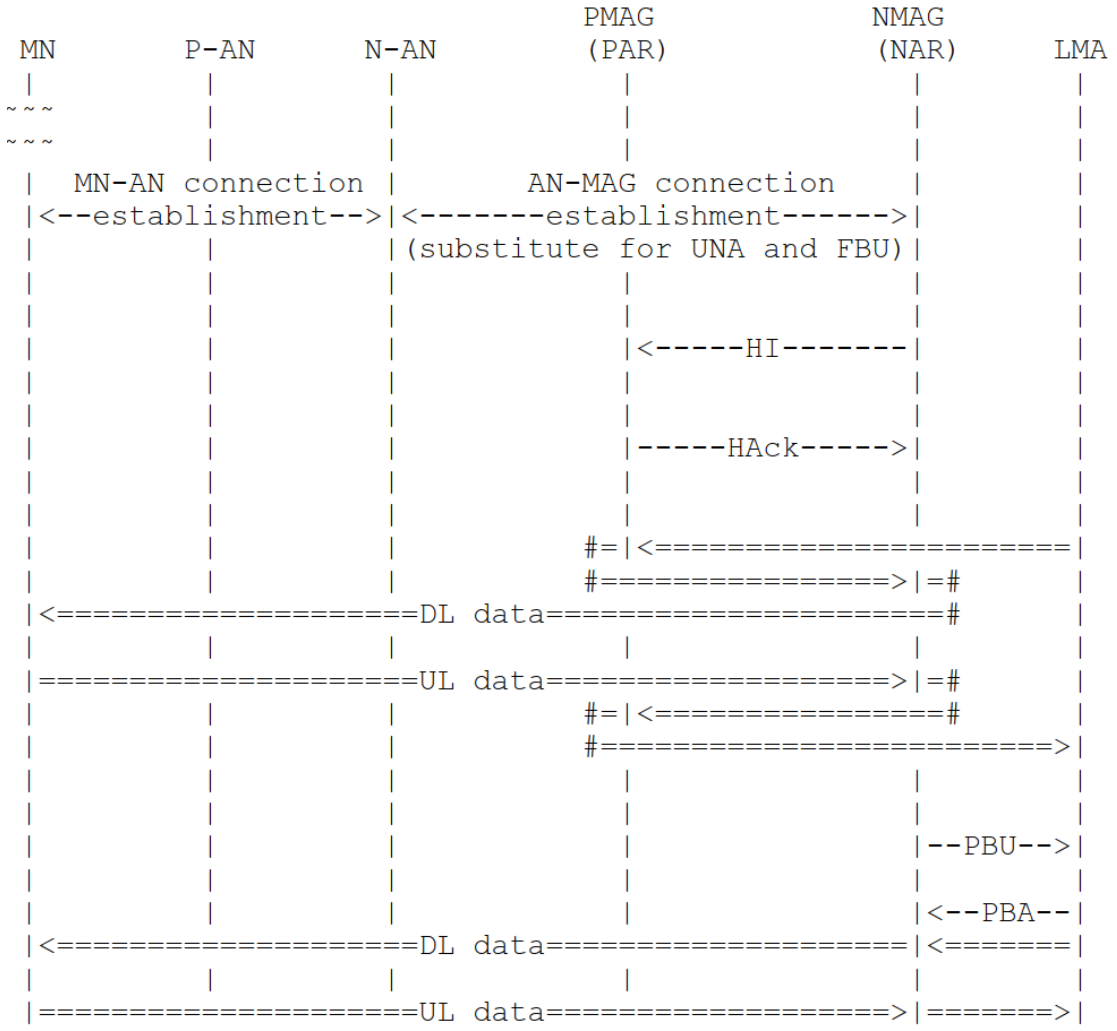

Figure 16. Σηματοδοσία reactive λειτουργίας για διαπομπή στο FPMIPv6 [20].

3.3.5 802.21 Media Independent Handover (MIH)

Το 802.21 είναι ένα πρωτόκολλο που συστάθηκε από την IEEE με σκοπό να διευκολύνει τις διαπομπές μεταξύ ετερογενών τεχνολογιών πρόσβασης (π.χ. κυψελωτά δίκτυα και 802.11 δίκτυα). Σύμφωνα με την λειτουργία αντιμετωπίζεται η διακοπή των υπηρεσιών κατά την διαπομπή και έτσι βελτιώνεται η εμπειρία των χρηστών. Το 802.21 παρέχει ένα framework που επιτρέπει την συνεχή επικοινωνία μεταξύ των ανώτερων και κατώτερων επίπεδων δικτυού για να συνεχίζουν να υποστηρίζουν τις συνεδρίες των MN ανεξάρτητα των ιδιαιτεροτήτων που παρουσιάζει η κάθε τεχνολογία πρόσβασης.

Τα χαρακτηριστικά γύρω από το οποία επικεντρώνεται ο σχεδιασμός του 802.21 είναι:

- Η δημιουργία ενός framework που επιτρέπει την απρόσκοπτη διαπομπή μεταξύ ετερογενών τεχνολογιών δικτυών. Το framework αποτελείται από μια λίστα πρωτοκολλούν στην οποία βασίζονται όλες οι οντότητες που εμπλέκονται στην διαδικασία της διαπομπής.
- Ο ορισμός ενός καινούριου επιπέδου αποτελούμενο απο διεπαφές SAP προσφέροντας μια κοινή βάση για τις λειτουργίες του επιπέδου ζεύξής. Επίσης το νέο επίπεδο θα πρέπει να είναι ανεξάρτητο από τις ιδιαιτερότητες της κάθε τεχνολογίας δικτύου.
- Ο ορισμός νέων διαδικασιών και λειτουργιών που θα προσθέσουν στα πρωτόκολλα κινητικότητας (MIPv6, FPMIPV6) την δυνατότητα να εκτελέσουν τις βελτιωμένες διαπομπές. Οι νέες λειτουργίες ενεργοποιούν μέσω του framework τα αντίστοιχα τοπικά η απομακρυσμένα πρωτοκολλά επιπέδου ζεύξης για κάθε ξεχωριστή τεχνολογία πρόσβασης που χρησιμοποιείται.

Παρόλου που ο κύριος στόχος του 802.21 είναι να επιτρέψει την διαπομπή μεταξύ των ετερογενών δίκτυών, ορίζονται και κάποιοι δευτερεύοντες στόχοι για το πρωτόκολλο:

- Η συνέχιση των υπηρεσιών που χρησιμοποιούν τα MN κατά την διάρκεια τις διαπομπής καθώς και μετά την ολοκλήρωση της. Δηλαδή το πρωτόκολλο στοχεύει στην αντιμετώπιση της ανάγκης για επανεκκίνηση των συνεδρίων των MN μετά την διαπομπή.
- Η δημιουργία εφαρμογών με την δυνατότητα επίγνωσης της διαπομπής. Το framework του 802.21 επιτρέπει στις εφαρμογές να συμμετέχουν στην

διαδικασία της διαπομπής. Για παράδειγμα, μια εφαρμογή φωνής μπορεί συμβουλέψει το MN να εκτελέσει διαπομπή κατά την περίοδο σιωπής ώστε να ελαχιστοποιηθεί η διακοπή της υπηρεσίας.

- Διαπομπές με βάση το QoS. Το framework παρέχει τις δυνατότητες ώστε η λήψη αποφάσεων για την διαπομπή να γίνονται με βάση τα κριτήρια QoS, ώστε να καλύπτονται οι απαιτήσεις των εφαρμογών.
- Ανακάλυψη του δικτύου. Το 802.21 προσφέρει την δυνατότητα στους χρήστες να ενημερώνονται με πληροφορίες σχετικά με κοντινούς γειτονικούς κόμβους για να εκτελέσουν διαπομπή.

Η αρχιτεκτονική των πρωτοκόλλων του 802.21 είναι κοινή μεταξύ του MN και των δίκτυών πρόσβασης. Η δομή των οντοτήτων του δικτύου επικεντρώνεται γύρω από το επίπεδο media-independed handover function(MIHF). Το MIHF αποτελεί ένα ενδιάμεσο επίπεδο ανάμεσα στα ανώτερα και στα κατώτερα επίπεδα πρωτοκόλλων με κυρία λειτουργία τον συντονισμό της ανταλλαγής των πληροφοριών εντολών μεταξύ των οντοτήτων που συμμετέχουν στην διαπομπή. Από την προοπτική του MIHF, κάθε οντότητα έχει ένα σύνολο χρηστών MIHF όπως είναι τα πρωτόκολλα κινητικότητας, που χρησιμοποιούν τις δυνατότητες του MIHF για τον έλεγχο και την συλλογή πληροφοριών της διαπομπής. Η επικοινωνία μεταξύ του MIHF επιπέδου των οντοτήτων και των υπόλοιπων επιπέδων βασίζεται σε ένα πλήθος καθορισμένων υπηρεσιών που ομαδοποιούνται σε διεπαφές SAP. Τα SAP που ορίζονται από το 802.21 είναι τα εξής:

- MIH_SAP: Αποτελεί την διεπαφή μεταξύ του επιπέδου MIHF και του υψηλότερου επιπέδου που είναι οι χρήστες MIH.
- MIH_LINK_SAP: Αποτελεί την διεπαφή μεταξύ του επιπέδου MIHF και των χαμηλότερων επιπέδων της λίστας πρωτοκόλλων.
- MIH_NET_SAP: Αυτή η διεπαφή υποστηρίζει την επικοινωνία μεταξύ απομακρυσμένων MIHF οντοτήτων. Για παράδειγμα το MIHF επίπεδο στο MN μπορεί να επικοινωνήσει με το αντίστοιχο MIHF επίπεδο που βρίσκεται στο 802.11 δίκτυο πρόσβασης.

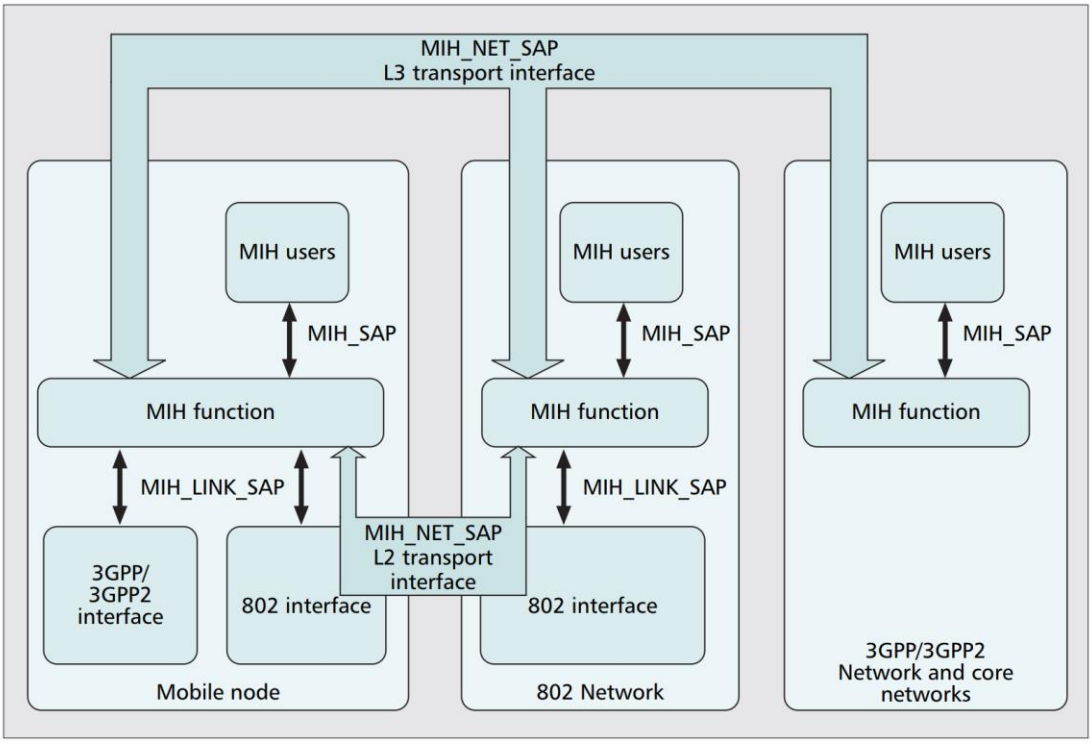

Figure 17. Αρχιτεκτονική πρωτοκόλλων στο 802.21 [37].

Επίσης στο 802.21 ορίζεται ένα μοντέλο αναφοράς για την σχεδίαση του δικτύου που περιλαμβάνει τις ακόλουθες οντότητες δικτύου:

- MIH MN (MIH mobile node): Αναφέρεται στο MN που ενσωματώνει τις λειτουργίες MIH και έχει πολλαπλές ασύρματες διεπαφές.
- MIH PoS (MIH point of service): Αναφέρεται σε μια οντότητα δικτύου που ενσωματώνει τις λειτουργίες MIH και ανταλλάσσει μηνύματα MIH με το MN. Σημειώνεται πως ένα MN μπορεί να επικοινωνεί με περισσότερα από ένα PoS κάθε στιγμή καθώς μπορεί να χρησιμοποίει πολλαπλές τεχνολογίες πρόσβασης.
- MIH non-POS: Αναφέρεται σε μια οντότητα δικτύου που ενσωματώνει τις λειτουργίες MIH και δεν έχει επικοινωνία με το MN.
- MIH PoA (MIH point of attachment): Αναφέρεται στο τελικό σημείο μιας σύνδεσης L2 όπου στο αρχικό σημείο βρίσκεται το MN.

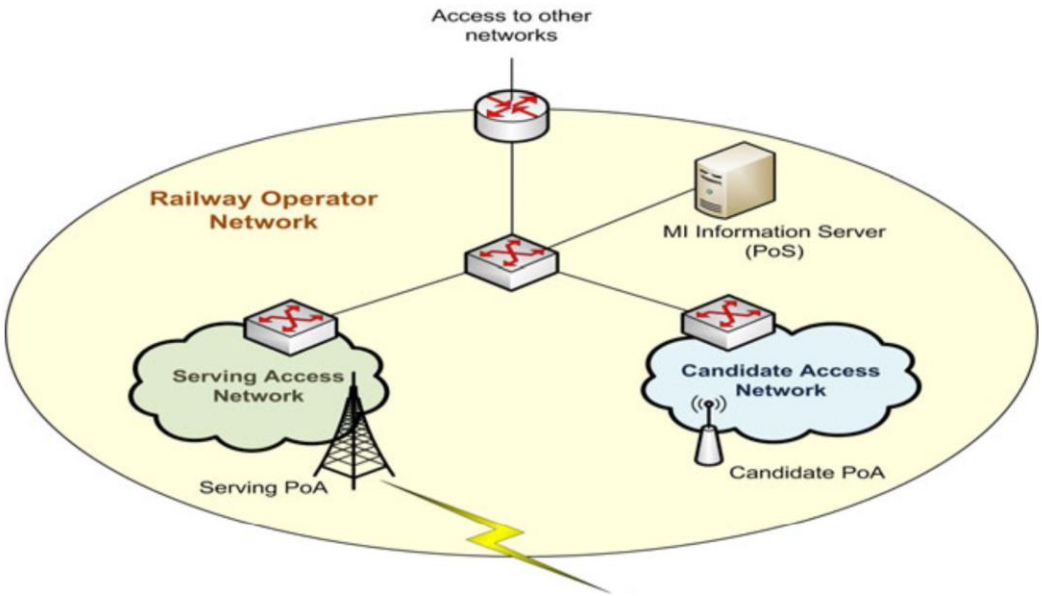

Figure 18. Οντότητες δικτύου στο 802.21 [36].

Τέλος στο σχεδιασμό του 802.21 ορίζονται 3 διαφορετικοί τρόποι επικοινωνίας που ονομάζονται υπηρεσίες MIH. Ο στόχος των υπηρεσιών MIH είναι η βοήθεια των χρηστών MIH σχετικά με την απόφαση για διαπομπή. Επίσης είναι υπεύθυνες για την έναρξη της διαπομπής καθώς και για την επιλογή του κατάλληλου δικτύου για διαπομπή. Ακόμα επιτρέπουν στους χρήστες MIH την πρόσβαση σε πληροφορίες για την διαπομπή και τέλος μεταφέρουν εντολές στα κατωτέρα επίπεδα της λίστας πρωτοκόλλου. Αναλυτικότερα, οι υπηρεσίες που ορίζονται στο πρωτόκολλο είναι οι εξής:

- MIES (media independent event services): Χρησιμοποιούνται για την αναφορά των δυναμικών αλλαγών που συμβαίνουν σχετικά με την κατάσταση, τα χαρακτηριστικά και την ποιότητα της ζεύξης. Οι αναφορές χωρίζονται σε δυο κατηγορίες. Η πρώτη κατηγορία ονομάζεται ως γεγονότα ζεύξης (link events), παράγονται στο επίπεδο ζεύξης και λαμβάνονται από το MIHF. Η δεύτερη κατηγορία ονομάζεται ως γεγονότα MIHF (MIHF events), παράγονται από το επίπεδο MIHF και αφορά τους χρήστες MIHF.
- MICS (media independent command services): Αντιπροσωπεύουν εντολές που στέλνονται από τα ανωτέρα επίπεδά της λίστας πρωτοκόλλων στα κατώτερα για τον προσδιορισμό της κατάστασης της ζεύξης ή για τον έλεγχο και την διαμόρφωση των MN. Οι εντολές αυτές είναι ιδιαίτερα σημαντικές στις περιπτώσεις των διαπομπών που ενεργοποιούνται και υποβοηθούνται από το

δίκτυο. Οι εντολές κατηγοριοποιούνται σε δυο κατηγορίες. Οι εντολές MIH (MIH commands) στέλνονται από τα ανώτερα επίπεδα στο επίπεδο MIHF. Παράδειγμα είναι οι εντολές “MIH Handover Initiate” και “MIH Handover Prepare”. Η άλλη κατηγορία είναι οι εντολές ζεύξης (Link commands). Παράγονται στο MIHF επίπεδο εκ μέρους των χρηστών MIHF και η χρήση τους είναι η διαμόρφωση και ο έλεγχος των κατώτερων επιπέδων.

- MISS (media independent information services): Επιτρέπει στο MIHF να λαμβάνει και να διανέμει πληροφορείς σχετικά με τα διαθέσιμα δίκτυα σε μια περιοχή. Με αυτό τον τρόπο το MN ενημερώνεται από την υπάρχουσα σύνδεση του για τα διάφορα δίκτυα πρόσβασης που είναι διαθέσιμα προς διαπομπή στην περιοχή του. Οι υπηρεσίες MISS χρησιμοποιούν ένα νέο τύπο δομών πληροφοριών που ονομάζονται Information Elements (IEs). Τα IEs παρέχουν πληροφορίες στα κατώτερα επίπεδά όπως είναι οι χάρτες γειτονικών κόμβων, οι ζώνες κάλυψης και άλλες παραμέτρους σύνδεσης. Επίσης παρέχουν πληροφορίες και στα ανώτερα επίπεδά όπως είναι η έλλειψη της συνδεσιμότητας στο διαδίκτυο και η διαθεσιμότητα ορισμένων υπηρεσιών.

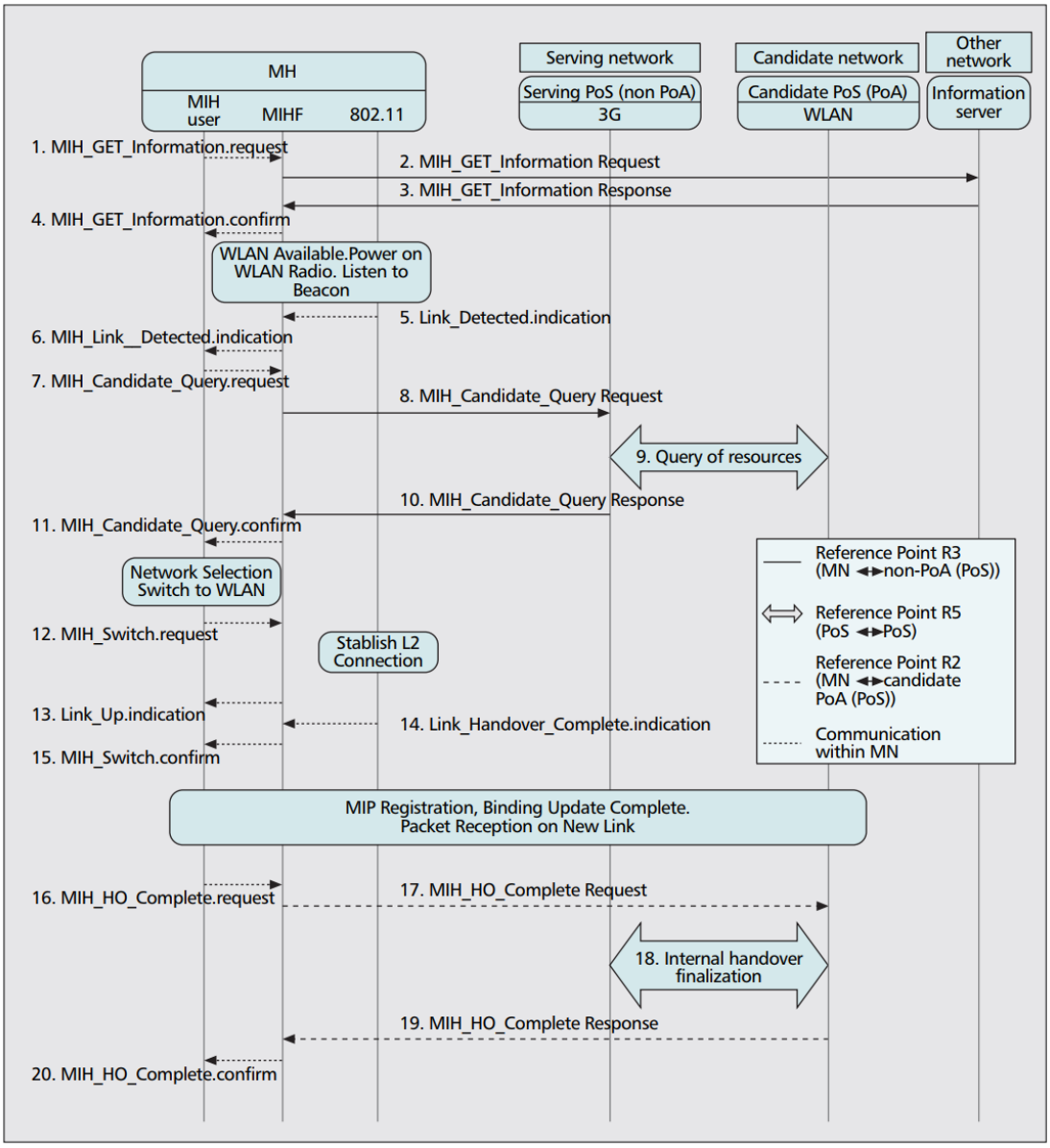

Figure 19. Διαπομπή βασισμένη στο 802.21 [37].

Στο Figure 19 παρουσιάζεται ένα παράδειγμα διαπομπής μεταξύ 2 ετερογενών δικτυών (3G->WiFi). Η διαδικασία της διαπομπής ξεκινάει με το αίτημα ανακάλυψης γειτονικών κόμβων που στέλνει το MN στον MIHF επίπεδο. Στην συνέχεια το αίτημα προωθείται από το MIHF στο server πληροφοριών του πάροχου. Έπειτα ο πάροχος απαντάει παρέχοντας πληροφορίες σχετικά με την δυνατότητα για διαπομπή σε δίκτυο WLAN για το συγκεκριμένο παράδειγμα. Το MN άμεσα ενεργοποιεί την WLAN διεπαφή και ξεκινάει την ανίχνευση για beacons μέσω του επιπέδου ζεύξης 802.11.

Μόλις ληφθεί κάποιο beacon, το επίπεδο ζεύξης του 802.11 δημιουργεί ένα Link_detected.indication μήνυμα και προωθείται στο MN μέσω του MIHF επιπέδου. Στην συνέχεια μόλις το MN λάβει το προηγούμενο μήνυμα, στέλνει στο MIHF ένα

μήνυμα σχετικά με την αναζήτηση των υποψήφιων δικτύων προς διαπομπή. Το MIHF προωθεί το μήνυμα στο PoS εξυπηρετεί το MN πριν την διαπομπή (PoS στο δίκτυο 3G). Το 3G PoS με την λήψη του μηνύματος ξεκινάει την αναζήτηση και επιλογή των διαθέσιμων υποψήφιων δίκτυών βασισμένο στους ελευθέρους πόρους του κάθε δικτύου. Η αναζήτηση γίνεται στέλνοντας διαδοχικά ερωτήματα για τους ελευθέρους πόρους στα PoS των γειτονικών δίκτυών. Το αποτέλεσμα της αναζήτησης προωθείται στο MN μέσω του MIHF με την μορφή μιας λίστας με τα υποψήφια δίκτυα.

Στην συνέχεια, το MN επιλέγει από την λίστα το κατάλληλο δίκτυο προς διαπομπή και στέλνει ένα αίτημα διαπομπής στο MIHF με αποτέλεσμα την αρχικοποίηση μιας σύνδεσης L2 WLAN. Το MIHF εκδίδει τις εντολές για την έναρξη της σύνδεσης και στέλνει στο MN ένα μήνυμα υποδεικνύοντας την έναρξη. Μόλις εγκαθιδρυθεί η σύνδεση, το MAC επίπεδο του WLAN εκδίδει ένα μήνυμα ολοκλήρωσης προς το MIHF και έπειτα προωθείται στο MN. Ακολουθεί η διαδικασία διαπομπής των ανωτέρων επιπέδων όπως παρουσιάζεται στα πρωτοκολλά κινητικότητας MIPv6 και το FPMIPv6.

Όταν η διαδικασία των ανώτερων επιπέδων ολοκληρωθεί το MN στέλνει το MIH_HO_Complete μήνυμα μέσω του MIHF στο επιλεγμένο PoS έτσι ώστε να ενημερώσει το ότι θα είναι το PoS που πλέον θα εξυπηρετεί το MN. Έπειτα το επιλεγμένο PoS (WLAN PoS) ενημερώνει το 3G PoS για την ολοκλήρωση της διαπομπής και την απελευθέρωση των πόρων του.

Τέλος, η διαδικασία της διαπομπής ολοκληρώνεται με την αποστολή του μηνύματος ολοκλήρωσης από το WLAN PoS στο MN μέσω του MIHF [36],[37].

3.3.6 Transient Binding for PMIPv6

Το Transient Binding για το PMIPv6 είναι ένας μηχανισμός που προτείνουν οι συγγράφεις για να βελτιώσουν την λειτουργία του PMIPv6. Η κύρια λειτουργεία του μηχανισμού είναι η δημιουργία μιας προσωρινής σύζευξης του MN με τον NMAG διατηρώντας ταυτόχρονα την ήδη ενεργή σύζευξη με το PMAG, σε αντίθεσή με την λειτουργία του PMIPv6 στην όποια άμεσα διαγράφεται η προηγουμένη συσχέτισης του MN με το PMAG μετα την διαπομπή. Έτσι το LMA έχει την δυνατότητα να δέχεται πακέτα ανόδου (uplink) και από τα δυο MAG. Τα δεδομένά καθόδου θα συνεχίσουν

να στέλνονται μέσω του PMAG όπως ορίζεται στο PMIPv6. Αυτή η δυνατότητα μπορεί να βοηθήσει στην αποφυγή απώλειών δεδομένων ανόδου και καθόδου, στην περίπτωση που η διαπομπή δεν ολοκληρωθεί και τα δεδομένα στο PMAG διαγραφτούν. Επίσης μειώνεται η πιθανότητα για την απώλεια πακέτων ανόδου λόγο υπερβολικού buffering πακέτων στο PMAG. Η διαδικασία διαπομπής με Transient Binding ξεκινάει με την αποστολή του πρώτου PBU μηνύματος από το NMAG στο LMA, με ενεργοποιημένη την επιλογή Transient θέτοντας την σημαία T με την τιμή 1. Έτσι πλέον το LMA έχει την δυνατότητα να δέχεται πακέτα ανόδου από το MN μέσω του PMAG και του NMAG. Στην συνέχεια αφού το MN έχει συνδεθεί στο NMAG και έχει ολοκληρώσει την ρύθμιση της νέας σύνδεσης του, το NMAG στέλνει ένα δεύτερο PBU με απενεργοποιημένη την επιλογή Transient, μετατρέποντας την προσωρινή συσχέτιση του με το MN σε ενεργή [21].

3.3.7 Partial Bicasting with Buffering for Proxy Mobile IPV6 Mobility Management in CoAP-BasedIoT Networks

Στο [22], οι συγγραφείς προτείνουν ένα βελτιωμένο σχήμα για διαπομπές βασισμένο στο PMIPv6. Το προτεινόμενο σχήμα βασίζεται στην ιδέα ότι ο LMA μπορεί να ξεκινήσει μια προσωρινή προώθηση των δεδομένων στο NMAG που θα εξυπηρετεί τον MN μετα την διαπομπή όσο και στο PMAG που τον εξυπηρετούσε προηγούμενα. Στο Partial Bicasting for PMIP, αφού το NMAG λάβει το Handover Initiation μήνυμα από το PMAG, στέλνει ένα PBU στο LMA δίνοντάς του εντολή να αρχίσει να προωθεί πακέτα και στα δύο MAG. Στη συνέχεια, το NMAG αρχίζει να αποθηκεύει τα δεδομένα downlink και δίνει εντολή στο PMAG να στείλει ένα PBU στο LMA για να διαγράψει την συσχέτιση του με το MN. Έτσι, με την αξιοποίηση μιας πρόωρης προσωρινής αποθήκευσης δεδομένων στο NMAG, μειώνεται η απώλεια πακέτων, ενώ επίσης μειώνεται και η καθυστέρηση της διαπομπής αφού τα δεδομένα του MN μπορούν να προωθηθούν απευθείας από το NMAG στο MN. Τέλος, οι συγγραφείς αναλύουν το σύστημά τους με προσομοίωση χρησιμοποιώντας το NS3. Η καθυστέρηση διαπομπής και η απώλεια πακέτων μειώνεται σημαντικά σε σύγκριση με το PMIPv6, ενώ επίσης και η ρυθμό-απόδοση βελτιώνεται ελαφρώς.

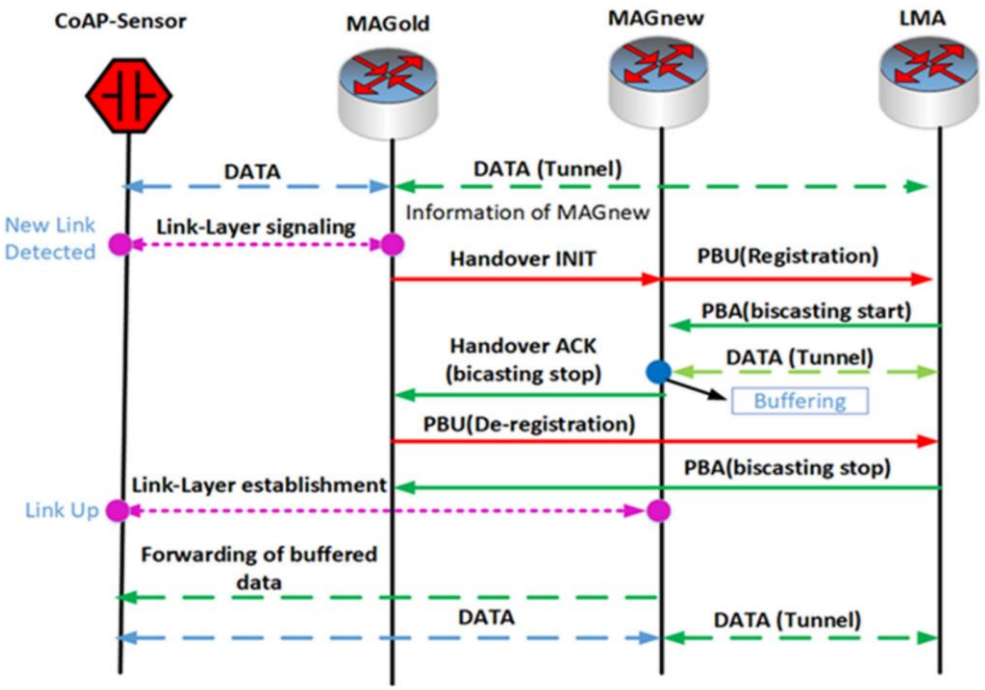

Figure 20. Σηματοδοσία στο Partial Bicasting for PMIP (PB-PMIP) [22].

3.3.8 FPMIPv6-S: A new network-based mobility management scheme for 6LoWPAN

Στο [23], οι συγγραφείς προτείνουν ένα βελτιωμένο σύστημα διαχείρισης κινητικότητας για ασύρματα δίκτυα αισθητήρων ονομαζόμενο ως FPMIPv6-S, ώστε να μειωθεί η καθυστέρηση της διαπομπής ενός MN. Οι δικτυακές οντότητες και οι λειτουργίες τους είναι παρόμοιες με εκείνες που παρουσιάζονται στο FMIPv6. Επίσης, εισάγονται δύο νέοι τύποι μηνυμάτων, το SBU, μια τροποποίηση του μηνύματος PBU και το SBA, μια τροποποίηση του μηνύματος PBA. Αυτά τα νέα μηνύματα χρησιμοποιούν το bit σημαίας "S-bit" για την τροποποίηση του μηνυμάτων PBU και PBA. Η διαδικασία της σηματοδοσίας είναι επίσης παρόμοια με τη διαδικασία του FMIPv6 με τη μόνη διαφορά ότι το μήνυμα SBU για τη συσχέτιση του MN με NMAG αποστέλλεται από το PMAG. Στη συνέχεια οι συγγραφείς αξιολογούν την απόδοση του προτεινόμενου σχήματος και το συγκρίνουν με το πρωτόκολλο MIPv6 και παρατηρούνται βελτιώσεις όσο αφορά την καθυστέρηση διαπομπής, την απώλεια πακέτων και την ρυθμό-απόδοση.

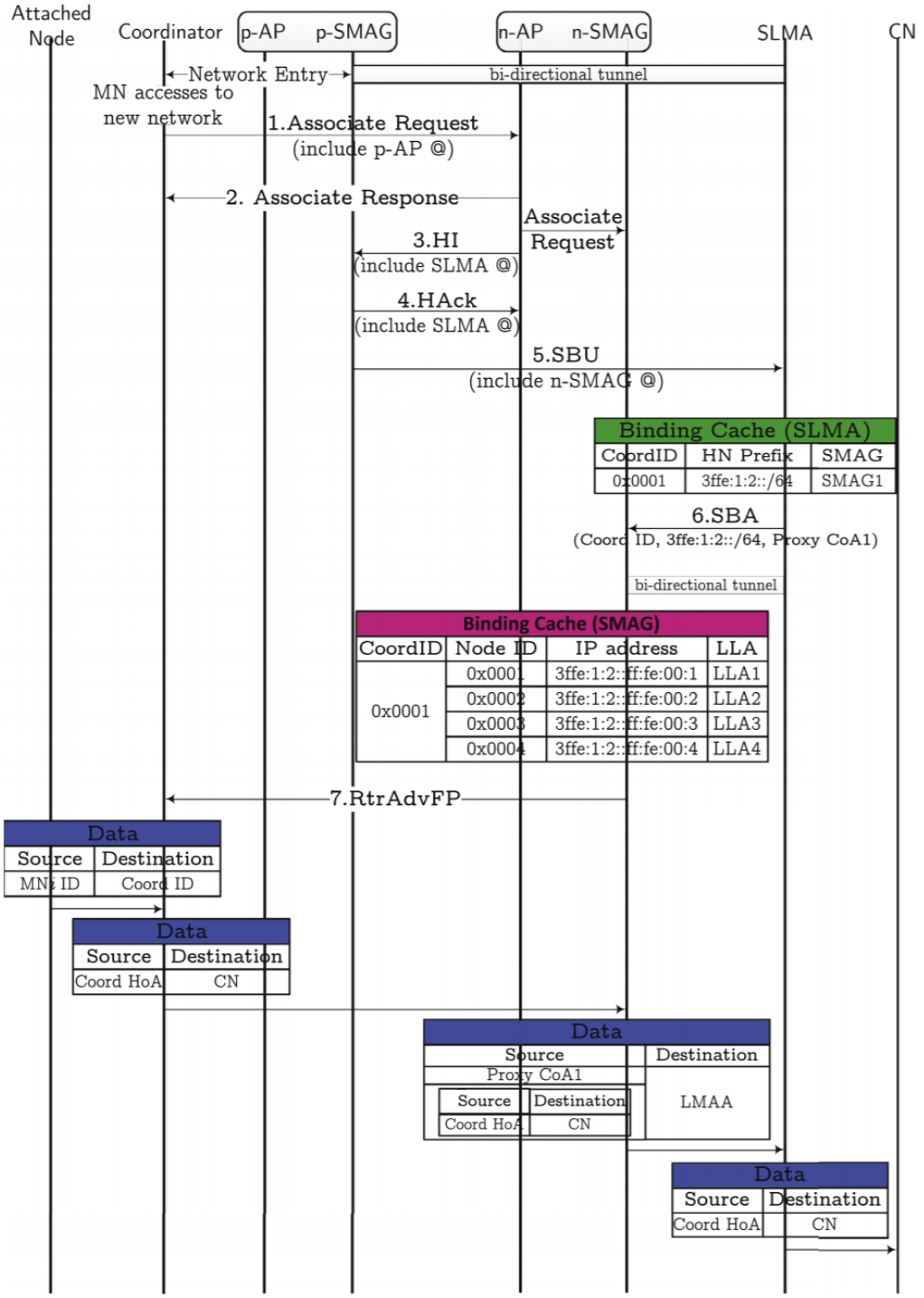

Figure 21. Σηματοδοσία στο FPMIPv6-S [23].

3.3.9 A Network-Based Seamless Handover Scheme for VANETs

Στο [24], προτείνεται ένα βελτιωμένο σχήμα για διαπομπές σε δίκτυα VANET. Το προτεινόμενο σχήμα υιοθετεί το πρωτόκολλο PMIPv6 και χρησιμοποιεί το δίκτυο πρόσβασης 802.11p για την επικοινωνία των οχημάτων. Οι συγγραφείς καλύπτουν τόσο τις inter-AR (handover μεταξύ RSUs που εξυπηρετούνται από το ίδιο MAG) όσο και τις intra-AR handover που είναι από MAG σε άλλο MAG. Εμείς δίνουμε έμφαση στη μελέτη της intra-AR διαπομπής, δεδομένου ότι το προτεινόμενο σχήμα μας αφορά κάθετες διαπομπές. Κατά τη διαδικασία σηματοδοσίας, όταν το MN αποσυνδεθεί από το προηγούμενο RSU, το RSU στέλνει το Detachment Indication μήνυμα στο PMAG. Το PMAG τότε σταματά την προώθηση των downlink δεδομένων προς το MN αλλά συνεχίζει να αποθηκεύει τα δεδομένα που έρχονται από το LMA. Στη συνέχεια, το MN συνδέεται με τη νέα RSU και κατά συνέπεια η RSU στέλνει το Attachment Indication μήνυμα στο NMAG. Αμέσως μετά το NMAG συνδέεται με το MN ανταλλάσσοντας τα μηνύματα PBU και PBA με το LMA. Στη συνέχεια, το NMAG στέλνει το μήνυμα Buffered Packet Request στο PMAG και το PMAG προωθεί τα buffered δεδομένα του στο NMAG. Τέλος, το NMAG διαβιβάζει στο MN τα buffered δεδομένα μαζί με τα νέα δεδομένα από τον LMA.

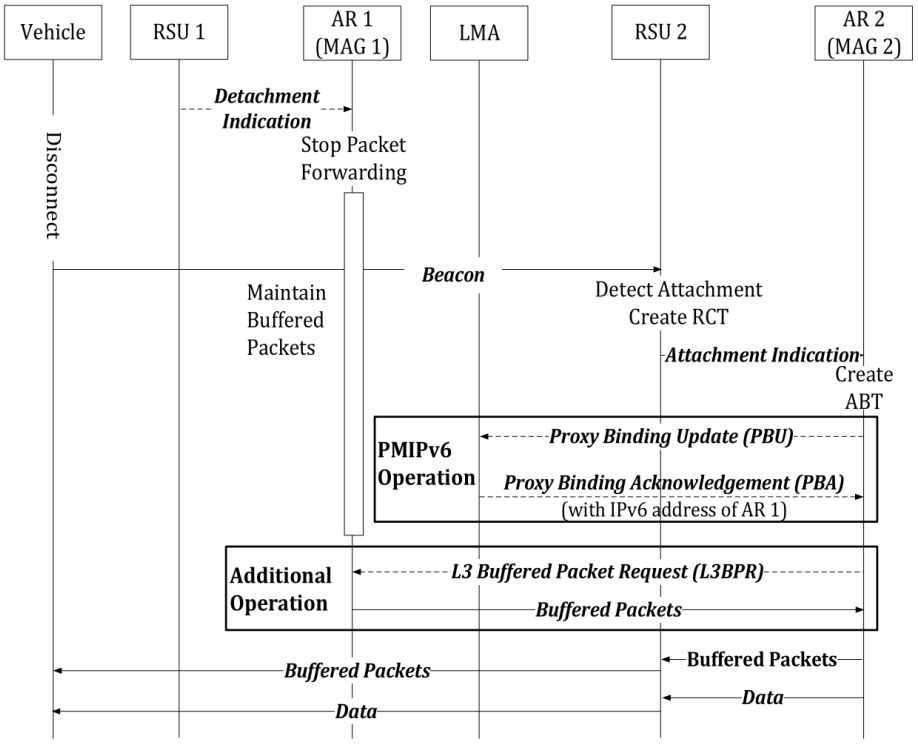

Figure 22. Σηματοδοσία intra-AR διαπομπής [24].

Κεφάλαιο 4: Προτεινόμενο Μοντέλο για διαπομπή

4.1 Εισαγωγή

Στα προτεινόμενο μοντέλο, το περιβάλλον στο οποίο λαμβάνουν χώρα οι διαπομπές αποτελείται από το δίκτυο κορμού 5GC που περιλαμβάνει τα Network Functions, καθώς και από το NG-RAN. Το NG-RAN περιλαμβάνει τους σταθμούς βάσης ενώ επίσης ενσωματώνει και τα δίκτυα πρόσβασης 802.11p και LTE. Έτσι το MN μπορεί συνδεθεί στο δίκτυο κορμού χρησιμοποιώντας οποιαδήποτε από τις διαθέσιμες τεχνολογίες πρόσβασης. Τα σημεία πρόσβασης μπορούν να θεωρηθούν ως ένα NG-RAN gNB, 802.11p RSU ή LTE gNobeB. Αντίστοιχα, ο ρόλος του MAG μπορεί να εκτελεστεί από το AMF το οποίο μπορεί να διασυνδεθεί με τα δίκτυα εκτός της 3GPP μέσω των N3IWF (Non-3GPP Interworking Function) και TNGF (Trusted Non-3GPP Gateway Function). Επίσης, το AMF μπορεί να διασυνδεθεί με SGW (Service Gateway) του EPC για να παρέχει πρόσβαση στο δίκτυο LTE. Τέλος, η λειτουργικότητα της LMA καλύπτεται από το UPF [13],[14].

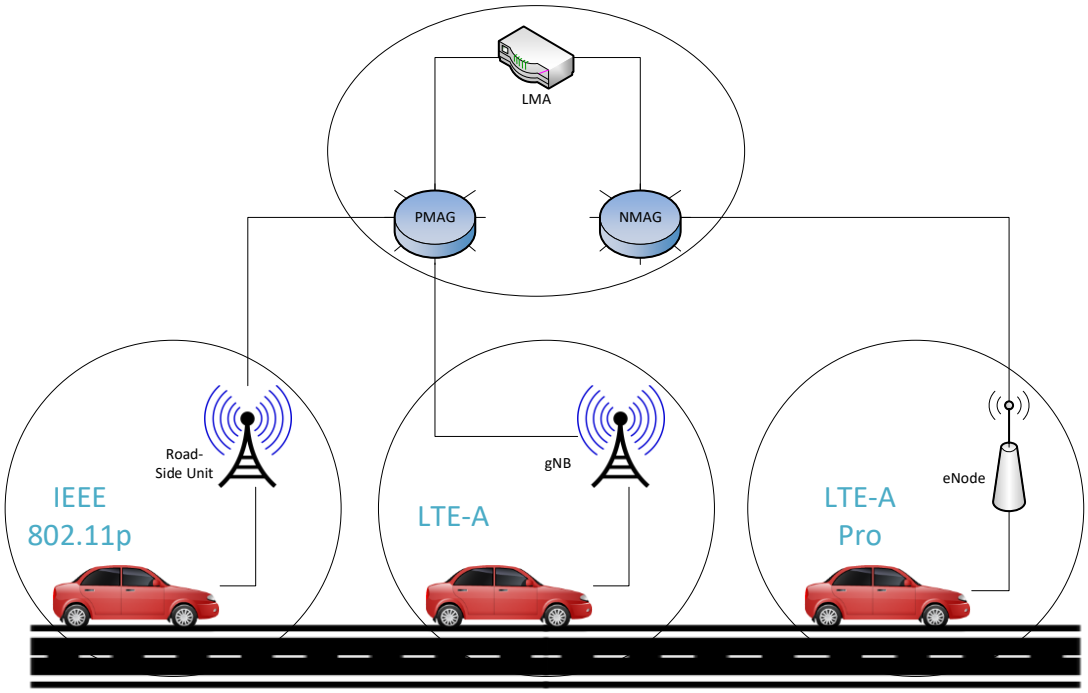

Figure 23. Αρχιτεκτονική του σχηματικού περιβάλλοντος για το προτεινόμενο μοντέλο

4.2 Περιγραφή Predictive λειτουργίας

Στο πρωτόκολλο FPMIPv6 η δρομολόγηση των πακέτων γίνεται μέσω του PMAG έως ότου πραγματοποιηθεί το Binding Update. Αυτό μπορεί να οδηγήσει σε υπερχείλιση του buffer του PMAG από πακέτα σε περιπτώσεις όπου το Binding Update εκτελεσθεί με καθυστέρηση. Στο προτεινόμενο σχήμα, όπως φαίνεται στο Figure 21, ο LMA μπορεί να προωθήσει αμέσως την κίνηση καθόδου του MN στο NMAG για να αποθηκευτεί εκεί μέχρι το MN να συνδεθεί στο νέο σημείο πρόσβασης και να λάβει τα δεδομένα καθόδου. Επίσης το PMAG μπορεί να στείλει τα αποθηκευμένα δεδομένα του στο NMAG μέσω της μεταξύ τους σήραγγας για να είναι επίσης διαθέσιμα για το MN κατά την σύνδεση του.

Η διαδικασία σηματοδοσίας αρχίζει όταν το MN ανιχνεύει ότι το σήμα που λαμβάνει από το σημείο πρόσβασης έχει πέσει κάτω από ένα όριο και αποφασίζει να εκτελέσει διαπομπή. Έτσι, μεταδίδει το μήνυμα Handover Indication στο PMAG προκειμένου να το ενημερώσει για την ανάγκη για διαπομπή. Αντίστοιχα, το PMAG έχοντας λάβει το μήνυμα αρχίζει να αποθηκεύει τα δεδομένα καθοδικής ζεύξης που προορίζονται για το MN (1). Κατά συνέπεια, το PMAG αποστέλλει το μήνυμα Handover Initiation (HI) στο NMAG που θα συνεχίσει να εξυπηρετεί το MN μετά την παράδοση. Το μήνυμα έχει ενεργοποιημένη την σημαία F(tunnel) με την τιμή 1, ώστε να ξεκινήσει η δημιουργία ενός tunnel μεταξύ του PMAG και του NMAG (2).

Στη συνέχεια, το NMAG απαντά στο PMAG με ένα μήνυμα Handover Acknowledgment (HACK) και δημιουργείται το tunnel μεταξύ των δύο MAG. Ομοίως με το προηγούμενο μήνυμα, η σημαία F (tunnel) τίθεται σε 1. Στη συνέχεια, το PMAG προωθεί όλα τα προηγούμενα αποθηκευμένα δεδομένα του στο NMAG. Ωστόσο, το PMAG δεν απορρίπτει τα δεδομένα που προέρχονται από το LMA μετά την προώθησή τους στο NMAG. Αντίθετα, τα αποθηκεύει, ώστε σε ένα σενάριο false predictive διαπομπής τα δεδομένα να μην χαθούν και δεν τα απορρίπτει μέχρι να σταλεί το τελικό μήνυμα PBU, σύμφωνα με το βήμα 10 (3).

Στη συνέχεια, το NMAG στέλνει ένα μήνυμα PBU στο LMA, ώστε να αντιστοιχίσει το MN στο NMAG και να το ενημερώσει ότι θα είναι το νέο MAG που θα εξυπηρετεί το MN. Επίσης, εισάγεται μια νέα χρονική παράμετρος προστίθεται στο μήνυμα PBU (Thand), η οποία υποδεικνύει τον εκτιμώμενο χρόνο που θα χρειαστεί το MN για να

ολοκληρώσει την διαπομπή στο NMAG (και να εκτελεσθεί το τελικό PBU μήνυμα). Το μήνυμα έχει επίσης τη σημαία T(transient) ενεργοποιημένη , έτσι ώστε να δημιουργηθεί μια προσωρινή σύζευξη (Transient Binding) μεταξύ του MN και του NMAG μέχρι η σύζευξη να γίνει μόνιμη σύμφωνα με τα βήματα 7 και 8. Έτσι, δημιουργείται μια σήραγγα μεταξύ του NMAG και του LMA, προκειμένου ο LMA να προωθήσει στο NMAG τα αποθηκευμένα δεδομένα της καθοδικής ζεύξης του MN (4).

Στη συνέχεια, ο LMA απαντά με μήνυμα PBA και δημιουργείται το tunnel μεταξύ του LMA και του NMAG. Έτσι, το LMA αρχίζει να προωθεί τα δεδομένα απευθείας στο NMAG. Αυτό μπορεί να διευκολύνει τη μετάβαση του NM από το PMAG στο NMAG, αφού το MN δεν θα χρειάζεται το PMAG ως ενδιάμεσο μετά τη σύνδεση του στο MNAG για να λάβει τα αποθηκευμένα δεδομένα του. Ωστόσο, ο LMA συνεχίζει επίσης να προωθεί τα δεδομένα καθοδικής ζεύξης στο PMAG μέσω της προηγούμενου υφιστάμενου tunnel του LMA-PMAG (5).

Στη συνέχεια, το MN πραγματοποιεί τη σύνδεσή του με το NMAG. Ως εκ τούτου, τα δεδομένα ανόδου και καθόδου θα αποστέλλονται στο MN μέσω του NMAG χωρίς την ανάγκη του PMAG. Αρχικά, το NMAG στέλνει στο MN τα αποθηκευμένα δεδομένα που προέρχονται από το LMA και το PMAG. Στη συνέχεια, το NMAG μεταδίδει τα καινούρια δεδομένα κατερχόμενης ζεύξης (6). Κατά συνέπεια, το NMAG στέλνει ένα μήνυμα PBU στο LMA ενημερώνοντάς ότι η σύζευξη με το MN γίνεται μόνιμη έχοντας θέσει τη σημαία T(transient) ίση με την τιμή 0 (7).

Ως αποτέλεσμα, ο LMA απαντάει στον NMAG με ένα μήνυμα PBA το οποίο έχει ως αποτέλεσμα τον τερματισμό της προσωρινής σύζευξης των βημάτων 4 και 5 (8). Στη συνέχεια, το NMAG στέλνει ένα μήνυμα Handover Complete (HOC) στο PMAG για να το ενημερώσει για το τέλος της διαπομπής (9). Τέλος, το PMAG απαντά με ένα μήνυμα Handover Complete Acknowledgement (HOCA) και η διαδικασία της διαπομπής ολοκληρώνεται. Ως αποτέλεσμα, το tunnel μεταξύ του PMAG και του NMAG τερματίζεται και το PMAG μπορεί πλέον να διαγράψει τα αποθηκευμένα δεδομένα του (10).

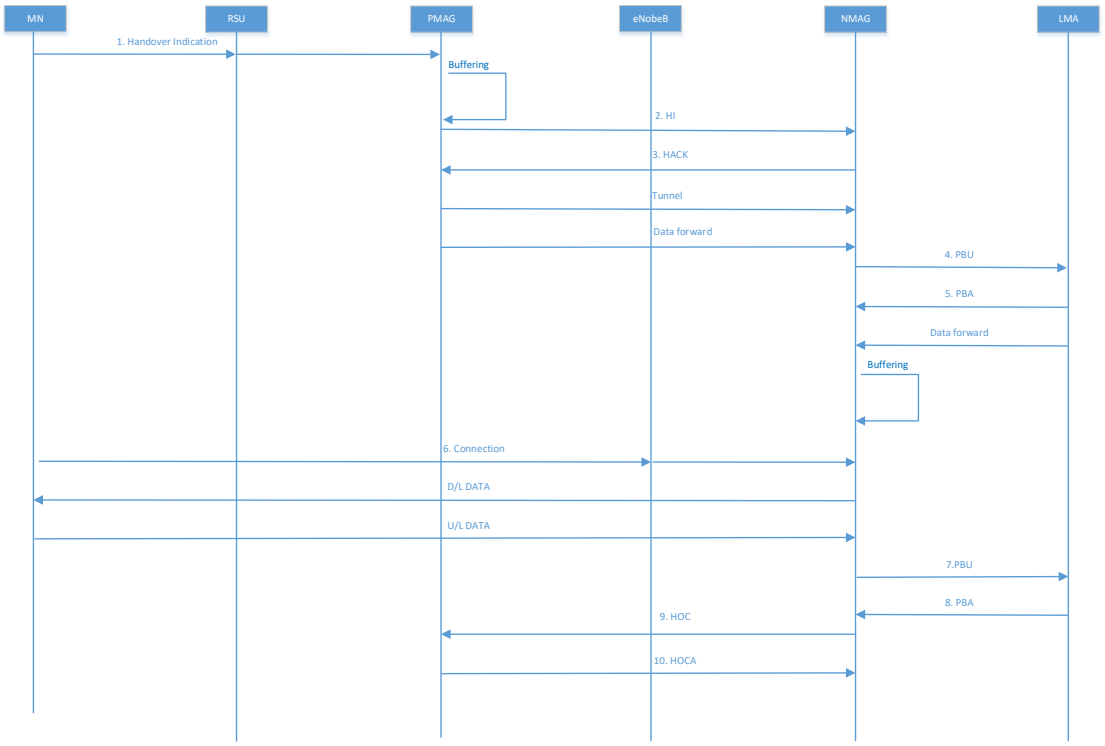

Figure 24. Σηματοδοσία predictive λειτουργίας προτεινόμενου μοντέλου

4.3 False Predictive περίπτωση

Στην περίπτωση που συμβαίνει μια false predictive διαπομπή, το αποτέλεσμα είναι το MN να επιστρέψει στο PMAG. Σε αυτή την περίπτωση, η χρονική περίοδος (T_hand) της προσωρινής σύζευξης μεταξύ του LMA και του PMAG έχει λήξει. Κατά συνέπεια, το NMAG απορρίπτει τα αποθηκευμένα δεδομένα του και τερματίζει τα tunnel με το PMAG και το LMA. Δεδομένου ότι η προηγούμενη σύζευξη μεταξύ του LMA και του PMAG εξακολουθεί να είναι ενεργή, το MN είναι σε θέση να συνεχίσει να λαμβάνει δεδομένα ανόδου και καθόδου από το PMAG. Επίσης, αντιμετωπίζεται η απώλεια πακέτων αφού το LMA δεν σταμάτησε να προωθεί δεδομένα στο PMAG κατά την διάρκεια της διαπομπής.

4.4 Περιγραφή Reactive λειτουργίας

Η διαδικασία της σηματοδοσίας της Reactive λειτουργίας, όπως απεικονίζεται στο Figure 19, ξεκινάει με την σύνδεση του MN με το NMAG μετα την απότομη αποσύνδεση του από το PMAG (1). Στη συνέχεια, το NMAG στέλνει ένα μήνυμα Handover Initiate (HI) στο PMAG το οποίο ενημερώνει το PMAG ότι το MN έχει συνδεθεί στο NMAG. Το PMAG αρχίζει αμέσως να αποθηκεύει τα δεδομένα της

καθοδικής του ζεύξης για το MN (2). Αντίστοιχα, το PMAG απαντά με ένα μήνυμα Handover Acknowledgment (HACK) (3).

Στη συνέχεια, το NMAG στέλνει ένα μήνυμα PBU στο LMA για να συζεύξει το MN με το NMAG και να ενημερώσει ότι το MN έχει συνδεθεί σε αυτό (4). Ως αποτέλεσμα, ο LMA πιστοποιεί τα διαπιστευτήρια του NMAG και απαντά με ένα μήνυμα PBA. Επομένως, το NMAG είναι πλέον συζευγμένο με το MN και μπορεί να προωθήσει τα δεδομένα στο MN (5).

Κατά συνέπεια, το NMAG στέλνει ένα μήνυμα Handover Complete (HOC) στο PMAG για να το ενημερώσει για το τέλος της διαπομπής και την απελευθέρωση των πόρων του. Ως αποτέλεσμα, το PMAG προωθεί τα αποθηκευμένα δεδομένα του στο LMA. Στη συνέχεια, ο LMA ξεκινά τη μετάδοση δεδομένων καθοδικής ζεύξης για το MN προς το NMAG, συμπεριλαμβανομένων των buffered δεδομένων που έλαβε από το PMAG (6). Τέλος, το PMAG απαντάει με ένα Handover Complete Acknowledgment (HOCA) και η διαδικασία της διαπομπής ολοκληρώνεται (7).

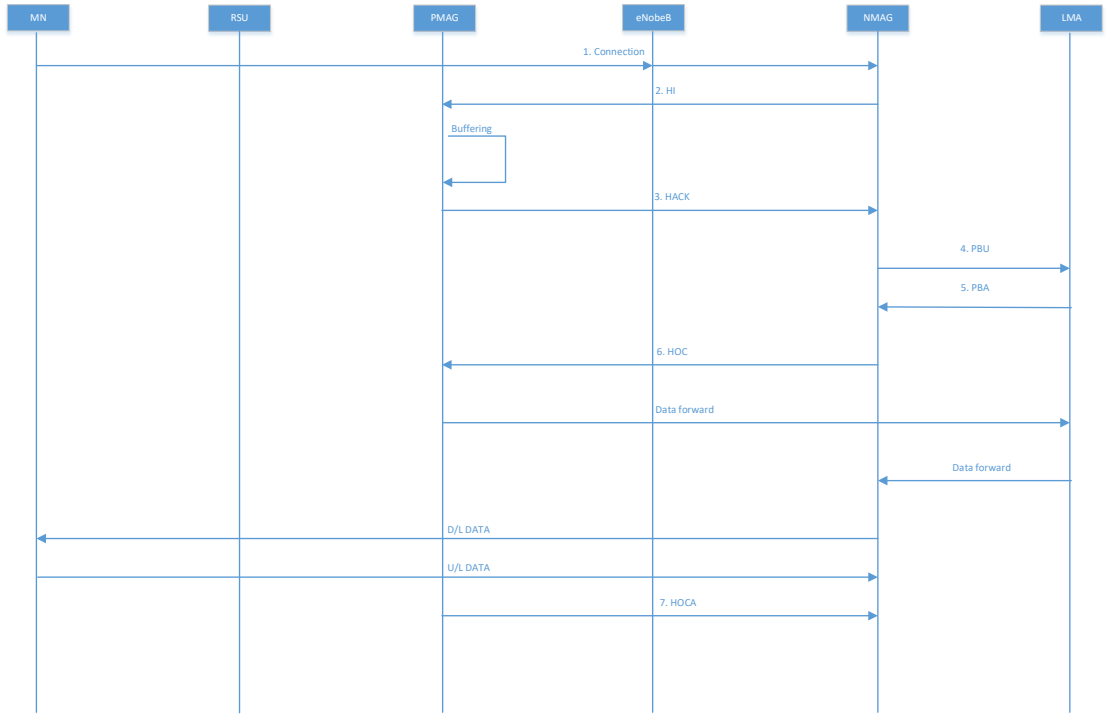

Figure 25. Σηματοδοσία reactive λειτουργίας προτεινόμενου μοντέλου

Κεφάλαιο 5: Ανάλυση απόδοσης προτεινόμενου μοντέλου

Σε αυτή την ενότητα, αναλύουμε την απόδοση του προτεινόμενου βελτιωμένου σχήματος διαπομπής οχήματος που συμβολίζεται ως VPMIPv6 όσον αφορά την καθυστέρηση διαπομπής, το κόστος σηματοδοσίας και tunneling, καθώς και την απώλεια πακέτων. Αρχικά περιγράφεται το μαθηματικό μοντέλο που χρησιμοποιείται για την ανάλυση του συστήματος VPMIPv6. Για την αξιολόγηση της απόδοσης, υποθέτουμε ότι η περιοχή κάλυψης κάθε κινητής κυψέλης είναι κυκλική με ακτίνα R. Επίσης, η ανάλυση που πραγματοποιείται βασίζεται στο hop distance (αριθμός αλμάτων μεταξύ των δικτυακών οντοτήτων), όπως παρουσιάζεται στο Table 1.

Sign	**Description**	**Value**
$H_{MAG\text{-}LMA}$	Hop distance μεταξύ MAG και LMA	2
$H_{MAG\text{-}MAG}$	Hop distance μεταξύ 2 MAGs	1
$H_{acess\ point\text{-}MAG}$	Hop distance μεταξύ ενός σημείου πρόσβασης και αντίστοιχου MAG	1

Table 1. Αποστάσεις μεταξύ των οντοτήτων δικτύου.

Όσον αφορά την κινητικότητα ενός MN, υιοθετείται το μοντέλο κινητικότητας και κίνησης όπως ορίζεται στο [12]. Κατά συνέπεια, ο ρυθμός μετακίνησης ή ο ρυθμός διέλευσης κυψελών εκφράζεται ως εξής:

$\mu_c = \frac{2 \cdot u}{\pi \cdot R}$, όπου u είναι η μέση ταχύτητα του MN.

Επίσης, θεωρείται ότι ο ρυθμός άφιξης των συνεδρίων του MN ακολουθεί μια διαδικασία Poisson με μέση τιμή λ_S. Έτσι, ο αριθμός των ενημερώσεων θέσης κατά τη διάρκεια του χρονικού διαστήματος μεταξύ των συνεδρίων εκτιμάται ως εξής:

$$\lambda = E(N_c) = \frac{\mu_c}{\lambda_s}$$

Επιπλέον, η πιθανότητα ενεργοποίησης της predictive η της reactive λειτουργίας του μοντέλου υπολογίζεται στην συνέχεια:

Η πιθανότητα ενεργοποίησης της reactive λειτουργίας εκφράζεται ως εξής:

$P_{REAC}(T < T_{INIT} + T_{PRE}) = e^{-\lambda(T_{INIT}+T_{PRE})}$, όπου T είναι μια εκθετική τυχαία μεταβλητή που δείχνει το χρόνο παραμονής του MN στην περιοχή επικάλυψης μεταξύ δύο κυψελών. Επίσης, T_{INIT} είναι ο χρόνος που χρειάζεται το MN για να αποφασίσει

να μεταβεί σε ένα νέο δίκτυο πρόσβασης, ενώ T_{PRE} είναι η καθυστέρηση από την έναρξη της predictive λειτουργίας μέχρι τη στιγμή που εκδίδεται το μήνυμα HACK από το NMAG.

λ είναι ο ρυθμός μετακίνησης που δίνεται στην σχέση (2).

Κατά συνέπεια, η πιθανότητα ενεργοποίησης της predictive λειτουργίας είναι:

$$P_{PRE} = 1 - P_{REAC}(T < T_{INIT} + T_{PRE})$$

Τέλος, η πιθανότητα να συμβεί μια false predictive διαπομπή δίνεται από:

$p_f = 1 - \frac{\theta 1 + \theta 2}{\pi}$ (5) ,όπου η κίνηση του τερματικού από το σημείο της απόφασης για διαπομπή βρίσκεται στο διάστημα $[\theta_1, \theta_2]$ σύμφωνα με το [25].

5.1 Καθυστέρησης διαπομπής

Στη συνέχεια μετράμε την καθυστέρηση διαπομπής του συστήματος VPMIPv6. Η καθυστέρηση διαπομπής ορίζεται ως η χρονική περίοδος που ξεκινά από τη στιγμή που το MN αποφασίζει να εκτελέσει διαπομπή μέχρι τη στιγμή που το MN λαμβάνει τα πρώτα πακέτα από το LMA μέσω του NMAG. Για τον υπολογισμό της καθυστέρησης ορίζονται κάποια χρονικά διαστήματα για την ανταλλαγή των σχετικών μηνυμάτων που χρησιμοποιούνται στη σηματοδοσία της διαπομπής.

Sign	**Description**
T_{Hind}	Delay of the Handover Indication message sent by the MN to the PMAG
T_{HI}	Delay of the Handover Initiate message sent by a MAG to another MAG.
T_{HACK}	Delay of the Handover Acknowledgement message sent by a MAG to another MAG.
T_{PBU}	Delay of Process Binding Update message sent by a MAG to the LMA.
T_{PBA}	Delay of the Process Binding Acknowledgement sent by the LMA to a MAG.

Table 2. Καθυστερήσεις για τα ανταλλασσόμενα μηνύματα.

Επιπλέον, η καθυστέρηση μετάδοσης ενός πακέτου με ενσύρματη σύνδεση ορίζεται ως T_L^{packet}, ενώ η καθυστέρηση μετάδοσης ενός πακέτου με ασύρματη σύνδεση ορίζεται ως T_W^{packet}. Τέλος, στην περίπτωση μιας λανθασμένης διαπομπής το T_f αντιπροσωπεύει το χρονικό διάστημα από τη στιγμή που το MN στέλνει την αρχική

αναφορά Handover Indication στο προηγούμενο δίκτυο πρόσβασης για να ξεκινήσει τη διαπομπή μέχρι τη στιγμή που το MN αποφασίζει να επανασυνδεθεί σε αυτό εκδίδοντας ένα νέο Handover Indication.

5.1.1 Predictive λειτουργία

Η συνολική καθυστέρηση παράδοσης στο σχήμα VPMIPv6 για μια επιτυχής Predictive διαπομπή αποτελείται από τρία χρονικά διαστήματα. Το πρώτο που συμβολίζεται ως T_{PRE}^{VP} ορίζει το διάστημα από την έναρξη της διαπομπής μέχρι τη στιγμή που το MN συνδέεται στο NMAG. Το δεύτερο χρονικό διάστημα T_{L2}^{VP} είναι ο χρόνος που χρειάζεται το MN για να συνδεθεί στο NMAG και να διαμορφώσει τις νέες ρυθμίσεις του μετά την ανταλλαγή των πρώτων μηνυμάτων PBU και PBA μεταξύ του NMAG και του LMA. Τέλος, το T_{POST}^{VP} είναι το χρονικό διάστημα μεταξύ της εγκαθίδρυσης σύνδεσης του MN με το NMAG και της λήψης στο MN του πρώτου πακέτου από το LMA μέσω του NMAG. Κατά συνέπεια, η συνολική καθυστέρηση για μια επιτυχή predictive διαπομπή είναι:

$T_{HO}^{VPS} = T_{PRE}^{VP} + T_{L2}^{VP} + T_{POST}^{VP}$ όπου:

$T_{PRE}{}^{VP} = T_{Hind} + T_{HI} + T_{HACK} + T_{PBU} + T_{PBA} = T_w{}^{Hind} + H_{RSU\text{-}MAG}{}^{Hind} * T_L{}^{Hind} + 2H_{MAG\text{-}LMA}{}^{HI} * T_L{}^{HI} + 2H_{MAG\text{-}LMA}{}^{HACK} * T_L{}^{HACK} + H_{MAG\text{-}LMA}{}^{PBU} * T_L{}^{PBU} + H_{MAG\text{-}LMA}{}^{PBA} * T_L{}^{PBA}$

$T_{L2}{}^{VP} = T_{L2}{}^{P} + T_{PRE}{}^{P} - T_{PRE}{}^{VP}$

όπου $T_{L2}{}^{P}$ είναι η περίοδος που χρειάζεται το MN για να πραγματοποιήσει τη σύνδεση με το νέο MAG και να διαμορφώσει τις νέες ρυθμίσεις της μετά την πρώτη ανταλλαγή HI από το PMAG στο NMAG στο σενάριο πρόβλεψης στο τυπικό σχήμα FPMIPv6.

$$T_{POST}^{VP} = T_{data} = T_W^{data} + H_{eNB-MAG}^{data} \cdot T_L^{data} + H_{MAG-LMA}^{data} \cdot T_L^{data}$$

Η καθυστέρηση μιας false predictive διαπομπής στο VPMIPv6 είναι:

$$T_{HO}^{VPF} = T_f + T_{Hind} + T_{packet} = T_f + T_W^{Hind} + H_{RSU-MAG}^{Hind} \cdot T_L^{Hind} + T_W^{data} + H_{RSU-MAG}^{data} \cdot T_L^{data}$$

Κατά συνέπεια, η συνολική καθυστέρηση για μια predictive διαπομπή εκφράζεται ως εξής:

$$T_{HO}^{VP} = (1 - p_f) \cdot T_{HO}^{VPS} + p_f \cdot T_{HO}^{VPF}$$

5.1.2 Reactive λειτουργία

Η συνολική καθυστέρηση παράδοσης στο reactive σχήμα VPMIPv6 είναι:

$$T_{HO}^{VR} = T_{L2}^{VR} + T_{POST}^{VR}$$

όπου T_{L2}^{VR}είναι το χρονικό διάστημα που χρειάζεται το τερματικό για να συνδεθεί στο νέο δίκτυο πρόσβασης. Επίσης, ο όρος T_{POST}^{VR} είναι παρόμοιος με τον αντίστοιχο όρο T_{POST}^{VP} της predictive λειτουργίας και δίνεται ως εξής:

$T_{L2}{}^{VR} = T_{L2}{}^{R} = T_{L2}{}^{P}$

$T_{POST}{}^{VR} = T_{HI} + T_{HACK} + T_{PBU} + T_{PBA} + T_{DATA} + T_{HOC} + T_{DATA} = 2H_{MAG\text{-}LMA}{}^{HI} * T_{L}{}^{HI} + 2H_{MAG\text{-}LMA}{}^{HACK} * T_{L}{}^{HACK} + H_{MAG\text{-}LMA}{}^{PBU} * T_{L}{}^{PBU} + H_{MAG\text{-}LMA}{}^{PBA} * T_{L}{}^{PBA} + 2H_{MAG\text{-}LMA}{}^{HOC} * T_{L}{}^{HOC} + T_{w}{}^{DATA} + H_{eNodeb\text{-}MAG}{}^{DATA} * T_{L}{}^{DATA} + H_{MAG\text{-}LMA}{}^{DATA} * T_{L}{}^{DATA}$

Τέλος, η συνολική καθυστέρηση διαπομπής για το προτεινόμενο σχήμα εκτιμάται ως εξής:

$$T_{HO}^{VFPMIP} = P_{PRE} \cdot T_{HO}^{VP} + (1 - P_{PRE}) \cdot T_{HO}^{VR}$$

5.2 Κόστος Σηματοδοσίας

Στη συνέχεια μετράμε το κόστος σηματοδότησης του μοντέλου χωρίς να εξετάζουμε περιπτώσεις λανθασμένης διαπομπής. Πρώτα πρέπει να ορίσουμε το κόστος μετάδοσης των μηνυμάτων που αποστέλλονται από τις επιμέρους οντότητες. Το κόστος μετάδοσης αποτελείται από την απόσταση άλματος μεταξύ των δύο συγκεκριμένων οντοτήτων πολλαπλασιασμένη με το μήκος του μηνύματος που αναφέρεται ως $L_{message}$.

$S^{VP}{}_{MAG\text{-}MAG} = 2H_{MAG\text{-}LMA}{}^{HI} * L_{HI} + 2H_{MAG\text{-}LMA}{}^{HACK} * L_{HACK}$

$S^{VP}{}_{LMA\text{-}MAG} = 2*(H_{MAG\text{-}LMA}{}^{PBU} * L_{PBU} + H_{MAG\text{-}LMA}{}^{PBA} * L_{PBA})$

$S^{VR}{}_{MAG\text{-}MAG} = 2H_{MAG\text{-}LMA}{}^{HI} * L_{HI} + 2H_{MAG\text{-}LMA}{}^{HACK} * L_{HACK} + 2H_{MAG\text{-}LMA}{}^{HOC} * L_{HOC}$ (17)

$S^{VR}{}_{LMA\text{-}MAG} = H_{MAG\text{-}LMA}{}^{PBU} * L_{PBU} + 2H_{MAG\text{-}LMA}{}^{PBA} * L_{PBA}$

Έτσι, το κόστος σηματοδότησης για την βελτιωμένη predictive διαπομπή εκτιμάται ως εξής:

$$C_{SIG}^{VP} = E(N_c) \cdot (S_{MAG-MAG}^{VP} + S_{LMA-MAG}^{VP})$$

Αντίστοιχα, το κόστος σηματοδότησης για την βελτιωμένη reactive διαπομπή εκτιμάται ως εξής:

$$C_{SIG}^{VR} = E(N_c) \cdot (S_{MAG-MAG}^{VR} + S_{LMA-MAG}^{VR})$$

Συνεπώς, το τελικό κόστος σηματοδότησης για το προτεινόμενο σύστημα εκτιμάται ως εξής:

$$C_{SIG}^{VFPMIP} = P_{PRE} \cdot C_{SIG}^{VP} + (1 - P_{PRE}) \cdot C_{SIG}^{VR}$$

5.3 Κόστος Tunneling

Παρόμοια με το κόστος σηματοδοσίας, το κόστος tunneling του VFPMIP αξιολογείται για την predictive και reactive λειτουργία. Ειδικότερα, το κόστος tunneling για την predictive λειτουργία υπολογίζεται με τον ακόλουθο τύπο:

$C_{TUN}^{VP} = E(N_c) \cdot \lambda_p \cdot (P_{LMA-MAG} \cdot T_{HO}^{VP} + P_{MAG-MAG} \cdot T_{TNL}^{VP})$, όπου λ_p αντιπροσωπεύει τον ρυθμό άφιξης πακέτων στην περιοχή που επικαλύπτεται από κυψέλες. Επιπλέον, η διάρκεια του tunneling μεταξύ των δύο MAG ορίζεται ως T_{TNL}^{VP} και εκτιμάται ως εξής:

$$T_{TNL}^{VP} = T_{L2}^{VP} + T_{PBU} + T_{PBA}$$

Το $P_{LMA-MAG}$ αντιπροσωπεύει το κόστος της επικεφαλίδας tunnel LHD ανά πακέτο δεδομένων που ανταλλάσσεται μεταξύ του LMA και του MAG και υπολογίζεται ως εξής:

$$P_{LMA-MAG} = H_{LMA-MAG} \cdot L_{HD}$$

Επίσης, $P_{MAG-MAG}$ είναι το κόστος της επικεφαλίδας tunnel LHD ανά πακέτο δεδομένων που ανταλλάσσεται μεταξύ των MAG και εκφράζεται ως εξής:

$$P_{MAG-MAG} = H_{MAG-MAG} \cdot (L_{HD} + L_{HD})$$

Το κόστος tunneling για την reactive λειτουργία του VFPMIP δίνεται ως εξής:

$C_{TUN}^{VR} = E(N_c) \cdot \lambda_p \cdot (n \cdot P_{LMA-MAG} \cdot T_{LOSS}^{VR} + P_{LMA-MAG} \cdot (T_{HO}^{VR} - T_{LOSS}^{VR}))$, οπού το n δηλώνει το πλήθος επαναμετάδοσεων πακέτων λόγω απώλειας.

Επιπλέον, η περίοδος απώλειας πακέτων $\mathrm{T}_{\mathrm{LOSS}}^{\mathrm{VR}}$ διαρκεί από τη στιγμή που το MN αποσυνδέεται από το προηγούμενο δίκτυο πρόσβασης μέχρι να συνδεθεί στο νέο δίκτυο πρόσβασης και το NMAG να στείλει το μήνυμα HI στο PMAG.

Εκφράζεται ως εξής:

$$\mathrm{T}_{\mathrm{LOSS}}^{\mathrm{VR}} = \mathrm{T}_{\mathrm{L2}}^{\mathrm{VR}} + \mathrm{T}_{\mathrm{HI}}$$

Συνεπώς, το συνολικό κόστος tunneling προκύπτει ως εξής:

$$\mathrm{C}_{\mathrm{TUN}}^{\mathrm{VFPMIP}} = \mathrm{P}_{\mathrm{PRE}} \cdot \mathrm{C}_{\mathrm{TUN}}^{\mathrm{VP}} + (1 - \mathrm{P}_{\mathrm{PRE}}) \cdot \mathrm{C}_{\mathrm{TUN}}^{\mathrm{VR}}$$

5.4 Απώλεια Πακέτων

Σε μια επιτυχημένη predictive διαπομπή εφαρμόζεται προσωρινή αποθήκευση πακέτων στο PMAG και στο NMAG. Έτσι, η απώλεια πακέτων μπορεί να συμβεί σε περίπτωση που το buffer των MAG υπερχειλίσει. Κατά συνέπεια, η απώλεια πακέτων αξιολογείται ως εξής:

$$\mathrm{C}_{\mathrm{LOSS}}^{\mathrm{VPS}} = \max\{\lambda_{\mathrm{p}} \cdot \mathrm{L}_{\mathrm{p}} \cdot (\mathrm{T}_{\mathrm{HI}} + \mathrm{T}_{\mathrm{HACK}}) - \mathrm{B}_{\mathrm{P}}, 0\} +$$

$$\max\left\{\lambda_p \cdot L_p \cdot \begin{pmatrix} T_{HI} + T_{HACK} + \\ T_{PBU} + T_{PBA} + T_{L2}^{PRE} \end{pmatrix} - B_N, 0\right\} =$$

$$\max\left\{\lambda_{\mathrm{p}} \cdot \mathrm{L}_{\mathrm{p}} \cdot \begin{pmatrix} 2 \cdot \mathrm{H}_{\mathrm{MAG-LMA}}^{\mathrm{HI}} \cdot \mathrm{T}_{\mathrm{L}}^{\mathrm{HI}} + \\ 2 \cdot \mathrm{H}_{\mathrm{MAG-LMA}}^{\mathrm{HACK}} \cdot \mathrm{T}_{\mathrm{L}}^{\mathrm{HACK}} \end{pmatrix} - \mathrm{B}_{\mathrm{N}}, 0\right\} +$$

$$\max\{\lambda_{\mathrm{p}} \cdot \mathrm{L}_{\mathrm{p}} \cdot \begin{pmatrix} 2 \cdot \mathrm{H}_{\mathrm{MAG-LMA}}^{\mathrm{HI}} \cdot \mathrm{T}_{\mathrm{L}}^{\mathrm{HI}} + \\ 2 \cdot \mathrm{H}_{\mathrm{MAG-LMA}}^{\mathrm{HACK}} \cdot \mathrm{T}_{\mathrm{L}}^{\mathrm{HACK}} + \\ \mathrm{H}_{\mathrm{MAG-LMA}}^{\mathrm{PBU}} \cdot \mathrm{T}_{\mathrm{L}}^{\mathrm{PBU}} + \\ \mathrm{H}_{\mathrm{MAG-LMA}}^{\mathrm{PBA}} \cdot \mathrm{T}_{\mathrm{L}}^{\mathrm{PBA}} + \mathrm{T}_{\mathrm{L2}}^{\mathrm{EPRE}} \end{pmatrix} - \mathrm{B}_{\mathrm{N}}, 0\}$$

όπου B_P, B_N και B_L συμβολίζουν το μέγεθος του buffer του PMAG, του NMAG και του LMA αντίστοιχα και L_P είναι το μήκος ενός πακέτου δεδομένων. Επιπλέον, σε περίπτωση false predictive διαπομπής η απώλεια πακέτων εκτιμάται λαμβάνοντας υπόψη δύο διαφορετικά σενάρια. Συγκεκριμένα, στην περίπτωση που το MN στέλνει την δεύτερη αναφορά Handover Indication για επανασύνδεση με το PMAG πριν την αποστολή του μηνύματος HACK από το NMAG στο PMAG, οι απώλειες πακέτων αποδίδονται μόνο στο μέγεθος του buffer του PMAG. Έτσι, η απώλεια πακέτων αξιολογείται ως εξής:

$$C_{LOSS}^{VPS} = \max\{\lambda_P \cdot L_p \cdot (T_f + T_{Hind}) - B_p, 0\}$$

Αντίθετα, εάν το MN στείλει την αναφορά Handover Indication για επανασύνδεση με το PMAG οποιαδήποτε στιγμή μετά την αποστολή του μηνύματος HACK, ενδέχεται να προκύψουν απώλειες πακέτων λόγω της υπερχείλισης των buffers τόσο του PMAG όσο και του NMAG. Έτσι, το C_{LOSS}^{VPF} δίνεται από:

$$C_{LOSS}^{VPF} = \max\{\lambda_p \cdot L_p \cdot (T_{HI} + T_{HACK}) - B_p, 0\} +$$

$$\max\{\lambda_P \cdot L_p \cdot (T_f + T_{Hind}) - B_N, 0\}$$

Συνεπώς, η συνολική απώλεια πακέτων για την predictive διαπομπή VFPMIP εκτιμάται ως εξής:

$$C_{LOSS}^{VP} = (1 - p_f) \cdot C_{LOSS}^{VP} + p_f \cdot C_{LOSS}^{VPF}$$

Στην reactive διαπομπή τα πακέτα χάνονται έως ότου οι οντότητες του δικτύου λάβουν εντολή να προωθήσουν τα δεδομένα καθοδικής ζεύξης στο NMAG. Κατά συνέπεια, η απώλεια πακέτων C_{LOSS}^{VR} αξιολογείται ως εξής:

$$C_{LOSS}^{VR} = \lambda_p \cdot L_p \cdot \begin{pmatrix} T_{L2}^{REA} + T_{HI} + T_{HACK} \\ + T_{PBU} + T_{PBA} \end{pmatrix} + \quad \max\{\lambda_p \cdot L_p \cdot T_{HOC} - B_p, 0\} =$$

$$\lambda_p \cdot L_p \cdot \begin{pmatrix} T_{L2}^{REA} + 2 \cdot H_{MAG-LMA}^{HI} \cdot T_L^{HI} + \\ 2 \cdot H_{MAG-LMA}^{HACK} \cdot T_L^{HACK} + \\ H_{MAG-LMA}^{PBU} \cdot T_L^{PBU} + \\ H_{MAG-LMA}^{PBA} \cdot T_L^{PBA} \\ - B_p, 0\} \end{pmatrix} + \max\{\lambda_p \cdot L_p \cdot 2 \cdot H_{MAG-LMA}^{HOC} \cdot T_L^{HOC}$$

Τέλος, η συνολική απώλεια πακέτων για το σύστημα VFPMIP είναι:

$C_{LOSS}^{VFPMIP} = P_{PRE} \cdot C_{LOSS}^{VP} + (1 - P_{PRE}) \cdot C_{LOSS}^{VR}$ [25],[28].

5.5 Αποτελέσματα Αξιολόγησης

Στην παρούσα ενότητα, πραγματοποιείται συγκριτική αξιολόγηση τόσο του VPMIPv6 όσο και του τυπικού μοντέλου FPMIPv6.

Στο Table 3 παρουσιάζονται οι παράμετροι που επιλέχθηκαν για την αξιολόγηση των δύο μοντέλων.

Sign	**Description**	**Value**
λ	Number of location updates during an intersession	10
L_{Hind}	Length of the Hind message	52 Bytes
L_{HI}	Length of the HI message	52 Bytes
L_{HACK}	Length of the HACK message	52 Bytes
L_{HOC}	Length of the HOC message	52 Bytes
L_{PBU}	Length of the PBU message	76 Bytes
L_{PBA}	Length of the PBA message	76 Bytes
L_{DATA}	Length of a data packet	1500 Bytes
L_{HD}	Length of the tunnel header	40 Bytes
B_L	Bandwidth of wired connection	1 Gbps
B_W	Bandwidth of wireless connection	54 Mpbs
T_f	Unsuccessful predictive handover delay	10ms
n	Packet retransmissions due to packet loss	2
λ_p	Mean packet arrival rate	50 packets/sec
$T_{L2}{}^P/T_{L2}{}^R$	Time for the MN to connect to the NAN in predictive/reactive handover	50ms

Table 3. Παράμετροι Αξιολόγησης

Στο Figure 26 αξιολογείται η καθυστέρηση διαπομπής των δύο μοντέλων ως προς το hop distance. Όπως φαίνεται, το VPMIPv6 παρουσιάζει μειωμένη καθυστέρηση σε σύγκριση με το FPMIPv6 καθώς αυξάνεται η απόσταση hop του LMA-MAG λόγω των περιορισμένων αλληλεπιδράσεων των MAGs με το LMA. Συγκεκριμένα, στο VPMIPv6 λόγο της πρόωρης συσχέτισης του MN με το NMAG στέλνοντας το πρώτο PBU μήνυμα το MN μπορεί να λάβει τα πρώτα του downlink πακέτα άμεσα από το NMAG χωρίς να χρειάζεται να προωθηθούν μέσω του PMAG όπως στο FPMIPv6. Αυτό συμβαίνει στην Predictive λειτουργία καθώς και στην Reactive λειτουργία και έτσι μειώνεται η συνολική καθυστέρηση του μοντέλου.

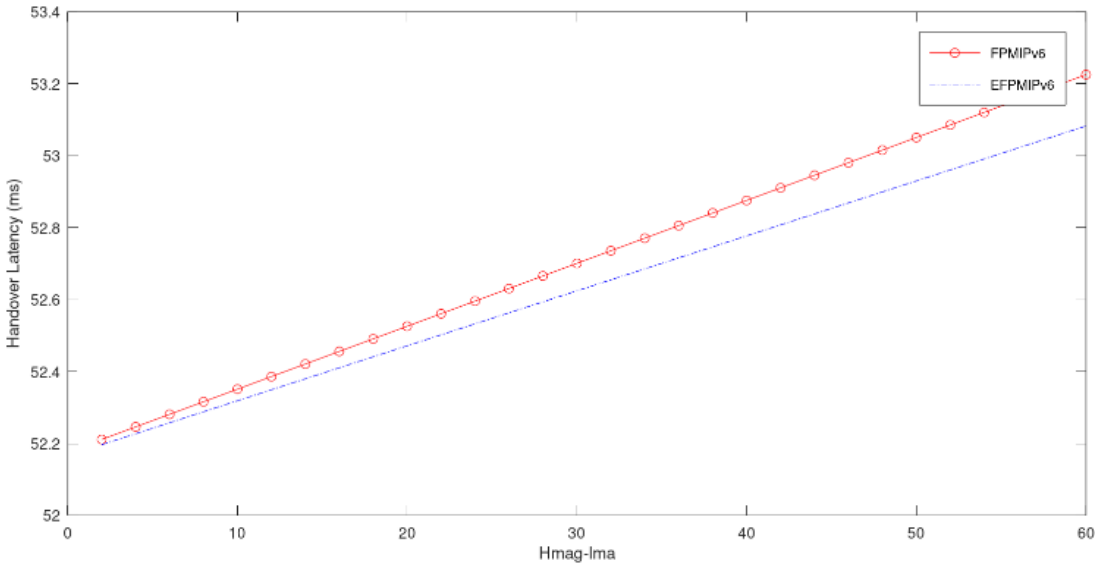

Figure 26. Handover Latency vs $H_{MAG-LMA}$.

Στην συνέχεια, όπως φαίνεται στο Figure 27, παρουσιάζεται το κόστος σηματοδοσίας για την διαπομπή για τα δυο μοντέλα, FPMIPv6 και VPMIPv6. Διακρίνεται ότι το προτεινόμενο VPMIPv6 έχει μεγαλύτερο κόστος σηματοδοσίας από το FPMIPv6 καθώς αυξάνεται το hop distance του LMA-MAG. Το επιπλέον κόστος που εισάγεται είναι λόγο των διπλών μηνυμάτων συσχέτισης PBU και PBA που ανταλλάσσονται μεταξύ του NMAG και του LMA στην Predictive λειτουργία του μοντέλου. Στην Reactive λειτουργία το VPMIPv6 έχει το ίδιο κόστος σηματοδοσίας με το FPMIPv6, αφού και στα δυο μοντέλα ανταλλάσσονται μόνο 1 φορά τα μηνύματα συσχέτισης PBU και PBA.

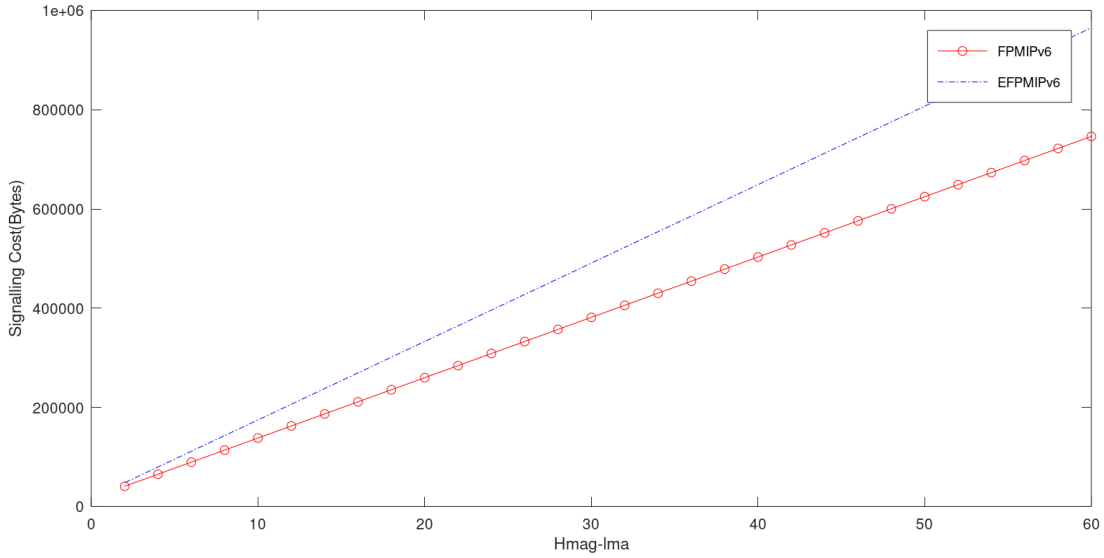

Figure 27. Κόστος Σηματοδοσίας vs $H_{MAG-LMA}$.

Στο Figure 28 απεικονίζεται το κόστος Tunneling για τα δυο μοντέλα σε συνάρτηση με το hop distance LMA-MAG. Το VPMIPv6 έχει μικρότερο κόστος από το FPMIPv6 και όσο αυξάνει το hop distance η απόδοση του βελτιώνεται. Η μείωση στο κόστος Tunneling οφείλεται σε δυο βελτιωμένα χαρακτηριστικά του VPMIPv6. Αρχικά στην Predictive λειτουργία του VPMIPv6 το Tunneling μεταξύ των δυο MAG εφαρμόζεται για μικρότερο χρονικό διάστημα καθώς μετά την προώθησή των buffered πακέτων του PMAG στο NMAG, το LMA προωθεί τα υπόλοιπα πακέτα απευθείας στο NMAG και δεν είναι απαραίτητη η περαιτέρω επικοινωνία μεταξύ των δυο MAG. Επίσης στην Reactive λειτουργία του VPMIPv6 δεν εφαρμόζεται Tunneling μεταξύ των δυο MAG σε αντίθεση με το FPMIPv6 και έτσι μειώνεται περαιτέρω το κόστος Tunneling.

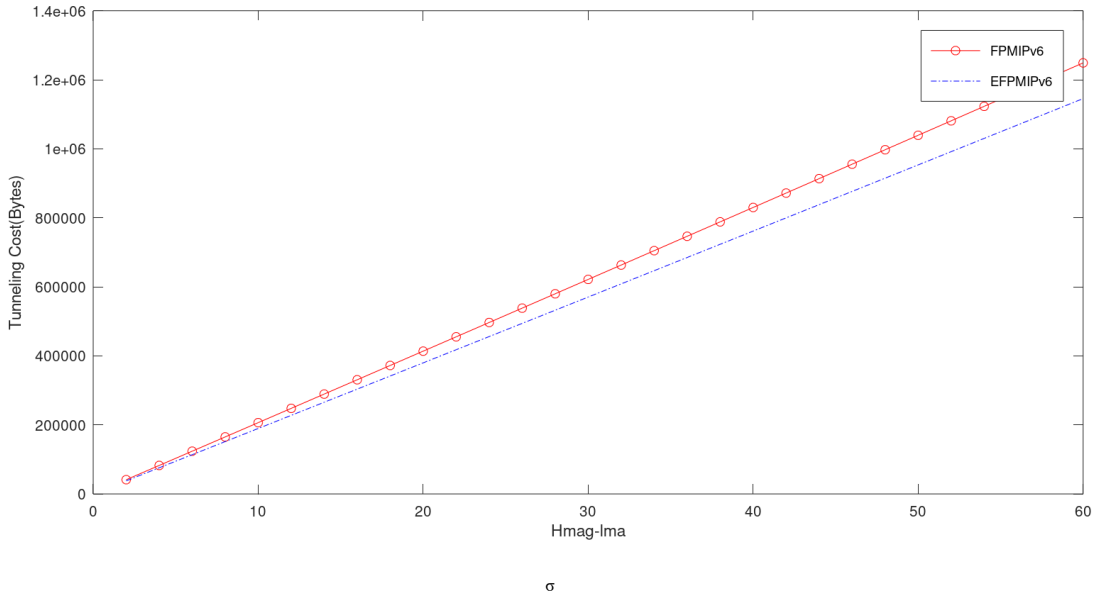

Figure 28. Tunneling Cost vs $H_{MAG-LMA}$.

Τέλος, η απώλεια πακέτων των δύο μοντέλων ως συνάρτηση του hop distance παρατηρείται στο Figure 29. Η απώλεια πακέτων στο VPMIPv6 μειώνεται δραστικά λόγω της αποτελεσματικής αντίδρασής του σε false predictive διαπομπές. Συγκεκριμένα, στην Predictive και Reactive λειτουργία το VPMIPv6 εμφανίζει μικρές βελτιώσεις στην απώλεια πακέτων σε σχέση με το FPMIPv6. Στην περίπτωση όμως που συμβαίνει μια false predictive διαπομπή, το VPMIPv6 εμφανίζει σημαντική βελτίωση. Το MN στην false predictive διαπομπή επανασυνδέεται στο προηγούμενο σημείο πρόσβασης που εξυπηρετείται από το PMAG και πρέπει να λάβει από εκείνο τα downlink πακέτα με όσο το δυνατό λιγότερες απώλειες. Το VPMIPv6 το καταφέρνει καθώς το LMA υλοποιεί ταυτόχρονη προώθηση πακέτων στο PMAG και στο NMAG μέχρι να ανταλλαχθούν τα τελικά μηνύματα συσχέτισης. Έτσι το MN κατά την είσοδο του στο PMAG, μπορεί να λάβει όλα τα πακέτα του χωρίς να υπάρξουν απώλειες. Σε αντίθεση στο FPMIPv6 δεν υπάρχει κάποιος μηχανισμός για να αντιμετωπίσει την απώλεια πακέτων στην false predictive διαπομπή.

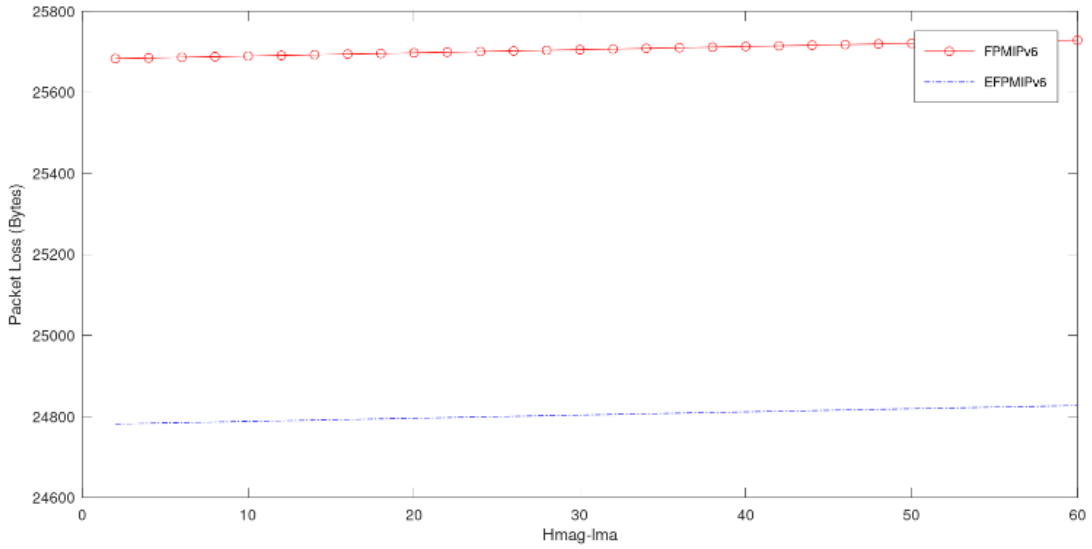

Figure 29. Packet Loss vs $H_{MAG-LMA}$.

Κεφάλαιο 6: Συμπεράσματα

Ολοκληρώνοντας την παρούσα εργασία, αφού μελετήσαμε τα οχηματικα δίκτυα καθώς και τα πρωτόκολλα της διαχείρισης κινητικότητάς, παρουσιάζουμε τα συμπεράσματα που προκύπτουν. Τα ασύρματα δίκτυα επικοινωνίας και ιδιαίτερα τα οχηματικα δίκτυα εξελίσσονται ταχύτατα και χαρακτηριστικά όπως υψηλοί ρυθμοί μετάδοσης, μικρή καθυστέρηση και ελάχιστες απώλειες είναι άκρως απαραίτητα. Τα δίκτυα νέας γενιάς 5G ως εξέλιξη των 4G δικτύων μπορούν να καλύψουν τα παραπάνω χαρακτηριστικά, ενώ ανοίγουν το δρόμο για εφαρμογές σε πολλούς καινούριους τομείς όπως είναι η ενέργεια, οι έξυπνες πόλεις, τα έξυπνα συστήματα μεταφορών και η απομακρυσμένη φροντίδα υγείας.

Ταυτόχρονα όμως οι διαδικασίες τις διαχείρισης κινητικότητας, όπως είναι η εγγραφή χρηστών στο δίκτυο και η διαπομπή πρέπει συνεχώς να βελτιώνονται με σκοπό την αντιμετώπιση της καθυστέρησης. Επίσης τα μοντέλα διαπομπής πρέπει να διαθέτουν μηχανισμούς αντιμετώπισης των περιπτώσεων που οδηγούν στην απώλεια δεδομένων. Το προτεινόμενο μοντέλο διαπομπής εφαρμόζεται για τα δίκτυα 5ης γενιάς και βασίζεται στο πρωτόκολλο FPMIPv6. Το βελτιωμένο μοντέλο προσφέρει βελτιστοποιήσεις στο κομμάτι της καθυστέρησης και του κόστους tunneling καθώς οι αλληλεπιδράσεις μεταξύ των οντοτήτων είναι μειωμένες και τα δεδομένα δρομολογούνται μέσω μιας πιο άμεσης διαδρομής. Επίσης όσο αφορά την απώλεια πακέτων το προτεινόμενο μοντέλο εμφανίζει αρκετά καλύτερες επιδόσεις σε σχέση με το FPMIPv6 χάρη στην αποτελεσματική αντιμετώπιση των false predictive διαπομπών. Όμως σε αντίθεσή με την καλύτερη απόδοση του βελτιωμένου μοντέλου στους παραπάνω τομείς, το βελτιωμένο μοντέλο έχει μεγαλύτερο κόστος σηματοδοσίας σε σχέση με το FPMIPv6. Το μειονέκτημα αυτό οφείλεται στην ανταλλαγή περισσότερων μηνυμάτων συσχέτισης μεταξύ των οντοτήτων, το οποίο είναι αναπόφευκτο καθώς η λειτουργία του μοντέλου βασίζεται στην ανταλλαγή αυτών των μηνυμάτων.

Το προτεινόμενο μοντέλο μπορεί να εξελιχθεί περαιτέρω ενσωματώνοντας τον μηχανισμό MIH, καθώς οι οντότητές του δίκτυού θα έχουν την δυνατότητα να ανταλλάσσουν μηνύματα μεταξύ τους χωρίς περαιτέρω καθυστερήσεις όπως είναι η αναγκαία προώθηση των μηνυμάτων μέσω του LMA. Έτσι είναι δυνατό να μειωθεί περεταίρω η καθυστέρηση και το κόστος tunneling καθώς και να αντιμετωπιστεί το μειονέκτημα του μοντέλου όσο αφορά το κόστος σηματοδοσίας.

Βιβλιογραφία

[1] Z. Machardy, A. Khan, K. Obana and S. Iwashina, "V2x Access Technologies: Regulation, Research, And Remaining Challenges," Ieee Communications Surveys & Tutorials Volume 20, No. 3, Pages 1858-1877, 2018.

[2] Ghosal Amrita, Conti Mauro, "Security Issues and Challenges In V2x: A Survey" 2019.

[3] Shrestha Rakesh, Bajracharya Rojeena and Nam Seung Yeob, "Challenges of Future Vanet and Cloud-Based Approaches", Wireless Communications And Mobile Computing,
Pages 1-15, 2018.

[4] Corporate Finance Institute, "What Is Vehicle To Everything (V2x)?", retrieved from https://corporatefinanceinstitute.com/resources/knowledge/other/vehicle-to-everything-v2x.

[5] V2X Network Limited, "Use Cases", retrieved from https://www.v2x.network/#usecases.

[6] F. Arena, G. Pau, A. Severino, "A Review on IEEE 802.11p for Intelligent Transportation Systems", Journal of Sensor and Actuator Networks, Volume 9, 2020.

[7] Chen Shuai, Nai Wei, Dong Decun, Zheng Wenyi and Jing Weiping, "Key Indices Analysis of IEEE 802.11p Based Vehicle to Infrastructure System in Highway Environment", Procedia - Social and Behavioral Sciences, Volume 96, Pages 188-195, 2013.

[8] Ali-Yahiya Tara, "Network Architecture and Protocols" In "Understanding LTE and its Performance", 2011.

[9] Z. Hameed Mir, F. Filali, "LTE and IEEE 802.11p for vehicular networking: a performance evaluation", Wireless Com Network, Article Number 89, 2014.

[10] A. Detti, "Functional Architecture" In M. A. Marsan, N. B. Melazzi and S. Buzzi, "5g Italy White Book: From Research To Market", Pages 59-68, 2018.

[11] N. Akkari, N. Dimitriou, "Mobility Management Solutions for 5G Networks: Architecture and Services", Computer Networks, Elsevier, Vol.169, 2020.

[12] Gabriel Brown, Principal Analyst, Heavy Reading, "Service-Based Architecture For 5g Core Networks" [White Paper], 2017.

[13] WBA 5g Workgroup, "Unlicensed Integration with 5g Networks" [White Paper], October 2018.

[14] Samsung Electronics Co., Ltd, "4g-5g Interworking" [White Paper], 2017.

[15] Jaydip Sen, "Mobility and Handoff Management in Wireless Networks" In Christos J Bouras," Trends in Telecommunications Technologies", InTech, 2010.

[16] Mark Grayson, Kevin Shatzkamer, Klaas Wierenga, "Mobile Internet Basics: Mobile Ipv6 Technology Overview", Retrieved from https://Www.Embedded.Com/Mobile-Internet-Basics-Mobile-Ipv6-Technology-Overview/, 2012.

[17] K. Kong, W. Lee, Y. Han, M. Shin and H. You, "Mobility Management For All-Ip Mobile Networks: Mobile Ipv6 Vs. Proxy Mobile Ipv6", Ieee Wireless Communications Volume 15 No. 2, Pages 36-45, April 2008.

[18] S. Gundavelli , K. Leung, V. Devarapalli, K. Chowdhury And B. Patil, "Proxy Mobile Ipv6",Ietf Rfc-5213, August 2008.

[19] R. Koodli, "Fast Handovers for Mobile IPv6", Ietf Rfc-4068, 2005.

[20] H. Yokota, K. Chowdhury, R. Koodli, B Patil, & F. Xia,"Fast Handovers For Proxy Mobile Ipv6",Ietf Rfc-5949, May 2010.

[21] M. Liebsch, A Muhanna, And O. Blume, "Transient Binding For Proxy Mobile Ipv6", Ietf Rfc-6058, March 2011.

[22] Gohar Moneeb, Anwar Sajid, Ali Moazam, Choi Jin-Ghoo, Alquhayz Hani, Koh Seok-Joo. "Partial Bicasting With Buffering For Proxy Mobile Ipv6 Mobility Management In Coap-Based Iot Networks", Electronics Volume 9,2020.

[23] Berguiga Abdelwahed, Harchay Ahlem, Massaoudi Ayman Youssef Habib, "Fpmipv6-S: A New Network-Based Mobility Management Scheme For 6lowpan", Internet Of Things Volume 13, 2019.

[24] Eddine Afilal, “A Mobile Internal Vertical Handover Mechanism For Distributed Mobility Management In Vanets”, Vehicular Communications, Volume 26, 2020
[25] Mun-Suk Kim, Sukyoung Lee, David Cypher, Nada Golmie, “Performance Analysis Of Fast Handover For Proxy Mobile Ipv6”, Information Sciences Volume 219, Pages 208-224, 2013
[26] E. Skondras, A. Michalas, and D. D. Vergados, “Mobility management on 5g vehicular cloud computing systems,” Vehicular Communications, Elsevier, vol. 16, pp. 15–44, 2019.
[27] I. Kosmopoulos, E. Skondras, A. Michalas, and D. D. Vergados, “An efficient mobility management scheme for 5g network architectures,” in 2020 5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). IEEE, 2020, pp. 1–6.
[28] A. Michalas, A. Sgora, and D. D. Vergados, “An integrated mih-fpmipv6 mobility management approach for evolved-packet system architectures,” Journal of Network and Computer Applications, vol. 91, pp. 104–119, 2017.
[29] Allan K Lewis, “Refining Mobility, retrieved from http://refiningmobility.blogspot.com/2015/01/dedicated-short-range-communication.html
[30] Debashri Roy, Mainak Chatterjee, Eduardo Pasiliao, “Video quality assessment for inter-vehicular streaming with IEEE 802.11p, LTE, and LTE Direct networks over fading channels”, Computer Communications Volume 118, Pages 69-80, 2019.
[31] Ana Orozco, Roger Michoud, Gonzalo Ramírez, “Routing Protocols simulation for Efficiency Applications in Vehicular Environments”, Sistemas y Telemática Volume 11,2013.
[32] Hebergementwebs, “LTE protocol stack layers”, retrieved from https://www.hebergementwebs.com/lte-tutorial/lte-protocol-stack-layers.
[33] Resurchify, “5G NR PDCP (Packet Data Convergence Protocol)”, retrieved from https://www.resurchify.com/5G-tutorial/5G-NR-PDCP.php#Introduction
[34] Kim Daehyeok, Lim Wan-Seon, Suh Young-Joo, “Multicast Extension to Proxy Mobile IPv6 for Mobile Multicast Services”, Journal of Computing Science and Engineering Volume 5, Pages 316-323, 2011.
[35] Chen Zhikui, Yang Song, “A Privacy Enabled Fast Dynamic Authentication and Authorization for B3G/4G Mobility”, Communications and Network Volume 1, Pages 74-81, 2009.
[36] Marina Aguado, Jasone Astorga, Jon Matias, Maider Huarte, “The MIH (Media Independent Handover) Contribution to Mobility Management in a Heterogeneous Railway Communication Context: A IEEE802.11/802.16 Case Study”, Pages 69-82, 2011.
[37] Antonio de la Oliva, Albert Banchs, Ignacio Soto, Telemaco Melia, Albert Vidal, “An overview of IEEE 802.21: Media-independent handover services” IEEE Wireless Communications Volume 15, Pages 96 – 103,2008.

Παράρτημα Κώδικα

```
%hop distance between mag and lma
Hmag_lma=2:2:60;
%hop distance between rsu/eNodeB and lma
HenodeB_mag=1;
%hop distance between mags
Hmag_mag=1;
%nubmer of location updates
lambda=10;
%length of  handover indication message
L_hind=52*8;
%length of  handover initiation message
L_hi=52*8;
%length of  handover acknowledgement message
L_hack=52*8;
%length of  handover complete message
L_hoc=52*8;
%length of  pbu message
L_pbu=76*8;
%length of  pba message s
L_pba=76*8;
%length of  data packet
L_data=1500*8;
%length of tunnel header
L_hd=40*8;
%probabilty of wireless link failure
pwf=0.1:0.05:1;
%bandwidth of the wired connection
Bl=10^9;
%bandwidth of the wireless connection
Bw=54*10^6;

%delay of the handover indication message over wired connection
Tl_hind=L_hind/Bl;
%delay of the handover indication message over wireless connection
Tw_hind=(1+1*pwf)/(1-pwf)*L_hind/Bw;
%delay of the handover initiation message
Tl_hi=(1+1*pwf)/(1-pwf)*L_hi/Bl;
%delay of the handover acknowledgement message
Tl_hack=(1+1*pwf)/(1-pwf)*L_hack/Bl;
%delay of the handover complete message
Tl_hoc=(1+1*pwf)/(1-pwf)*L_hoc/Bl;
%delay of the pbu message
Tl_pbu=(1+1*pwf)/(1-pwf)*L_pbu/Bl;
%delay of the pba message
Tl_pba=(1+1*pwf)/(1-pwf)*L_pba/Bl;
%delay of the data packet over wired connection
Tl_data=L_data/Bl;
%delay of the data packet over wireless connection
Tw_data=(1+1*pwf)/(1-pwf)*L_data/Bw;

```

```
%%%%%%%%Handover Latency%%%%%%%%

%tf is the period from when the MN sends the handover indication to
%the new access point untill it decides to reconnect to the previous access point.

Tf=10*10^(-3);

%probabilty factor for a false predictive handover to occur
pf=0.5;

%probabilty of predictive scenario to activate
Pp=0.3;

%%%%%%%%predictive scenario%%%%%%%%

%Tpre for  predictive scenario
Tpre_p=Tw_hind + Tl_hind*HenodeB_mag + 2*Hmag_lma*Tl_hi + 2*Hmag_lma* Tl_hack;

%Tl2 for  predictive scenario
Tl2_p=59*10^(-3);

%Tpost for  predictive scenario
Tpost_p = Tw_data + Tl_data*HenodeB_mag + Tl_data*Hmag_lma +Tl_data*Hmag_mag
 Hmag_lma* Tl_pbu+ Hmag_lma* Tl_pba;

%handover latency for a sucessful  predictive handover
Tho_ps = Tpre_p + Tl2_p + Tpost_p;

%handover latency for a false predictive handover
Tho_pf=Tf+ Tw_hind + Tl_hind*HenodeB_mag + Tw_data + Tl_data*HenodeB_mag
+ Tl_data*Hmag_lma ;

%total handover latency for  predictive scenario
Tho_p=(1-pf)*Tho_ps + pf*Tho_pf;

%%%%%%%%enhanced predictive scenario%%%%%%%%

%Tpre for enhanced predictive scenario
Tpre_ep=Tw_hind + Tl_hind*HenodeB_mag + 2*Hmag_lma*Tl_hi+ 2*Hmag_lma* Tl_hack
+ Hmag_lma* Tl_pbu+ Hmag_lma* Tl_pba;

%Tl2 for enhanced predictive scenario
Tl2_ep= Tpre_p + Tl2_p - Tpre_ep;

%Tpost for enhanced predictive scenario
Tpost_ep = Tw_data + Tl_data*HenodeB_mag;

%handover latency for a sucessful enhanced predictive handover
Tho_eps = Tpre_ep + Tl2_ep + Tpost_ep;

```

```
%handover latency for a enhanced false predictive handover
Tho_epf=Tf+ Tw_hind + Tl_hind*HenodeB_mag + Tw_data + Tl_data*HenodeB_mag
+ Tl_data*Hmag_lma ;

%total handover latency for enhanced predictive scenario
Tho_ep=(1-pf)*Tho_eps + pf*Tho_epf;

%%%%%%%%reactive scenario%%%%%%%%

%Tl2 for  reactive scenario
Tl2_r=59*10^(-3);

%Tpost for  reactive scenario
Tpost_r= 2*Tl_hi*Hmag_lma + 2*Tl_hack*Hmag_lma + Tl_pbu*Hmag_lma + Tl_pba*Hmag_lma
+ Tw_data + Tl_data*HenodeB_mag + Tl_data*Hmag_mag + Tl_data*Hmag_lma;

%total handover latency for  reactive handover
Tho_r=Tl2_r + Tpost_r;

%Total handover latency for the scheme
Tho_=Pp*Tho_p + (1-Pp)*Tho_r;

%%%%%%%%enhanced reactive scenario%%%%%%%%

%Tl2 for enhanced reactive scenario
Tl2_er= Tl2_r;

%Tpost for enhanced reactive scenario
Tpost_er= 2*Tl_hi*Hmag_lma + 2*Tl_hack*Hmag_lma + Tl_pbu*Hmag_lma
+Tl_pba*Hmag_lma + Tw_data + Tl_data*HenodeB_mag + Tl_data*Hmag_lma;

%total handover latency for enhanced reactive handover
Tho_er=Tl2_er + Tpost_er;

%Total handover latency for the enhanced scheme
Tho_e=Pp*Tho_ep + (1-Pp)*Tho_er;

%%%%%%%%handover latency figure%%%%%%%%

figure
plot( Hmag_lma,Tho_*1000,'-ro', Hmag_lma,Tho_e*1000,'-.b')
legend('FPMIPv6','EFPMIPv6')
xlabel('Hmag-lma')
ylabel('Handover Latency (ms)')

%%%%%%%%Signaling Cost%%%%%%%%

%%%%%%%%FPMIPv6%%%%%%%%

%transimission cost between MAGs in predictive scenario
```

```
SPmag_mag= 2*Hmag_mag*L_hi + 2*Hmag_mag*L_hack;

%transimission cost between MAG and LMA in predictive scenario
SPmag_lma=Hmag_lma*L_pbu + Hmag_lma*L_pba;

%transimission cost between MAGs in reactive scenario
SRmag_mag = 2*Hmag_mag*L_hi + 2*Hmag_mag*L_hack;

%transimission cost between MAG and LMA in reactive scenario
SRmag_lma = Hmag_lma*L_pbu + Hmag_lma*L_pba;

%signaling cost for the  predictive scenario
Csig_p=lambda*(SPmag_mag + SPmag_lma);

%signaling cost for the  reactive scenario
Csig_r=lambda*(SRmag_mag + SRmag_lma);

%Total signalling cost forenchanced scheme
Csig_=Pp*Csig_p + (1-Pp)*Csig_r;

%%%%%%%%enhanced FMIPv6%%%%%%%%

%transimission cost between MAGs in predictive scenario
SEPmag_mag= 2*Hmag_mag*L_hi + 2*Hmag_mag*L_hack;

%transimission cost between MAG and LMA in predictive scenario
SEPmag_lma=2*(Hmag_lma*L_pbu + Hmag_lma*L_pba);

%transimission cost between MAGs in reactive scenario
SERmag_mag = 2*Hmag_mag*L_hi + 2*Hmag_mag*L_hack;

%transimission cost between MAG and LMA in reactive scenario
SERmag_lma = Hmag_lma*L_pbu + Hmag_lma*L_pba;

%signaling cost for the enhanced predictive scenario
Csig_ep=lambda*(SEPmag_mag + SEPmag_lma);

%signaling cost for the enhanced reactive scenario
Csig_er=lambda*(SERmag_mag + SERmag_lma);

%Total signalling cost for the the enhanced scheme
Csig_e=Pp*Csig_ep + (1-Pp)*Csig_er;

%%%%%%%%signalling cost figure%%%%%%%%
figure;
plot( Hmag_lma,Csig_,'-ro', Hmag_lma,Csig_e,'-.b');
legend('FPMIPv6','EFPMIPv6')
xlabel('Hmag-lma')
ylabel('Signalling Cost(Bytes)')

```

```
%%%%%%%%Tunneling Cost%%%%%%%%

%number of packets transmitted due to packet loss
n_retr=2;

%packet arrival rate at overlapping cells
lambdap=50;

%transimission cost from LMA to MAG
Pmag_lma= Hmag_lma*L_hd;

%transimission cost from MAG to MAG
Pmag_mag= Hmag_lma*(L_hd+L_hd);

%%%%%%%%FPMIPv6%%%%%%%%
%duration on tunneling between 2 MAG
Ttnl_p=Tl2_p + Hmag_lma* Tl_pbu + Hmag_lma*Tl_pba;

Ttnl_r=Hmag_lma* Tl_pbu + Hmag_lma*Tl_pba;

%period when packets are lost in reactive scenario
Tloss_r= Tl2_r + 2*Hmag_lma*Tl_hi;

%tunneling cost of predictive scenario
Ctun_p=lambda*lambdap*(Pmag_lma.*Tho_p + Pmag_mag.*Ttnl_p);

%tunneling cost of reactive scenario
Ctun_r=lambda*lambdap*(n_retr*Pmag_lma.*Tloss_r + Pmag_lma.*(Tho_r-Tloss_r))
+ Pmag_mag.*Ttnl_r;

%Total tunneling cost for the scheme
Ctun_=Pp*Ctun_p + (1-Pp)*Ctun_r;

%%%%%%%%Enhanced FPMIPv6%%%%%%%%

%duaration on tunneling between 2 MAG
Ttnl_ep=Tl2_ep + Hmag_lma* Tl_pbu + Hmag_lma*Tl_pba;

%period when packets are lost in reactive scenario
Tloss_er= Tl2_er + 2*Hmag_lma*Tl_hi

%tunneling cost of predictive scenario
Ctun_ep=lambda*lambdap*(Pmag_lma.*(2*Hmag_lma*Tl_hi+2*Hmag_lma*Tl_hack+Hmag_lma*Tl_pbu+Hmag_lma*Tl_pba)
+ Pmag_mag.*Ttnl_ep);

%tunneling cost of reactive scenario
Ctun_er=lambda*lambdap*(n_retr*Pmag_lma.*Tloss_er + Pmag_lma.*(Tho_er-Tloss_er));

%Total tunneling cost for the the enhanced scheme
Ctun_e=Pp*Ctun_ep + (1-Pp)*Ctun_er;
```

```
%%%%%%%%tunneling cost figure%%%%%%%%

figure;
plot( Hmag_lma,Ctun_,'-ro', Hmag_lma,Ctun_e,'-.b');
legend('FPMIPv6','EFPMIPv6')
xlabel('Hmag-lma')
ylabel('Tunneling Cost(Bytes)')

%%%%%%%%Total Cost%%%%%%%%

Ctot_=Csig_+Ctun_;
Ctot_e=Csig_e+Ctun_e;

%%%%%%%%Total cost figure%%%%%%%%

figure;
plot( Hmag_lma,Ctot_,'-ro', Hmag_lma,Ctot_e,'-.b');
legend('FPMIPv6','EFPMIPv6')
xlabel('Hmag-lma')
ylabel('Tunneling Cost(Bytes)')

%%%%%%%%Packet Loss%%%%%%%%

%size of buffer in PMAG
Bp=500*8*1000;

%size of buffer in NMAG
Bn=500*8*1000;

%size of buffer in LMA
Bl=500*8*1000;

%%%%%%%%FPMIPv6%%%%%%%%

%packet loss of enchanced sucessful predictive scenario
Closs_ps=max(lambdap*L_data*(2*Hmag_lma*Tl_hi + 2*Hmag_lma* Tl_hack)-Bp ,0)
+max(lambdap*L_data*(2*Hmag_lma*Tl_hi+2*Hmag_lma*Tl_hack+Tl2_p)-Bn, 0);

%false predictive case where the HI message to reconnect to the previoud MAG is
%sent before the HACK

if(Tf + Tw_hind < Tw_hind + Tl_hi + Tl_hack)
    Closs_pf = max(lambdap*L_data*(Tf + Tw_hind) -Bp , 0);
else
    Closs_pf = lambdap*L_data*(Tf + Tw_hind);
end

%total packet loss for predictive scenario
Closs_p = (1-pf)*Closs_ps + pf*Closs_pf;
```

```
%packet loss of reactive scenario
Closs_r = lambdap*L_data*(Tl2_r + 2*Hmag_lma*Tl_hi) +
max(lambdap*L_data*(2*Hmag_lma*Tl_hack) - Bp, 0);

%total packet loss for FPMIPv6 scheme
Closs_= Pp*Closs_p + (1-Pp)*Closs_r;

%%%%%%%%Enhanced FPMIPv6%%%%%%%%

%packet loss of enchanced sucessful predictive scenario
Closs_eps = max(lambdap*L_data*(2*Hmag_lma*Tl_hi + 2*Hmag_lma* Tl_hack) - Bp , 0)
+max(lambdap*L_data*(2*Hmag_lma*Tl_hi + 2*Hmag_lma* Tl_hack
+ Hmag_lma* Tl_pbu+ Hmag_lma* Tl_pba + Tl2_ep) - Bn, 0);

%fasle predictive case where the HI message to reconnect to the previoud MAG is
%sent before the HACK

if(Tf + Tw_hind < Tw_hind + Tl_hi + Tl_hack)

    Closs_epf = max(lambdap*L_data*(Tf + Tw_hind) -Bp , 0);
else
    Closs_epf = max(lambdap*L_data*(2*Hmag_lma*Tl_hi + 2*Hmag_lma* Tl_hack) - Bp, 0)
    + max(lambdap*L_data*(Tf + Tw_hind) - Bn, 0);
end

%total packet loss for predictive scenario
Closs_ep = (1-pf)*Closs_eps + pf*Closs_epf;

%packet loss of enhanced reactive scenario
Closs_er = lambdap*L_data*(Tl2_er + 2*Hmag_lma*Tl_hi)
+max(lambdap*L_data*(2*Hmag_lma*Tl_hack+Hmag_lma*Tl_pbu
+Hmag_lma*Tl_pba+2*Hmag_lma*Tl_hoc)-Bp, 0);

%total packet loss for enhanced scheme
Closs_e= Pp*Closs_ep + (1-Pp)*Closs_er;

%%%%%%%%Packet loss figure%%%%%%%%

plot(Hmag_lma,Closs_,'-ro', Hmag_lma,Closs_e ,'-.b');
legend('FPMIPv6','EFPMIPv6')
xlabel('Hmag-lma')
ylabel('Packet Loss (Bytes)')
```