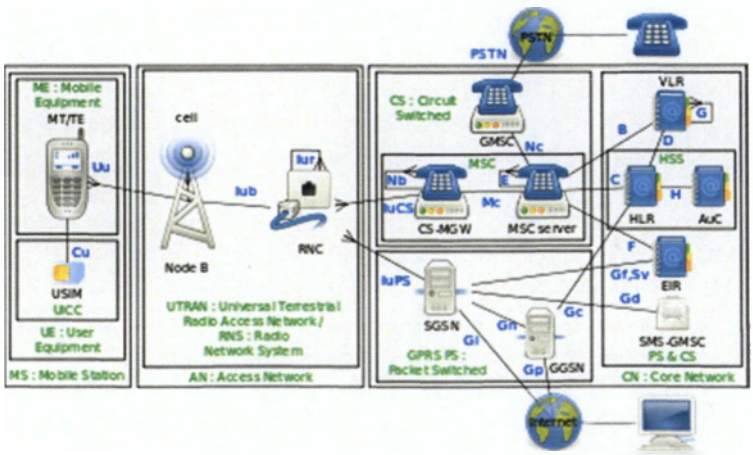
Α.Τ.Ε.Ι Καλαμάτας
Παράρτημα Σπάρτης
Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών

Πτυχιακή Εργασία

"Περιγραφή και ανάλυση του δικτύου κινητών επικοινωνιών UMTS και προσομοίωση της τεχνολογίας Mobile Ip"



ΚΟΡΟΜΗΛΑ ΕΥΑΓΓΕΛΙΑ

Α.Μ. : 2007273

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΝΑΣΤΑΚΟΣ ΜΙΧΑΗΛ

Σπάρτη 2013

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΑΚΡΩΝΥΜΙΑ

3GPP	3rd Generation Partnership Project
3G	3rd Generation
AH	Authentication Header
AKA	Authentication and Key Agreement
AMPS	Advanced Mobile Phone Service
AMR	Adaptive MultiRate Codec
API	Application Programming Interface
AuC	Authentication Centre
ATM	Asynchronous Transfer Mode,
BSC	Base Station Subsystem
BM-SC	Broadcast/multicast service center
BTS	Base transceiver station
CN	Correspondent Node
CN	Core network
CS	Circuit
CSE	Camel Service Environment
CDMA	Code Division Multiple Access
CRNC	Controlling RNC
CSE	Camel Service Environment
DI	Data Integrity
DC	Data Confidentiality
DCH	Dedicated Channel
DMZ	Demilitarized zone
DHCP	Dynamic Host Configuration Protocol
DSCH	Downlink Shared Channel
DRNC	Drift RNC
ESP	Encapsulating Security Payload/Encapsulated Security Protocol
ETSI	European Telecommunications Standards Institute
EDGE	Enhanced Data Rates for GSM Evolution
FA	Foreign Agent
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Multiple Access
FTP	File Transfer Protocol
GIO	GSM Intranet Office
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Services Switching Center
GMSK	Gaussian Minimum Shift Keying
GSM	Global System for Mobile communications
GPRS	General Packet Radio Service
GPS	Global Positioning System
GTP	GPRS tunneling protocol
HA	Home Agent
HLR	Home Location Register
HSCSD	High Speed Circuit Switched Data
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HS-DSCH	High-speed DSCH
HSUPA	High Speed Uplink Packet Access
HN	Home Network
IETF	Internet Engineering Task Force
IGSN	Internet GPRS Support Node

IK	Integrity Key
IKE	Internet Key Exchange
IMS	IP Multimedia subsystem
IMSI	International Mobile Subscriber Identity
IM-SSF	IP Multimedia Service Switching Function
IMTS	International Mobile telephone Service
ISIM	IMS Subscriber Identity Module
ISDN	Integrated Services Data Digital Network
ISAKMP	Internet Security Association and Key Management Protocol
IS-136	Interim Standard 136
IS-95	Interim Standard 95 Code Division Multiple Access
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPsec	Internet Protocol Security
ITU	International Telecommunication Union
KAC	Key Administration Centre
LAN	Local area network
LTE	Long Term Evolution
MAC	Medium Access Control
MAC(-I)	Message Authentication Code (for data Integrity)
MAP	Mobile Application Part
MAPsec	MAP Security Protocol
MBMS	Multimedia Broadcast Multicast Services
ME	Mobile Equipment
MGW	Media Gateway
MIMO	Multiple-input and multiple-output
MITM	Man-in -the-Middle
MS	Mobile Station
MSC	Mobile Services Switching Center
MN	Mobile Node
MPLS	Multiprotocol Label Switching
MTS	Mobile Telephone Service
NADC	North American Digital Cellular
NMT	Nordic Mobile Telephony
NTT	Nippon Telegraph and Telephone
OFDM	Orthogonal Frequency Division Multiplexing
OSA	Open Service Architecture
PDC	Pacific Digital Cellular
PDP	Packet Data Protocol
PS	Packet Switched
PMM	Packet MM
PLMN	public land mobile network
PSK	Phase-shift keying
PSTN	Public switched telephone network
RAB	Radio access bearer
RAs	Routing areas
RFC	Requests for Comments
RNC	Radio Network Controller
RRC	Radio Resource Control
RSVP	Resource Reservation Protocol
SCF	Service Capability Features
SCS	Service Capability Server
SCP	Secure copy protocol
S-CSCF	Serving Call Session Control Function
SEG	Security Gateway
SGSN	Serving GPRS Support Node

SIM	Subscriber identity module
SIP AS	Session Initiation Protocol Application Server
SIP-CGI	Session Initiation Protocol-Common Gateway Interface
SKIP	Simple Key-Management for Internet Protocol
SMS	Short Messaging Service
SN	Serving Network
SPI	Security Parameters Index
SS7	Signaling System Number 7
SRNS	Serving Radio Network Subsystem
TACS	Total Access Communication System
TCP	Transmission Control Protocol
TE	Terminal Equipment
TEID	Tunnel endpoint identifier
TDD	Time-division duplex
TDMA	Time Division Multiple Access
UDP	User Datagram Protocol
URAs	UTRAN registration areas
UTRAN	UMTS terrestrial radio-access network
UMTS	Universal Mobile Telecommunications System
UE	User equipment
UIC	Identification Confidentiality
USB	Universal Serial Bus
USDC	US Digital Cellular
USIM	Universal Subscriber Identity Module
VAS	Value-added service
VLR	Visitor Location Register
VPN	Virtual Private Networks
WIMAX	Worldwide Interoperability for Microwave Access
WAP	Wireless Applications protocol
WARP	Wireless Adjunct Internet Platform
W-CDMA	Wideband-CDMA
WLAN	wireless local area network

Γενικά

Αντικείμενο της πτυχιακής αυτής εργασίας είναι η ανάπτυξη μιας εφαρμογής με στόχο την προσομοίωση της λειτουργίας των πρωτοκόλλων Mobile IP και RSVP που χρησιμοποιούνται για την παροχή υπηρεσιών διαδικτύου σε κινητούς χρήστες που συνδέονται σε δίκτυο ενοποιημένων υπηρεσιών μεταγωγής πακέτου. Η εφαρμογή αυτή αναπτύσσεται σε γλώσσα προγραμματισμού Java.

Το μεν πρώτο πρωτόκολλο επιτρέπει τη διατήρηση της συνδεσιμότητας του κινητού τερματικού με το υπόλοιπο δίκτυο (δηλαδή αντιμετωπίζει το πρόβλημα που δημιουργεί η κινητικότητα των τερματικών κόμβων), το δε δεύτερο τη δέσμευση πόρων του δικτύου για τη διατήρηση της ποιότητας υπηρεσίας που του παρέχεται παρά την κίνησή του.

Έτσι λοιπόν, στο πρώτο μέρος της εργασίας μελετάμε και αναλύουμε τη λειτουργία των δύο πρωτοκόλλων σε θεωρητικό επίπεδο, δικαιολογώντας την ανάγκη ύπαρξής τους. Στο δεύτερο και βασικό μέρος της εργασίας, δηλαδή το πρακτικό μέρος, γίνεται η ανάπτυξη και η επεξήγηση της λειτουργίας της εφαρμογής μας. Η τελευταία προσομοιώνει σε υψηλό επίπεδο τα μηνύματα που ανταλλάσσονται μεταξύ κινητών και σταθερών κόμβων του δικτύου κατά τη διάρκεια της διαπομπής από ένα υποδίκτυο σε ένα άλλο. Η εκτέλεση της εφαρμογής με διάφορες τιμές για τις παραμέτρους του δικτύου επιτρέπει την εξαγωγή χρήσιμων συμπερασμάτων για τη λειτουργία και την επίδοση τω δύο πρωτοκόλλων.

Κεφάλαιο 1. Εισαγωγή

Τα κινητά τερματικά συστήματα συχνά αλλάζουν σημείο πρόσδεσης στο δίκτυο. Σε ένα τέτοιο περιβάλλον, για να μπορούν τα κινητά τερματικά να λειτουργούν χωρίς διακοπή, είναι απαραίτητη μια κατάλληλη διαδικτυακή υποδομή. Απαιτείται λοιπόν ένα πρωτόκολλο το οποίο να μπορεί να υποστηρίξει την κινητικότητα (mobility) στο δίκτυο. Οι κινητές συσκευές πρέπει επίσης να μπορούν να επικοινωνούν με τους υπάρχοντες εξυπηρετητές πληροφοριών και αρχείων, πράγμα που σημαίνει ότι απαιτούνται επίσης και δυνατότητες για τη διασύνδεση σταθερών και κινητών συστημάτων. Δυστυχώς όμως, το πρωτόκολλο IP (Internet Protocol), το οποίο αποτελεί το σκελετό του υπάρχοντος παγκοσμίου δικτύου επικοινωνιών, δεν είναι αρκετό για να ικανοποιήσει τις απαιτήσεις αυτές. Τα υπάρχοντα πρωτόκολλα TCP/IP σχεδιάστηκαν κάτω από την παραδοχή ότι τα τερματικά συστήματα θα είναι σταθερά. Αν λοιπόν κατά τη διάρκεια μιας ενεργούς δικτυακής συνόδου ένα από τα άκρα της σύνδεσης μετακινηθεί, η σύνοδος διακόπτεται. Φυσικά, όλες οι διαδικτυακές υπηρεσίες που είναι διαστρωματομένες πάνω στο TCP/IP διακόπτονται επίσης όταν τα τερματικά συστήματα γίνονται κινητά.

Υπάρχουν δύο προσεγγίσεις για την επίλυση του προβλήματος αυτού. Η μία είναι η ολοκληρωτική επανασχεδίαση των διαδικτυακών πρωτοκόλλων με συγκεκριμένο στόχο την υποστήριξη κινητών τερματικών συστημάτων. Η άλλη είναι να παρέχει το στρώμα δικτύου επιπλέον υπηρεσίες με ένα συμβατό προς τα πίσω τρόπο και έτσι να καθίσταται η υποστήριξη κινητών τερματικών συστημάτων δυνατή. Η πρώτη προσέγγιση, αν και αποτελεί μια ενδιαφέρουσα δυνατότητα από μια ερευνητική σκοπιά, είναι αδύνατη επί του πρακτέου αφού θα απαιτούσε ριζικές αλλαγές στην ήδη υπάρχουσα αναπτυγμένη δικτυακή υποδομή. Η δεύτερη προσέγγιση λοιπόν είναι αυτή που εστιάζει το ενδιαφέρον της εξέτασης που θα επακολουθήσει.

Για να διασφαλιστεί η λειτουργία με την υπάρχουσα υποδομή, ο χειρισμός της κινητικότητας πρέπει να είναι τελείως διάφανος στα πρωτόκολλα και στις εφαρμογές που τρέχουν σε σταθερά (ενσύρματα) τερματικά (stationary hosts). Με άλλα λόγια από την πλευρά ενός σταθερού τερματικού συστήματος, ένα κινητό τερματικό (mobile host) θα πρέπει να εμφανίζεται σαν ένα οποιοδήποτε άλλο σταθερό τερματικό το οποίο είναι συνδεδεμένο στο Internet. Αυτό σημαίνει ότι ίδιες συμβάσεις ονοματοδοσίας (naming) και διευθυνσιοδότησης (addressing) σαν αυτές που έχουν αναπτυχθεί για σταθερά συστήματα πρέπει να εφαρμοστούν και στα κινητά συστήματα επικοινωνιών. Επιπρόσθετα, οποιεσδήποτε αλλαγές στο σημείο πρόσδεσης του κινητού στο

δίκτυο θα πρέπει να είναι εντελώς κρυμμένες από τα πρωτόκολλα και τις εφαρμογές που τρέχουν στα ενσύρματα συστήματα.

Θα δούμε λοιπόν ότι η κινητικότητα είναι στην ουσία ένα πρόβλημα μετάφρασης της διεύθυνσης (address translation problem) και ότι ο καλύτερος τρόπος για την επίλυσή του είναι η αντιμετώπισή του στο στρώμα δικτύου. Θα δούμε επίσης τις θεμελιώδεις υπηρεσίες που πρέπει να υποστηρίζονται στο στρώμα δικτύου για να μπορεί αυτό να φέρει εις πέρας το έργο της μετάφρασης της διεύθυνσης. Με βάση αυτά θα περιγραφεί μια αρχιτεκτονική στρώματος δικτύου η οποία καθιστά απρόσκοπτη την ολοκλήρωση της υποστήριξης κινητών τερματικών συστημάτων στην υπάρχουσα δομή του Internet.

1.1. Ιστορική Αναδρομή

Όταν μιλάμε για δίκτυα το μυαλό μας πηγαίνει συνήθως στα δίκτυα υπολογιστών που δεν είναι παρά συνδεδεμένοι μεταξύ τους υπολογιστές που ανταλλάσσουν πληροφορίες. Ωστόσο η ιστορία των δικτύων ξεκινάει πολύ παλαιότερα! Στα τέλη του 20ου αιώνα άρχισε να έχει ραγδαία ανάπτυξη η ασύρματη επικοινωνία μεταξύ των ανθρώπων, οι οποίοι αγκάλιασαν αυτήν την τεχνολογία και την ώθησαν στην άνθιση που παρουσιάζει η κινητή επικοινωνία στις μέρες μας. Για την επικοινωνία των χρηστών χρησιμοποιούνται τα ηλεκτρομαγνητικά κύματα που μπορούν να μεταδώσουν ένα σήμα σε μεγάλη απόσταση.

Οι ρίζες των κινητών τηλεφώνων εντοπίζονται ήδη από το δεύτερο μισό του 18ου αιώνα, όταν άρχισαν να ξεπηδούν τεχνολογίες κι εφευρέσεις όπως το τηλέφωνο, ο τηλέγραφος ή η ανακάλυψη και μελέτη των ηλεκτρομαγνητικών κυμάτων. Τα ονόματα μεγάλων και πρωτοπόρων, όπως του Alexander Graham Bell, του Marconi, του Herz κι άλλων χαράχτηκαν μαζί με τις βάσεις της σύγχρονης εποχής στις τηλεπικοινωνίες. Είναι χαρακτηριστικό το ότι σχεδόν παράλληλα με την ανάπτυξη του τηλεφώνου, υπήρξε κι η ιδέα για ασύρματη τηλεπικοινωνία, αν και οι αντίστοιχες τεχνολογίες εμφανίστηκαν αρκετά αργότερα, όσον αφορά στον τομέα αυτόν.

Το κινητό τηλέφωνο συνδυάζει θα λέγαμε δύο βασικές τεχνολογίες. Είναι τηλέφωνο, ωστόσο το όλο σύστημα από πλευράς δικτύου θυμίζει ραδιόφωνο. Λειτουργεί, μιλώντας πιο απλά, σαν το ραδιόφωνο, όπου υπάρχουν σταθμοί – κεραίες που αναμεταδίδουν το σήμα, ώστε να βρίσκεται σε συνεχή σύνδεση η μονάδα – συσκευή κινητής τηλεφωνίας. Μάλιστα, πριν υπάρξει η κινητή τηλεφωνία, με την τελική σημασία της λέξης, τα ραδιοτηλέφωνα ήταν το καταλληλότερο σύστημα κινητής τηλεπικοινωνίας. Σε αυτήν την περίπτωση,

υπήρχε ένας κεντρικός πομποδέκτης, μια μόνο κεραία σε κάθε πόλη, στην οποία υπήρχαν περίπου 25 διαθέσιμα κανάλια. Αυτό σήμαινε αυτομάτως πως χρειαζόταν ένας αρκετά ισχυρός πομπός, τόσος ώστε να είναι ικανός να εκπέμπει σε απόσταση περίπου 70 χιλιομέτρων, πράγμα που σήμαινε ότι δεν μπορούσε ο καθένας να χρησιμοποιήσει τα ραδιοτηλέφωνα, καθώς δεν υπήρχαν αρκετά κανάλια επικοινωνίας.

Με μια επιστροφή πίσω στις πρώτες σπίθες της τεχνολογικής αυτής επανάστασης, γυρίζουμε στον Alexander Graham Bell, ο οποίος επινόησε το τηλέφωνο, επιχειρώντας να ξεπεράσει τις δυνατότητες του τηλέγραφου. Ο τελευταίος αποτελούσε μια διάταξη που αναπτύχθηκε κι εξελίχθηκε κατά το 1838 από τον Morse (Samuel Finley Breese Morse, 1791-1872) και ήταν δυνατόν να μεταφέρει μόνο σήματα. Επιχειρώντας να μεταδώσει τη φωνή λοιπόν, ο Bell οδηγήθηκε στο τηλέφωνο, κατά το 1876. Επόμενος σημαντικός σταθμός ήταν το 1885, όταν ο Giuglielmo Marconi κατάφερε να απελευθερώσει από τα σύρματα την επικοινωνία, και πραγματοποίησε το 1901 μέσω ραδιοκυμάτων την αποστολή μηνύματος από την Αγγλία στη Αμερική, η πρώτη υπερατλαντική εκπομπή μηνύματος. Τα ίδια τα ραδιοκύματα έχουν τις ρίζες τους στο Nicola Tesla, ο οποίος αναγνώρισε την ύπαρξή τους, που είναι η όλη βάση της ασύρματης τηλεπικοινωνίας.

Το 1903, οι Γερμανικές AEG και Siemens&Halske ιδρύουν την Deutsche Telefunken GmbH και σε συνεργασία με την Lorezn AG πραγματοποιούν την πρώτη εκπομπή ήχου και ομιλίας μόλις 3 χρόνια μετά. Όταν κι η Αμερικανική Τηλεφωνική και Τηλεγραφική Εταιρεία AT&T συνεργάστηκε το κατόρθωμα αυτό βελτιώθηκε, οδηγώντας στην πρώτη υπερατλαντική μετάδοση ήχου, από τις Η.Π.Α. στη Γαλλία.

1.2. Γενιές Κινητών Δικτύων Επικοινωνιών

Στο κεφάλαιο αυτό θα γίνει μια αναφορά στα δίκτυα που προηγήθηκαν, του UMTS και της 3ης γενιάς. Γίνεται μια αναδρομή στην πορεία που έχουν διανύσει μέχρι τώρα τα κινητά δίκτυα επικοινωνιών, στα χαρακτηριστικά που είχαν, τις δυσκολίες που αντιμετώπιζαν και στους λόγους που τα ώθησαν για να εξελιχθούν.

Κινητά δίκτυα 0ης γενιάς(0G)

Επισήμως μπορούμε να τοποθετήσουμε τη γένεση της κινητής τηλεφωνίας, όπως την αντιλαμβανόμαστε σήμερα, γύρω στα 1918 ,αν και μετά

το δεύτερο μισό του 20ού αιώνα συνέβησαν οι πιο σημαντικές εξελίξεις. Είναι χαρακτηριστικό ότι εγκαταστάσεις κινητής τηλεφωνίας υπήρχαν σε τρένα. Συγκεκριμένα, μερικές πρώτες δοκιμές είχαν πραγματοποιηθεί στη Γερμανία, στην στρατιωτική γραμμή Βερολίνο– Zossen. Ύστερα, και σε ιδιωτική γραμμή που συνέδεε το Teltow, προάστιο του Βερολίνου, με την Saxony – Anhalt πόλη Lichterfelde. Πλέον, το 1926, κάθε ταχύ τρένο που εκτελούσε το δρομολόγιο Αμβούργο – Βερολίνο ήταν εξοπλισμένο με σύστημα κινητής τηλεφωνίας, ενώ από διάφορες στατιστικές προκύπτουν κατά μέσο όρο 40 τηλεφωνικές κλήσεις την ημέρα, κατά την περίοδο 1926-1927. Από την άλλη μεριά ο εξοπλισμός που υπήρχε στα τρένα ήταν τεράστιος σε διαστάσεις, ενώ και το κόστος χρήσης ήταν ανάλογα μεγάλο. Για να πραγματοποιήσει κάποιος μια κλήση, χρειαζόταν να χρησιμοποιήσει μια ειδική καμπίνα στο τρένο, με ένα συμβατικό σετ συσκευής τηλεφώνου. Στη συνέχεια, το σήμα μεταδιδόταν μέσω καλωδίων στην οροφή του τρένου, όπου υπήρχαν στερεωμένα διάφορα καλώδια. Κεραίες ύστερα μετέδιδαν το σήμα σε τηλεφωνικές γραμμές, οι οποίες βρίσκονταν δίπλα στις σιδηροτροχιές. Ακολούθως, χειροκίνητοι διακόπτες μετέδιδαν τη σύνδεση στο σταθερό τηλεφωνικό δίκτυο.

Τα πρώτα συστήματα κινητής τηλεφωνίας εξυπηρετούσαν πολύ λίγους χρήστες καθώς διέθεταν μικρό αριθμό καναλιών αλλά είχαν και πολύ μεγάλες απαιτήσεις σε ισχύ. Η ισχύς εκπομπής από το σταθμό βάσης μπορεί να ξεπερνούσε και τα 200 Watt!. Το πρώτο τέτοιο εγκατεστημένο σύστημα σε αυτοκίνητο ήταν το MTS (Mobile Telephone Service) και ακολούθησε το IMTS.

Στην Ευρώπη υπήρχε από το 1958 το German-A Network και από το 1972 η εξέλιξη του, το German-B Network, το οποίο κατάφερε να διπλασιάσει τους συνδρομητές. Χρησιμοποιούσε FM διαμόρφωση και δούλευε στις συχνότητες από 154 MHz ως 177 MHz .

Ο αναλογικός όπως λέγεται, αυτός ο τύπος δικτύων κινητής τηλεφωνίας άρχισε από τότε να εμφανίζεται κι επέζησε ως και τις αρχές περίπου της δεκαετίας του 90', όταν κι η ψηφιακή εποχή άρχισε να εδραιώνεται.

Κινητά δίκτυα 1ης γενιάς(1G)

Τα πρώτα δίκτυα κινητών τηλεπικοινωνιών έκαναν την εμφάνισή τους στα τέλη της δεκαετίας του 70 στις Η.Π.Α. και στις αρχές της δεκαετίας του 80 στην Ευρώπη. Τα αποκάλεσαν ασύρματα δίκτυα 1ης γενιάς ή αλλιώς αναλογικά. Παρόλο που οι δυνατότητες τους ήταν λίγες, η εμφάνιση τους την εποχή εκείνη θεωρήθηκε ως ένα τεράστιο τεχνολογικό επίτευγμα. Το Advanced Mobile Phone Service(AMPS), ήταν το πρώτο σύστημα στις κινητές τηλεπικοινωνίες που έκανε την εμφάνιση του το 1978 σε μερικές πολιτείες των Η.Π.Α. και στη συνέχεια, η ιδέα (της κινητής τηλεφωνίας), διαδόθηκε στις υπόλοιπες ηπείρους.

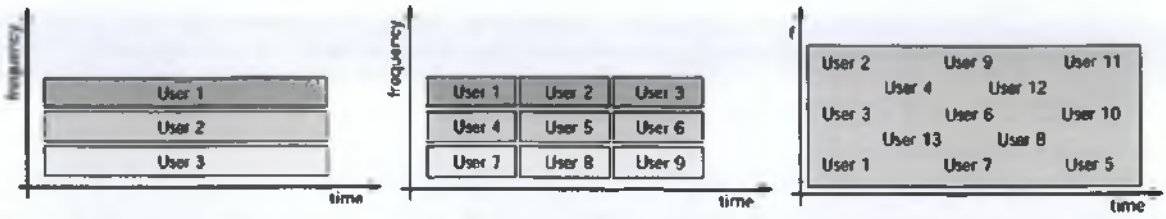
Στην Ευρώπη έκαναν την εμφάνιση τους δύο συστήματα κινητών τηλεπικοινωνιών τα οποία ήταν: (α) το Nordic Mobile Telephony (NMT) και (β) το Total Access Communication System (TACS).

Μια από τις πιο σημαντικές ανακαλύψεις στο χώρο των κινητών τηλεπικοινωνιών ήταν η έννοια της κυψέλης. Ο λόγος για τον οποίο τα συστήματα αυτά ονομάζονται κυψελωτά, είναι γιατί ακόμα και σήμερα στηρίζουν την λειτουργία τους στις κυψέλες, το Σχήμα 1 αντιπροσωπεύει κατά μια έννοια τα γεωγραφικά όρια μέσα στα οποία μπορούν να εξυπηρετούνται οι κινητοί χρήστες. Σε κάθε κυψέλη αντιστοιχεί ένας σταθμός βάσης ο οποίος αναλαμβάνει τη δημιουργία και τη δρομολόγηση των κλήσεων.

Ένα κύριο χαρακτηριστικό που μπορούσε κανείς να παρατηρήσει, ήταν το γεγονός ότι η πομπός και ο δέκτης επικοινωνούσαν χρησιμοποιώντας την ίδια συχνότητα. Από την άλλη πλευρά, όταν κάποιος χρήστης μιλούσε την στιγμή όπου βρισκόταν εν κινήσει, αυτό είχε σαν αποτέλεσμα η κλήση να τερματίζεται, τη στιγμή που ξεπερνούσε τα όρια της περιοχής κάλυψης. Η έλλειψη της δυνατότητας για διατήρηση της κλήσης κατά τη διάρκεια μετάβασης σε μια άλλη κυψέλη (handover), περιόριζε σημαντικά τις δυνατότητες της κινητής επικοινωνίας καθώς εμπόδιζε την κινητικότητα του χρήστη. Ένα άλλο πρόβλημα ήταν η χαμηλή απόδοση των συστημάτων αυτών καθώς ήταν πολύ μικρός ο αριθμός των χρηστών που μπορούσαν να μιλήσουν ταυτόχρονα, από τη στιγμή που το διαθέσιμο φάσμα συχνοτήτων δεν ήταν αρκετό. Σε γενικότερες γραμμές τα πρώτα συστήματα, δεν άφηναν περιθώρια για βελτιώσεις και για την εφαρμογή τεχνικών όπως συμπίεση και κωδικοποίηση της πληροφορίας, καθώς αυτό θα είχε σαν προϋπόθεση την χρήση ψηφιακού σήματος. Ακόμα και τα τερματικά, δηλαδή οι συσκευές που χρησιμοποιούσαν οι χρήστες, ήταν ογκώδεις με μεγάλες κεραίες και υψηλού για την εποχή εκείνη κόστους.

Κινητά δίκτυα 2ης γενιάς(2G)

Καθώς τα δίκτυα 1ης γενιάς ανήκουν πλέον στο παρελθόν, δε συνέβη το ίδιο με τα δίκτυα 2ης γενιάς αφού αρκετά από τα χαρακτηριστικά τους λήφθηκαν υπ' όψη για το σχεδιασμό των δικτύων της 3ης γενιάς. Σε αντίθεση με τα πρώτα δίκτυα που μετέδιδαν αναλογικό σήμα και ο διαχωρισμός μεταξύ των χρηστών για ταυτόχρονη πρόσβαση στο ασύρματο μέσο γινόταν με την Frequency Division Multiple Access (FDMA) τεχνική, τα δίκτυα 2ης γενιάς χρησιμοποιούσαν τεχνικές ψηφιακής διαμόρφωσης του σήματος, ενώ οι χρήστες διαχωρίζονταν με Time Division Multiple Access (TDMA) ή Code Division Multiple Access (CDMA) όπως φαίνεται στο Σχήμα 1: Τεχνικές πολλαπλής πρόσβασης.

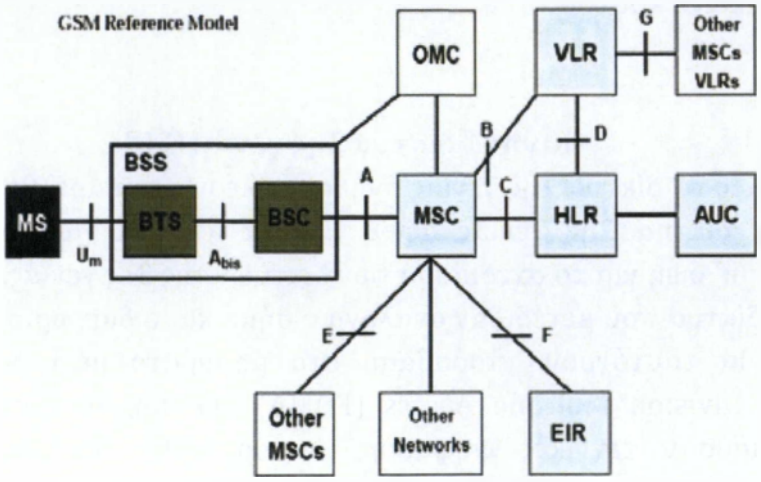


Η τεχνική FDMA *Η τεχνική TDMA* *Η τεχνική CDMA*

Σχήμα 1 : Τεχνικές πολλαπλής πρόσβασης

Τα πιο γνωστά συστήματα 2ης γενιάς ήταν (α) το Global System for Mobile communication (GSM) το οποίο χρησιμοποιεί την TDMA τεχνική και υποστηρίζει 8 χρονοσχισμές (time-slots) με εύρος ζώνης 200 KHz η κάθε μια, (β) το Interim Standard 136 (IS-136) γνωστό και σαν North American Digital Cellular (NADC) ή US Digital Cellular (USDC), (γ) το Pacific Digital Cellular (PDC) ένα Ιαπωνικό σύστημα που είχε αρκετές ομοιότητες με το IS-136 και (δ) το Interim Standard 95 Code Division Multiple Access (IS-95) επίσης γνωστό σαν cdmaOne το οποίο χρησιμοποιεί την CDMA τεχνική η οποία ήταν ευρέως διαδεδομένη στη Βόρεια Αμερική αλλά και σε χώρες όπως Κορέα, Ιαπωνία, Κίνα και Αυστραλία.

Στην Ευρώπη, η ανάγκη για τη δημιουργία ενός ενιαίου συστήματος που θα εξυπηρετούσε όλους τους Ευρωπαίους πολίτες ανεξαρτήτως χώρας, οδήγησε στη δημιουργία του GSM υπό την επίβλεψη του European Technical Standards Institute (ETSI). Το σύστημα αυτό ήταν το πιο ευρέως διαδεδομένο, μετρώντας 350 εκατομμύρια χρήστες σε 140 χώρες και 400 δίκτυα κινητών τηλεπικοινωνιών. Το GSM ξεκίνησε να λειτουργεί στην ζώνη των 800-900 MHz ενώ σε κάποιες άλλες χώρες που το υιοθέτησαν, λειτουργεί στα 1.8 και 2 GHz. Στο Σχήμα 2 φαίνεται η δομή του GSM δικτύου.



Σχήμα 2 : Η δομή του GSM δικτύου

Τέλος, μερικές από τις υπηρεσίες οι οποίες έκαναν την εμφάνιση τους μαζί με τα δίκτυα 2ης γενιάς ήταν η δυνατότητα για περιορισμένη πρόσβαση

στο Internet και η αποστολή σύντομων γραπτών μηνυμάτων μεταξύ των χρηστών γνωστά και σαν Short Messaging Service (SMS).

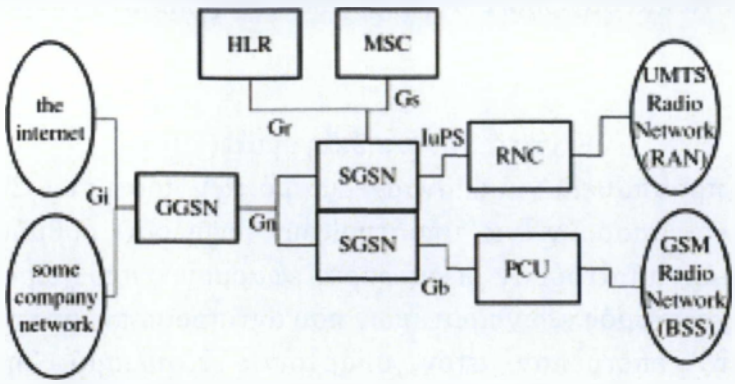
Κινητά δίκτυα 2.5 γενιάς(2.5G)

Σε μια προσπάθεια για επανασχεδιασμό των προτύπων 2ης γενιάς, έτσι ώστε αυτά να μπορούν να υποστηρίξουν υψηλούς ρυθμούς μετάδοσης δεδομένων όπως απαιτούσαν οι διάφορες εφαρμογές στο χώρο του Internet, προέκυψε ο σχεδιασμός νέων προτύπων που αντιπροσώπευαν την γενιά 2.5. Τα πρότυπα αυτά επέτρεπαν στον υπάρχοντα εξοπλισμό 2ης γενιάς, να τροποποιηθεί έτσι ώστε να μπορεί να υποστηρίζει υπηρεσίες όπως πλοήγηση στο Internet, e-mail, Wireless Applications Protocol (WAP) κ.α.

Στα πλαίσια της αναβάθμισης των συστημάτων προέκυψαν τρία νέα συστήματα που αντιπροσώπευαν την γενιά 2.5. Αυτά είναι τα: (α) High Speed Circuit Switched Data (HSCSD), (β) General Packet Radio Service (GPRS) και (γ) Enhanced Data Rates for GSM Evolution (EDGE).

Το όνομα HSCSD αντιπροσωπεύει την τεχνική της μεταγωγής κυκλώματος, η οποία επιτρέπει σε ένα κινητό χρήστη να χρησιμοποιεί διαδοχικές χρονοσχισμές του GSM προτύπου. Σε συνδυασμό με κάποιες άλλες τροποποιήσεις το HSCSD καταφέρνει να πετύχει ρυθμούς μετάδοσης στα 14,4 Kbps από τα 9,6 Kbps που προσέφερε το GSM. Επίσης, κάνοντας χρήση τεσσάρων συνεχόμενων χρονοσχισμών το πρότυπο αυτό, έδινε τη δυνατότητα για ρυθμό μέχρι και 57,6 Kbps ανοίγοντας έτσι τον δρόμο για εφαρμογές όπως streaming. Το βασικότερο μειονέκτημα του HSCSD ήταν το γεγονός ότι η χρήση της μεταγωγής κυκλώματος σπαταλούσε τους πόρους του δικτύου αφού οι χρονοσχισμές δεσμεύονταν ακόμα και όταν η χωρητικότητα τους δεν χρησιμοποιούνταν.

Το GPRS πρότυπο, βασίζεται στη λειτουργία της μεταγωγής πακέτου, γεγονός που το καθιστά κατάλληλο για υπηρεσίες όπως e-mail, fax και asymmetric web browsing όπου ο χρήστης κατεβάζει από το Internet πολύ περισσότερα δεδομένα από ότι ανεβάζει. Τα κύρια πλεονεκτήματά του είναι ότι δεσμεύει τους πόρους του δικτύου μόνο όταν υπάρχουν δεδομένα που πρέπει να μεταδοθούν και ότι δεν εξαρτάται τόσο πολύ από τα μέρη εκείνα των δικτύων που λειτουργούν με μεταγωγή κυκλώματος. Επειδή στο GPRS το κανάλι, δε δεσμεύεται από τον κινητό χρήστη με τον τρόπο που γίνεται στο HSCSD, το GPRS έχει τη δυνατότητα να υποστηρίζει περισσότερους χρήστες. Όταν και οι οκτώ χρονοσχισμές του GSM είναι δεσμευμένες στο GPRS από ένα χρήστη, τότε αυτός μπορεί να πετύχει ρυθμό μετάδοσης μέχρι και 171,2 Kbps. Στο Σχήμα 3 : Η δομή του GPRS δικτύου φαίνεται η δομή του GPRS δικτύου.



Σχήμα 3 : Η δομή του GPRS δικτύου

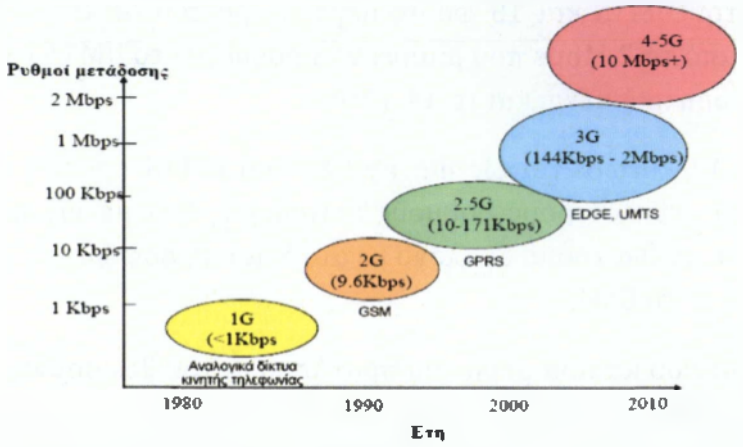
Τέλος το πρότυπο EDGE, θεωρείται ως μια αρκετά προηγμένη βελτιστοποίηση του προτύπου GSM και αυτό γιατί απαιτεί την αναβάθμιση τόσο στο λογισμικό (software) αλλά και στο υλικό (hardware). Το EDGE θεωρείται ως το αποτέλεσμα της επιθυμίας, των υπεύθυνων για τα δίκτυα GSM και IS-136, για μια από κοινού τεχνολογική εξέλιξη που θα τους οδηγούσε σε δίκτυα υψηλών ταχυτήτων 3ης γενιάς. Το EDGE εισάγει μια καινούργια ψηφιακή διαμόρφωση με το όνομα 8-PSK η οποία προσφέρει ρυθμό μετάδοσης μέχρι και 547,2 Kbps όταν χρησιμοποιείται χωρίς διόρθωση λαθών και όλες οι οκτώ χρονοσχισμές είναι δεσμευμένες σε ένα μόνο χρήστη.

Κινητά δίκτυα 3ης γενιάς(3G)

Ο ερχομός των δικτύων 3ης γενιάς, άνοιξε το δρόμο για την εμφάνιση ακόμα περισσότερων υπηρεσιών, που μέχρι τη στιγμή εκείνη, κανένα από τα προηγούμενα πρότυπα δε μπορούσε να τους προσφέρει. Με ταχύτητες επιπέδου Megabit κάποιος που έχει πρόσβαση σε ένα τέτοιο δίκτυο μπορεί να πλοηγηθεί στο Internet, να επικοινωνήσει χρησιμοποιώντας την υπηρεσία Voice over Internet Protocol (VoIP), να κατεβάσει μουσικά κομμάτια και να χρησιμοποιήσει διάφορες άλλες υπηρεσίες με τη βοήθεια το κινητού του τηλεφώνου.

Στα πλαίσια της εξέλιξης των ήδη υπαρχόντων δικτύων 2ης γενιάς, προέκυψαν το πρότυπο cdma2000 σαν συνέχεια του CDMA και το Wideband-CDMA (W-CDMA) ή αλλιώς Universal Mobile Telecommunications System (UMTS) σαν συνέχεια των GSM, IS-136 και PDC, όπως φαίνεται και στο Σχήμα 4 : Η εξέλιξη των κινητών συστημάτων τηλεπικοινωνιών. Το W-CDMA είναι ένα πρότυπο το οποίο έχει επηρεαστεί από τη φιλοσοφία και τον τρόπο λειτουργίας του GSM.

Βασικός στόχος της ανάπτυξης των κινητών δικτύων 3ης γενιάς είναι η παροχή υπηρεσιών σε οποιοδήποτε μέρος, οποιαδήποτε χρονική στιγμή. Το γεγονός αυτό σημαίνει ότι ένας χρήστης των δικτύων αυτών, θα έχει τη δυνατότητα να μετακινείται οπουδήποτε και να εξυπηρετείται, ακόμα και σε γεωγραφικές περιοχές όπου η κάλυψη που παρέχεται, δεν είναι από δίκτυο της 3ης γενιάς.



Σχήμα 4 : Η εξέλιξη των κινητών συστημάτων τηλεπικοινωνιών

Οι υπηρεσίες που προσφέρονται επεκτείνονται σε υπηρεσίες Internet και σε υπηρεσίες που συνδυάζουν εικόνα και ήχο (multimedia) με υψηλούς ρυθμούς μετάδοσης. Θα πρέπει τέλος να αναφερθεί ότι τα συστήματα 3ης γενιάς που έχουν επικρατήσει μέχρι τώρα είναι τα (α) UMTS στην Ευρώπη, (β) CDMA2000 στην Βόρεια Αμερική και (γ) το NTT Docomo στην Ιαπωνία.

Πλεονεκτήματα 3G

- Οι βίντεο-κλήσεις είναι χωρίς αμφιβολία μια από τις πιο πολυσυζητημένες υπηρεσίες των δικτύων 3G.
- Οι υψηλές ταχύτητες ασύρματης μεταφοράς δεδομένων. Η σύνδεση στο Internet εκτός από άμεση και απρόσκοπτη, θα σας δώσει πλέον και ταχύτητες που φθάνουν τα 384kbps.
- Οι υψηλές ταχύτητες μεταφοράς δεδομένων βοηθούν αρκετά στην πιο γρήγορη και άμεση χρήση διαφόρων multimedia εφαρμογών.
- Το video-streaming. Το αυξημένο bandwidth επιτρέπει τη μετάδοση σε πραγματικό χρόνο, κινούμενης εικόνας και ήχου υψηλής ανάλυσης.
- Υψηλής ποιότητας παιχνίδια και Υπηρεσίες εύρεσης θέσεως, σε συνδυασμό με την τεχνολογία GPS.
- Μετά την ευρεία διείσδυση της τεχνολογίας 3G, αναμένεται να διατεθούν ακόμη περισσότερες υπηρεσίες, όπως μετάδοση τηλεοπτικών εκπομπών και υπηρεσίες παγκόσμιας περιαγωγής.

Κινητά δίκτυα 3.5 γενιάς(3.5G)

Η γενιά 3.5, περιλαμβάνει τα δίκτυα εκείνα όπου, εκτός από την τεχνολογία WCDMA, έχουν ενσωματώσει και την τεχνολογία High Speed Downlink Packet Access (HSDPA). Το πρότυπο αυτό, αφορά την μετάδοση πακέτων από το σταθμό βάσης προς το χρήστη (downlink) με ρυθμό 5 φορές μεγαλύτερο του UMTS και 15 φορές μεγαλύτερο του GPRS. Το γεγονός αυτό σημαίνει ότι από τα 2 Mbps που μπορεί να προσφέρει το UMTS ο ρυθμός μπορεί να φτάσει θεωρητικά μέχρι και τα 14.4 Mbps.

Το HSDPA θεωρείται ως μια εξέλιξη του UMTS προτύπου, παρέχοντας στους χρήστες υψηλότερους ρυθμούς μεταφοράς δεδομένων και μεγαλύτερη χωρητικότητα, με ένα τρόπο ανάλογο με αυτό που προσφέρει το EDGE πρότυπο συγκρινόμενο με το GSM.

Παρόλο που κάποια μέρη του προτύπου αυτού θεωρούνται απλά στο να υλοποιηθούν με το υπάρχον υλικό (hardware), το HSDPA σαν γενικότερη έννοια απαιτεί επανασχεδιασμό στην αρχιτεκτονική του δικτύου και αναβάθμιση στο υλικό, όπως αυτό που πρόκειται να χρησιμοποιηθεί στους σταθμούς βάσης. Οι τελευταίοι, θα πρέπει να είναι ικανοί όχι μόνο να λειτουργούν αποδοτικά με τέτοιους υψηλούς ρυθμούς δεδομένων, αλλά και να υποστηρίζουν τη λειτουργία περισσότερο πολύπλοκων πρωτοκόλλων.

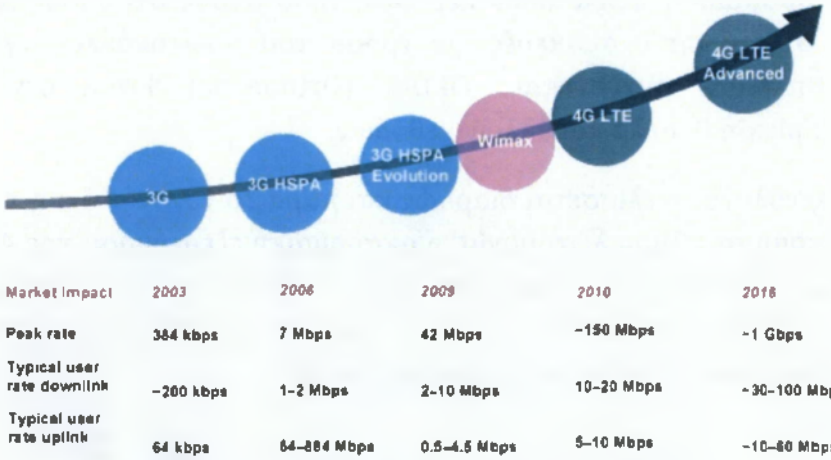
Η λειτουργία του HSDPA στηρίζεται στο γεγονός ότι αντί να χρησιμοποιούνται ξεχωριστά Dedicated Channel (DCH) κανάλια για την αποστολή δεδομένων, θα χρησιμοποιείται ένα Downlink Shared Channel (DSCH) κανάλι το οποίο θα μοιράζονται μεταξύ τους οι χρήστες για την μεταφορά των πακέτων. Το κανάλι αυτό έχει πολύ μεγαλύτερο εύρος ζώνης (bandwidth) και για το λόγο αυτό καλείται high-speed DSCH (HS-DSCH).

Κινητά δίκτυα 4ης γενιάς(4G)

Πρόκειται για το διάδοχο των προτύπων τρίτης γενιάς (3G). Ένα σύστημα 4G παρέχει στα κινητά υπερ-ευρυζωνική πρόσβαση στο Διαδίκτυο, για παράδειγμα, στους φορητούς υπολογιστές με USB ασύρματο μόντεμ, σε smartphones, καθώς και σε άλλες φορητές συσκευές. Έξυπνες εφαρμογές περιλαμβάνουν τροποποιημένη κινητή πρόσβαση στο διαδίκτυο, τηλεφωνία IP, υπηρεσίες παιχνιδιών, υψηλής ευκρίνειας κινητή τηλεόραση, συνδιάσκεψη με βίντεο, 3D τηλεόραση και τη χρήση «σύννεφου».

Δύο υποψήφια εμπορικά συστήματα 4G που έχουν αναπτυχθεί είναι (α)το πρότυπο Mobile WiMAX (αρχικά στη Νότια Κορέα το 2006), καθώς και (β)η πρώτη έκδοση πρότυπου Long Term Evolution (LTE) (στο Όσλο της

Νορβηγίας από το 2009). Σε σχέση με τις υπάρχουσες τεχνολογίες GSM,GPRS,EDGE,W-CDMA και το HSPA, το LTE αυξάνει την χωρητικότητα του δικτύου, του ρυθμού μετάδοσης δεδομένων, ενώ ταυτόχρονα μειώνει τις καθυστερήσεις. Το 3 GPP συγκεκριμενοποιεί τις προδιαγραφές του LTE στο Release 8 και υπόσχεται ρυθμούς μετάδοσης μέχρι και 300 Mbps στην κάτω ζεύξη με χρήση κεραιών MIMO 4x4 και 75Mbps στην άνω ζεύξη με απλή κεραία για κάθε 20 MHz του ταξινομημένου κατά ζεύγος φάσματος. Σύμφωνα με τις προδιαγραφές οι ελάχιστοι ρυθμοί μετάδοσης για το LTE είναι τουλάχιστον 100Mbps για την κάτω ζεύξη και 50Mbps για την άνω ζεύξη και η μέγιστη καθυστέρηση με επιστροφή υπολογίζεται στα 10 ms. Για την επίτευξη πλήρους απόδοσης των δυνατοτήτων του LTE σε δικτυακό επίπεδο είναι αναγκαία η μετατροπή των σημερινών υβριδικών δικτύων (κυκλώματος/πακέτου) σε δίκτυα πλήρως βασισμένα σε IP (Internet Protocol).



Σχήμα 5 : Κινητά τέταρτης γενιάς 4G(LTE)

Στις ΗΠΑ, η Sprint Nextel έχει αναπτύξει δίκτυα Mobile WiMAX από το 2008, και η MetroPCS ήταν η πρώτη εταιρεία που προσέφερε υπηρεσία LTE το 2010. Το USB ασύρματο μόντεμ ήταν αρχικά διαθέσιμο, ενώ τα WiMAX smartphones έχουν διατεθεί από το 2010, και τα LTE smartphones από το 2011.

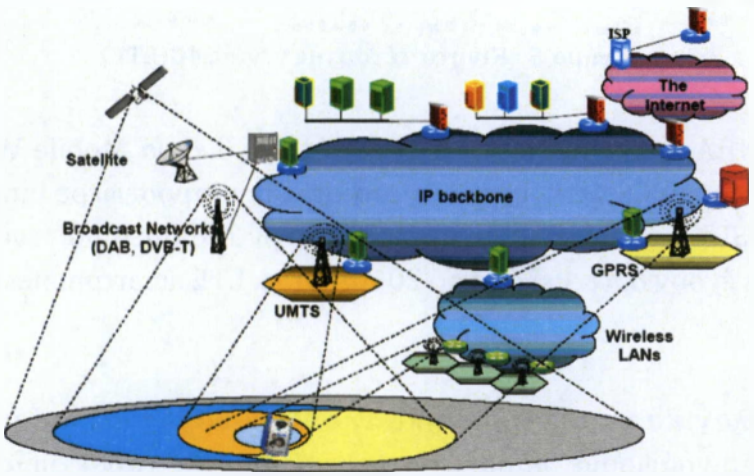
Τεχνολογικά χαρακτηριστικά της 4G ασύρματης επικοινωνίας

Θα περιγράψουμε παρακάτω μερικά από τα χαρακτηριστικά της 4ης τεχνολογικής γενιάς:

- Ο υψηλός ρυθμός μετάδοσης με εύρος από 20 έως 200 Mbps. Ασύρματα LAN και ασύρματα συστήματα πρόσβασης ευρείας ζώνης λειτουργούν ήδη στη ζώνη των 5 GHz και έχουν αναπτυχθεί στην Ιαπωνία (MMAC), στην Ευρώπη (Hyperlan 2) και στην Αμερική (IEEE 802.11) έχουν ταχύτητα μετάδοσης 20-30 Mbps.
- Η 10 φορές μεγαλύτερη χωρητικότητα και το μικρότερο κόστος ανά bit σε σύγκριση με την 3G τεχνολογία.

- Η υποστήριξη πρωτοκόλλων Internet νέας γενιάς (IPv6) και πολυμετάδοσης (multicasting).
- Η δημιουργία αλγορίθμων για εξοικονόμηση ενέργειας από την μπαταρία της συσκευής και η ύπαρξη ειδικού λογισμικού μέσα στις φορητές συσκευές με σκοπό την προσαρμογή της φυσικής και λογικής πρόσβασης(physical and MAC interface) αναλόγως του δικτύου που χρησιμοποιείται κάθε φορά.
- Η χρήση τεχνολογίας μέσω πρωτοκόλλων IP που θα επιτρέπει την ομαλή διασύνδεση με σταθερά και ασύρματα δίκτυα, καθώς και με συστήματα 3G.
- Πληρέστερη κάλυψη χώρου με μεταβλητή ταχύτητα μετάδοσης.
- Υψηλότερες χρησιμοποιούμενες συχνότητες (μέχρι 5 GHz), με εύρος ζώνης ραδιοσυχνοτήτων (RF) ανά κανάλι, 20~100 MHz.
- Χρησιμοποίηση πολλαπλών κεραιών, τόσο στους σταθμούς βάσης όσο και στις κινητές συσκευές, με χρήση του πρωτοκόλλου ορθογώνιας πολυπλεξίας συχνότητας, OFDM (Orthogonal Frequency Division Multiplexing), αλλά και άλλων μεθόδων.

Η τεχνολογία εξελίσσεται διαρκώς και παρά το γεγονός ότι η τρίτη γενιά δεν είναι ακόμη σε πλήρη λειτουργία, η ακαδημαϊκή εξερεύνηση της 4G κινητής επικοινωνίας έχει ήδη ξεκινήσει. Καταρχήν η τρίτη γενιά ασφαλώς ήταν το βασικότερο βήμα για την επίτευξη των προσωπικών τηλεπικοινωνιών, αλλά ωστόσο δεν κατάφερε να τις κάνει πραγματικότητα.



Σχήμα 6 : Συνδεσιμότητα μεταξύ UMTS και διαφόρων τεχνολογιών

Η τέταρτη γενιά θα προσεγγίσει περισσότερο τις προσωπικές επικοινωνίες παρέχοντας επικοινωνία οποιαδήποτε μορφής, σε κάθε χώρο και χρόνο, με οποιονδήποτε. Θα απαιτήσει επίσης καλή απόδοση επικοινωνίας, που θα αφορά κυρίως media παρά φωνή. Στις εφαρμογές τα τερματικά της τέταρτης γενιάς δε θα παρέχουν μόνο ομιλία ή εικόνα αλλά επιπλέον θα προειδοποιεί και θα ενημερώνει το χρήστη. Τα τερματικά μπορεί ακόμα να γίνουν μέρος του

ανθρώπινου σώματος, ενημερώνοντας το χρήστη για την πίεσή του, τη θερμοκρασία του κ.α.

1.3. Τι είναι το δίκτυο UMTS;

Ο όρος UMTS προέρχεται από τα αρχικά των λέξεων "Universal Mobile Telecommunications System" (Παγκόσμιο Σύστημα Κινητών Τηλεπικοινωνιών). Πρόκειται για την εξέλιξη σε σχέση με την χωρητικότητα, την ταχύτητα μετάδοσης των δεδομένων και την ύπαρξη νέων υπηρεσιών, των κινητών δικτύων δεύτερης γενιάς. Σήμερα, περισσότερα από εξήντα 3G/UMTS δίκτυα που χρησιμοποιούν την WCDMA τεχνολογία λειτουργούν σε 25 χώρες. Για την οργάνωση του όλου εγχειρήματος έχει θεσπιστεί ειδικός μη κερδοσκοπικός οργανισμός με την ονομασία Third Generation Partnership Project (3GPP) του οποίου μέλημα είναι η παρακολούθηση και η καθοδήγηση των εξελίξεων στην συγκεκριμένη τεχνολογική περιοχή. Το UMTS είναι ένα από τα ασύρματα δίκτυα 3ής γενιάς που αναπτύσσονται στο πλαίσιο(International Mobile Telecommunication)IMT-2000 της (International Telecommunication Union)ITU. Είναι η υλοποίηση μιας νέας γενιάς τεχνολογιών υψηλής εμβέλειας τηλεπικοινωνίας πολυμέσων. Η περιοχή εμβέλειας της είναι παγκόσμιας διάταξης με τη μορφή του IMT-2000.

1.4. Γενικά χαρακτηριστικά

Το UMTS έχοντας σαν βάση το GSM, επέκτεινε κάποια από τα χαρακτηριστικά του δικτύου 2ης γενιάς και με τη βοήθεια νέων τεχνολογιών που χρησιμοποιήθηκαν, κατάφερε να εισάγει ορισμένα νέα χαρακτηριστικά και υπηρεσίες στα συστήματα 3ης γενιάς.

Τα πιο σημαντικά από αυτά είναι τα εξής:

- Η διεπαφή (interface) του κινητού χρήστη με το σύστημα είναι μοναδική και ανεξάρτητη της γεωγραφικής του θέσης. Αυτό σημαίνει ότι ο χρήστης μπορεί να έχει πρόσβαση στο σύστημα και να εξυπηρετείται από τις παρεχόμενες υπηρεσίες μέσω του κινητού τηλεφώνου, σε οποιοδήποτε σημείο και αν βρίσκεται και από οποιοδήποτε δίκτυο.
- Ένας και μοναδικός τύπος διεπαφής, ασχέτως του τερματικού του χρήστη.

- Ο χρήστης θα μπορεί να χρησιμοποιεί μόνο μια συσκευή συμβατή με την τεχνολογία 3ης γενιάς χωρίς να χρειάζεται περαιτέρω εξοπλισμό.
- Παροχή από άκρο σε άκρο των υπηρεσιών του δικτύου χωρίς διακοπές. Ο χρήστης θα μπορεί να ταξιδεύει οπουδήποτε και παράλληλα να εξυπηρετείται από τις υπηρεσίες του δικτύου.
- Ικανότητα για πολυμεσικά δεδομένα. Το δίκτυο έχει την ικανότητα να μεταφέρει πολυμεσικά δεδομένα όπως φωνή, video και άλλες εφαρμογές.
- Αυξημένος ρυθμός μετάδοσης των δεδομένων και την ταυτόχρονη υποστήριξη μεγαλύτερου όγκου δεδομένων και φωνής. Πιο συγκεκριμένα, το UMTS δίκτυο στην αρχική του φάση, θεωρητικά προσφέρει ρυθμούς μετάδοσης δεδομένων έως και 384 kbps σε περιπτώσεις όπου παρατηρείται αυξημένη κινητικότητα του χρήστη. Αντίθετα, όταν ο χρήστης παραμένει ακίνητος οι ρυθμοί μετάδοσης αυξάνουν κατά πολύ φθάνοντας την τιμή των 2 Mbps.

Εκτιμάται ότι στο μέλλον θα υπάρξει περαιτέρω αύξηση των ρυθμών μετάδοσης δεδομένων. Ήδη, ο 3GPP έχει θέσει σαν standard δύο νέες τεχνολογίες. Πρόκειται για το High Speed Downlink Packet Access (HSDPA) και το High Speed Uplink Packet Access (HSUPA) αντίστοιχα. Οι συγκεκριμένες τεχνολογίες ουσιαστικά αποτελούν εξέλιξη του UMTS, αφού υπόσχονται ρυθμούς μετάδοσης των δεδομένων έως και 14,4 Mbps στο downlink και 5.8 Mbps στο uplink.

1.5. Σε τι διαφέρει από τα δίκτυα 2ης γενιάς;

Προσφέρει υψηλότερη ποιότητα υπηρεσία ομιλίας μαζί με προηγμένες υπηρεσίες σε δεδομένα και πληροφορίες έτσι ώστε να αποτελεί ένα δίκτυο πολυμέσων. Το UMTS έχει διευκρινιστεί ως ενσωματωμένη λύση για την κινητή φωνή και τα δεδομένα με την ευρεία κάλυψη περιοχής. Το UMTS στην αρχική φάση του προσφέρει θεωρητικά μέχρι 384 Kbps στις υψηλές καταστάσεις κινητικότητας και έως 2 Mbps στα στάσιμα/νομαδικά περιβάλλοντα χρηστών. Η συμμετρία μεταξύ ανιούσας (UL) και κατιούσας σύνδεσης (DL) των ποσοστών δεδομένων κατά τη χρησιμοποίηση του Frequency Division Duplex (FDD), σημαίνει ότι στο UMTS είναι ιδανικά ταιριαγμένες οι συνδέσεις για εφαρμογές όπως τηλεοπτική τηλεφωνία σε πραγματικό χρόνο.

Το UMTS ως κινητό δίκτυο 3ής γενιάς εισάγει την ευέλικτη παράδοση οποιουδήποτε τύπου υπηρεσίας. Οι ικανότητες του UMTS υπόσχονται αναρίθμητες νέες υπηρεσίες για τη μαζική αγορά. Στη έκδοση 6 του 3GPP όλες οι υπηρεσίες μπορούν να παραδοθούν στο IP-domain. Η υπηρεσία MBMS έρχεται

να ικανοποιήσει την ανάγκη για υπηρεσίες ροής πολυμέσων (streaming) και μεταφόρτωσης αρχείων. Η υπηρεσία MBMS μπορεί να παρέχει συρροή πολυμέσων καθώς το αρχείο μεταφορτώνεται. Η 3GPP με την έκδοση έξι (6) δεν διευκρινίζει πώς μια αρχιτεκτονική υπηρεσιών MBMS πρέπει να μοιάζει, είναι ευθύνη των χειριστών ασύρματου δικτύου να αποφασίσουν την οργάνωση της.

Κεφάλαιο 2. Περιγραφή Συστημάτων UMTS

2.1. Η εξέλιξη των Σταθμών Βάσης προς το UMTS

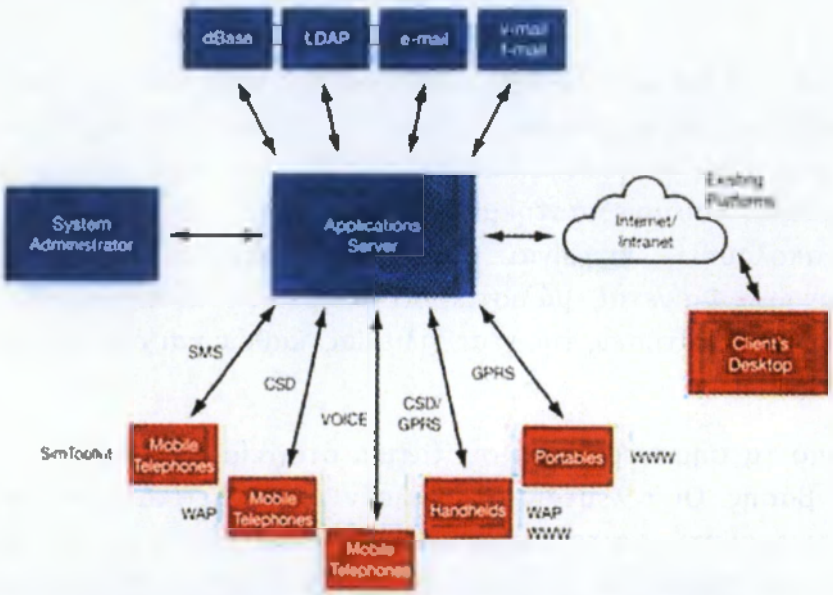
Μία από τις μεγαλύτερες επιτυχίες του GSM είναι η ικανότητά του να προσαρμόζεται και να ανταποκρίνεται στις ραγδαίες αλλαγές, που συντελούνται στον τομέα των κινητών επικοινωνιών. Παρόλο που σε μεγάλο βαθμό οι προδιαγραφές του σχεδιάστηκαν στις αρχές της προηγούμενης δεκαετίας, το GSM εξακολουθεί να είναι το πλέον επιτυχημένο σύστημα κινητών επικοινωνιών. Φαίνεται, μάλιστα, ότι μπορεί να ανταποκριθεί με απόλυτη επιτυχία στις απαιτήσεις της νέας χιλιετίας, καθώς και στη νέα πρόκληση του EDGE.

Από τα σημαντικότερα συστατικά στοιχεία των δικτύων GSM είναι οι σταθμοί βάσης. Οι τελευταίοι αποτελούν το συνδετικό κρίκο ανάμεσα στον κινητό συνδρομητή και το δίκτυο GSM. Είναι υπεύθυνοι για την ικανοποιητική κάλυψη των περιοχών, την ποιότητα του σήματος, τη χωρητικότητα του δικτύου, καθώς και για οποιαδήποτε επικοινωνία ανάμεσα στο συνδρομητή και στο δίκτυο GSM.

Προκειμένου να ικανοποιηθούν οι ολοένα αυξανόμενες απαιτήσεις των κινητών συνδρομητών, η τεχνολογία κατευθύνεται προς τη μετάδοση "πακέτων δεδομένων" από και προς τους σταθμούς βάσης. Με τον τρόπο αυτό θα επιτευχθεί τεράστια αύξηση του ρυθμού μετάδοσης, γεγονός που θα καταστήσει δυνατή την ομαλή μετάβαση προς τα συστήματα 3ης γενιάς. Ο δρόμος προς το UMTS περνάει μέσα από το GPRS και το EDGE.

Η εισαγωγή του GPRS απαιτεί την εισαγωγή στο δίκτυο του GGSN (Gateway GPRS Support Node), καθώς και του SGSN (Serving GPRS Support Node), προκειμένου να γίνεται η διαχείριση των «πακέτων δεδομένων». Όσον αφορά στο σταθμό βάσης, το GPRS απαιτεί μόνο την προσθήκη κατάλληλου λογισμικού (software) στον ήδη υπάρχοντα εξοπλισμό. Αυτό συμβαίνει, επειδή τα λειτουργικά χαρακτηριστικά του δικτύου (τεχνική διαμόρφωσης-GMSK, εύρος ζώνης φέροντος σήματος-200kHZ, ίδια δομή για τα frames και για τα

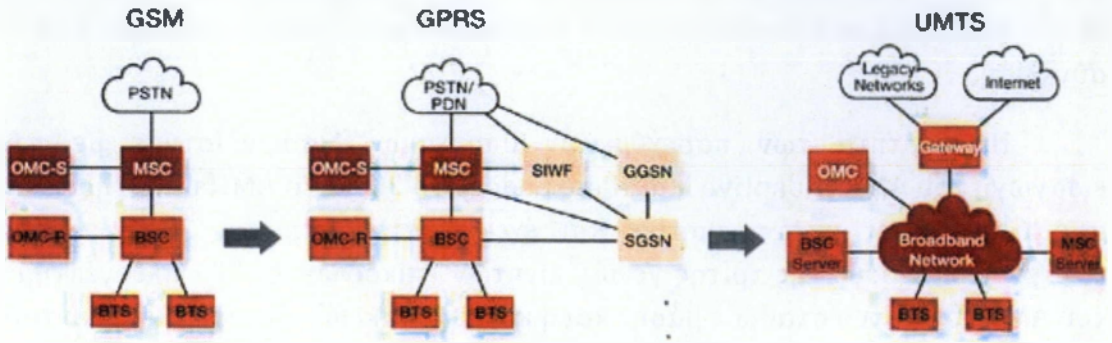
λογικά κανάλια) παραμένουν αμετάβλητα. Θεωρητικά, το GPRS είναι σε θέση να παρέχει ρυθμούς μετάδοσης μέχρι 171.2 kbps, δεδομένου ότι κάθε συνδρομητής μπορεί να χρησιμοποιεί, ταυτόχρονα, περισσότερες από μία χρονοθυρίδες (timeslots). Το κόστος για την εγκατάστασή του GPRS είναι σχετικά μικρό και η χρονική διάρκεια που απαιτείται για την εγκατάστασή του είναι, επίσης, σχετικά μικρή. Το όφελος για το συνδρομητή θα είναι, αφενός μεν οι αυξημένες σε αριθμό και βελτιωμένες σε ποιότητα υπηρεσίες, αλλά και τα μειωμένα τιμολόγια, αφού η χρέωση θα είναι ανάλογη με την ποσότητα των «πακέτων» που θα χρησιμοποιεί και όχι με το χρόνο σύνδεσης στο δίκτυο. Για παράδειγμα, ο κινητός συνδρομητής θα μπορεί να είναι συνδεδεμένος όλη τη μέρα στο δίκτυο, αλλά να χρεώνεται μόνο για την ποσότητα δεδομένων που «κατεβάζει» από το Internet.



Σχήμα 7 : Η εξέλιξη των Σταθμών Βάσης προς το UMTS

Το επόμενο βήμα προς το UMTS είναι το EDGE. Η τεχνολογία αυτή θα συνεχίσει να διαχειρίζεται «πακέτα δεδομένων», με όλα τα πλεονεκτήματα που αυτό συνεπάγεται, όπως αναφέρθηκε προηγουμένως. Η χρησιμοποιούμενη τεχνική διαμόρφωσης, όμως, θα είναι διαφορετική (8-PSK) , πετυχαίνοντας, έτσι, πιο αποτελεσματική διαχείριση του διαθέσιμου φάσματος (48 kbps ανά χρονοθυρίδα, αντί των 9.6 kbps ανά χρονοθυρίδα, που ισχύει σήμερα) και ρυθμούς μετάδοσης της τάξης των 384 kbps. Οι Οργανισμοί Θέσπισης Προτύπων μελετούν το ενδεχόμενο επέκτασης του EDGE μέχρι τα 2 Mbps, για εσωτερικούς χώρους. Τα υπόλοιπα, λειτουργικά χαρακτηριστικά του δικτύου (το εύρος ζώνης φέροντος σήματος-200KHZ, η δομή των frames, καθώς και τα λογικά κανάλια) θα παραμείνουν αμετάβλητα. Όμως, εξαιτίας κυρίως της διαφορετικής τεχνικής διαμόρφωσης του σήματος, δε θα μπορεί να γίνει αντιστοίχιση μίας χρονοθυρίδας του air-interface (δηλαδή ανάμεσα στον κινητό συνδρομητή και το σταθμό βάσης) με μία χρονοθυρίδα του A-bis interface

(δηλαδή ανάμεσα στο σταθμό βάσης και το BSC). Έτσι, απαιτείται η προσθήκη νέου υλικού (hardware -κυρίως σε μορφή καρτών) αλλά και λογισμικού (software) στους σταθμούς βάσης.



Σχήμα 8 : Φάσεις του UMTS

Εκτός από την παροχή νέων υπηρεσιών και τη βελτίωση της ποιότητας επικοινωνίας ανάμεσα στους συνδρομητές, ένας άλλος παράγοντας, που θα πρέπει να ληφθεί πολύ σοβαρά υπόψη, είναι η ολοένα αυξανόμενη ζήτηση των παραδοσιακών, φωνητικών υπηρεσιών στην κινητή τηλεφωνία. Η μέση τηλεφωνική κίνηση από φωνητικές υπηρεσίες σε πολυσύχναστες περιοχές (όπως στα κέντρα των πόλεων) ανέρχεται, σήμερα, σε περίπου 300 Erlangs, ανά τετραγωνικό χιλιόμετρο. Σε περιπτώσεις πολύ μεγάλων πόλεων, η τηλεφωνική κίνηση μπορεί να φτάσει μέχρι τα 700 Erlangs. Εκτιμάται ότι, στην επόμενη πενταετία, οι απαιτήσεις για φωνητικές υπηρεσίες θα φθάσουν τα 2000 Erlangs, ανά τετραγωνικό χιλιόμετρο. Επομένως, αναμένεται μια αύξηση μεγαλύτερη του 500%.

Προκειμένου να αντιμετωπιστεί το ολοένα αυξανόμενο πρόβλημα της χωρητικότητας, έχουν αναπτυχθεί σταθμοί βάσης για pico-cells (pico base stations), οι οποίοι διακρίνονται για το μικρό τους όγκο, το χαμηλό τους βάρος και τα μικρά επίπεδα ακτινοβολίας, ενώ, ταυτόχρονα, προσφέρουν πολύ καλή κάλυψη και αυξημένη χωρητικότητα. Το Libra picocell της Motorola, το RBS 2401 της Ericsson, το InSite της Nokia και το e-cell της Nortel, αποτελούν χαρακτηριστικά παραδείγματα. Η Siemens διαθέτει το Supr@Cell, το οποίο καταλαμβάνει μικρό όγκο και μπορεί να υποστηρίξει εξαιρετικά υψηλή τηλεφωνική κίνηση (μέχρι 150 Erlangs ανά pico-cell, με 24 TRX). Οι λύσεις όλων των εταιρειών διακρίνονται για την επεκτασιμότητα και την προσαρμοστικότητά τους, ώστε να είναι εύκολη η εγκατάστασή τους και να προσαρμόζονται σε οποιεσδήποτε συνθήκες.

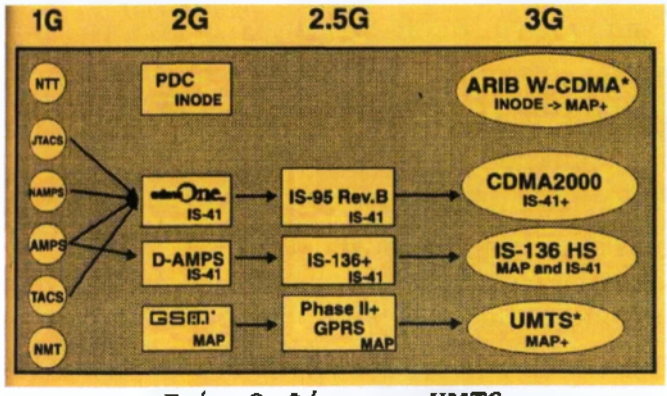
Μεγάλη, επίσης, σημασία δίνεται στην αντικατάσταση των PBX με pico-cells, προκειμένου να δοθεί κίνητρο στους κινητούς συνδρομητές να χρησιμοποιούν το κινητό τους τηλέφωνο στο γραφείο, αντί του σταθερού. Έτσι, προσφέρονται ολοκληρωμένες ασύρματες λύσεις για περιβάλλον LAN, βασισμένες στη μετάδοση «πακέτων δεδομένων». Τέτοιες ολοκληρωμένες

λύσεις αποτελούν το «Horizonoffice» της Motorola, το «GSM on the Net» της Ericsson και το «GSM Intranet Office» (GIO) της Nokia. Το «Corporate GSM» της Siemens, με το WARP (Wireless Adjunct InteRnet Platform) που διαθέτει, αποτελεί ολοκληρωμένη λύση για περιβάλλον LAN και προσφέρει σύγκλιση των IP και των κινητών δικτύων, με όλα τα πλεονεκτήματα που συνεπάγεται αυτή σύγκλιση.

Η ποιότητα των παρεχόμενων υπηρεσιών διασφαλίστηκε με την εισαγωγή του AMR (Adaptive MultiRate Codec), το 2001. Το AMR υποστηρίζεται από όλους τους κατασκευαστές και έχει επιλεγεί από το 3GPP, ως το υποχρεωτικό codec της τρίτης γενιάς κινητών επικοινωνιών. Το πλεονέκτημα του AMR είναι ότι ο σταθμός βάσης και η κινητή συσκευή «διαπραγματεύονται» μεταξύ τους για ποιο codec θα χρησιμοποιήσουν, λαμβάνοντας υπόψη τόσο την ποιότητα, των παρεχόμενων υπηρεσιών, όσο και τη χωρητικότητα του δικτύου. Το codec μπορεί να αλλάξει κατά τη διάρκεια της κλήσης, αν αυτό κριθεί απαραίτητο. Το AMR υποστηρίζει ένα πλήθος codec επιλογών, συμπεριλαμβανόμενων των GSM Full Rate, Half Rate και Enhanced Full Rate (GSM EFR-12.2 kbps), καθώς και του IS-136 EFR (7.4 kbps). Η ποιότητα των δικτύων GSM θα βελτιωθεί και με το πρωτόκολλο επικοινωνίας TFO (Tandem Free Operation).

Όταν η τηλεφωνική κλήση γίνεται μεταξύ κινητών συνδρομητών, το σήμα περνάει δύο φορές από transcoders, με αποτέλεσμα την υποβάθμισή του. Με το TFO, οι κλήσεις αυτές θα περνούν από transcoder μόνο μία φορά, με αποτέλεσμα τη βελτίωση της ποιότητας του σήματος. Αξίζει να σημειωθεί ότι το TFO δεν απαιτεί καμία τροποποίηση των υπαρχόντων κινητών συσκευών.

Εκτός από τα προαναφερθέντα, υπάρχουν και άλλες τεχνικές βελτίωσης των δικτύων GSM. Στις τεχνικές αυτές περιλαμβάνεται η χρήση πολυκαναλικών ενισχυτών (multicarrier power amplifiers), γραμμικών ενισχυτών (linear amplifiers), «έξυπνων» κεραιών (smart antennas), καθώς και τεχνικές αποτελεσματικότερης διαχείρισης του φάσματος.

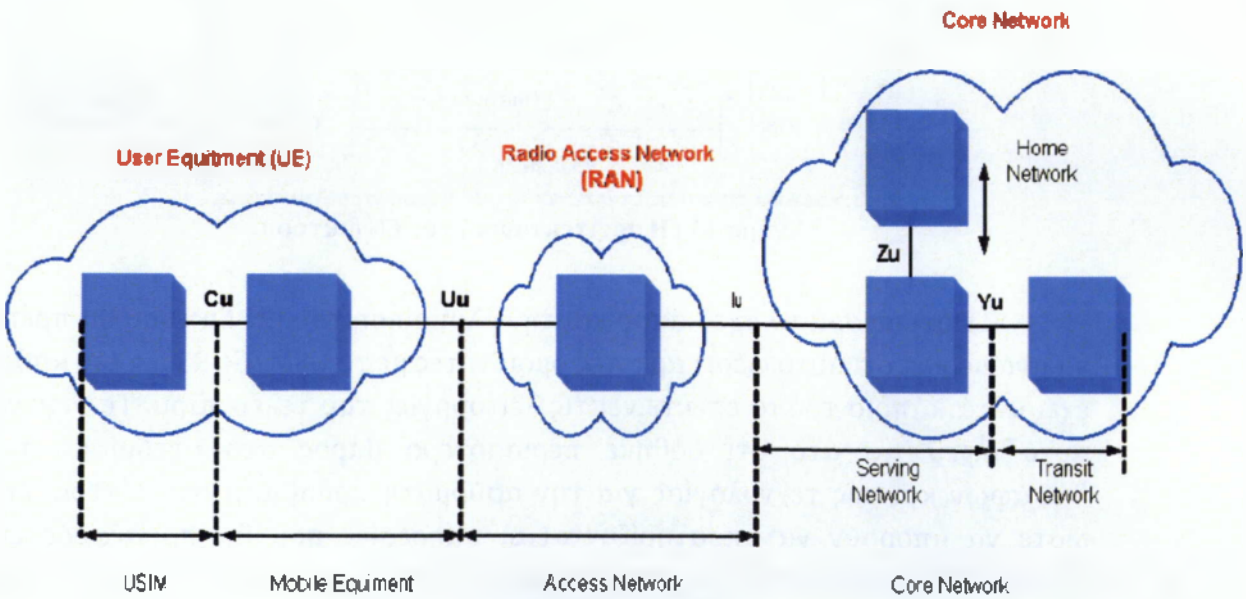


Σχήμα 9 : Φάσεις του UMTS

Οι τεχνικές αυτές είναι ενδεικτικές των τάσεων, που επικρατούν στη συνεχή προσπάθεια παροχής όσο το δυνατόν καλύτερων υπηρεσιών στον κινητό συνδρομητή. Με την εφαρμογή των συγκεκριμένων τεχνικών, εκτιμάται ότι τα δίκτυα κινητής τηλεφωνίας θα μπορέσουν να ανταποκριθούν στην τεράστια ζήτηση, προσφέροντας επαρκή κάλυψη στις απαιτήσεις των συνδρομητών, που επιθυμούν εξειδικευμένες υπηρεσίες, και στο big bang των mobile data, που βρίσκεται προ των πυλών.

2.2. Η Αρχιτεκτονική του UMTS

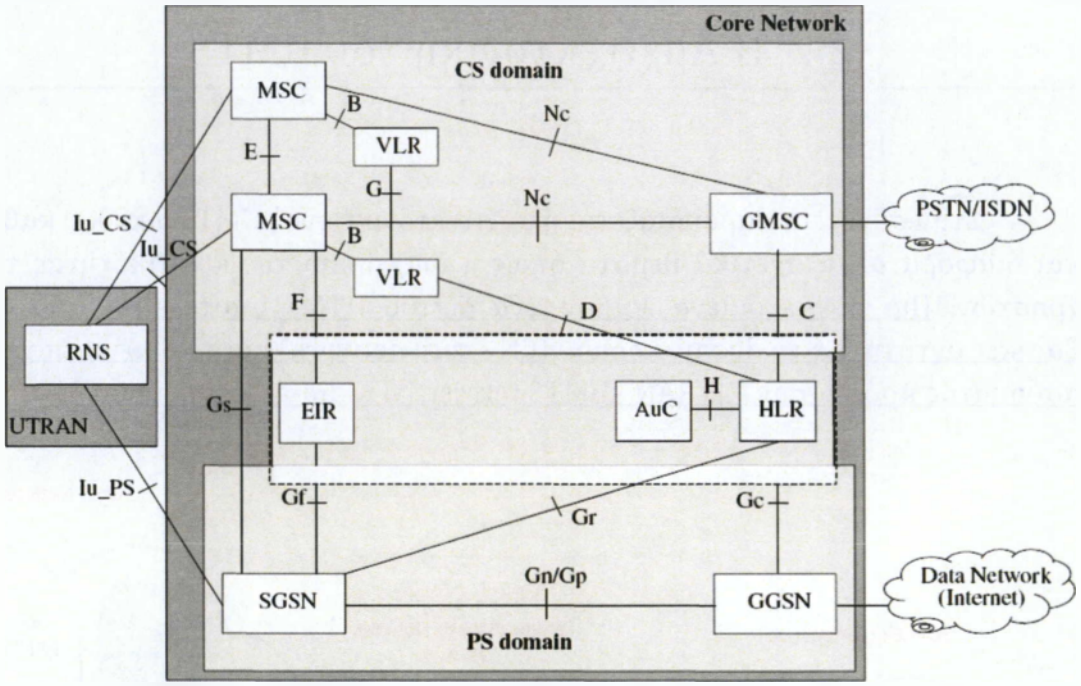
Στην συνέχεια παρουσιάζεται η αρχιτεκτονική ενός UMTS δικτύου καθώς και διάφορα άλλα σχετικά θέματα όπως η διαχείριση της κινητικότητας των χρηστών. Πιο συγκεκριμένα λοιπόν, ένα δίκτυο UTMS αποτελείται από δύο βασικές οντότητες: το δίκτυο κορμού (CN - core network) και το δίκτυο επίγειας ασύρματης πρόσβασης (UTRAN - UMTS terrestrial radio-access network).



Σχήμα 10 : Η δομή του UMTS

Το δίκτυο κορμού (CN - core network)

Το δίκτυο κορμού είναι υπεύθυνο για την δρομολόγηση των τηλεφωνημάτων καθώς και για τις συνδέσεις για μεταφορά δεδομένων με εξωτερικά δίκτυα. Καλύπτει όλες εκείνες τις λειτουργίες του δικτύου που δε σχετίζονται με πρόσβαση στο ασύρματο κανάλι. Μερικές από τις λειτουργίες μπορούν να είναι η εγκαθίδρυση και η διαχείριση μιας σύνδεσης καθώς και η παρακολούθηση της γεωγραφικής θέσης του UE με σκοπό την ταχύτερη δρομολόγηση των κλίσεων.



Σχήμα 11 : Η αρχιτεκτονική του CN δικτύου

Σε ότι αφορά το σχεδιασμό και την υλοποίηση του CN δικτύου θα πρέπει να αναφερθεί ότι αυτό φέρει αρκετές ομοιότητες με το GSM/GPRS δίκτυο καθώς έχει κατά κάποιο τρόπο επεκτείνει τις λειτουργίες του τελευταίου. Το γεγονός αυτό οφείλεται στο ότι δόθηκε περισσότερο βάρος στο σχεδιασμό των διεπαφών και της τεχνολογίας για την ασύρματη πρόσβαση στο δίκτυο, έτσι ώστε να μπορούν να υποστηρίζονται οι υπηρεσίες που θα προσέφερε ένα σύστημα 3ης γενιάς. Βέβαια στη συνέχεια εμφανίστηκαν κάποιες σημαντικές αλλαγές στην αρχιτεκτονική του CN δικτύου δίνοντας την εντύπωση, για τον ερχομό ενός πλήρους IP-δικτύου.

Το CN αποτελείται από δύο domain: α) circuit -switched (CS - μεταγωγή κυκλώματος), β) packet-switched (PS - μεταγωγή πακέτου). Το CS τμήμα υποστηρίζει τη μεταφορά φωνής καθώς η δρομολόγηση γίνεται με μεταγωγή κυκλώματος που σημαίνει ότι είναι απαραίτητη η δημιουργία ενός δεσμευμένου μονοπατιού από το ένα άκρο μέχρι το άλλο. Μέσω του δικτύου αυτού, υπάρχει

επίσης διασύνδεση με PSTN και ISDN δίκτυα. Το CS μέρος του δικτύου περιλαμβάνει τα εξής:

- **Mobile Services Switching Center (MSC).** Ο κόμβος MSC αποτελεί έναν κόμβο μεταγωγής ο οποίος δρομολογεί τα δεδομένα των υπηρεσιών μεταγωγής κυκλώματος εντός του δικτύου UMTS. Κάθε κόμβος MSC διαχειρίζεται πολλά RNC τα οποία συνδέονται σε αυτόν μέσω της διεπαφής Iu_CS. Επίσης είναι συνδεδεμένος με τις βάσεις δεδομένων του δικτύου όπως τη βάση δεδομένων Home Location Register (HLR) και την Visitor Location Register (VLR). Τέλος μια άλλη πολύ χρήσιμη λειτουργία του κόμβου MSC είναι η διαχείριση της κινητικότητας των χρηστών για τις υπηρεσίες μεταγωγής κυκλώματος.
- **Gateway Mobile Services Switching Center (GMSC).** Ο κόμβος GMSC είναι συνδεδεμένος με τους κόμβους MSC. Η λειτουργία του είναι να διασυνδέει το δίκτυο UMTS με άλλα δίκτυα μεταγωγής κυκλώματος όπως PSTN και ISDN.
- **Visitor Location Register (VLR).** Ο κόμβος VLR είναι μια βάση δεδομένων. Συνήθως κάθε VLR αντιστοιχεί σε έναν MSC. Η βάση VLR αποθηκεύει προσωρινή πληροφορία σχετικά με την ταυτοποίηση και την ασφάλεια καθώς και άλλες χρήσιμες πληροφορίες που σχετίζονται με όλους τους χρήστες που διαχειρίζεται κάθε δεδομένη στιγμή ο αντίστοιχος MSC. Η βάση VLR λαμβάνει την αρχική πληροφορία από τη βάση HLR και αναλαμβάνει να την ενημερώσει για τυχόν μεταβολές στα δεδομένα της. Όλες οι συναλλαγές μεταξύ VLR και HLR γίνονται μέσω ενός MSC.

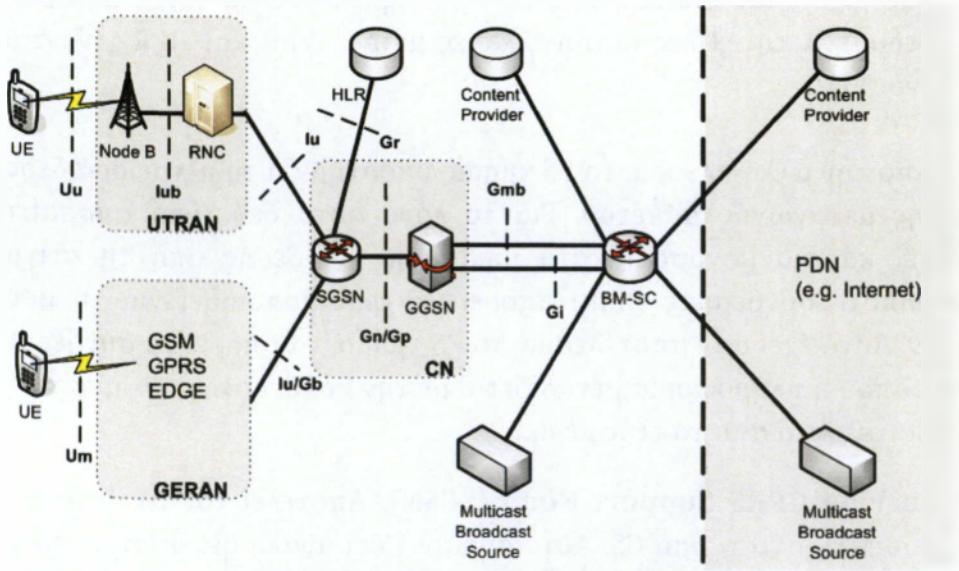
Από την άλλη πλευρά, το PS τμήμα, υποστηρίζει τη μεταφορά δεδομένων μέσω της μεταγωγής πακέτου. Για το λόγο αυτό δεν είναι απαραίτητο να δεσμευτεί κάποιο μονοπάτι κατά μήκος της σύνδεσης από τη στιγμή που οποιοσδήποτε σύνδεσμος (link) μπορεί να χρησιμοποιηθεί για τη μεταφορά πακέτων. Αυτό έχει σαν αποτέλεσμα, το PS τμήμα, να μπορεί να συνδέεται με το Internet όπου η πληροφορία μεταδίδεται με την βοήθεια των IP-πακέτων. Το PS μέρος αποτελείται από τα εξής μέρη:

- **Serving GPRS Support Node (SGSN).** Αποτελεί τον αντίστοιχο κόμβο του MSC στο τμήμα CS. Αυτό σημαίνει ότι αναλαμβάνει τη δρομολόγηση δεδομένων των υπηρεσιών μεταγωγής πακέτων εντός του δικτύου UMTS. Επιπλέον διαχειρίζεται τους κόμβους RNC οι οποίοι είναι συνδεδεμένοι σε αυτόν μέσω της διεπαφής Iu_PS. Επίσης αλληλεπιδρά με βάσεις δεδομένων, όπως η βάση HLR. Τέλος ο κόμβος SGSN είναι υπεύθυνος για τη διαχείριση της κινητικότητας των χρηστών και για τις υπηρεσίες μεταγωγής πακέτων.
- **Gateway GPRS Support Node (GGSN).** Πρόκειται για έναν κόμβο αντίστοιχο του GMSC του CS. Διασυνδέει τους κόμβους SGSN με

εξωτερικά δίκτυα μεταγωγής πακέτων όπως το X.25 και το Internet. Τέλος, υπάρχουν οι κόμβοι HLR και AuC οι οποίοι είναι κοινοί και για τα δύο μέρη CS και PS. Σε ότι αφορά τον Home Location Register, πρόκειται για μια βάση δεδομένων η οποία αποθηκεύει δεδομένα των χρηστών τα οποία μένουν σχετικά σταθερά στο χρόνο. Ο κόμβος AuC αποτελεί έναν κόμβο που είναι συσχετισμένος με έναν HLR. Ο κόμβος αυτός αποθηκεύει πληροφορίες ταυτοποίησης και κρυπτογράφησης για τους συνδρομητές.

Το δίκτυο επίγειας ασύρματης πρόσβασης (UTRAN - UMTS terrestrial radio-access network).

Το UTRAN είναι υπεύθυνο για οτιδήποτε σχετίζεται με το ασύρματο μέρος του δικτύου. Το UTRAN αποτελείται από τον ελεγκτή ασύρματης πρόσβασης (RNC - radio network controller) και το Node B το οποίο αποτελεί την βάση που προσφέρει κάλυψη στο αντίστοιχο κελί. Το Node B συνδέεται με τον εξοπλισμό του χρήστη (user equipment - UE) μέσω της διεπαφής Uu (βασισμένο στην τεχνολογία W-CDMA) και με το RNC μέσω της διεπαφής Gi . Επιπλέον, υπάρχει και ένας άλλος κόμβος σχετιζόμενος με τις υπηρεσίες broadcast/multicast (BM-SC - broadcast/multicast service center), ο οποίος λειτουργεί σαν το σημείο εισόδου για την παραλαβή των δεδομένων για εσωτερικές πηγές. Τα παραπάνω παρουσιάζονται καλύτερα στο Σχήμα 12 που ακολουθεί:



Σχήμα 12 : Η αρχιτεκτονική του UTRAN

Μερικά από τα κύρια χαρακτηριστικά της λειτουργίας του UTRAN είναι τα εξής:

- Υποστήριξη όλων των λειτουργιών που συμβαίνουν μέσα στο δίκτυο, όπως soft handover, WCDMA-specific Radio Resource Management.
- Μεγιστοποίηση των κοινών χαρακτηριστικών στο χειρισμό των δεδομένων που δρομολογούνται μέσω των τμημάτων του δικτύου τα

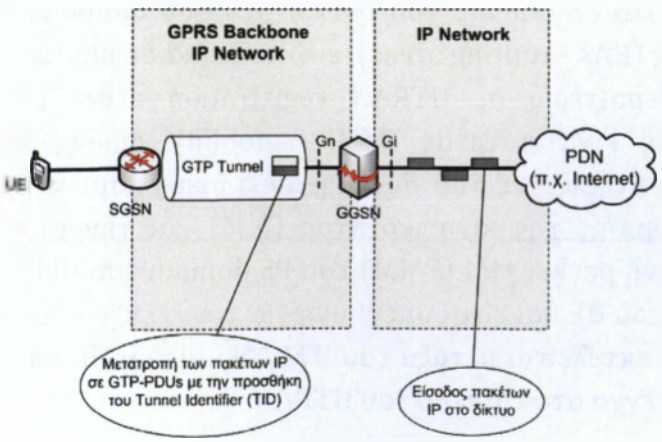
οποία υποστηρίζουν μεταγωγή κυκλώματος (circuit-switched) και μεταγωγή πακέτου (packet-switched). Σκοπός είναι η ύπαρξη μίας μόνο στοίβας πρωτοκόλλων και της χρήσης της ίδιας διεπαφής για την επικοινωνία των τμημάτων αυτών με το UTRAN.

- Μεγιστοποίηση των κοινών χαρακτηριστικών με το GSM.
- Χρήση ATM τεχνολογίας για τη μεταφορά των δεδομένων μέσα στο UTRAN.

Ο ρόλος του RNC είναι η διαχείριση των πόρων του δικτύου στο UTRAN. Συγκεκριμένα ελέγχει ένα ή περισσότερα κελιά σε ότι αφορά την κίνηση ενώ παράλληλα είναι υπεύθυνος για την ανάθεση κωδικών στα ασύρματα link μεταξύ Node B και UE όπως επιβάλλει η WCDMA πρόσβαση. Τέλος, διαχειρίζεται λειτουργίες όπως handover μεταξύ διαφορετικών RNS και έλεγχο ισχύος στον Node B και στον UE.

2.3. Μετάδοση δεδομένων στο UMTS

Προτού ένας χρήστης είναι σε θέση να ανταλλάξει δεδομένα με ένα εξωτερικό PDN (Public Data Network), πρέπει να εγκαθιδρύσει μία εικονική σύνδεση με αυτό το PDN. Από την στιγμή που ο συγκεκριμένος κινητός χρήστης γίνει γνωστός στο δίκτυο, τα πακέτα μεταφέρονται μεταξύ αυτού και του δικτύου, βασισμένα στο packet data protocol (PDP), το οποίο αποτελεί το πρωτόκολλο του επιπέδου δικτύου του UMTS. Ένα στιγμιότυπο του PDP ονομάζεται PDP context και περιέχει όλες τις παραμέτρους που χαρακτηρίζουν την σύνδεση με το εξωτερικό δίκτυο όπως τις διευθύνσεις αποστολέα και παραλήπτη καθώς και την ποιότητα της υπηρεσίας.

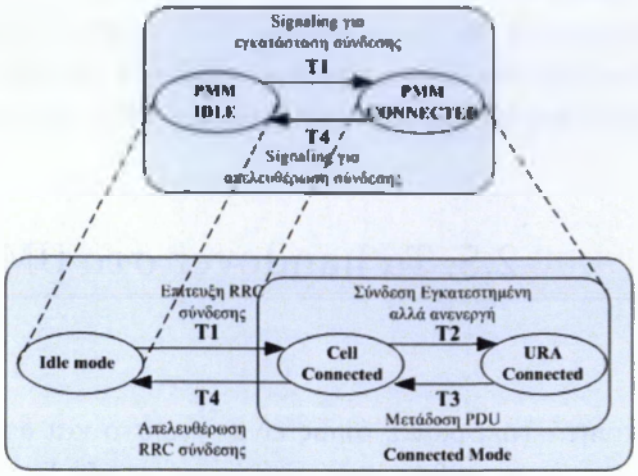


Σχήμα 13 : PDP context

Ένα PDP context εγκαθιδρύεται για όλες τις εφαρμογές που κατευθύνονται προς ή προέρχονται από μία IP διεύθυνση. Μία ενεργοποίηση ενός PDP context ουσιαστικά αποτελεί μία διαδικασία αίτησης - απάντησης μεταξύ του κινητού χρήστη (UE) και του GGSN. Μία επιτυχής PDP context ενεργοποίηση οδηγεί στην δημιουργία δύο GPRS tunneling protocol (GTP) συνόδων για τον εκάστοτε χρήστη. Η πρώτη GTP σύνοδος δημιουργείται μεταξύ του GGSN και του SGSN πάνω από την διεπαφή Gn, ενώ η δεύτερη δημιουργείται μεταξύ του SGSN και του RNC πάνω από την διεπαφή Iu. Τα IP πακέτα τα οποία προορίζονται για μία εφαρμογή, χρησιμοποιώντας συγκεκριμένα GTP contexts, προσαρτώνται σε αυτά και μέσω του PDP μεταφέρονται στο αντίστοιχο SGSN. Το SGSN ανακτά τα IP πακέτα, ζητά το κατάλληλο PDP context βασισμένο στο UE και στο PDP και προωθεί τα πακέτα στο κατάλληλο RNC. Παράλληλα, το RNC διατηρεί έναν φορέα ασύρματης πρόσβασης (RAB - radio access bearer). Αντίστοιχα με τα PDP context, ένα RAB context επιτρέπει στο RNC να ανακτήσει την ταυτότητα του αποστολέα που έχει συσχετιστεί με ένα GTP. Αφού πλέον, το RNC έχει ανακτήσει το πακέτο, το προωθεί στο κατάλληλο Node B. Τέλος, χρησιμοποιείται ένας tunnel endpoint identifier (TEID) στις διεπαφές Gn και Iu έτσι ώστε να μπορεί να αναγνωριστεί το τέλος του tunnel στον κόμβο που δέχεται τα πακέτα.

2.4. Μηχανισμοί διαχείρισης κινητικότητας των χρηστών

Στην συνέχεια, αναλύεται ο τρόπος με τον οποίο γίνεται η διαχείριση της κινητικότητας των UE (λεπτομέρειες παρουσιάζονται στο αντίστοιχο Σχήμα 14). Έτσι λοιπόν, στο PS domain του UMTS, τα κελιά ομαδοποιούνται σε περιοχές δρομολόγησης (RAs - routing areas), ενώ τα κελιά σε μία περιοχή δρομολόγησης χωρίζονται περαιτέρω σε UTRAN registration areas (URAs). Επιπλέον, η διαχείριση της κινητικότητας (MM - mobility management) των κινητών χρηστών χαρακτηρίζεται από δύο μηχανές πεπερασμένων καταστάσεων: την μηχανή διαχείρισης της κινητικότητας (MM) και την radio resource control (RRC). Η μηχανή packet MM (PMM) του PS domain του UMTS εκτελείται μεταξύ του SGSN και του UE και είναι υπεύθυνη για τον έλεγχο στο επίπεδο του CN, ενώ η μηχανή RRC εκτελείται μεταξύ του UTRAN και του UE και είναι υπεύθυνη για τον σχετικό έλεγχο στο επίπεδο του UTRAN.



Σχήμα 14 : (1)PMM Διάγραμμα, (2)RRC Διάγραμμα

Πιο συγκεκριμένα λοιπόν, αφότου ένα UE συνδεθεί στο PS domain, η μηχανή πεπερασμένων καταστάσεων PMM βρίσκεται σε μία από τις εξής δύο καταστάσεις: PMM idle ή PMM connected. Αντίστοιχα η μηχανή RRC μπορεί να βρίσκεται σε μία από τις εξής τρεις καταστάσεις: RRC idle, RRC cell - connected και RRC URA connected. Σημειώνεται ότι όταν δεν υπάρχει ροή δεδομένων μεταξύ του UE και του CN, το UE βρίσκεται στις καταστάσεις PMM idle και RRC idle αντίστοιχα. Στην περίπτωση αυτή το UTRAN δεν έχει καμία πληροφορία για το UE και παρακολουθείται μόνο από το αντίστοιχο SGSN στο επίπεδο RA. Όταν ύστερα ξεκινήσει μία σύνδεση μεταξύ του UE και του SGSN, το UE μεταβαίνει στην κατάσταση PMM connected. Από την στιγμή που η σύνδεση στο PS λάβει χώρα, αυτόματα ξεκινά και μία RRC σύνδεση μεταξύ του UE και του αντίστοιχου RNC που το εξυπηρετεί. Σε αυτή την περίπτωση η RRC μηχανή για το συγκεκριμένο UE μεταβαίνει στην κατάσταση RRC cell - connected. Όταν κάτι τέτοιο συμβεί, το SGSN παρακολουθεί το UE με ακρίβεια μέσω του αντίστοιχου RNC που εξυπηρετεί το UE. Το συγκεκριμένο RNC είναι υπεύθυνο να παρακολουθεί το κελί όπου το UE βρίσκεται κάθε στιγμή. Σημειώνεται ότι τα πακέτα μπορούν να ληφθούν από το UE μόνο όταν βρίσκεται σε αυτή την κατάσταση. Στην PMM connected/RRC cell - connected κατάσταση, αν το UE δεν έχει μεταδώσει/λάβει πακέτα για ένα συγκεκριμένο χρονικό διάστημα, η RRC μηχανή μεταβαίνει στην κατάσταση RRC URA connected. Σε αυτή την περίπτωση, η RCC σύνδεση διατηρείται ακόμη, ενώ το UE παρακολουθείται από το RNC που το εξυπηρετεί. Η συγκεκριμένη μετάβαση δεν επηρεάζει καθόλου την κατάσταση της PMM μηχανής για το συγκεκριμένο UE. Στην PMM connected / RRC URA connected κατάσταση, αν το UE μεταδώσει/λάβει ένα πακέτο, η RRC μηχανή μεταβαίνει πάλι στην κατάσταση RRC cell - connected. Αντίθετα, αν οι πόροι για τις συνδέσεις στο PS και RRC επίπεδο αποδεσμευτούν (για παράδειγμα όταν μία σύνοδος επικοινωνίας ολοκληρωθεί) ή αν κανένα πακέτο δεν έχει μεταδοθεί για ένα μεγάλο χρονικό διάστημα, η RRC μηχανή αρχικά

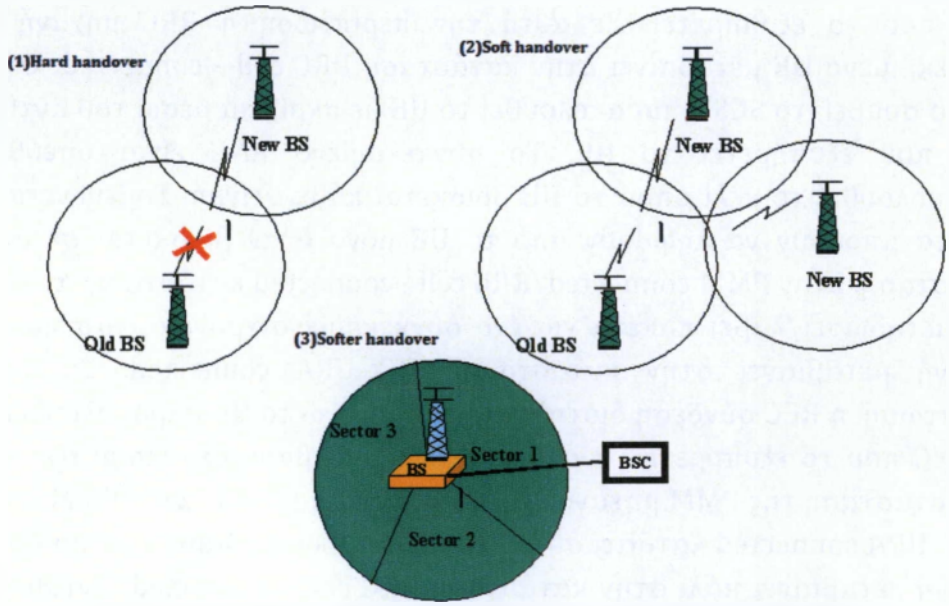
μεταβαίνει στην RRC cell - connected κατάσταση και μετά στην RRC idle κατάσταση. Σε αυτή την περίπτωση, η PMM μηχανή αντίστοιχα μεταβαίνει στην PMM idle κατάσταση. Τέλος, όταν ένα UE δεν μπορεί να εντοπιστεί από το δίκτυο, η κατάστασή του χαρακτηρίζεται σαν PMM detached.

2.5. Τα handover στο UMTS

Τα κινητά τηλέφωνα, όπως είναι γνωστό και από το GSM, μπορούν να διατηρούν μια κλήση καθώς αυτά κινούνται μεταξύ δύο κυψελών. Η διαδικασία η οποία είναι υπεύθυνη για τη διατήρηση της κλήσης λέγεται handover και σε ότι αφορά το UMTS, θεωρείται ως η μεταφορά της σύνδεσης από τον ένα Node B στον άλλο. Εντούτοις υπάρχουν σημαντικές διαφορές μεταξύ των handover που γίνονται στο UMTS με CDMA και στο GSM με TDMA. Το γεγονός αυτό οφείλεται στο ότι όλα τα UE στο UMTS χρησιμοποιούν διαρκώς το ίδιο φάσμα συχνοτήτων.

2.5.1. Hard, Soft και Softer handover

Στο UMTS υπάρχουν τρεις διαφορετικοί τύποι handover. Με την βοήθεια του Σχήματος 15, ακολουθεί μια περιγραφή των χαρακτηριστικών τους:



Σχήμα 15 : (1)Hard, (2)Soft και (3)Softer handover στο UMTS

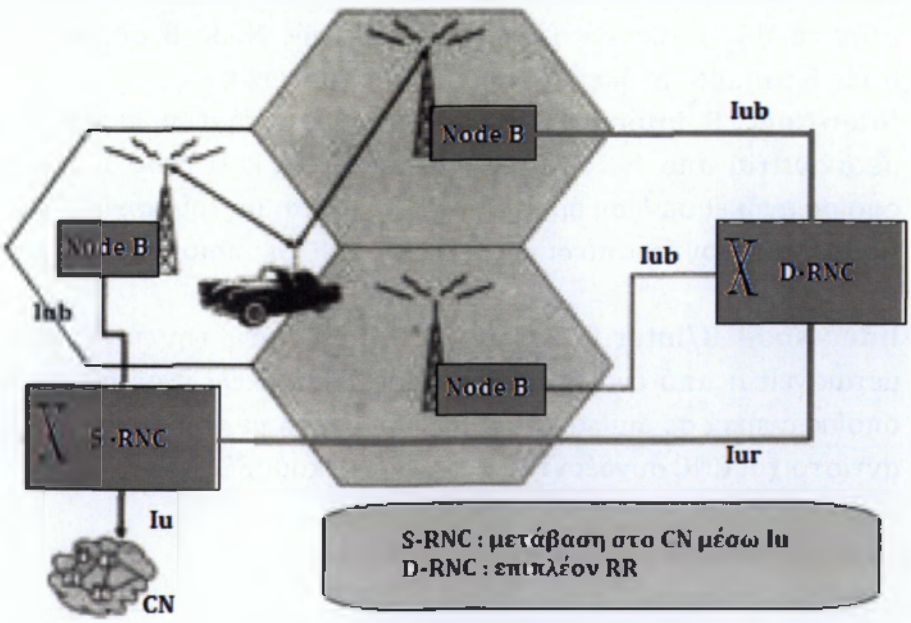
(1) Στο hard handover, γνωστό και από το GSM, γίνεται αλλαγή μεταξύ TDD και FDD όταν ο UE είναι αναγκασμένος να αλλάξει συχνότητα. Ο χρόνος μετάβασης από την μια κυψέλη στην άλλη θεωρείται αρκετός προκειμένου να προλάβει ο UE να εγκαθιδρύσει μια σύνδεση χρησιμοποιώντας ένα καινούργιο κανάλι καθώς αυτό μπορεί να συμβεί σε χρονικό διάστημα μεταξύ δύο frame.

(2) Στο soft handover, ο UE μπορεί να επικοινωνεί ταυτόχρονα μέχρι και με τρεις διαφορετικούς Node B. Τα δεδομένα χωρίζονται μέσα στον RNC και μεταδίδονται μέσω broadcast στους εμπλεκόμενους Node B. Τα δεδομένα που καταφθάνουν στους Node B από το uplink κανάλι προωθούνται στον RNC. Στη συνέχεια ο RNC συνδυάζει δυο ροές δεδομένων και μεταφέρει την πληροφορία προς το CN.

(3) Το softer handover θεωρείται μια ειδική έκδοση του soft handover καθώς είναι εφικτή η παράλληλη μετάδοση δεδομένων σε διαφορετικούς τομείς (sector) του ίδιου Node B.

2.5.2. Ο ρόλος του RNC στο handover

Το soft handover είναι μια διαδικασία απλή και σχετικά εύκολη στην περίπτωση που οι συμμετέχοντες Node B ανήκουν στον ίδιο RNC. Παρόλα αυτά, το πρόβλημα εντοπίζεται όταν οι Node B ελέγχονται από διαφορετικά RNC. Το CN δεν επιτρέπεται να ασχολείται με τα προβλήματα που απασχολούν το RAN ή να συμμετέχει σε διαδικασίες που αφορούν τις ασύρματες διεπαφές.



Σχήμα 16 : Ο ρόλος του RNC στο handover

Εντούτοις, αυτό θα ήταν επιθυμητό εάν τα δυο RNC δεν ήταν δυνατό να έχουν μια απευθείας επικοινωνία μέσω της Iur διεπαφής.

Καταφεύγοντας σε ένα παράδειγμα, ας υποθέσουμε ότι ο κινητός χρήστης του παραπάνω Σχήματος 16, εξυπηρετείται από την αριστερή κυψέλη. Το RNC που φαίνεται στα αριστερά στο Σχήμα 16 ελέγχει την σύνδεση αυτή μέσω της διεπαφής Iu. Συνεπώς το RNC αυτό καλείται Controlling RNC (CRNC).

Αν ο χρήστης κινηθεί προς τα δεξιά, ένα soft handover θα λάβει χώρα. Ο χρήστης τώρα εξυπηρετείται από δυο Node B. Στην περίπτωση αυτή ο δεύτερος Node B, ελέγχεται από διαφορετικό RNC του οποίου ο CRNC δεσμεύει φυσικούς πόρους για το χρήστη. Καθώς τον έλεγχο της σύνδεσης συνεχίζει να τον έχει ο RNC στα αριστερά, (παίζει το ρόλο του Serving RNC S-RNC), ενώ ο RNC στα δεξιά ελέγχεται με απομακρυσμένο τρόπο μέσω της Iur διεπαφής και αποκαλείται ως Drift RNC (DRNC). Δουλειά του SRNC είναι ο συνδυασμός των δεδομένων που μεταδίδονται με το uplink κανάλι. Ο DRNC προωθεί τα δεδομένα χωρίς να τα επεξεργαστεί στον SRNC. Σε ότι αφορά το downlink κανάλι ο SRNC στέλνει ένα αντίγραφο της πληροφορίας που καταφθάνει από το CN στον DRNC, και αυτός στην συνέχεια την προωθεί μέσω των Node B στον κινητό χρήστη. Καθώς ο χρήστης απομακρύνεται από τον αριστερό Node B, ο ρόλος αυτού μειώνεται σταδιακά με αποτέλεσμα κάποια στιγμή η σύνδεση να τερματιστεί.

Ανάλογα με το πού βρίσκεται τοπολογικά ο νέος Node B σε σχέση με τον αρχικό, υπάρχουν οι εξής τύποι soft handover:

- **Inter-Node B/intra-RNS handover:** Αυτός ο τύπος handover εκτελείται όταν το UE μετακινείται από ένα κελί ενός Node B σε ένα κελί άλλου Node B ο οποίος ανήκει στο ίδιο RNS με τον αρχικό.
- **Inter-Node B/inter-RNS/intra-SGSN:** Σε αυτή την περίπτωση το UE μετακινείται από ένα κελί ενός Node B στο κελί ενός άλλου Node B ο οποίος ανήκει σε διαφορετικό RNS σε σχέση με τον αρχικό. Συνεπώς, οι Node B ελέγχονται από διαφορετικούς RNC οι οποίοι όμως συνδέονται με τον ίδιο SGSN.
- **Inter-Node B/inter-RNS/inter-SGSN:** Σε αυτή την περίπτωση το UE μετακινείται από ένα κελί ενός Node B στο κελί ενός άλλου Node B ο οποίος ανήκει σε διαφορετικό RNS σε σχέση με τον αρχικό. Επιπλέον, οι αντίστοιχοι RNC συνδέονται με διαφορετικούς SGSN.

2.5.3. SRNS Relocation

Στην περίπτωση που αναφέρθηκε παραπάνω, υπάρχει μια τεχνική γνωστή ως Serving Radio Network Subsystem (SRNS) relocation. Είναι η

διαδικασία κατά την οποία αλλάζει η σύνδεση του UTRAN με το CN για τη σύνδεση που αφορά ένα συγκεκριμένο UE. Η SRNS relocation, συμβαίνει όταν έχει ήδη προηγηθεί ένα inter-RNS soft handover. Καθώς το soft handover έχει εκτελεστεί, ο SRNC αναλαμβάνει να προωθήσει προς τον DRNC τα δεδομένα που απευθύνονται στο συγκεκριμένο UE.

Ανάλογα με την σχετική θέση του αρχικού ως προς τον τελικό SRNC υπάρχουν δυο είδη διαδικασιών SRNS relocation. Η intra-SGSN SRNS relocation και η inter- SGSN SRNS relocation. Η πρώτη συμβαίνει όταν οι δυο RNC είναι συνδεδεμένοι με τον ίδιο κόμβο SGSN του CN. Είναι μια διαδικασία που ακολουθεί ένα inter-RNS/intra-SGSN handover. Από την άλλη πλευρά, η δεύτερη διαδικασία ακολουθεί ένα inter-RNS/inter-SGSN, γεγονός που σημαίνει ότι οι δυο RNC συνδέονται με διαφορετικούς SGSN.

Η ενεργοποίηση της διαδικασίας SRNS relocation πετυχαίνει οικονομία στους πόρους του δικτύου. Όσο διαρκεί το soft handover ο UE λαμβάνει την ίδια πληροφορία από κεραίες που ελέγχονται από τον SRNC αλλά και από κεραίες που ελέγχονται από τον DRNC. Καθώς ο UE απομακρύνεται από τον SRNC η ισχύς του σήματος πέφτει. Επειδή η εκπομπή του σήματος αυτού δεν πετυχαίνει την επιθυμητή μετάδοση της πληροφορίας προς τον UE και για να μην υπάρχει σπατάλη στους πόρους του κόμβου, κάποιο άλλο RNC αναλαμβάνει τον ρόλο του SRNC για τον UE. Επίσης, η χρήση της διαδικασίας αυτής συνεισφέρει και στην αποφυγή της άσκοπης χρήσης του bandwidth της διεπαφής Iur.

2.5.4. Intersystem handover

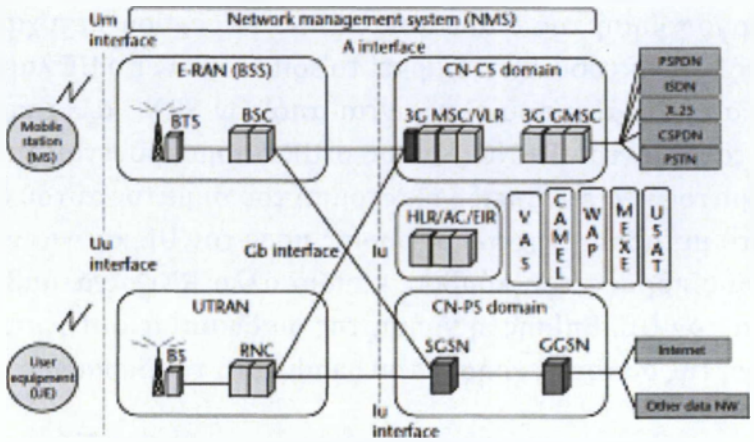
Ένα intersystem handover θεωρείται ότι είναι ένα handover μεταξύ δυο διαφορετικών τεχνολογιών ασύρματης πρόσβασης. Προς το παρόν το 3GPP έχει θέσει τις προδιαγραφές για intersystem handover μεταξύ των συστημάτων GSM και UMTS. Κατά συνέπεια υπάρχει ένα handover από UMTS προς GSM και ένα από GSM σε UMTS. Δεδομένου ότι τα δίκτυα UMTS δεν παρέχουν επαρκή κάλυψη σε γεωγραφικές περιοχές, η υποστήριξη της διαδικασίας αυτής κρίνεται απαραίτητη.

Έτσι οι χρήστες των δικτύων UMTS θα εξυπηρετούνται σε μεγάλο βαθμό από δίκτυα πρόσβασης GSM.

2.6. Εκδόσεις UMTS

Η εξέλιξη του UMTS εξελίσσεται σύμφωνα με τις προγραμματισμένες εκδόσεις. Κάθε έκδοση έχει σχεδιαστεί για να εισαγάγει νέα χαρακτηριστικά και βελτιώσεις στο ήδη υπάρχουσες.

2.6.1. Έκδοση '99



Σχήμα 17 : Αρχιτεκτονική UMTS έκδοσης 1999

Η εισαγωγή των 3G κινητών συστημάτων με το UMTS έχει απαιτήσει την εγκατάσταση ενός απολύτως νέου ασύρματου υποσυστήματος, του UMTS Radio Access Network(UTRAN). Το κεντρικό δίκτυο UMTS είναι βασισμένο στην ίδια τεχνολογία με το GSS, με πρόσθετους όμως εξοπλισμούς, όπως οι πύλες πολυμέσων(multimedia gateways – MGs), για τη διασύνδεση των packet switched(πακέτο μεταγωγής) και circuit switched(διακόπτης μεταγωγής) δικτύων, που επιτρέπουν τη σύγκλιση των υπηρεσιών που βασίζονται σε αυτές τις δύο διαφορετικές τεχνικές.

Η πρώτη έκδοση του UMTS αυξάνει το data bit rate στην ασύρματη διεπαφή έτσι ώστε υπηρεσίες πολυμέσων, όπως π.χ. η βιντεοκλήση να μπορούν να προταθούν στους συνδρομητές. Το μεταβλητό data bit rate στην ασύρματη διεπαφή είναι ένα άλλο πλεονέκτημα που προσφέρεται από το UMTS έναντι της 2 και 2.5G.

Ο εξοπλισμός των χρηστών UE(User Equipment), περιλαμβάνει (1) τον κινητό εξοπλισμό(ME), δηλαδή το ασύρματο τερματικό που χειρίζεται την επικοινωνία σχετικά με την διεπαφή Uu(Uu Interface) και (2) το UMTS

Subscriber Identity Module(USIM), που είναι μια έξυπνη κάρτα συμπεριλαμβανομένων των στοιχείων-ταυτότητα, αλγόριθμους αυθεντικοποίησης και πληροφορίες συνδρομής.

Το Radio Network Controller(RNC), είναι το αντίστοιχο του BSC στο GSM. Ελέγχει τους ασύρματους πόρους(radio resource), μέσα στη σχετική κάλυψή του, μέσω των κόμβων B(nodes B). Ο κόμβος B(nodes B), αντίστοιχο του σταθμού πομποδεκτών βάσεων GSM(BTS), μετατρέπει τις ροές δεδομένων μέσω των διεπαφών Iub και Uu. Ο ρόλος του είναι κυρίως να εκτελέσει τις λειτουργίες του physical layer(διαμόρφωση, κωδικοποίηση, προσαρμογή ποσοστού, διάδοση, κλπ.).

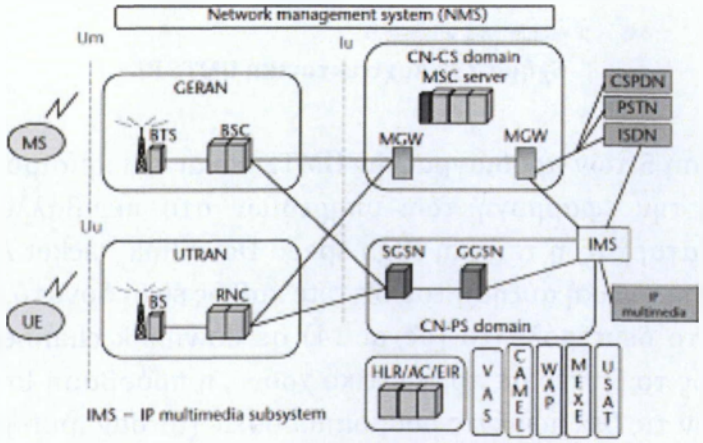
Το κεντρικό δίκτυο (Core Network)- συλλέγει όλα τα πρωτόκολλα δικτύων (για την καθιέρωση και το χειρισμό κλήσης, τη μετάδοση στοιχείων, τη διαχείριση κινητικότητας, κλπ.). Δύο στρώματα καθορίζονται, το Radio Network Layer και το Transport Layer.

Τα μέγιστα bit rates που λαμβάνονται στα πειράματα δείχνουν ότι ένας κόμβος B μπορεί να χειριστεί (σε ιδανικές συνθήκες) το πολύ 3 ταυτόχρονους χρήστες βιντεοκλήσεων σε ένα ενιαίο μεταφορέα UMTS, ο οποίος είναι τρείς φορές το 384kb/s για γύρω από το εύρος ζώνης των 5 MHz.

Με την Έκδοση 3(UMTS R3) ένα ασύρματο δίκτυο πρόσβασης(radio access network) αποκαλούμενο UTRAN(UMTS Terrestrial Radio Access Network) εισάγεται, βασισμένο σε W-CDMA αντί TDMA/FDMA) μετάδοση διεπαφών αέρα.

2.6.2. Έκδοση 2000

Έκδοση 4



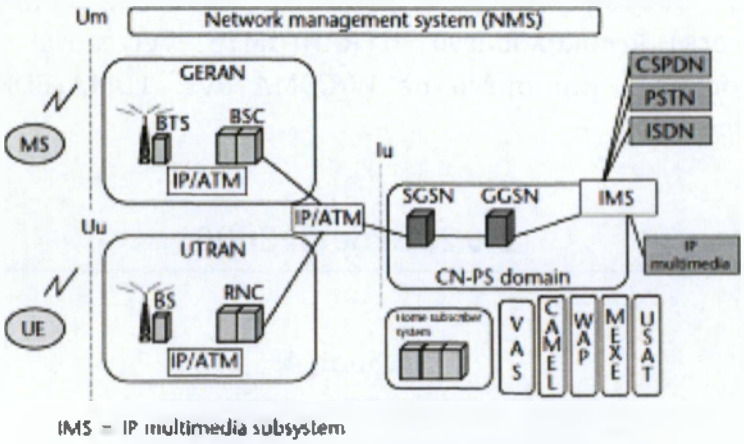
Σχήμα 18 : Αρχιτεκτονική UMTS R4

Στην ακόλουθη φάση εξέλιξης του UMTS, το ασύρματο μέρος παραμένει βασικά αμετάβλητο. Στο επίπεδο κεντρικών δικτύων, το mobile switching center(Msc) και ο κατάλογος θέσης επισκεπτών (visitor location register, VLR) γίνεται MSC servers και MGs. Οι MSC servers διαχειρίζονται τις επικοινωνίες και την κινητικότητα χρηστών και τα MGs είναι αρμόδια για τις λειτουργίες δρομολόγησης. Ο MSC server μπορεί να διαχειριστεί πολλά MG, το οποίο επιτρέπει έναν καλύτερο χωρισμό μεταξύ των λειτουργιών δρομολόγησης. Αυτή η εξέλιξη επιτρέπει έναν καλύτερο χωρισμό μεταξύ των λειτουργιών ελέγχου και επεξεργασίας στο δίκτυο. Επομένως διευκολύνει την εισαγωγή των νέων χαρακτηριστικών γνωρισμάτων και συνεπώς τις νέες υπηρεσίες.

Με την Έκδοση 4, η λειτουργία του MSC είναι χωρισμένη σε δύο οντότητες:

- Ο MSC Server, ο οποίος παρέχει τα control functions.
- Media Gateway (MGW) server παρέχει τις λειτουργίες μετατροπής και, εάν είναι απαραίτητο, τα functions μετατροπής μεταξύ δύο διαφορετικών format. Ένας MSC Server μπορεί να ελέγξει πολλαπλάσια MGWs.

Έκδοση 5



Σχήμα 19 : Αρχιτεκτονική UMTS R5

Η Έκδοση 5 των προδιαγραφών UMTS είναι ένα κρίσιμο βήμα προς την ανάπτυξη και την εφαρμογή των υπηρεσιών στο περιβάλλον της κινητής τηλεφωνίας. Καταρχάς, η τεχνική High-speed Downlink Packet Access (HSDPA) επιτρέπει μια σημαντική αύξηση του bit rate καθώς είναι δυνατό να επιτευχθούν πολλά Mbits το δευτερόλεπτο (μέχρι 14) σε downlink channel συνδέσεις. Οι υπηρεσίες όπως το βίντεο σε πραγματικό χρόνο, η πρόσβαση Ιστού και το FTP, κλπ., θα λάβουν τις βελτιωμένες ρυθμοαποδόσεις (throughputs) και, επομένως, ο τελικός χρήστης αντιλαμβάνεται την ποιότητα τη υπηρεσίας. Το HSDPA επιτυγχάνεται κυρίως από τις τροποποιήσεις στο ασύρματο υποσύστημα. Στο

επίπεδο δικτύων, η σημαντικότερη εξέλιξη που εισάγεται στο UMTS R5 είναι το υποσύστημα πολυμέσων IP (IMS, Multimedia subsystem), το οποίο φέρνει στους πάροχους τα μέσα για να διευκολύνει την εισαγωγή των νέων υπηρεσιών και των εφαρμογών πολυμέσων. Το IMS είναι ένα υποσύστημα που ελέγχει την παροχή υπηρεσιών μεταξύ των κεντρικών υπολογιστών(servers) και του κεντρικού δικτύου (core network). Επιτρέπει την ολοκλήρωση των εφαρμογών και των υπηρεσιών σε πραγματικό χρόνο. Τέλος, το UMTS R5 εισάγει την IP στο ασύρματο υποσύστημα (IP UTRAN) που γενικεύει τη χρήση της IP σε ολόκληρο το δίκτυο(UTRAN και Core Network).

Τα κύρια στοιχεία του IMS είναι τα παρακάτω:

- Call Status Control Function (S-CSCF) ελέγχει τις κυκλοφοριακές ροές IP (IP traffic flows), κλήσεις και συνόδους (calls and sessions), και ότι συσχετίζεται με τη λειτουργία προστιθέμενης αξίας υπηρεσιών (value-added services).
- SIP Application Server (SIP AS) μπορεί να προγραμματιστεί μέσω scripts (SIP-CGI or APIs) για το VAS.
- Open Service Architecture (OSA) Service Capability Server (SCS) αντιπροσώπευση ενός ή περισσότερων χαρακτηριστικών γνωρισμάτων OSA (SCF, Service Capability Features).
- Inter-working Module (IMS-SSF) SIP-CAMEL interworking module.
- Camel Service Environment (CSE) SCP χρησιμοποίηση των χαρακτηριστικών γνωρισμάτων του CAMEL και του GSM.
- Home Subscriber Server (HSS) είναι το δίκτυο με το HLR σε ένα IMS περιβάλλον. Περιλαμβάνει τα στοιχεία IMS για την επικύρωση και την καθιέρωση συνόδου.

Επομένως, το IMS είναι μια νέα περιοχή(domain) που επιτρέπει τη σύγκλιση μεταξύ των σταθερών και κινητών δικτύων. Διαχειρίζεται όλες τις υπηρεσίες (υπάρχουσες υπηρεσίες, όπως circuit switched voice, voice-over IP, κλπ.). Το IMS είναι ένας μέσος όρος για τους πάροχους για να αναπτύξει και να εφαρμόσει τις νέες υπηρεσίες και να ενσωματώσει τον κόσμο του Διαδικτύου και επομένως όλη την σχετική επιχείρηση. Το άλλο κύριο πλεονέκτημα του IMS είναι οι προσδοκίες από την άποψη της αποταμίευσης OPEX(OPEX savings). Το IMS έχει δύο κύρια κίνητρα: (1) οι υπηρεσίες και (2) το πρότυπο των παροχών, να μην καταλήγει ως bit pipe ή ISP. Οι πρώτες εφαρμογές που δοκιμάστηκαν με το IMS είναι το στιγμιαίο μήνυμα(instant messaging), τηλεοπτική-διανομή(video-sharing) και τυχερά παιχνίδια σε πραγματικό χρόνο(real-time gaming). Άλλες εφαρμογές, όπως το Pashto-Talk, θεωρείται επίσης υποψήφιο για να εφαρμοστεί χρησιμοποιώντας το IMS.

Η φανταστική αύξηση των ασύρματων δικτύων τοπικής περιοχής (LANs) στα τελευταία έτη έχει παρακινήσει τους πάροχους να ενσωματώσουν αυτήν την νέα τεχνολογία στις δραστηριότητες και τα επιχειρησιακά πρότυπά τους. Η χρήση αυτής της τεχνολογίας στην πρόσβαση στο Διαδίκτυο και των βασισμένων στην IP υπηρεσιών και των εφαρμογών, ειδικά για τους εσωτερικούς χρήστες και τους αστικούς υπαίθρους χρήστες(low mobility urban outdoors users), είναι ένα σημαντικό κίνητρο για τους πάροχους να ενδιαφερθούν για αυτήν την σχετική με τον υπολογιστή τεχνολογία. Η UMTS R6 εξετάζει τα WLANs ως τμήμα ολόκληρου του δικτύου. Μέσω ενός πλουσιότερου IMS(από την άποψη των χαρακτηριστικών γνωρισμάτων) θα είναι σε θέση να διαχειριστεί τις end-to- end επικοινωνίες σχετικά με σταθερά, κινητά και WLANs δίκτυα. Με βελτιώσεις στην ποιότητα της υπηρεσίας και του IMS που εφαρμόζονται στα σταθερά δίκτυα.

2.7. All IP UMTS

Το τρίτης γενιάς δίκτυο για το οποίο στοχεύει το IETF, σύμφωνα με τις περιγραφές στις προδιαγραφές, είναι ένα και μοναδικό συνενωμένο δίκτυο το οποίο είναι 100% IP.

2.7.1. All IP UMTS πλεονεκτήματα και μειονεκτήματα

Η εξέλιξη στο IP based δίκτυο έχει τέσσερα σημαντικά πλεονεκτήματα:

1. Ένα IP based δίκτυο υπόσχεται χαμηλότερη χρέωση επικοινωνίας και μειωμένο κόστος κατασκευής συστήματος.
2. Γίνεται πιο εύκολη η ανάπτυξη εφαρμογών που θα συνδυάζουν επικοινωνία φωνής και δεδομένων.
3. Αφού είναι δυνατή η διαχείριση φωνής και δεδομένων σε ένα μοναδικό all –IP κυρίως δίκτυο, τα κόστη συντήρησης και διατήρησης σε ενεργεία του δικτύου μειώνονται σημαντικά.
4. Οι υποδομές που οι πωλητές παρέχουν κατασκευάζονται με τέτοιο τρόπο, έτσι ώστε να μπορούν εύκολα να αναβαθμιστούν σε IP based διαχείριση.

Ωστόσο, η υλοποίηση του IP μπορεί να παρουσιάσει μερικά αρχικά προβλήματα. Επειδή το IP από μόνο του δεν ικανοποιεί μερικές απαιτήσεις για QoS, κινητικότητα και bandwidth αποδοτικότητα σε narrowband συνδέσεις, νέα

πρωτόκολλα πρέπει να προστεθούν στο σύστημα. Η χρήση οποιασδήποτε τεχνικής προσαρμογής – συμπίεση header, MPLS, ή PPP επεκτάσεις – για την αύξηση του IP σε narrowband συνδέσεις, έχει ως αποτέλεσμα υψηλό επίπεδο πολυπλοκότητας. Για να αντιμετωπιστεί αυτή η κατάσταση, μερικοί εισηγούν broadband ή κατανεμημένες αρχιτεκτονικές.

2.7.2. Συνενωμένο Δίκτυο

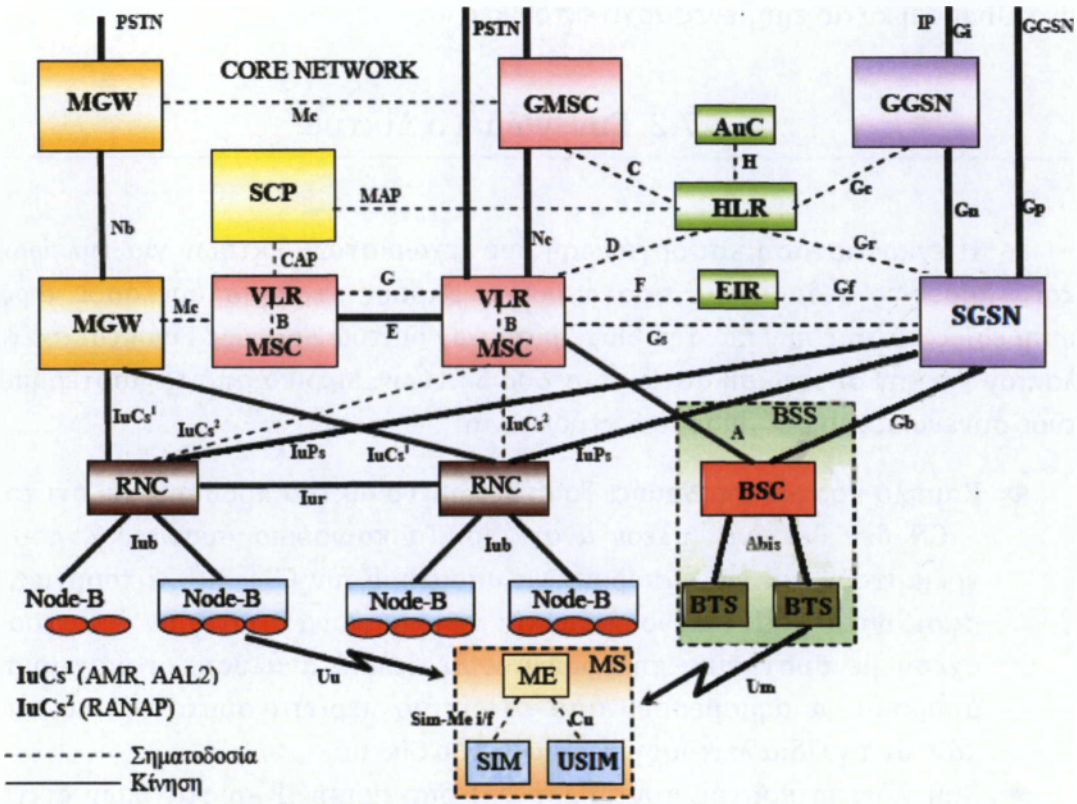
Η εγκατάσταση και οργάνωση δυο ξεχωριστών δικτύων για τηλεφωνία και υπηρεσίες δεδομένων, εισαγάγουν σοβαρούς περιορισμούς όσον αφορά υπηρεσίες πολυμέσων και την διαχείριση των δικτύων αυτών. Γίνονται σκέψεις λοιπόν για την συνένωση αυτών των δυο δικτύων. Μερικά από τα προτερήματα ενός συνενωμένου ασύρματου δικτύου είναι:

- Χαμηλό κόστος υποδομής: Το συνενωμένο δίκτυο προϋποθέτει ότι το CS – CN δεν θα είναι πλέον αναγκαίο. Τα καινούρια συστατικά, που θα χρειαστούν για να μπορούν να υποστηρίζουν CS – CN λειτουργίες, θα βασίζονται σε IP τεχνολογίες και κατά κανόνα κοστίζουν λιγότερο σε σχέση με συστατικά τηλεφωνίας.. Σε τελική ανάλυση, οι διαχειριστές μπορούν να αφαιρέσουν από το δίκτυο περιττά συστατικά τα οποία κάνουν την ίδια λειτουργία και στα δυο δίκτυα.
- Χαμηλότερο κόστος συντήρησης: Η διαχείριση IP συστατικών δικτύου είναι λιγότερο δαπανηρή σε σχέση με συστατικά τηλεφωνίας. Επίσης οι διαχειριστές μπορούν να διευθύνουν το συνενωμένο δίκτυο εργοδοτώντας λιγότερα στελέχη.
- Ανεπτυγμένες Υπηρεσίες: Η ανάμιξη δικτύων φωνής και δεδομένων προσφέρει ευκαιρίες για ανάπτυξη ανεπτυγμένων υπηρεσιών πολυμέσων. Σχεδόν κάθε υπηρεσία, εκτός από τις τηλεφωνικές υπηρεσίες, είναι διαθέσιμη στο Διαδίκτυο σήμερα. Ο συνδυασμός του Διαδικτύου και των τηλεφωνικών υπηρεσιών δημιουργεί πολλές καινούριες ευκαιρίες αποκόμισης κέρδους για τους παροχείς υπηρεσιών.
- Ανάπτυξη Ταχείας Υπηρεσίας (Rapid Service Deployment): Πολλά από τα αναγκαία που χρειάζονται για την εισαγωγή καινούργιων υπηρεσιών μειώνονται λόγω της ανάμιξης της διαχείρισης των ασύρματων δικτύων.

2.7.3. All IP UMTS αρχιτεκτονική

Όπως έχει ήδη αναφερθεί, τα κυριότερα πλεονεκτήματα μιας all IP αρχιτεκτονικής είναι: ευκαμψία, αυξομειωσιμότητα και η μείωση του κόστους. Μερικά προβλήματα που παρουσιάστηκαν (QoS, κινητικότητα και bandwidth

αποδοτικότητα) ακόμη επιλύονται. Η διαδικασία προτυποποίησης της all IP αρχιτεκτονικής στο UMTS έχει ήδη αρχίσει και αναμένεται να τελειώσει μέχρι την Έκδοση 5 των 3GPP προτύπων.



Σχήμα 20 : Cosmote δικτυακή αρχιτεκτονική

Όπως φαίνεται στο Σχήμα 20, τα PS-CN και CS-CN έχουν αντικατασταθεί από το συνενωμένο δίκτυο.

Επεξήγηση συστατικών μερών Σχήματος 20:

- **RNC (Radio Network Controller)** - είναι το αντίστοιχο του BSC στο GSM. Ελέγχει τους ασύρματους πόρους(radio resource), μέσα στη σχετική κάλυψή του, μέσω των κόμβων B(nodes B).
- **MGW (Media Gateway)** - παρέχει interworking αλληλεπίδραση μεταξύ των δικτύων πρόσβασης και μεταφοράς, για να ελέγχεται η ροή μέσων στο PSTN.
- **SCP (Session Control Protocol)**
- **VLR (Visitor Location Register)** - Η βάση VLR λαμβάνει την αρχική πληροφορία από τη βάση HLR και αναλαμβάνει να την ενημερώσει για τυχόν μεταβολές στα δεδομένα της. Όλες οι συναλλαγές μεταξύ VLR και HLR γίνονται μέσω ενός MSC.
- **HLR (Home Location Register)** - κεντρική βάση δεδομένων που περιέχει τις λεπτομέρειες του κάθε συνδρομητή κινητού τηλεφώνου που έχει λάβει άδεια να χρησιμοποιεί το GSM και WCDMA core network της PLMN.

- **AuC-** αποτελεί έναν κόμβο που είναι συσχετισμένος με τον HLR. Ο κόμβος αυτός αποθηκεύει πληροφορίες ταυτοποίησης και κρυπτογράφησης για τους συνδρομητές.
- **GMSC (Gateway Mobile Services Switching Center)** - Ο κόμβος GMSC είναι συνδεδεμένος με τους κόμβους MSC. Η λειτουργία του είναι να διασυνδέει το δίκτυο UMTS με άλλα δίκτυα μεταγωγής κυκλώματος όπως PSTN και ISDN.
- **GGSN (Gateway GPRS Support Node)** – παρέχει πρόσβαση σε υπηρεσίες Διαδικτύου.
- **SGSN (Servicing GPRS Support Node)** – παρέχει τις λειτουργίες πρόσβασης κόμβου δικτύου (network access node) και διαχείριση κινητικότητας.
- **BSC (Base Station Subsystem)** - υπεύθυνη για τον χειρισμό κίνησης και σηματοδοσίας μεταξύ του κινητού τηλεφώνου και του υποσυστήματος μεταγωγής δικτύου.
- **BTS (Base Transceiver Station)** - διευκολύνει την ασύρματη επικοινωνία μεταξύ του εξοπλισμού χρήστη (UE) και το δίκτυο.
- **USIM (UMTS Subscriber Identity Module)** - μια έξυπνη κάρτα που περιλαμβάνει τα στοιχεία-ταυτότητα, αλγόριθμους αυθεντικοποίησης και πληροφορίες συνδρομής.
- **SIM (Subscriber Identity Module)** - ολοκληρωμένο κύκλωμα που αποθηκεύει με ασφάλεια τη διεθνή ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI) και το σχετικό κλειδί που χρησιμοποιείται για τον εντοπισμό και έλεγχο ταυτότητας για τους συνδρομητές.

2.7.4. 3 στάδια εισαγωγής της All – IP

Η γενική UMTS All – IP αρχιτεκτονική έχει πολλά κοινά με την Έκδοση 99. Αποτελείται από terminal equipment (TE) και κινητούς κόμβους που συνδέονται μέσω ενός ράδιο συστήματος (UTRAN) σε ένα Serving GPRS Support Node (SGSN). Το SGSN επικοινωνεί με άλλα SGSN ή με άλλα GGSN (Gateway GPRS Support Node). Η λειτουργία καταγραφής τοποθεσίας στο SGSN φυλάει δυο ειδών δεδομένα συνδρομητή, (1) τις πληροφορίες του συνδρομητή και (2) τις πληροφορίες τοποθεσίας.

1ο βήμα: να συμπεριλάβει το Mobile IP, σαν μια υπηρεσία που θα προσφέρει κινητικότητα στους UMTS κόμβους. Επιπρόσθετα, θα μπορεί να χρησιμοποιείται σαν ενδιάμεσο GPRS – Mobile IP σύστημα και για Intra System Mobility (τοπική κίνηση, μέσα στην εμβέλεια του συγκεκριμένου UMTS συστήματος). Αυτό απαιτεί Foreign Agent λειτουργίες στο GGSN και υποστήριξη Mobile IP στα κινητά τερματικά.

2ο βήμα: μπορεί να είναι η χρήση του Mobile IP για προσφορά GGSN handover κατά την διάρκεια ενός session. Αυτό επίσης απαιτεί υποστήριξη Mobile IP στα κινητά τερματικά αλλά θεωρούμε ότι αυτό έχει τακτοποιηθεί στο πρώτο βήμα.

3ο βήμα: προσφέρει μια πιο δραστική αλλαγή από την τρέχουσα έκδοση και υπάρχει περισσότερη αβεβαιότητα σχετικά με μια εξέλιξη εκείνη τη στιγμή. Η λύση που παρουσιάζεται εδώ είναι η χρήση του GTP πρωτοκόλλου μόνο για έλεγχο μέσα στο κυρίως δίκτυο, καθώς για τον χρήστη θα χρησιμοποιείται καθαρό IP. Τα SGSN και GGSN θα συνενωθούν στο IGSN (Internet GPRS Support Node). Η διαχείριση της κινητικότητας, σε μακροχρόνιο επίπεδο, βασίζεται στο ότι το Mobile IP θα απαιτεί υποστήριξη για Mobile IP σε όλα τα κινητά τερματικά. Δεν υπάρχει καθαρή εξέλιξη από πλευράς προτυποποίησης προς αυτή την εναλλακτική λύση που παρουσιάζεται, αλλά οι πωλητές εξοπλισμού και η κοινωνία Διαδικτύου υποστηρίζουν αυτή την εξέλιξη αφού θα μειώσει το κόστος εξοπλισμού – λόγο συνένωσης των SGSN και GGSN. Υποστηρίζεται ακόμη σε αυτή την λύση, μια πιο κοντινή συνένωση των UMTS και του Διαδικτύου, λόγο χρήσης καθαρού IP.

2.8. IP έκδοση στο UMTS

Σύμφωνα με πηγές από το EURESCOM, η επιλογή της έκδοσης του IP δεν ήταν η πρωτεύουσα ανησυχία στην διαδικασία προτυποποίησης του UMTS. Τελευταίως όμως, το θέμα αυτό έχει γίνει περισσότερο αντικείμενο συζήτησης και είναι πολύ πιθανό ότι θα είναι αναγκαία η υποστήριξη των UMTS τερματικών τόσο του IPv4, όσο και του IPv6.

Η επιλογή της έκδοσης του πρωτοκόλλου που θα υποστηρίζεται από το UMTS δίκτυο, ίσως να αφεθεί στην κρίση του διαχειριστή του δικτύου. Είναι λογικό τότε, ότι η κρίση των διαχειριστών θα επηρεαστεί από την διαθεσιμότητα των IP διευθύνσεων, την υποστήριξη που θα παρέχεται από την βιομηχανία, από την πληρότητα του κάθε πρωτοκόλλου και τα λοιπά. Όμως, η άποψη τους θα διαμορφωθεί και από την γνώμη άλλων διαχειριστών: δηλαδή αν πολλοί διαχειριστές αποφασίσουν να τραβήξουν προς το IPv6, αυτό θα δημιουργήσει προώθηση προς καθαρά IPv6 δίκτυα.

Επομένως, με την πάροδο του χρόνου είναι πολύ πιθανό να: σε αρχικό στάδιο τα περισσότερα UMTS δίκτυα να βασίζονται σε διπλή στοίβα (IPv4 και IPv6) και σε μετέπειτα στάδιο να αναπτυχθούν πλήρη IPv6 δίκτυα.

2.9. Αδυναμίες, Ελλείψεις και κενά Ασφαλείας

Αρκετά γνωστά προβλήματα και αδυναμίες του μηχανισμού αυθεντικοποίησης του GSM φαίνεται ότι έχουν λυθεί ή επαρκώς καλυφθεί στον αντίστοιχο του UMTS.

Παρόλα αυτά, υπάρχουν ακόμη ορισμένα κενά ασφαλείας ή αδυναμίες, τις οποίες οι επιτιθέμενοι μπορούν να εκμεταλλευτούν. Οι αδυναμίες αυτές περιγράφονται στα παρακάτω:

A.

Επιτιθέμενοι, που εφαρμόζουν παθητικές(passive) ή ενεργητικές (active) μεθόδους, μπορούν να υποκλέψουν διανύσματα(vectors) αυθεντικοποίησης είτε από τα SGSN, HSS είτε από το δίαυλο επικοινωνίας μεταξύ αυτών. Το πρόβλημα απαιτεί ιδιαίτερη προσοχή στην περίπτωση που ένας συνδρομητής περιάγει μεταξύ διαφορετικών PLMNS. Τότε, το HN είναι υποχρεωμένο να αποστείλει στο SN διανύσματα αυθεντικοποίησης προκειμένου το τελευταίο να μπορεί να αυθεντικοποιήσει το συνδρομητή.

Σε τέτοιες περιπτώσεις τα διανύσματα μεταφέρονται μεταξύ των διαφορετικών δικτύων των παρόχων (οι οποίοι μπορεί να εφαρμόζουν διάφορες πολιτικές ασφάλειας) και έτσι είναι περισσότερο πιθανό να υποκλαπούν ή να καταστραφούν. Σε κάθε περίπτωση, όπως συνέβαινε και στο GSM, οι χρήστες πρέπει να εμπιστεύονται το SN και τις πολιτικές ασφάλειας που αυτό εφαρμόζει.

B.

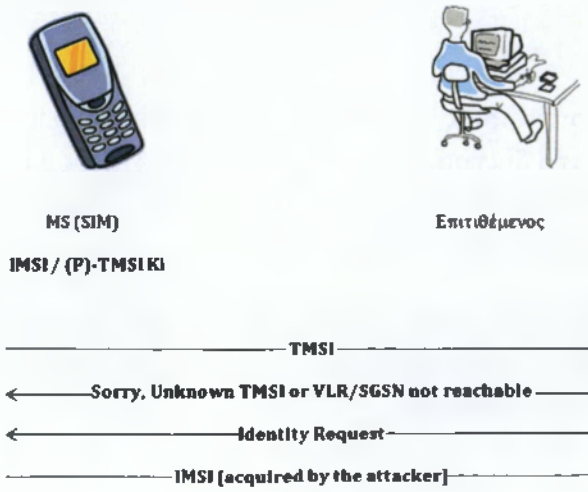
Σε ορισμένες περιπτώσεις, το σύστημα επιτρέπει την εκπομπή του IMSI του χρήστη από το UE στο δίκτυο σε μορφή καθαρού κειμένου (clear-text) με σκοπό αυτός να αυθεντικοποιηθεί. Η συγκεκριμένη διαδικασία μπορεί να ξεκινήσει από το HN ή το SN στις ακόλουθες περιπτώσεις:

- Όταν ο συνδρομητής εγγράφεται για πρώτη φορά στο δίκτυο ή μετά από μεγάλο διάστημα κατά το οποίο διατηρούσε τη συσκευή του εκτός λειτουργίας και
- Όταν το δίκτυο δεν μπορεί να αποκτήσει το IMSI του συνδρομητή. Όπως για παράδειγμα, σε περιπτώσεις μεταβίβασης κλήσης ή συνεδρίας (session) από κυψέλη ή από δίκτυο σε δίκτυο (handover), όπου το ζευγάρι IMSI, (P)-TMSI μεταδίδεται από προηγούμενο SGSN στο νέο και η διεύθυνση (LAI/RAI) του προηγούμενου SGSN δεν μπορεί να επιλυθεί (resolved).

Επίσης, σε περιπτώσεις κατά τις οποίες η βάση δεδομένων ενός SGSN παρουσιάζει βλάβη. Η διαδικασία αυτή είναι ανοικτή σε παθητικού τύπου επιθέσεις, όπου ο επιτιθέμενος περιμένει για πιθανές εκπομπές απροστάτευτων IMSI ή σε επιθέσεις τύπου Man-in –the-Middle(MITM). Η εκπομπή του IMSI αποτελεί κυρίως απειλή εναντίον της εμπιστευτικότητας της ταυτότητας του χρήστη (identity confidentiality) και της θέσης που αυτός κινείται (location privacy).

Επιπλέον, όμως, η γνώση του IMSI μπορεί να επιτρέψει την πλαστογράφηση της ταυτότητας του χρήστη. Δεν είναι βέβαια σαφές το πώς ένας επιτιθέμενος μπορεί να εκμεταλλευτεί αυτή τη δυνατότητα πλαστογράφησης, εκτός από το να προκαλέσει γενική αναστάτωση (commotion)στο σύστημα. Γενικότερα, υπάρχουν τοποθεσίες ή σήμερα στα οποία πολλά IMSIs εκπέμπονται συνεχώς. Τέτοιες τοποθεσίες περιλαμβάνουν αεροδρόμια, λιμάνια, κλπ, όπου οι χρήστες ανοίγουν τα κινητά τους μετά την πτήση ή γενικότερα το ταξίδι τους. Αυτό σημαίνει ότι ο επιτιθέμενος που γνωρίζει το IMSI κάποιου ή κάποιων συνδρομητών είναι σε θέση να τους αναγνωρίσει. Από την άλλη πλευρά αυτό είναι επίσης δυνατό απλώς παρατηρώντας ποιοι κατεβαίνουν π.χ. από το πλοίο.

Οπωσδήποτε όμως, ο μηχανισμός αυθεντικοποίησης του UMTS δεν προσφέρει πολύ καλή προστασία από ένα ενεργό επιτιθέμενο, ο οποίος μπορεί να προσποιηθεί (masquerade) το δίκτυο εξυπηρέτησης (false base station- RNC attack) με αποτέλεσμα να καταφέρει σχετικά εύκολα να αποκτήσει το IMSI του χρήστη θύματος. Η κατάσταση αυτή περιγράφεται στο παρακάτω Σχήμα 21.



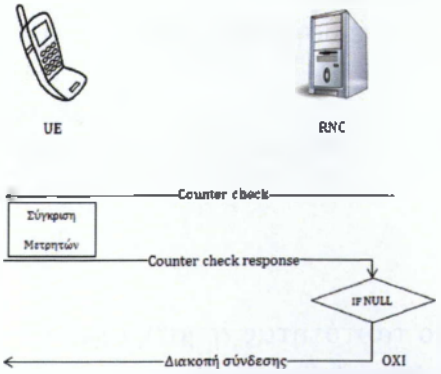
Σχήμα 21 : Μηχανισμός αυθεντικοποίησης του UMTS

Γ.

Το μήκος των κλειδιών και οι αλγόριθμοι κρυπτογράφησης/αποκρυπτογράφησης είναι σταθερά (fixed), με αποτέλεσμα ο μηχανισμός AKA να θεωρείται δύσκαμπτος (inflexible) και λιγότερο ασφαλής. Αυτό είναι ιδιαίτερα εμφανές σε περιπτώσεις όπου ανακαλύπτεται μια ευπάθεια (vulnerability) σε κάποιον αλγόριθμο ή διαδικασία, όπως στην περίπτωση του αλγόριθμου GSM A5/1.

Αντίθετα, μεγαλύτερη ευελιξία θα ήταν δυνατόν να επιτευχθεί, έχοντας ένα δυναμικό μηχανισμό AKA, ο οποίος είναι ικανός να διαπραγματεύεται και να ενσωματώνει νέα στοιχεία (modules) ασφαλείας σε πραγματικό χρόνο και ανάλογα με τις συνθήκες (on-demand). Μια από τις βελτιώσεις ασφάλειας στο UMTS είναι η συμπερίληψη της δυνατότητας προστασίας της ακεραιότητας. Όμως, η προστασία της ακεραιότητας είναι εγγυημένη μόνο για τη σηματοδοσία μεταξύ UE και RNC. Όπως είδαμε, στα δεδομένα των χρηστών (U-plane) δεν προσαρτάται Message Authentication Code (MAC-I) για λόγους απόδοσης (performance reasons) και γι' αυτό το λόγο παραμένουν ευαίσθητα σε παραποιήσεις (manipulation). Παρόλα αυτά υπάρχει μια συγκεκριμένη διαδικασία, η οποία καλείται περιοδική αυθεντικοποίηση (periodic authentication) και μπορεί εν δυνάμει να παράσχει κάποιου είδους προστασία της ακεραιότητας του U-plane. Σύμφωνα με αυτή τη διαδικασία το πόσο (amount) των δεδομένων που στάλθηκαν κατά τη διάρκεια μιας RRC σύνδεσης ελέγχεται.

Αυτό έχει ως αποτέλεσμα τα δεδομένα των χρηστών να προστατεύονται περιοδικά όσο αφορά το μέγεθος τους (volume), παράλληλα με τη διαδικασία επανάληψης της αυθεντικοποίησης. Όπως περιγράφεται στο παρακάτω Σχήμα 22, η διαδικασία ξεκινάει από το υπεύθυνο RNC, αμέσως μόλις η παράμετρος COUNT-C φτάσει κάποιο προ-διευθετημένο όριο. Τότε το RNC στέλνει ένα counter check μήνυμα, το οποίο περιέχει το περισσότερο σημαντικό τμήμα όλων των COUNT-C που αντιστοιχούν σε κάθε ενεργό ραδιο-φορέα (radio beare).



Σχήμα 22 : Διαδικασία επανάληψης της αυθεντικοποίησης

Από την άλλη μεριά το UE συγκρίνει όλες τις λαμβανόμενες τιμές με τις αντίστοιχες δικές του. Τυχόν διαφορές αναφέρονται πίσω στο RNC με ένα μήνυμα counter check response. Σε περίπτωση που το συγκεκριμένο μήνυμα είναι κενό, τότε η διαδικασία ολοκληρώνεται με επιτυχία. Σε αντίθετη περίπτωση, το RNC ενδέχεται να διακόψει τη σύνδεση. Όπως είναι φυσικό , η διαδικασία αυτή έχει ως στόχο να εμποδίσει επιτιθέμενους να εισάγουν ή να διαγράψουν πακέτα δεδομένων και προς τις δύο κατευθύνσεις(uplink/downlink). Από την άλλη μεριά, ο επιτιθέμενος μπορεί να προσπαθήσει να εισάγει ή και να διαγράψει τον ίδιο ακριβώς αριθμό πακέτων προκειμένου να μη γίνει αντιληπτός.

Δ.

Επίσης, προστασία στο επίπεδο εφαρμογής, όπου αυτή απαιτείται, παρέχεται από το πρωτόκολλο WLTS. Είναι γνωστό πως το WLTS, τουλάχιστον μέχρι την έκδοση 2.0, χρησιμοποιεί WAP πύλη (gateway), η οποία θεωρείται γενικά ανασφαλής και σίγουρα δεν εξασφαλίζει end-to-end επικοινωνία. Επιπλέον, επιτρέπει τη χρησιμοποίηση «αδύνατων» (weak) αλγορίθμων κρυπτογράφησης και διαθέτει χαρακτηριστικά, τα οποία επιτρέπουν την ανάπτυξη επιθέσεων του τύπου επιλεγμένου αρχικού κειμένου (chosen-plaintext) και εξάντλησης αναζήτησης(brute force). Σε κάθε περίπτωση, η διαδικασία αυθεντικοποίησης του WLTS είναι συχνά ανώνυμη, ενώ ακόμη και όταν εκτελείται κανονικά, γίνεται μόνο μια φορά (έναντι της WAP πύλης) σε όλη τη διάρκεια χρησιμοποίησης της πύλης.

2.10. Υπηρεσίες Ασφάλειας UMTS

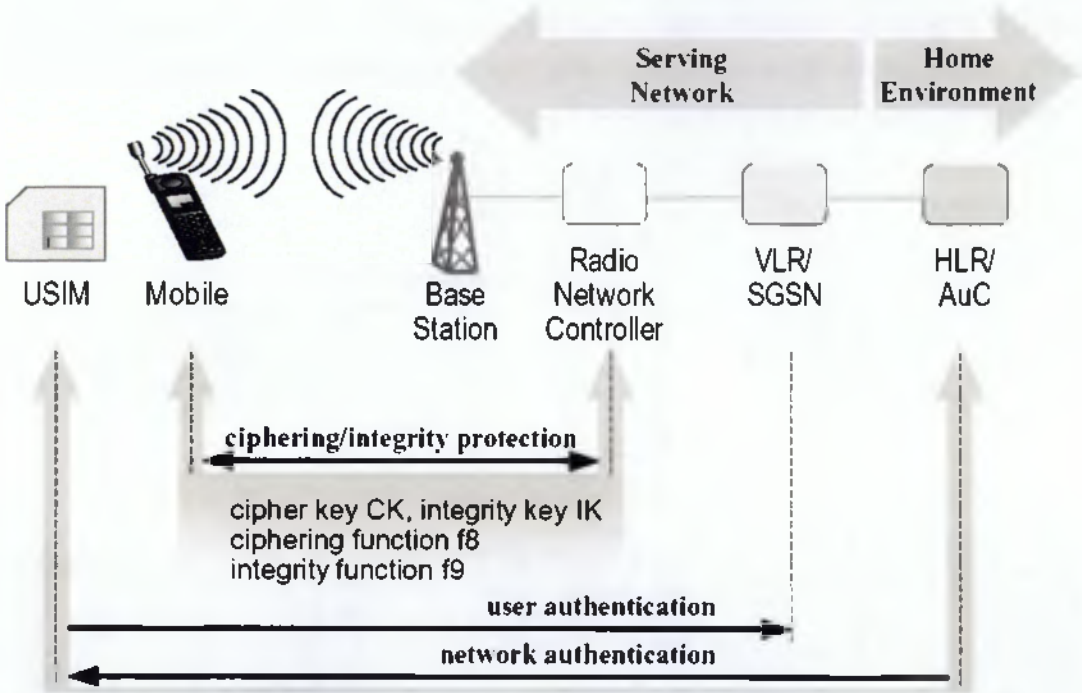
- Ασφάλεια δικτύου πρόσβασης
- Ασφάλεια πεδίου δικτύου
- Ασφάλεια πεδίου χρήστη
- Ασφάλεια πεδίου εφαρμογών
- Διαφάνεια και διαμόρφωση ασφάλειας

2.10.1. Ασφάλεια δικτύου πρόσβασης

Περιλαμβάνει:

- Εμπιστευτικότητα ταυτότητας χρήστη User
- Identification Confidentiality (UIC)

- Αυθεντικοποίηση και συμφωνία κλειδιού- Authentication and Key Agreement (AKA)
- Εμπιστευτικότητα δεδομένων- Data Confidentiality (DC)
- Ακεραιότητα δεδομένων-Data Integrity (DI)



Σχήμα 23 : Αρχιτεκτονική Ασφάλειας UMTS

2.10.2. Πιστοποίηση και συμφωνία χρήσης κλειδιών Authentication and Key Agreement (AKA)

Το HE/AUC του συνδρομητή και η κάρτα του (USIM) μοιράζονται τα ίδια:

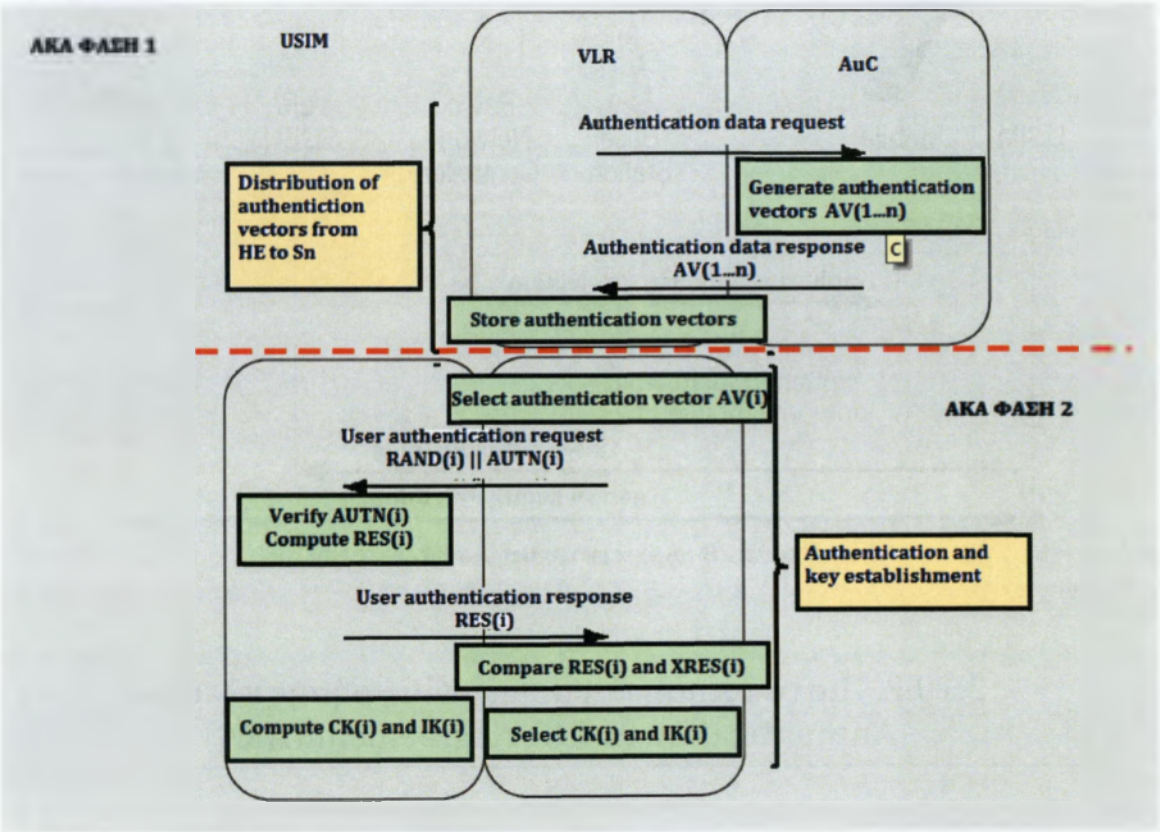
- K : μυστική κλείδα ειδική για κάθε χρήστη
- f1,f2 : συναρτήσεις μηνύματος πιστοποίησης
- f3,f4,f5 : συναρτήσεις δημιουργίας κλειδιών

ΑΚΑ ΦΑΣΗ 1: Δημιουργία Ανυσμάτων Πιστοποίησης.

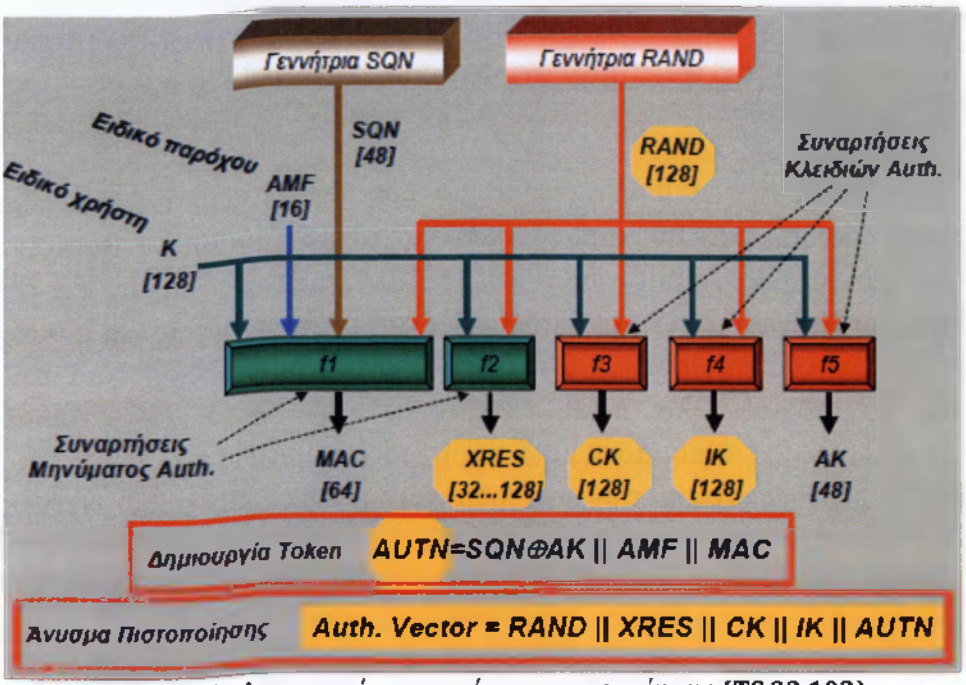
Με την λήψη αιτήματος αποστολής δεδομένων πιστοποίησης από ένα Serving Network, το HE/AUC δημιουργεί ένα array από n ανύσματα πιστοποίησης, που το καθένα αποτελείται από 5 συνιστώσες : RAND(i)||XRES(i)||CK(i)||IK(i)||AUTN(i). Αυτό το array ακολούθως αποστέλλεται στο αιτών SN.

ΑΚΑ ΦΑΣΗ 2 : Συμφωνία Πιστοποίησης και κλειδιών.

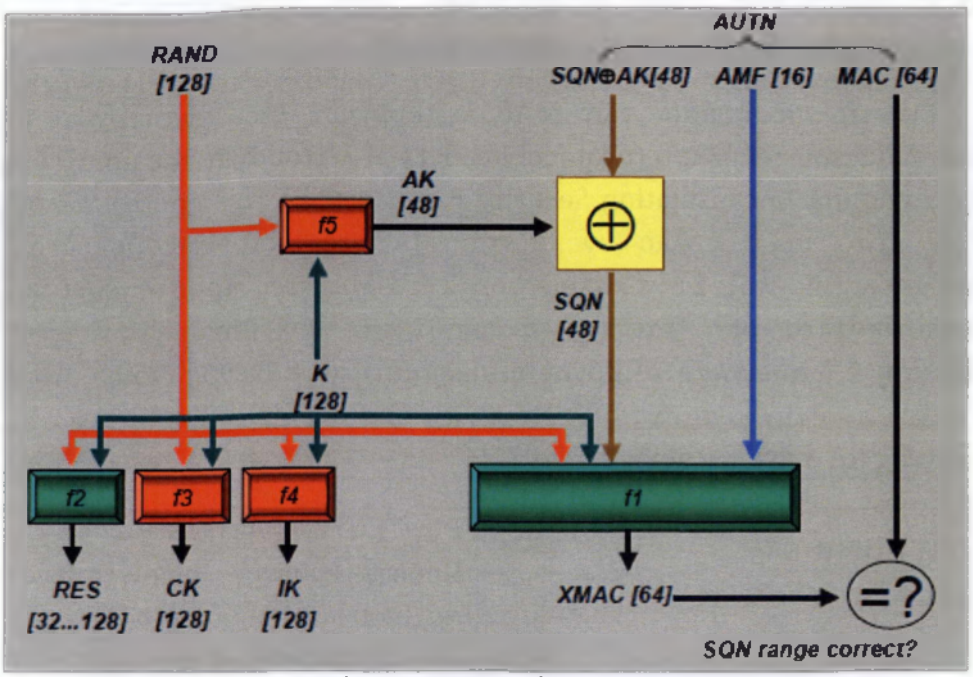
Το SN ανταποκρινόμενο σε μια από τις οντότητες του (VLR ή SGSN) επιλέγει το επόμενο άνυσμα πιστοποίησης (από το διατεταγμένο array) και αποστέλλει τα RAND(i), AUTN(i) στον χρήστη (συνδρομητή). Η USIM ελέγχει αν το AUTN(i) είναι αποδεκτό (δηλ. πιστοποιεί αν είναι έγκυρο το HE/AC) και αν ναι, παράγει και αποστέλλει την RES(i) στο SN (για την δική του πιστοποίηση RES(i)=XRES(i)). Κατόπιν υπολογίζει τα κλειδιά CK, IK που χρησιμοποιούνται στην συνέχεια για την κρυπτογράφηση των δεδομένων και την ακεραιότητα της σηματοδοσίας στην ασύρματη διεπαφή.



Σχήμα 24 : Φάσεις ΑΚΑ



Σχήμα 25 : Δημιουργία ανυσμάτων πιστοποίησης (TS 33.102)



Σχήμα 26 : Δραστηριότητες Πιστοποίησης στην USIM (TS 33.102)

Διαδικασία **AKA** γίνεται όταν:

- Εγγράφεται ο χρήστης σε ένα SN
- Μετά από αίτημα εξυπηρέτησης
- Μετά από αίτημα Location Update
- Μετά από αίτημα Σύνδεσης
- Μετά από αίτημα Αποσύνδεσης
- Μετά από αίτημα Connection re-establishment

2.10.3. Περιγραφή των δια-δικτυακών και ενδο-δικτυακών μηχανισμών ασφάλειας του UMTS.

Η ανταλλαγή των μηνυμάτων σηματοδοσίας μεταξύ των στοιχείων του κεντρικού δικτύου στα συστήματα GSM και UMTS έκδοσης 4 βασίζεται στο πρωτόκολλο Mobile Application Part (MAP). Για παράδειγμα, τα στοιχεία (profiles) των συνδρομητών, οι διαδικασίες αυθεντικοποίησης, και η διαχείριση της κινητικότητας (mobility) των χρηστών διεκπεραιώνεται μέσω του MAP. Τυπικά, το πρωτόκολλο MAP εκτελείται πάνω από τη στοίβα(stack) πρωτοκόλλων SS7. Για παράδειγμα, η σηματοδοσία μεταξύ του SGSN, του GGSN, της βάσης με τα στοιχεία των συνδρομητών (Home Subscriber Server, HSS) αλλά και του κέντρου διεκπεραίωσης SMS, βασίζεται αποκλειστικά σε SS7. Η 3GPP έχει ορίσει ένα μηχανισμό για την προστασία του MAP πρωτοκόλλου στο επίπεδο εφαρμογής (application layer). Το πρωτόκολλο MAP μπορεί επίσης να προστατευτεί στο επίπεδο δικτύου(network layer), όταν η μεταφορά των δεδομένων βασίζεται στο πρωτόκολλο IP. Όμως, η προστασία του MAP στο επίπεδο εφαρμογής είναι υποχρεωτική, όταν απαιτείται δια-δικτύωση (interworking) με δίκτυα που βασίζονται σε SS7.

Για την προστασία των MAP λειτουργιών έχει αναπτυχθεί μια νέα επικεφαλίδα πρωτοκόλλου (protocol header). Η λειτουργιά της μοιάζει με αυτή του μηχανισμού Encapsulating Security Payload(ESP) του πρωτοκόλλου IPsec. Το νέο αυτό πρωτόκολλο ονομάζεται MAP sec και λειτουργεί σε τρείς καταστάσεις (modes). Στην κατάσταση 2, το MAP sec προστατεύει τόσο την εμπιστευτικότητα όσο και την ακεραιότητα των μηνυμάτων, ενώ στην κατάσταση 1 διασφαλίζεται μόνον η ακεραιότητα. Κανενός είδους προστασία δεν παρέχεται στην κατάσταση λειτουργίας 0. Η δομή των μηνυμάτων MAP sec παρουσιάζεται στο ακόλουθο Σχήμα 27:

SECURITY HEADER Επικεφαλίδα ασφάλειας	PROTECTED PAYLOAD Προστατευμένο περιεχόμενο του αρχικού MAP μηνύματος

Σχήμα 27 : Η δομή των μηνυμάτων MAP sec

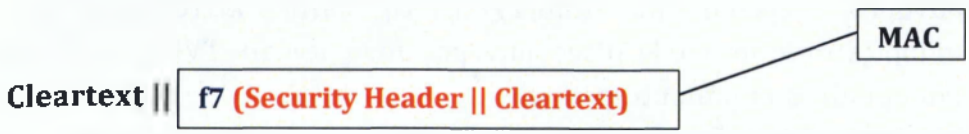
Πιο συγκεκριμένα, και στις 3 καταστάσεις ασφαλείας η επικεφαλίδα μεταδίδεται απροστάτευτη (cleartext). Η κατάσταση ασφαλείας 2(protection mode 2) παρέχει εμπιστευτικότητα και ακεραιότητα. Τα περιεχόμενα του αρχικού MAP μηνύματος κρυπτογραφούνται σχηματίζοντας το protected payload τμήμα του τελικού MAPsec μηνύματος. Η κατάσταση ασφαλείας 1(protected mode 1) παρέχει υπηρεσίες ακεραιότητας και αυθεντικότητας του αρχικού μηνύματος (integrity and authenticity). Για το σκοπό αυτό, ένας κωδικός αυθεντικοποίησης μηνύματος (MAC) υπολογίζεται σε ολόκληρο το αρχικό MAP μήνυμα (original message) συμπεριλαμβανομένης της επικεφαλίδας

ασφαλείας και κατόπιν συμπεριλαμβάνεται στο protected payload α του τελικού μηνύματος MAPsec.

Το MAC στην κατάσταση ασφαλείας 2 υπολογίζεται στην επικεφαλίδα ασφαλείας και στο ήδη κρυπτογραφημένο περιεχόμενο του αρχικού MAP μηνύματος πριν συμπεριληφθεί στο protected payload τμήμα του τελικού MAPsec μηνύματος. Αντίθετα, η κατάσταση ασφαλείας 0 (protected mode 0) δεν προσφέρει κανενός είδους προστασία και κατά συνέπεια, το protected payload τμήμα του MAPsec μηνύματος είναι ακριβώς ίδιο με το αρχικό MAP μήνυμα. Παρόλα τα παραπάνω είναι αναγκαίο να υπογραμμιστεί ότι θα πρέπει να ενσωματώσουν το συγκεκριμένο πρωτόκολλο ασφαλείας στο δίκτυο κορμού τους. Στο ενδιάμεσο, οι επιτιθέμενοι θα έχουν την ευκαιρία να εκμεταλλευτούν το γεγονός ότι το MAPsec δεν μπορεί να εφαρμοστεί όταν και οι δύο πάροχοι δεν το υποστηρίζουν στα στοιχεία του δικτυακού τους κορμού. Επιπλέον, για λόγους απόδοσης, μόνο οι σημαντικότερες MAP λειτουργίες (μηνύματα) προστατεύονται, όπως για παράδειγμα, η μεταφορά δεδομένων αυθεντικοποίησης (authentication data transfer). Διαφορετικά επίσης στοιχεία μιας MAP λειτουργίας μπορεί να προστατεύονται από διαφορετικές MAP καταστάσεις ασφαλείας (protection modes).

Protection Mode 1

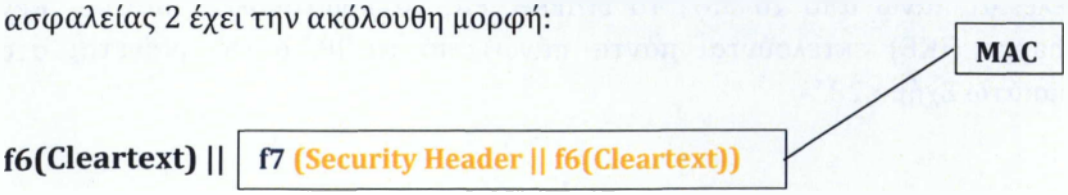
Το protected payload του Secured MAP μηνύματος έχει την ακόλουθη μορφή:



Η συνάρτηση ακεραιότητας f7 function εξασφαλίζει την αυθεντικότητα της πηγής του μηνύματος και την ακεραιότητα του. Το κλειδί ακεραιότητας(integrity key) ορίζεται κάθε φορά από την ισχύουσα SA. Το MAC έχει 32 bits.

Protection Mode 2

Το protected payload του Secured MAP μηνύματος στην κατάσταση ασφαλείας 2 έχει την ακόλουθη μορφή:



Η εμπιστευτικότητα επιτυγχάνεται κρυπτογραφώντας το Cleartext με τη βοήθεια της συνάρτησης f6. Το κλειδί κρυπτογράφησης (secret key) ορίζεται κάθε φορά από την ισχύουσα SA και το διάνυσμα αρχικοποίησης (Initilization Vector, IV). Το μήκος του ciphertext είναι ίδιο με το μήκος του Cleartext.

Η επικεφαλίδα ασφαλείας για το protection Mode 0 αποτελείται από τα ακόλουθα στοιχεία:

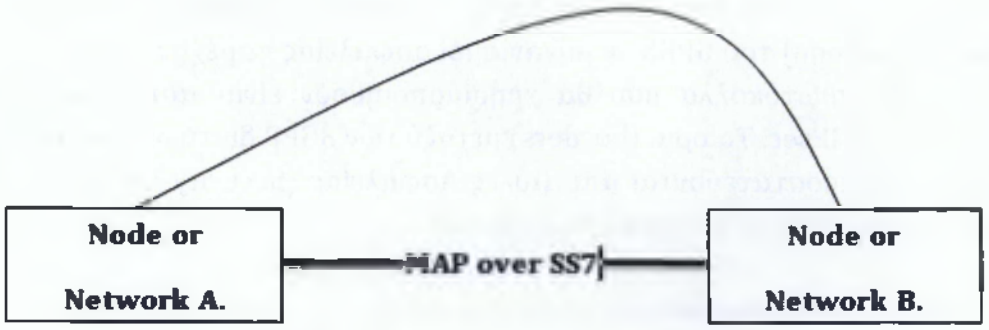
Security Header = SPI || Original Component Id

Επιπλέον, για τις καταστάσεις ασφαλείας 1 και 2, η επικεφαλίδα ασφαλείας έχει την ακόλουθη μορφή:

Security Header = SPI || Original Component Id || TVP || NE-Id || Prop

- **Security Parameters Index (SPI):** Το SPI είναι μια τυχαία τιμή μήκους 32-bit, η οποία χρησιμοποιείται σε συνδυασμό με το πεδίο Destination PLMN-Id με σκοπό να αναγνωρίζεται μοναδικά μια MAPsec SA.
- **Destination PLMN-Id:** Είναι το ID number του λαμβάνοντος (receiving) PLMN (Δηλαδή, ο συνδυασμός των κωδικών MCC και MNC του δικτύου που ανήκει ο λήπτης).
- **Original Component Id:** Αναγνωρίζει μοναδικά τον τύπο της πληροφορίας (π.χ. invoke, result, error) που εξασφαλίζει από το MAPsec μήνυμα.
- **TVP:** Χρησιμοποιείται για προστασία από επανεκπομπή (Replay protection) και είναι μια χρονοσφραγίδα (time stamp) μήκους 32 bit. Το λαμβανόμενο δίκτυο θα αποδεχτεί τη MAP λειτουργία που προσδιορίζεται από το MAPsec μήνυμα μόνο αν το TVP ανήκει σε προκαθορισμένο παράθυρο χρόνου.
- **NE-Id Proprietary Field (Prop):** το πρώτο χρησιμοποιείται για την ανάγνωση του NE που αποστέλλει το μήνυμα, ενώ το δεύτερο για τη δημιουργία διαφορετικών διανυσμάτων αρχικοποίησης (Initialization Vectors, IV – προς χρήση με τις συναρτήσεις f6 και f7) που αντιστοιχούν σε διαφορετικά MAP μηνύματα, τα οποί όμως αφορούν την ίδια TVP περίοδο.

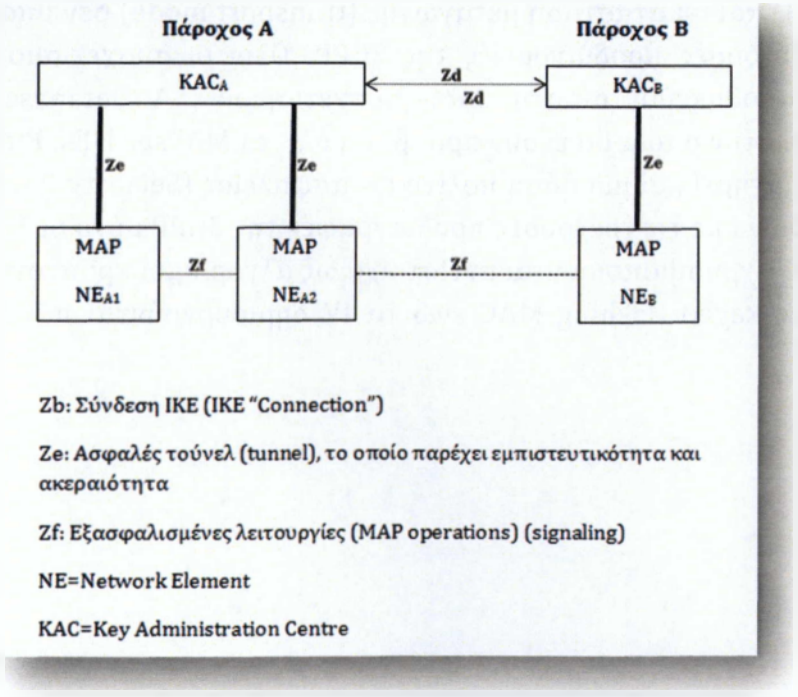
Τα διανύσματα αρχικοποίησης αποτελούνται από τα πεδία TVP, NE-Id και Prop συμπληρωμένα (padded) με το bit 0. Επιπλέον, ενώ τυπικά το MAP εκτελείται πάνω από το SS7, το MAPsec και το πρωτόκολλο Internet Key Exchange (IKE) εκτελούνται πάντα πάνω από τα IP, όπως φαίνεται στο παρακάτω Σχήμα 28.



Σχήμα 28 : MAPsec Key management over IP

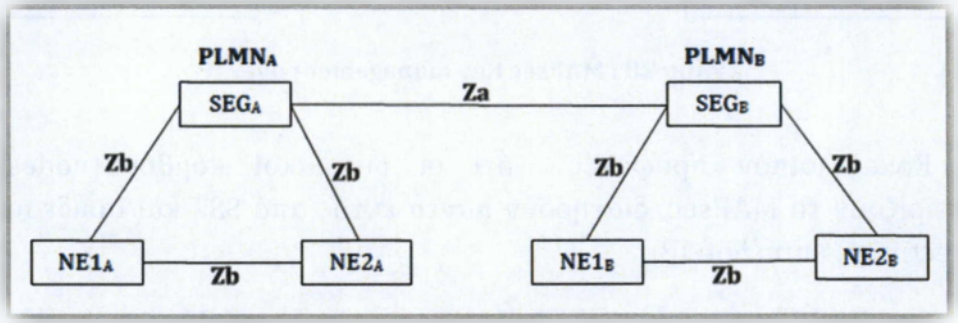
Είναι λοιπόν προφανές ότι οι δικτυακοί κόμβοι (nodes) που υποστηρίζουν το MAPsec, διατηρούν πάντα εκτός από SS7 και συνδεσιμότητα (connectivity) επιπέδου IP.

Στη 3GPP αρχιτεκτονική, το MAPsec τυπικά μεταξύ των δικτύων δύο διαφορετικών παρόχων και όχι μεταξύ MAP οντοτήτων. Οι απαραίτητες MAPsec-SAs μεταξύ δικτύων διαφορετικών παρόχων είναι προϊόν διαπραγμάτευσης μεταξύ των αντίστοιχων Κέντρων Διαχείρισης Κλειδιών(Key Administration Centers, KAC) των δικτύων, όπως παρουσιάζεται στο παρακάτω Σχήμα 29. Οι ίδιες συσχετίσεις ασφάλειας (Security Associations, SA), δηλαδή τα προϊόντα διαπραγμάτευσης μεταξύ των αντίστοιχων KACs, χρησιμοποιούνται από όλες τις MAP οντότητες των δύο δικτύων.



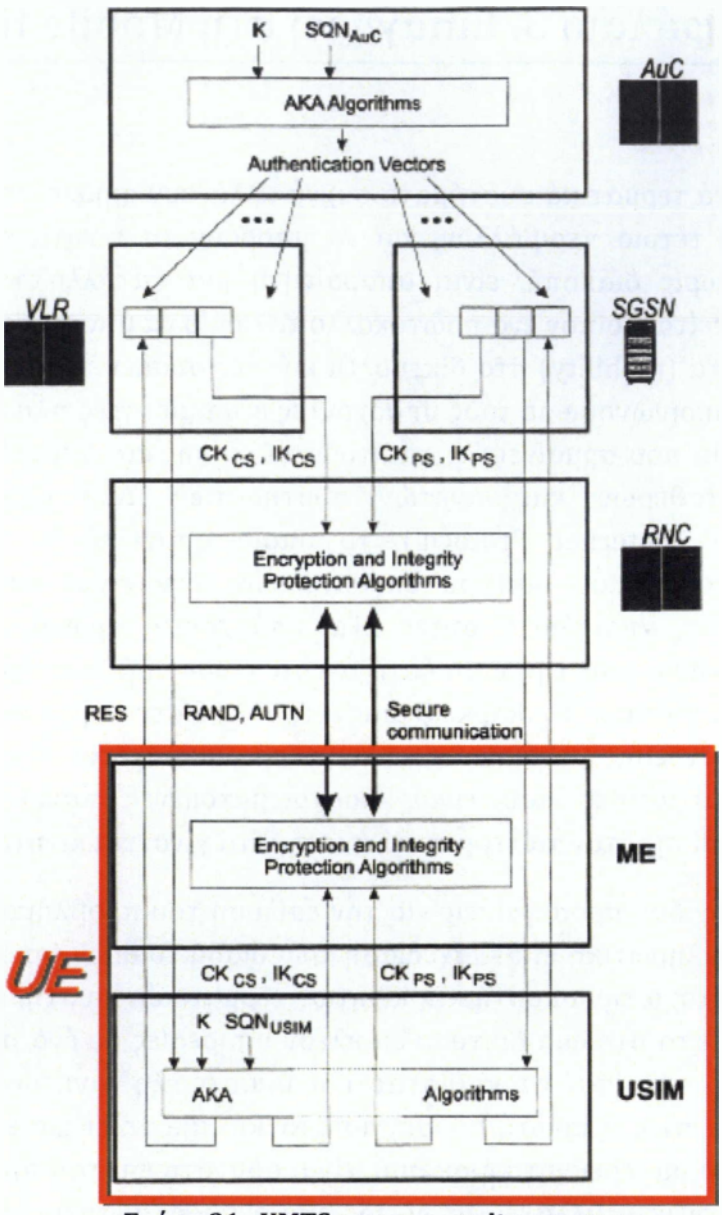
Σχήμα 29 : Οι Security Associations χρησιμοποιούνται από όλες τις MAP οντότητες των δύο δικτύων.

Από την άλλη πλευρά, για τις IP δικτυακές οντότητες, όπως είναι ο κορμός (backbone) του GPRS, οι μηχανισμοί ασφαλείας παρέχονται στο επίπεδο δικτύου. Τα πρωτόκολλα που θα χρησιμοποιηθούν είναι αυτά της σουίτας πρωτοκόλλων IPsec. Τα όρια (borders) μεταξύ των 3GPP δικτύων διαφορετικών παρόχων θα προστατεύονται από Πύλες Ασφαλείας (Security Gateways, SEG), όπως περιγράφεται στο παρακάτω Σχήμα 30.



Σχήμα 30 : Τα Za & Zb αναπαριστούν IKE και ESP SAs μεταξύ των στοιχείων του δικτύου

Με αυτόν τον τρόπο, όλη η κίνηση δεδομένων και σηματοδοσίας μεταξύ διαφορετικών IP υποσυστημάτων θα διέρχεται μέσω μιας SEG πριν εισέλθει ή εγκαταλείψει το συγκεκριμένο τομέα ασφαλείας (security domain). Η ασφάλεια των δικτυακών IP υποσυστημάτων (Network Domain Security/IP)υποστηρίζει μόνο IPsec-SAs κατάστασης διόδου (tunnel mode), Encapsulation Security Payload (ESP)και Main mode phase I. Αντίθετα, ο μηχανισμός Authentication Header (AH) και η κατάσταση μεταγωγής (transport mode) δεν υποστηρίζονται από τις τρέχουσες προδιαγραφές της 3GPP. Όλοι οι συσχετισμοί ασφαλείας (SAs) θα αποθηκεύονται στη βάση συσχετισμών (SA Database, SAD) των KACs/SEGs, στην οποία θα έχουν πρόσβαση όλα τα MAPsec NEs. Επιπλέον, κάθε KAC/SEG διατηρεί και μια βάση πολιτικών ασφαλείας (Security Policy Database, SPD). Σύμφωνα με τις τρέχουσες προδιαγραφές της 3GPP μόνο οι Triple DES και HMAC-SHA-1 χρησιμοποιούνται αντίστοιχα ως αλγόριθμοι κρυπτογράφησης και δημιουργίας keyed-Hashing MAC ενώ τα IV δημιουργούνται πάντα με τυχαίο τρόπο.



Σχήμα 31 : UMTS access security summary

Κεφάλαιο 3. Εισαγωγή στη Mobile IP

Τα κινητά τερματικά συστήματα συχνά αλλάζουν σημείο πρόσδεσης στο δίκτυο. Σε ένα τέτοιο περιβάλλον, για να μπορούν τα κινητά τερματικά να λειτουργούν χωρίς διακοπή, είναι απαραίτητη μια κατάλληλη διαδικτυακή υποδομή. Απαιτείται λοιπόν ένα πρωτόκολλο το οποίο να μπορεί να υποστηρίξει την κινητικότητα (mobility) στο δίκτυο. Οι κινητές συσκευές πρέπει επίσης να μπορούν να επικοινωνούν με τους υπάρχοντες εξυπηρετητές πληροφοριών και αρχείων, πράγμα που σημαίνει ότι απαιτούνται επίσης και δυνατότητες για τη διασύνδεση σταθερών και κινητών συστημάτων. Δυστυχώς όμως, το πρωτόκολλο IP (Internet Protocol), το οποίο αποτελεί το σκελετό του υπάρχοντος παγκοσμίου δικτύου επικοινωνιών, δεν είναι αρκετό για να ικανοποιήσει τις απαιτήσεις αυτές. Τα υπάρχοντα πρωτόκολλα TCP/IP σχεδιάστηκαν κάτω από την παραδοχή ότι τα τερματικά συστήματα θα είναι σταθερά. Αν λοιπόν κατά τη διάρκεια μιας ενεργούς δικτυακής συνόδου ένα από τα άκρα της σύνδεσης μετακινηθεί, η σύνοδος διακόπτεται. Φυσικά, όλες οι διαδικτυακές υπηρεσίες που είναι διαστρωματομένες πάνω στο TCP/IP διακόπτονται επίσης όταν τα τερματικά συστήματα γίνονται κινητά.

Υπάρχουν δύο προσεγγίσεις για την επίλυση του προβλήματος αυτού. Η μία είναι η ολοκληρωτική επανασχεδίαση των διαδικτυακών πρωτοκόλλων με συγκεκριμένο στόχο την υποστήριξη κινητών τερματικών συστημάτων. Η άλλη είναι να παρέχει το στρώμα δικτύου επιπλέον υπηρεσίες με ένα συμβατό προς τα πίσω τρόπο και έτσι να καθίσταται η υποστήριξη κινητών τερματικών συστημάτων δυνατή. Η πρώτη προσέγγιση, αν και αποτελεί μια ενδιαφέρουσα δυνατότητα από μια ερευνητική σκοπιά, είναι αδύνατη επί του πρακτέου αφού θα απαιτούσε ριζικές αλλαγές στην ήδη υπάρχουσα αναπτυγμένη δικτυακή υποδομή. Η δεύτερη προσέγγιση λοιπόν είναι αυτή που εστιάζει το ενδιαφέρον της εξέτασης που θα επακολουθήσει.

Για να διασφαλιστεί η λειτουργία με την υπάρχουσα υποδομή, ο χειρισμός της κινητικότητας πρέπει να είναι τελείως διάφανος στα πρωτοκολλά και στις εφαρμογές που τρέχουν σε σταθερά (ενσύρματα) τερματικά (stationary hosts). Με άλλα λόγια από την πλευρά ενός σταθερού τερματικού συστήματος, ένα κινητό τερματικό (mobile host) θα πρέπει να εμφανίζεται σαν ένα οποιοδήποτε άλλο σταθερό τερματικό το οποίο είναι συνδεδεμένο στο Internet. Αυτό σημαίνει ότι ίδιες συμβάσεις ονοματοδοσίας (naming) και διευθυνσιοδότησης (addressing) σαν αυτές που έχουν αναπτυχθεί για σταθερά συστήματα πρέπει να εφαρμοστούν και στα κινητά συστήματα επικοινωνιών. Επιπρόσθετα, οποιεσδήποτε αλλαγές στο σημείο πρόσδεσης του κινητού στο

δίκτυο θα πρέπει να είναι εντελώς κρυμμένες από τα πρωτόκολλα και τις εφαρμογές που τρέχουν στα ενσύρματα συστήματα.

Θα δούμε λοιπόν ότι η κινητικότητα είναι στην ουσία ένα πρόβλημα μετάφρασης της διεύθυνσης (address translation problem) και ότι ο καλύτερος τρόπος για την επίλυσή του είναι η αντιμετώπισή του στο στρώμα δικτύου. Θα δούμε επίσης τις θεμελιώδεις υπηρεσίες που πρέπει να υποστηρίζονται στο στρώμα δικτύου για να μπορεί αυτό να φέρει εις πέρας το έργο της μετάφρασης της διεύθυνσης. Με βάση αυτά θα περιγραφεί μια αρχιτεκτονική στρώματος δικτύου η οποία καθιστά απρόσκοπτη την ολοκλήρωση της υποστήριξης κινητών τερματικών συστημάτων στην υπάρχουσα δομή του Internet.

3.1. Κινητικότητα

Η διαχείριση της κινητικότητας των κόμβων στο Internet είναι ένα θέμα που αντιμετωπίστηκε ερευνητικά στην προηγούμενη δεκαετία. Αναπτύχθηκαν πρωτόκολλα σηματοδοσίας τόσο για τη γενική περίπτωση περιαγωγής σε επισκεπτόμενα IP δίκτυα, όσο και για ειδικότερες περιπτώσεις μεταπομπής (handoff) σε γειτονικά IP υποδίκτυα, που ελέγχονται από την ίδια διαχειριστική αρχή. Οι λύσεις που δόθηκαν χρησιμοποιούν ανταλλαγή σηματοδοσίας για τον έλεγχο της δρομολόγησης πακέτων από τον κινητό IP κόμβο. Ο έλεγχος αυτός επιτυγχάνεται είτε με κατάλληλη διαμόρφωση των IP πακέτων είτε με την αλλαγή του μηχανισμού δρομολόγησης. Τα σημαντικότερα πρωτόκολλα είναι το Mobile IP για IPv4 δίκτυα και το Mobile IPv6 για IPv6 δίκτυα.

Στην ενότητα αυτή αναφέρεται επιγραμματικά ο τρόπος λειτουργίας της δρομολόγησης στα δίκτυα Internet, το πρόβλημα που δημιουργείται από την αλλαγή θέσης ενός κόμβου και οι απαιτήσεις που πρέπει να πληροί ένα πρωτόκολλο υποστήριξης κινητικότητας. Παρουσιάζεται η προδιαγραφή του πρωτοκόλλου Mobile IP, οι βασικές λειτουργικές μονάδες και ο τρόπος λειτουργίας του. Στη συνέχεια αναλύονται τα προβλήματα της λειτουργίας του και αναφέρονται οι προτεινόμενοι τρόποι αντιμετώπισης τους. Ακολουθεί η περιγραφή της υποστήριξης κινητικότητας για το πρωτόκολλο IPv6, μαζί με μια σύντομη παρουσίαση του IPv6. Περιγράφεται το Mobile IPv6 και αναδεικνύονται οι σημαντικότερες διαφορές του από το Mobile IPv4. Οι επόμενες παράγραφοι αναφέρονται σε σχήματα βελτιστοποίησης της τοπικής διαχείρισης κινητικότητας σε γειτονικές περιοχές, δηλαδή της μικρό-κινητικότητας (micro-mobility) είτε με τη λογική διατήρησης της κλασικής δρομολόγησης στο Internet είτε με αλλαγή των μηχανισμών δρομολόγησης. Οι υπόλοιπες εναλλακτικές λύσεις διαχείρισης κινητικότητας αναφέρονται στη

συνέχεια και περιλαμβάνουν λιγότερο δημοφιλείς προσεγγίσεις, όπως διαχείριση κινητικότητας σε ανώτερα επίπεδα (μεταφοράς ή εφαρμογής) ή κινητικότητα μέσω multicast. Τέλος επιχειρείται η αποτίμηση της κατάστασης σε ότι αφορά τα πρωτόκολλα σηματοδοσίας και τη διαχείριση κινητικότητας.

3.2. Ονοματοδοσία και διευθυνσιοδότηση στο Internet

Το Internet αποτελείται από ένα μεγάλο αριθμό επιμέρους δικτύων τα οποία μοιράζονται τον ίδιο χώρο διευθύνσεων και λειτουργούν χρησιμοποιώντας κοινά πρωτόκολλα όπως το TCP/IP. Μία θεμελιώδης αρχή της αρχιτεκτονικής του Internet είναι ότι κάθε τερματικό σύστημα (host) έχει μια μοναδική δικτυακή διεύθυνση διαμέσου της οποίας είναι προσβάσιμο από άλλα τερματικά συστήματα στο δίκτυο. Τα δεδομένα μεταφέρονται με τα μορφή αυτόνομων πακέτων τα οποία περιέχουν τόσο τη διεύθυνση προέλευσης όσο και τη διεύθυνση προορισμού. Για την επικοινωνία με ένα άλλο τερματικό, το τερματικό-πηγή το μόνο που χρειάζεται να γνωρίζει είναι η διεύθυνση προορισμού. Στη συνέχεια οι δρομολογητές του Internet συνεργάζονται για τη μεταφορά των πακέτων από τον κόμβο-πηγή στον κόμβο προορισμού.

Οι δρομολογητές (routers) διατηρούν μια εικόνα της τοπολογίας του δικτύου με τη μορφή πινάκων δρομολόγησης τους οποίους συμβουλεύονται για να πραγματοποιήσουν τη δρομολόγηση των πακέτων. Η διαδικασία της δρομολόγησης περιλαμβάνει τον έλεγχο της διεύθυνσης προορισμού που περιέχεται στο πακέτο και, ανάλογα με τα περιεχόμενα του πίνακα δρομολόγησης, την επιλογή του επόμενου δρομολογητή στον οποίο πρέπει να αναμεταδοθεί το πακέτο (store and forward). Κάθε δρομολογητής κατά μήκος της διαδρομής από τον κόμβο-πηγή στον κόμβο-προορισμό επαναλαμβάνει την παραπάνω διαδικασία μέχρι τελικά το πακέτο να παραδοθεί στο τερματικό του προορισμού.

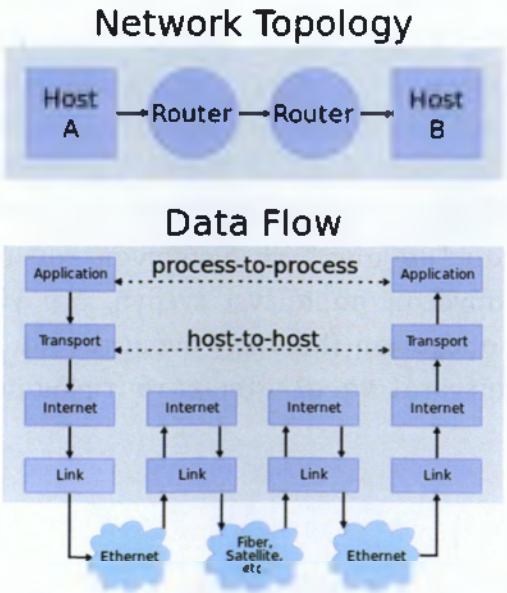
Αν οι διευθύνσεις των τερματικών αντιμετωπίζονταν σαν ενιαία αναγνωριστικά (flat identifiers), τότε θα απαιτούνταν από τους δρομολογητές να διατηρούν πληροφορίες δρομολόγησης για κάθε τερματικό. Προφανώς κάτι τέτοιο δεν είναι εφικτό δεδομένου του μεγάλου αριθμού τερματικών που συνδέονται στο Internet. Μία απλή λύση είναι επιλογή ιεραρχικής δομής για τις χρησιμοποιούμενες διευθύνσεις. Η ιεραρχική διευθυνσιοδότηση είναι απαραίτητη αν η αρχιτεκτονική δρομολόγησης είναι κλιμακωτή, όπως για παράδειγμα στο Internet όπου χρησιμοποιείται ένα πολλαπλών επιπέδων ιεραρχικό μοντέλο διευθυνσιοδότησης.

3.2.1. Διευθυνσιοδότηση (Addressing) στο Internet

Σε κάθε τερματικό στο internet ανατίθεται μια μοναδική διεύθυνση των 32-bit (διεύθυνση IP) η οποία αποτελείται από δύο μέρη: την ταυτότητα-δικτύου (network-id) και την ταυτότητα-τερματικού (host-id). Οι διευθύνσεις IP αναπαριστώνται χρησιμοποιώντας τη σημειογραφία τελείας όπου κάθε οκτάδα αναπαριστάται ως αριθμός (στο δεκαδικό σύστημα) και οι τελείες χρησιμοποιούνται ως διαχωριστικά των οκτάδων.

Σύμφωνα με το υπάρχον καθεστώς διευθυνσιοδότησης στο Internet, οι δρομολογητές χρειάζεται να διατηρούν πληροφορίες τοπολογίας δικτύου μόνο για κάθε ξεχωριστό υποδίκτυο. Αυτό σημαίνει ότι μόνο το μέρος ταυτότητας-δικτύου της διεύθυνσης προορισμού χρησιμοποιείται για τη δρομολόγηση. Αν και η ιεραρχική διευθυνσιοδότηση κάνει τη δρομολόγηση απλή και εύκολη στο χειρισμό, δημιουργεί συγκεκριμένους περιορισμούς στη χρησιμοποίηση των διευθύνσεων. Μία διεύθυνση με ιεραρχική δομή μπορεί να χρησιμοποιηθεί μόνο μέσα στο πεδίο ορισμού της. Για παράδειγμα, μία διεύθυνση στο Internet έχει νόημα μόνο όσο το τερματικό που τη χρησιμοποιεί παραμένει συνδεδεμένο στο δίκτυο που προσδιορίζεται από το μέρος της ταυτότητας-δικτύου της διεύθυνσης. Όταν το τερματικό μετακινηθεί σε ένα νέο δίκτυο, πρέπει να του χορηγηθεί μία νέα διεύθυνση, η οποία προέρχεται από το χώρο διευθύνσεων του νέου δικτύου. Συνεπώς:

Ένα κινητό τερματικό πρέπει να συσχετιστεί με μία νέα διεύθυνση όταν μετακινηθεί, ούτως ώστε να είναι δυνατή η δρομολόγηση των πακέτων που προορίζονται προς αυτό εντός του νέου δικτύου.

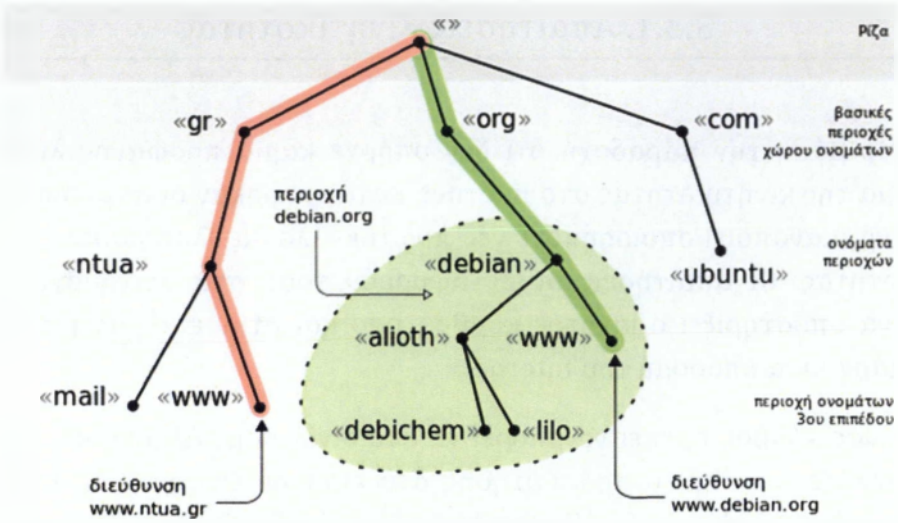


Σχήμα 32 : (Πάνω) Δύο συσκευές συνδεδεμένες μεταξύ τους μέσω δρομολογητών, (Κάτω) Η ροή των δεδομένων ανάμεσα στα διάφορα επίπεδα, της Σουίτας TCP/IP

3.2.2. Ονοματοδοσία (Naming)

Τα τερματικά αναγνωρίζονται επίσης στο δίκτυο από τα ονόματά τους (Host Names). Τα ονόματα αυτά είναι καθοριζόμενα από τους χρήστες ψευδώνυμα (συμβολοσειρές χαρακτήρων) τα οποία χρησιμοποιούνται για τη δήλωση των τερματικών συστημάτων. Μία σημαντική διάκριση μεταξύ ονομάτων και διευθύνσεων είναι ότι οι διευθύνσεις μπορεί να είναι συγκεκριμένες ανάλογα με το χρησιμοποιούμενο πρωτόκολλο (π.χ. IP διεύθυνση, CLNP διεύθυνση, IPX διεύθυνση, XNS διεύθυνση), αλλά τα ονόματα όχι. Τα ονόματα προσφέρουν ένα τρόπο αναφοράς από τις εφαρμογές στις οντότητες του δικτύου, χωρίς να χρειάζεται οι εφαρμογές αυτές να γνωρίζουν τίποτα επιπλέον για το υποκείμενο πρωτόκολλο δικτύου που χρησιμοποιείται. Κάτι τέτοιο είναι πολύ χρήσιμο αφού για τους χρήστες είναι πολύ πιο εύκολο να χρησιμοποιούν και να θυμούνται ονόματα σε σχέση με τις δύσχρηστες διευθύνσεις δικτύου.

Μολονότι λοιπόν οι εφαρμογές αναφέρονται στα τερματικά συστήματα με ονόματα, όταν τα πακέτα διακινούνται διαμέσου του Internet κάθε ένα από αυτά πρέπει να περιέχει μία IP διεύθυνση του κόμβου προορισμού. Αυτό γίνεται διότι οι δρομολογητές στο Internet δεν "καταλαβαίνουν" τα ονόματα, παρά μόνο μπορούν και μεταφράζουν διευθύνσεις. Απαιτείται συνεπώς ένας μηχανισμός μετασχηματισμού των ονομάτων των τερματικών σε διευθύνσεις. Για να εξυπηρετηθεί αυτό το τεράστιο και ραγδαία επεκτεινόμενο σύνολο ονομάτων, αναπτύχθηκε στο Internet ένας αποκεντρωμένος μηχανισμός ονοματοδοσίας ο οποίος λέγεται "Domain Name System" (DNS). Το σύστημα DNS αποθηκεύει την αντιστοιχία μεταξύ ονόματος και διεύθυνσης σε μια κατανεμημένη δομή δεδομένων και έτσι η εύρεση της διεύθυνσης ενός τερματικού αποτελεί ουσιαστικά μία λειτουργία εύρεσης καταλόγου (directory lookup operation). Όταν λοιπόν δύο τερματικά χρειάζεται να επικοινωνήσουν στο Internet, ο κόμβος-πηγή εκτελεί μια DNS αναζήτηση για να προμηθευτεί τη διεύθυνση του κόμβου-προορισμού και στη συνέχεια ξεκινά μια διαδικασία εγκατάστασης σύνδεσης. Κατά τη διάρκεια της εγκατάστασης της σύνδεσης κάθε άκρο της σύνδεσης λαμβάνει και "μαθαίνει" τη διεύθυνση του άλλου άκρου. Για όσο διάστημα λοιπόν η σύνδεση παραμένει ενεργή, δεν γίνονται επιπλέον DNS αναζητήσεις αφού η συσχέτιση (binding) ονόματος και διεύθυνσης θεωρείται στατική και δεν αναμένεται να αλλάξει κατά τη διάρκεια της ύπαρξης της σύνδεσης.



Σχήμα 33 : Ιεραρχική οργάνωση χώρου ονομάτων DNS - η Ελλάδα έχει ως βασική περιοχή ονομάτων το gr

3.3. Αλληλεπίδραση Κινητικότητας-Δρομολόγησης

Τα προβλήματα της αλληλεπίδρασης της κινητικότητας με τη δρομολόγηση έγκειται στο γεγονός ότι οι κινητοί κόμβοι με τη μετακινούνται μεταξύ IP δικτύων δεν μπορούν να επικοινωνήσουν με την ίδια IP διεύθυνση. Το πρόθεμα δικτύου που χρησιμοποιείται είναι διαφορετικό κάθε φορά. Το πρωτόκολλο IP δε σχεδιάστηκε για υποστήριξη κινητών κόμβων, οι οποίοι αλλάζουν θέσεις, ενώ έχουν ανοιχτές ενεργές συνδέσεις. Εάν ένας κόμβος επιθυμεί μα αλλάξει το σημείο προσάρτησης του στο δίκτυο, χωρίς να χάσει την ικανότητα επικοινωνίας, θα πρέπει να χρησιμοποιηθεί ένας από τους εξής μηχανισμούς:

Ο κόμβος πρέπει να αλλάζει την IP διεύθυνση του κάθε φορά που αλλάζει το σημείο προσάρτησης, έτσι ώστε η νέα IP διεύθυνση να ανήκει τοπολογικά στο νέο υποδίκτυο ή

Οι πληροφορίες δρομολόγησης προς τον συγκεκριμένο κόμβο πρέπει να διαδοθούν σε όλο το μηχανισμό δρομολόγησης του, έτσι ώστε τα πακέτα που προσδιορίζονται για τον κόμβο αυτό να μη δρομολογούνται τοπολογικά στο αντίστοιχο υποδίκτυο Internet.

Καμία από τις δυο αυτές εναλλακτικές λύσεις δεν είναι ικανοποιητική. Η πρώτη καθιστά αδύνατη τη διατήρηση των συνδέσεων επιπέδου μεταφοράς (κατά κανόνα TCP) όταν ο κόμβος αλλάζει τοποθεσία. Η δεύτερη έχει σοβαρά προβλήματα κλιμάκωσης, ειδικά με την αλματώδη αύξηση των κινούμενων υπολογιστικών συσκευών. Συνεπώς, χρειαζόταν μια πιο ριζοσπαστική λύση, η εγγενής υποστήριξη κινητών κόμβων στο επίπεδο δικτύου, δηλαδή στο IP.

3.3.1. Απαιτήσεις Κινητικότητας

Με βάση την παραδοχή ότι δεν υπήρχε καμιά προφανής λύση για το πρόβλημα της κινητικότητας στο Internet, καταγράφηκαν οι απαιτήσεις που θα έπρεπε να ικανοποιεί οποιοδήποτε νέο πρωτόκολλο θα υλοποιούσε υποστήριξη κινητικότητας. Οι απαιτήσεις αυτές αφορούν τόσο στις λειτουργίες που θα πρέπει να υποστηρίξει ο κινητός κόμβος, όσο και στην επίδραση που θα έχει στην υπάρχουσα υποδομή του Internet.

- Ένας κόμβος πρέπει να μπορεί να επικοινωνεί με άλλους κόμβους αφού αλλάξει το σημείο προσάρτησης στο επίπεδο ζεύξης (link layer), αλλά χωρίς ν αλλάζει η διεύθυνση του στο επίπεδο δικτύου (network layer), δηλαδή η IP διεύθυνση.
- Ο κινητός κόμβος πρέπει να μπορεί να επικοινωνεί με άλλους κόμβους οι οποίοι δεν υποστηρίζουν κατ' ανάγκη λειτουργίες αναγνώρισης και συνεργασίας με πρωτόκολλα κινητικότητας δεν πρέπει να απαιτούνται αλλαγές σε κόμβους ή δρομολογητές που δεν συμμετέχουν στο μηχανισμό κινητικότητας.
- Όλα τα μηνύματα που χρησιμοποιούνται για σηματοδοσία κινητικότητας πρέπει να πιστοποιούνται για λόγους ασφάλειας.
- Ο αριθμός και το μέγεθος των μηνυμάτων ελέγχου και σηματοδοσίας πρέπει να διατηρείται σε πολύ χαμηλά επίπεδα, αφού η σύνδεση ενός κινητού κόμβου με το Internet θα είναι κατά κανόνα ασύρματη, δηλαδή χαμηλής χωρητικότητας και με υψηλότερη πιθανότητα λάθους στην επικοινωνία σε σχέση με τα παραδοσιακά ενσύρματα δίκτυα.
- Θα πρέπει να αποφεύγεται η άσκοπη κατανάλωση ενέργειας (ανταλλαγή πολλών μηνυμάτων) εξαιτίας της τροφοδοσίας του κινητού κόμβου από μπαταρία.

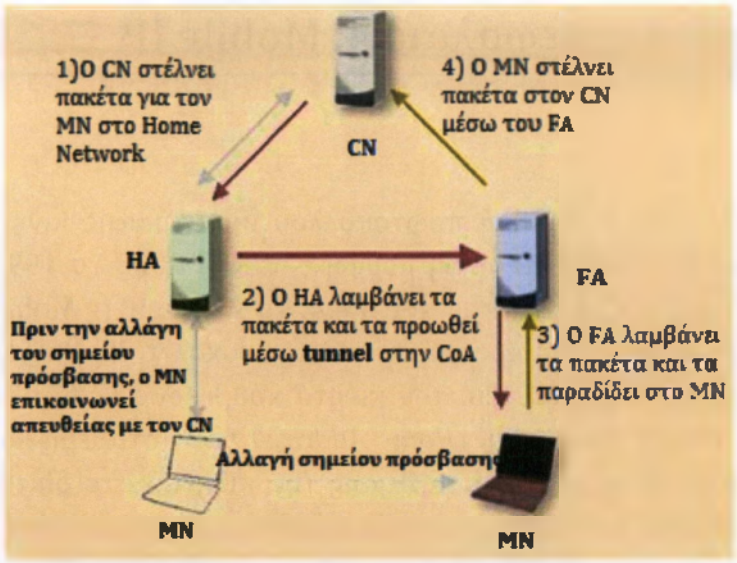
Η ύπαρξη του κινητού κόμβου όταν αλλάζει σημείο προσάρτησης ονομάζεται μεταπομπή(handoff).

Κεφάλαιο 4. Mobile IP

Η πρώτη προδιαγραφή πρωτοκόλλου υποστήριξης κινητικότητας από την IETF ήταν το Mobile IP με τη μορφή του RFC 2002 το 1996. Η τρέχουσα προδιαγραφή καθορίζεται από το RFC 3344. Το Mobile IP (ή Mobile IPv4 ή MIP ή MIPv4) έχει σχεδιαστεί ως προσθήκη στο πρωτόκολλο IP. Επιλύει το θέμα της κινητικότητας με τη χρήση από τον κινητό κόμβο δυο IP διευθύνσεων. Η μια διεύθυνση, η *Οικεία Διεύθυνση (Home Address)* είναι σταθερή και αναλλοίωτη, ανεξάρτητα από το σημείο προσάρτησης του κινητού στο δίκτυο. Αντιστοιχεί στην IP διεύθυνση που έχει ο κινητός κόμβος στο Οικείο Δίκτυο του (Home Network). Όπου και ανήκει διαχειριστικά. Χρησιμοποιείται ως διεύθυνση αναφοράς από τα ανώτερα στρώματα, π.χ. για την αναγνώριση TCP συνδέσεων. Η άλλη διεύθυνση, η *Διεύθυνση Μέριμνας (Care of Address)*, μεταβάλλεται σε κάθε σημείο προσάρτησης και μπορεί να θεωρηθεί ως η τοπολογικά σωστή διεύθυνση του κόμβου. Περιέχει το σωστό πρόθεμα δικτύου, αποδίδεται από τους εκάστοτε πράκτορες κινητικότητας στα επισκεπτόμενα Ξένα Δίκτυα (Foreign Networks) και προσδιορίζει το σημείο προσάρτησης του κόμβου ως προς την υπάρχουσα δικτυακή τοπολογία.

Η τοπολογία του δικτύου και οι λειτουργικές οντότητες του Mobile IP απεικονίζονται στο Σχήμα 34. Βασικές οντότητες της λειτουργίας του πρωτόκολλου είναι ο Κινητός Κόμβος (Mobile Node, MN), ο Οικείος Πράκτορας (Home Agent, HA) στο οικείο δίκτυο, ο Ξένος Πράκτορας (Foreign Agent, FA) στο επισκεπτόμενο ή ξένο δίκτυο και ο Ανταποκριτής Κόμβος (Correspondent Node, CN), ο οποίος είναι οποιοσδήποτε κόμβος στο Internet που θέλει να επικοινωνήσει με τον κινητό κόμβο. Η λειτουργία του πρωτοκόλλου Mobile IP περιγράφεται αναλυτικά στις παρακάτω παραγράφους.

Το Mobile IP απαιτεί την ύπαρξη ενός εξειδικευμένου κόμβου στο οικείο δίκτυο του κινητού κόμβου και συγκεκριμένα του οικείου πράκτορα. Ο Οικείος πράκτορας είναι ένας δρομολογητής επιφορτισμένος με λειτουργίες υποστήριξης κινητικότητας. Όταν ο κινητός βρίσκεται προσαρτημένος στο οικείο δίκτυο του, χρησιμοποιεί την οικεία του διεύθυνση και η δρομολόγηση των πακέτων που κατευθύνονται προς αυτόν πραγματοποιείται φυσιολογικά. Όταν ο κινητός κόμβος βρίσκεται προσαρτημένος σε κάποιο απομακρυσμένο (ξένο) δίκτυο, ο οικείος πράκτορας αναχαιτίζει όλα τα πακέτα που προορίζονται για την οικεία διεύθυνση του κινητού κόμβου και φροντίζει να παραδοθούν στο τρέχον σημείο προσάρτησης του κινητού κόμβου.



Σχήμα 34 : Τοπολογία λειτουργίας Mobile IP

Όταν ο κινητός κόμβος μετακινηθεί, του ανατίθεται μια νέα IP διεύθυνση (η διεύθυνση μέριμνας) την οποία πληροφορεί τον οικείο πράκτορα του. Η διεύθυνση μέριμνας είναι συνήθως η IP διεύθυνση του ξένου πράκτορα. Ο οικείος πράκτορας παραδίδει τα πακέτα που προορίζονται για τον κινητό κόμβο στη διεύθυνση μέριμνάς του. Η διαδικασία προώθησης των πακέτων από τον οικείο πράκτορα στον κινητό κόμβο προϋποθέτει ότι τα πακέτα θα μεταβληθούν με τέτοιο τρόπο ώστε η διεύθυνση προορισμού του πακέτου να είναι η διεύθυνση μέριμνας του κινητού κόμβου. Η τεχνική που χρησιμοποιείται είναι η ενθυλάκωση (encapsulation ή tunneling). Σύμφωνα με την τεχνική αυτή, ο οικείος πράκτορας κατασκευάζει και προσθέτει στο πακέτο μια IP επικεφαλίδα που περιέχει τη διεύθυνση μέριμνας ως διεύθυνση προορισμού. Η νέα αυτή επικεφαλίδα παρέχει όλη την πληροφορία δρομολόγησης που απαιτείται για να προωθηθεί το πακέτο στο τρέχον σημείο προσάρτησης του κινητού κόμβου. Όταν το πακέτο φθάσει στη διεύθυνση μέριμνας, πραγματοποιείται η αντίστροφη διαδικασία και το πρωτότυπο πακέτο αποθυλακώνεται (συνήθως από τον ξένο πράκτορα), επανεμφανίζεται η οικεία διεύθυνση προορισμού, και προωθείται στον κινητό κόμβο. Στη συνέχεια, το πακέτο φθάνει στον κινητό κόμβο με την ίδια μορφή που είχε στο οικείο δίκτυο και το επίπεδο μεταφοράς (TCP) δεν αντιλαμβάνεται καμιά διαφορά λόγω μετακίνησης.

4.1. Λειτουργικές αρχές

Ένας κινητός κόμβος έχει δύο διευθύνσεις, μια μόνιμη διεύθυνση κατοικίας και μια care-of address (CoA), η οποία συνδέεται με το δίκτυο του κινητού κόμβου που επισκέπτεται. Μια Mobile IP εφαρμογή περιλαμβάνει δύο είδη οντοτήτων:

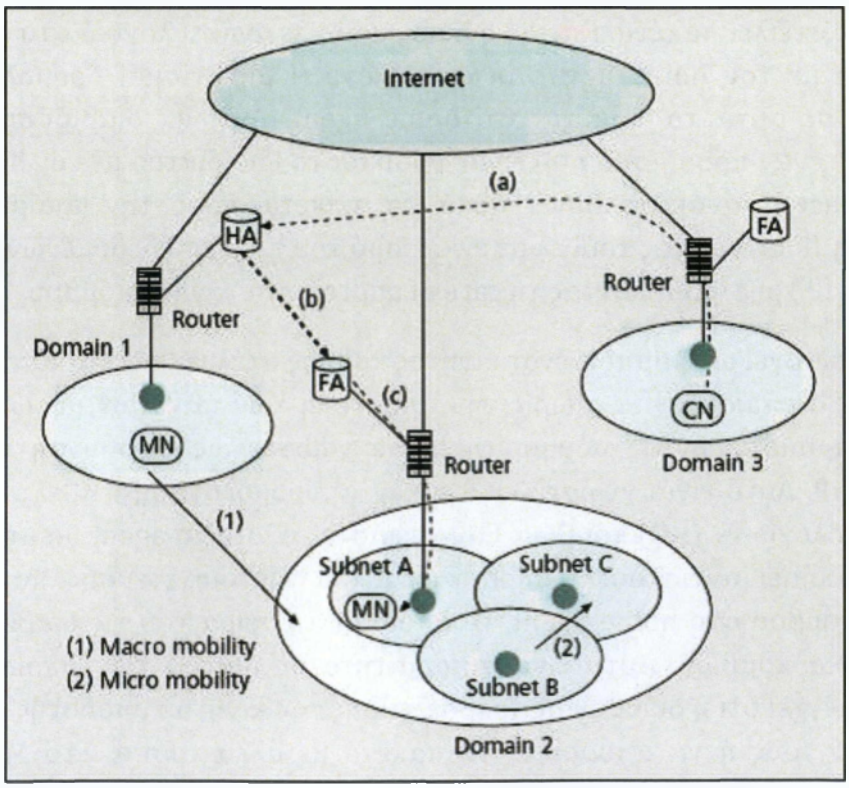
- Ένας home agent αποθηκεύει πληροφορίες σχετικά με τους κινητούς κόμβους των οποίων η μόνιμη διεύθυνση κατοικίας είναι στο δίκτυό του home agent.
- Ένας foreign agent αποθηκεύει πληροφορίες σχετικά με τους κινητούς κόμβους που επισκέπτονται το δίκτυό του. Foreign agents διαφημίζουν και care-of addresses, οι οποίες χρησιμοποιούνται από τη Mobile IP. Αν δεν υπάρχει foreign agent στο δίκτυο υποδοχής, η φορητή συσκευή θα πρέπει να φροντίσει να πάρει μια διεύθυνση και διαφημίζοντας τη, απευθύνεται με δικά της μέσα.

Ένας κόμβος που θέλει να επικοινωνήσει με τον κινητό κόμβο χρησιμοποιεί τη μόνιμη διεύθυνση κατοικίας του κινητού κόμβου ως διεύθυνση προορισμού για να της στείλει πακέτα. Επειδή η home address ανήκει λογικά στο δίκτυο που συνδέεται με τον home agent, οι φυσιολογικοί μηχανισμοί δρομολόγησης IP μπροστά σε αυτά τα πακέτα στο home agent. Αντί να διαβιβάσει αυτά τα πακέτα σε έναν προορισμό που είναι φυσικά στο ίδιο δίκτυο με τον home agent, ο home agent ανακατευθύνει αυτά τα πακέτα προς την απομακρυσμένη διεύθυνση IP μέσω ενός τούνελ με εγκλεισμό του πακέτου δεδομένων με μια νέα κεφαλίδα IP χρησιμοποιώντας τη care of address του κινητό κόμβου.

Όταν ενεργεί ως πομπός, ένας κινητός κόμβος στέλνει πακέτα απευθείας στο άλλο κόμβο επικοινωνίας, χωρίς την αποστολή των πακέτων μέσω του home agent, χρησιμοποιώντας μόνιμη τη home address ως διεύθυνση πηγής των πακέτων IP. Αυτό είναι γνωστό ως τριγωνική δρομολόγηση ή «βελτιστοποίηση των δρομολογίων» (RO) κόμβων. Εάν χρειαστεί, ο foreign agent θα μπορούσε να χρησιμοποιήσει αντιστροφή σηράγγων μέσω της διοχέτευσης πακέτων του κινητού κόμβου στο home agent, το οποίο με τη σειρά του τις διαβιβάζει στην επικοινωνία κόμβων. Αυτό είναι απαραίτητο σε δίκτυα των οποίων η πύλη routers ελέγχει ότι η διεύθυνση IP προέλευσης του κινητού υποδοχής ανήκει στο υποδίκτυο τους ή να απορρίψει το πακέτο με άλλο τρόπο. Στο Mobile IPv6 (MIPv6), η "αντιστροφή tunneling" είναι η προεπιλεγμένη συμπεριφορά, με την RO που είναι μια προαιρετική συμπεριφορά.

4.2. Υποστήριξη κινητικότητας (Mobility Support) στο IPv4

Η διεύθυνση IP αποτελείται από δύο μέρη: Το πρώτο καθορίζει το δίκτυο στο οποίο ανήκει ο κόμβος, ενώ το δεύτερο καθορίζει τον αριθμό του κόμβου στο υποδίκτυο. Έτσι λοιπόν το πρωτόκολλο IP αποφασίζει το επόμενο hop σύμφωνα με την IP διεύθυνση του προορισμού. Παράλληλα τα υψηλότερα επίπεδα, όπως το TCP, διατηρούν πληροφορίες για τις ενεργές συνδέσεις, αποτελούμενες από την τετράδα iP/port αφετηρίας προορισμού. Κατά συνέπεια, κατά την προσπάθεια υποστήριξης κινούμενων κόμβων στο Διαδίκτυο κάτω από τα υπάρχουσα πρωτοκόλλα, βρέθηκαν αντιμέτωποι με δύο αμοιβαία συγκρουόμενες απαιτήσεις: (1) ένας κινητός κόμβος πρέπει να αλλάξει τη διεύθυνση IP του όποτε αλλάζει το σημείο σύνδεσής του, έτσι ώστε τα πακέτα που προορίζονται στον κόμβο να καθοδηγούνται σωστά, (2) για να διατηρηθούν οι υπάρχουσες TCP συνδέσεις, ο κινητός κόμβος πρέπει να κρατήσει ίδια την διεύθυνση IP του, καθώς αλλαγή της IP διεύθυνσης θα τερματίσει την σύνδεση.



Σχήμα 35 : Κινητικότητα και Διαχείριση του Handover σε Ασύρματα Δίκτυα

Το Mobile IPv4, όπως προτάθηκε από την IETF, είναι σχεδιασμένο να λύνει αυτό το πρόβλημα επιτρέποντας σε κάθε κινητό κόμβο να έχει δύο IP

διευθύνσεις και διατηρώντας διαφανώς μία σύνδεση μεταξύ τους. Η μία διεύθυνση είναι η μόνιμη Home Address (HoA) που ορίζεται στο home network και χρησιμοποιείται στον καθορισμό endpoints επικοινωνίας. Η άλλη διεύθυνση, η λεγόμενη προσωρινή Careof-Address (CoA), αντιπροσωπεύει την τρέχουσα θέση του κόμβου. Οι κύριοι στόχοι του Mobile IP είναι να κατασταθεί η κινητικότητα διαφανής στα πρωτόκολλα υψηλότερων επιπέδων, με ταυτόχρονη ελαχιστοποίηση των αλλαγών στην υπάρχουσα υποδομή.

Αυτή η σύνδεση μεταξύ HoA και CoA διατηρείται από μερικούς εξειδικευμένους δρομολογητές γνωστούς ως mobility agents. Οι mobility agents είναι δύο τύπων – Home Agents (HA) και Foreign Agents (FA).

Ο home agent, ένας καθορισμένος δρομολογητής στο home network του κινητού κόμβου, διατηρεί την σύνδεση των διευθύνσεων σε ένα πίνακα, τον λεγόμενο mobility binging table, όπου κάθε εγγραφή ορίζεται από την τριάδα, < Home Address, Care of Address, Lifetime >. Το Σχήμα 36 παρουσιάζει έναν τέτοιο πίνακα. Σκοπός αυτού του πίνακα είναι να δέσει την Home Address ενός κινητού κόμβου με την Care of Address ώστε να διαβιβαστούν τα πακέτα αναλόγως.

Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

Σχήμα 36 : Mobility binding table

Οι foreign agents είναι ειδικευμένοι δρομολογητές στο foreign network όπου ο κινητός κόμβος βρίσκεται αυτήν την περίοδο. Ο foreign agent διατηρεί μία λίστα, την λεγόμενη visitor list. που περιέχει πληροφορίες για κινητούς κόμβους που επισκέπτονται αυτή την περίοδο το ξένο δίκτυο. Κάθε εγγραφή στη λίστα προσδιορίζεται από τετράδα < Home Address, Home Agent Address, MAC Address, Lifetime >, όπως φαίνεται στο Σχήμα 37.

Home Address	Home Agent Address	Media Address	Lifetime (in s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

Σχήμα 37 : Visitor List

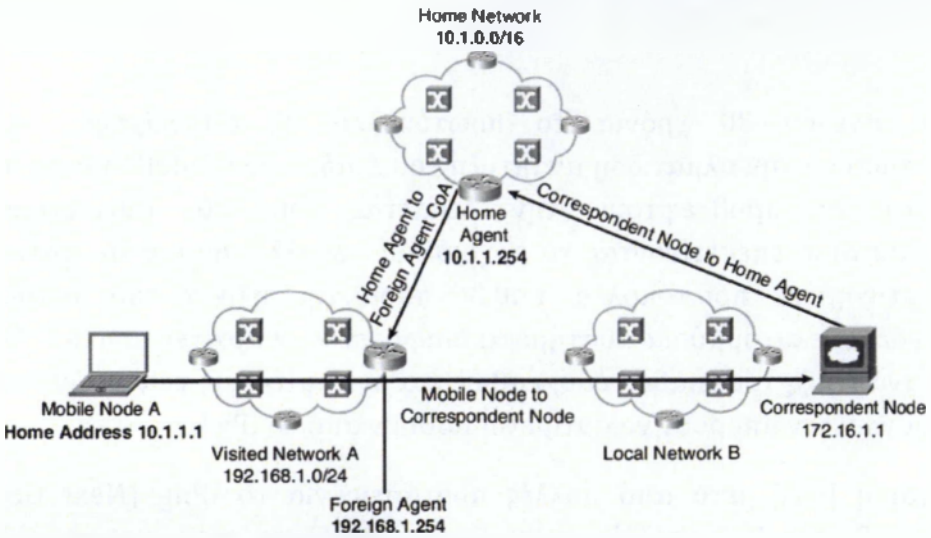
Σε ένα χαρακτηριστικό σενάριο, η CoA ενός κινητού κόμβου είναι η IP διεύθυνση του foreign agent. Μπορεί να υπάρξει και ένα άλλο είδος CoA, γνωστή ως collocated CoA, (cocoa), η οποία λαμβάνεται συνήθως από κάποιο εξωτερικό μηχανισμό διευθυνσιοδότησης, όπως ο Dynamic Host Configuration Protocol (DHCP).

Σύμφωνα λοιπόν με όλα αυτά η επικοινωνία με έναν κόμβο που βρίσκεται εκτός από το home network του γίνεται ως εξής:

- Όταν ο correspondent node (CN) θέλει να επικοινωνήσει με τον κινητό κόμβο (MN), στέλνει ένα πακέτο στη μόνιμη IP διεύθυνση (HoA) του κινητού κόμβου.
- Ο home agent αναχαιτίζει το πακέτο και ελέγχει το mobility binding table για να δει εάν ο κινητός κόμβος επισκέπτεται αυτήν την περίοδο κάποιο άλλο δίκτυο.
- Ο home agent βρίσκει την CoA του κινητού κόμβου και κατασκευάζει ένα νέο IP πακέτο που περιέχει την CoA του MN σαν διεύθυνση προορισμού του πακέτου. Το παλιό πακέτο εμφωλεύεται στο νέο και έπειτα δρομολογείται. Αυτή η διαδικασία ονομάζεται IP within IP encapsulation.
- Όταν το πακέτο φθάσει στο τρέχον δίκτυο του κινητού κόμβου, ο foreign agent εξάγει το αρχικό πακέτο και ανακαλύπτει την HoA του κινητού κόμβου. Συμβουλεύεται έπειτα την Visitor List για να δει εάν έχει κάποια εγγραφή για εκείνο τον κινητό κόμβο.
- Εάν υπάρχει εγγραφή ο foreign agent ανακτά την MAC διεύθυνση του κόμβου και του προωθεί το πακέτο.
- Όταν ο κινητός κόμβος θέλει να στείλει ένα μήνυμα σε έναν correspondent κόμβο, διαβιβάζει το πακέτο στον FA, το οποίο αναμεταδίδει στη συνέχεια στον CN χρησιμοποιώντας την κανονική IP δρομολόγηση.

Η τεχνική του Mobile IP έλυσε μεν ένα πολύ σημαντικό πρόβλημα, άφησε όμως πίσω της ένα πολύ σημαντικό θέμα, την τριγωνική δρομολόγηση (triangular routing). Η βασική ιδέα πίσω από την triangular routing είναι η ακόλουθη: Ένας κόμβος στέλνει ένα πακέτο σε έναν κινητό κόμβο που είναι στο

ίδιο δίκτυο. Τυχαίνει όμως ο home agent του κινητού κόμβου να είναι πολύ μακριά, στην άλλη ¨μεριά¨ του Διαδικτύου. Έτσι ο CN απευθύνει όλα τα πακέτα στο home network, περνούν δηλαδή διαμέσου όλου του Διαδικτύου για να φθάσουν στον home agent και έπειτα δρομολογούνται πάλι πίσω μέσω τούνελ στον foreign agent, ο οποίος τελικά τα προωθεί στον MN (Σχήμα 38).



Σχήμα 38 : Triangular Routing

Αυτή η προσέγγιση έχει αρκετά μειονεκτήματα. Η real-time κίνηση από εφαρμογές όπως video conference και Voice over IP (VoIP) απαιτούν σφιχτά όρια όσο αναφορά την end to end καθυστέρησης και απώλειας πακέτων. Η τριγωνική δρομολόγηση θα αυξήσει την end to end καθυστέρηση από τον CN στον MN καθώς η δρομολόγηση δεν είναι βέλτιστη. Επίσης ένα L3 handover περιλαμβάνει την απόκτηση μιας CoA και την ενημέρωση των mobility bindings των CNs και HA, και συνεπώς εισάγει μια επιπλέον καθυστέρηση εκτός από την καθυστέρηση του L2 handover. Αποτέλεσμα της handover καθυστέρησης είναι η διακοπή των εγκαθιδρυμένων συνδέσεων προς στιγμήν, άρα και η απώλεια πακέτων και τελικά την απώλεια ποιότητας του multimedia stream. Η Mobile IP τεχνική είναι επίσης πολύ ανεπαρκής όταν αναλογιστούμε το overhead από το tunneling κάθε πακέτου που λαμβάνεται όταν ο MN είναι εκτός του home network του.

Θα ήταν βέλτιστο εάν ο CN μπορούσε να ανακαλύψει ότι ο κινητός κόμβος είναι στο ίδιο δίκτυο και παραδίδει το πακέτο άμεσα. Στόχος είναι να παραδοθούν τα πακέτα όσο το δυνατόν γρηγορότερα. Δηλαδή αρκεί τα πακέτα του CN προς τον MN να δρομολογηθούν κατευθείαν στην CoA του MN, χωρίς να χρειαστεί να περάσουν από τον HA. Ο Perkins και Johnson πρότειναν την τεχνική του Route Optimization, η οποία θα έλυνε αυτό το πρόβλημα, αλλά πότε

δεν καθιερώθηκε από την IETF, καθώς οι προσπάθειες είχαν ήδη επικεντρωθεί στην νέα έκδοση του πρωτοκόλλου IP, την IPv6.

4.3. Υποστήριξη κινητικότητας (Mobility Support) στο IPv6

Για σχεδόν 30 χρόνια το πρωτόκολλο IP, αποδείχτηκε ικανό να αντιμετωπίσει την αλματώδη ανάπτυξη του Διαδικτύου. Προβλήματα που ήταν αδύνατο να προβλεφτούν την δεκαετία του '80, αντιμετωπίστηκαν ικανοποιητικά, επεκτείνοντας το αρχικό πρωτόκολλο. Δίκαια θεωρείται ως το πιο πετυχημένο πρωτόκολλο, καθώς παρά την ηλικία του κατάφερε να διασυνδέσει εκατομμύρια συστήματα διαφορετικών αρχιτεκτονικών. Η μεγάλη όμως ανάπτυξη του Διαδικτύου, καθώς και οι απαιτήσεις των νέων δικτυακών εφαρμογών δεν μπορούν να αντιμετωπισθούν από το IPv4.

Έτσι η IETF μετά από πολλές προτάσεις για το IPng (Next Generation Internet Protocol), κατέληξε στην δημιουργία ενός νέου πρωτοκόλλου στα χνάρια του IP και έτσι το 1998 παρουσιάστηκε η 6η έκδοση του πρωτοκόλλου IP, με την ονομασία IPv6.

4.4. Από το IPv4 στο IPv6

Το IPv6 δημιουργήθηκε όπως είπαμε για να λύσει τους έμφυτους περιορισμούς του πρωτοκόλλου IPv4. Ο πιο διαδεδομένος περιορισμός ήταν ο άδικος διαμοιρασμός των καθολικών IP διευθύνσεων, που ευνοούσαν ιδιαίτερα την Αμερική. Παραδείγματος χάριν το πανεπιστημίου του Stanford στην Αμερική διαθέτει περισσότερες δημόσιες IP διευθύνσεις από ολόκληρη την Κίνα. Η έλλειψη διευθύνσεων θα δημιουργούσε ένα πού σημαντικό πρόβλημα, που όμως αντιμετωπίστηκε το NAT (Network Address Translation), το οποίο υπόσχεται να επεκτείνει την IPv4 από τα 32bit στα 48. Παρόλο που το NAT επιτρέπει σε περισσότερους ανθρώπους να συνδεθούν στο internet, όπως επίσης επιτρέπει σε μικρούς οργανισμούς να διαμορφώσουν μόνοι τους το δικό τους χώρο διευθύνσεων, χωρίς να βασίζονται στις αρμόδιες αρχές να τους δώσουν μοναδικές διευθύνσεις, αποτυγχάνει να παρέχει τη καθολική δρομολόγηση. Έτσι αποκλείει κόμβους από τη λειτουργία ως server, ή την χρήση peer-to-peer εφαρμογών. Για να υπερνικηθεί αυτό το πρόβλημα ένας κεντρικός υπολογιστής

απαιτείται για να διαιτητεύσει μεταξύ των client, και συνεπώς το δίκτυο σταματά να είναι peer-to-peer. Επίσης το NAT δεν λύνει το πρόβλημα της άδικης κατανομής διευθύνσεων.

Η ανάπτυξη του διαδικτύου στο απώτερο μέλλον όμως δεν θα είναι δυνατή, παρόλη την πνοή που έφερε το NAT. Το IPv6 από την άλλη έχει IP διευθύνσεις των 128 bit, και είναι ήδη διαθέσιμο. Πολλές οργανώσεις έχουν προσπαθήσει να δώσουν επιπλέον ώθηση στο IPv6. Η Ευρωπαϊκή Ένωση έχει επενδύσει πάνω από 20 εκατομμύρια Ευρώ σε ένα IPv6 δίκτυο όπως το 6Net και το 6Diss σε μία προσπάθεια να επιταχυνθεί η μετάβαση στο IPv6. Η 3rd Generation Partnership Project (3GPP) έχει προτείνει η UMTS (Universal Mobile Telecommunications System) Release 5 για IMS (Internet Multimedia Service) να λειτουργεί μόνο σε IPv6. Χωρίς αμφιβολία η καθολική μετάβαση σε IPv6 είναι αναπόφευκτη.

4.5. IPv6

Αναφέρουμε μερικά από τα πλεονεκτήματα του IPv6 σε σχέση με το IPv4. Πολλά από αυτά θα λέγαμε πως δεν είναι απλά πλεονεκτήματα, αλλά άμεσες αναγκαίες αλλαγές στο IP πρωτόκολλο.

- **Εκτεταμένη δυνατότητα διευθυνσιοδότησης:** Το IPv6 αυξάνει το μέγεθος της επικεφαλίδας από 32 σε 128 bits, προσφέροντας δυνατότητες για περισσότερα επίπεδα διευθυνσιοδότησης, "ανεξάντλητο" χώρο διευθύνσεων και απλούστερη αυτοδιαμόρφωση των διευθύνσεων (*autoconfiguration*). Η διαβαθμισιμότητα της δρομολόγησης multicast έχει βελτιωθεί, προσθέτοντας το πεδίο scope στη διεύθυνση που πληροφορεί το δρομολογητή για την περιοχή των host που "ακούνε" (π.χ. LAN, WAN, internet).
- **Καθολική μοναδική ιεραρχική διευθυνσιοδότηση**: Η διευθυνσιοδότηση βασίζεται σε prefixes και όχι κλάσεις, προσφέροντας έτσι καλύτερη ταξινόμηση των κόμβων, μικρότερα routing tables και αποδοτικότερη δρομολόγηση στο δίκτυο κορμού.
- **Υποστήριξη ενθυλάκωσης**: Υποστηρίζεται ενθυλάκωση στο IPv6 πακέτο άλλων πρωτοκόλλων καθώς και του ίδιου του IPv6.
- **Απλοποιημένη επικεφαλίδα:** Ορισμένα πεδία του IPv4 απουσιάζουν από το IPv6 ή έχουν γίνει προαιρετικά. Αυτό βοηθά στη μείωση του κόστους δρομολόγησης για κάθε πακέτο και του κόστους σε εύρος ζώνης που καταναλώνει η επικεφαλίδα. Η επικεφαλίδα, επίσης, έχει σταθερό μήκος, και όπως αναφέραμε στο προηγούμενο κεφάλαιο οι δρομολογητές έχουν καλύτερη απόδοση για τέτοιες επικεφαλίδες.

- **Βελτιωμένη υποστήριξη για επεκτάσεις και επιλογές της επικεφαλίδας:** Το IPv6 διαθέτει υποστήριξη προαιρετικών πεδίων σε ξεχωριστές επικεφαλίδες. Αυτό διευκολύνει την απόδοση της απλής δρομολόγησης, αφού δεν χρειάζεται κάθε δρομολογητής να επεξεργαστεί αυτά τα πεδία, αν κάτι τέτοιο δεν είναι αναγκαίο.
- **Έλεγχος ροής στο επίπεδο IP:** Μια καινούρια λειτουργία έχει προστεθεί που κατηγοριοποιεί τα πακέτα ενός αποστολέα σε μια συγκεκριμένη ροή(flow). Αυτή η ροή μπορεί να αντιμετωπιστεί με κάποιο ειδικό τρόπο (π.χ. μια ροή δεδομένων live streaming video).
- **Ασφάλεια στο επίπεδο IP:** Το IPv6 προσφέρει, μέσω των επικεφαλίδων επέκτασης, ασφάλεια (Authentication Header) και κρυπτογράφηση δεδομένων (Encapsulated Security Payload).
- **Υποστήριξη mobility:** Το MIPv6 υλοποιείται βασιζόμενο σε χαρακτηριστικά του IPv6 που είναι ήδη ολοκληρωμένα.
- **Παροχή Quality of Service**: Παρέχετε η δυνατότητα ταξινόμησης πακέτων σε διάφορες ροές, διαφορετικής προτεραιότητας.

4.5.1. Ανάλυση Διεύθυνση (Address Resolution) στο IPv6

Το Address Resolution Protocol (ARP) του TCP/IP είναι ένα γενικό πρωτόκολλο για την δυναμική απεικόνιση Network layer διευθύνσεων, σε Link layer διευθύνσεις. Ακόμα κι αν σχεδιάστηκε για την 4η έκδοση του IP, τα μηνύματα που χρησιμοποιεί επιτρέπουν διευθύνσεις μεταβλητού μήκους και για τα δύο επίπεδα. Αυτή η ευελιξία σημαίνει ότι θα ήταν θεωρητικά δυνατό να χρησιμοποιηθεί αυτό το πρωτόκολλο και για την 6η έκδοση του IP (IPv6). Έτσι με ελάχιστες μετατροπές, θα μπορούσαμε να χρησιμοποιήσουμε το ARP σχεδόν αυτούσιο.

Οι σχεδιαστές του IPv6 επέλεξαν να μην το κάνουν αυτό. Η αλλαγή του IP είναι μια μεγάλη υπόθεση που είναι εν εξελίξει για πολλά έτη, και αντιπροσωπεύει μια σπάνια ευκαιρία να αλλαχτούν οι διάφορες πτυχές του TCP/IP. Έτσι η IETF αποφάσισε να εκμεταλλευθεί τις αλλαγές στο IPv6 και να εξετάσει λεπτομερώς όχι μόνο το ίδιο το IP, αλλά και πολλά από τα πρωτόκολλα που "υποστήριζαν" ή "βοηθούσαν" το IP. Στο IPv6 λοιπόν, το Address resolution έχει συνδυαστεί με διάφορες λειτουργίες που εκτελούνται από το ICMP και με κάποιες επιπλέον λειτουργίες για να δημιουργήσει το Neighbor Discovery Protocol (NDP). Ο όρος "neighbor" στο IPv6 αναφέρεται απλά σε συσκευές σε ένα τοπικό δίκτυο, και όπως το όνομα υπονοεί, το NDP είναι αρμόδιο για την επικοινωνία μεταξύ των γειτόνων.

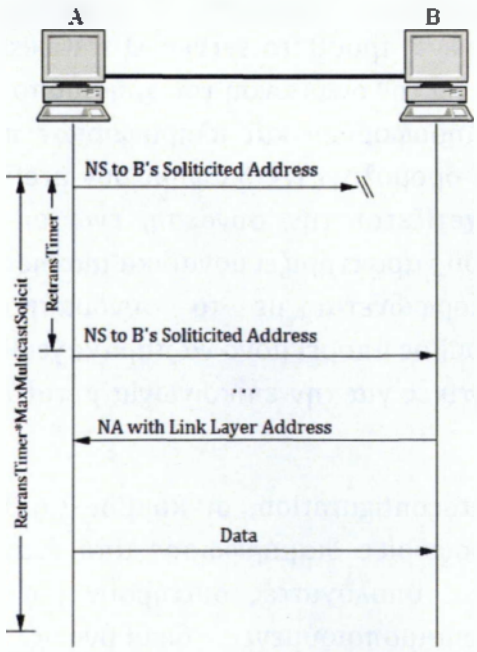
Οι βασικές λειτουργίες του NDP δεν διαφέρουν και πάρα πολύ από αυτές του ARP (Σχήμα 39). Η ανάλυση της διεύθυνσης είναι ακόμα δυναμική και

βασίζεται στη χρήση cache tables που διατηρούν ζευγάρια IP και MAC διευθύνσεων. Κάθε συσκευή σε ένα φυσικό δίκτυο κρατάει τέτοιες πληροφορίες για τους γείτονές της. Όταν μια συσκευή θέλει να στείλει ένα IPv6 πακέτο δεδομένων σε έναν γείτονα της αλλά δεν έχει τη MAC διεύθυνση του, ξεκινά τη διαδικασία ανάλυσης διεύθυνσης. Στο παρακάτω παράδειγμα ας θεωρήσουμε πως η συσκευή Α προσπαθεί να στείλει στη συσκευή Β.

Αντί της αποστολής ενός ARP Request μηνύματος, η Α δημιουργεί ένα ND Neighbor Solicitation μήνυμα. Εδώ υπάρχει η πρώτη μεγάλη αλλαγή σε σχέση με το ARP. Εάν το data link πρωτόκολλο που χρησιμοποιείται υποστηρίζει multicasting, όπως πχ το Ethernet, το Neighbor Solicitation δεν είναι broadcast μήνυμα. Άντ' αυτού, στέλνεται στη solicited-node address της συσκευής της οποίας την IPv6 διεύθυνση προσπαθούμε να αναλύσουμε. Έτσι το Α θα στείλει ένα multicast μήνυμα στη solicited-node multicast διεύθυνση της συσκευής Β. Το πακέτο θα περιέχει την link-layer διεύθυνση στο source link-layer address πεδίο.

Η συσκευή Β θα λάβει το Neighbor Solicitation και θα απαντήσει με Neighbor Advertisement, κάτι ανάλογο του ARP Reply. Το Neighbor Advertisement θα περιέχει την link-layer διεύθυνση της συσκευής Β στο target link-layer address πεδίο.

Η συσκευή Α θα περιμένει το Neighbor Advertisement της συσκευής Β για μια περίοδο MAX_MULTICAST_SOLICIT6*RetransTimer7 δευτερολέπτων, στέλνοντας νέο Neighbor Solicitation κάθε RetransTimer δευτερόλεπτα.



Σχήμα 39 : IPv6 Neighbor Discovery

Μέχρι η συσκευή Α να λάβει το Neighbor Advertisement τοποθετεί οποιοδήποτε πακέτο προορίζεται για τη συσκευή Β σε ουρά. Μόλις λοιπόν η συσκευή Α λάβει το Neighbor Advertisement στέλνει όλα τα πακέτα που βρίσκονται στην ουρά στον Β και προσθέτει την αντιστοίχηση των IP, link-layer διευθύνσεων του Β στην neighbor cache της. Από αυτή τη στιγμή και για όποια πακέτα προορίζονται για την συσκευή Β, η Α θα βρίσκει την link-layer διεύθυνση της Β στην neighbor cache της.

Για επιπλέον αποδοτικότητα, υποστηρίζεται cross-resolution όπως και στο IPv4. Αυτό επιτυγχάνεται ενσωματώνοντας την link-layer διεύθυνση της συσκευής Α στο Neighbor Solicitation. Έτσι η συσκευή Β θα μπορεί να εγγράψει το ζευγάρι IP, link layer διευθύνσεων της Α στην δικιά της neighbor cache.

4.5.2. Autoconfiguration

Στο IPv4 η διευθυνσιοδότηση γινόταν είτε χειροκίνητα, είτε με αυτόματα με τη χρήση κάποιου Dynamic Host Configuration Protocol (DHCP). Η διαδικασία αυτόματης ανάθεσης διεύθυνσης στο IPv6 περιλαμβάνει τη δημιουργία μιας τοπικής διεύθυνσης και η επαλήθευση της μοναδικότητάς της σε μια σύνδεση.

Το IPv6 ορίζει μηχανισμούς stateful και stateless address autoconfiguration. Η stateless autoconfiguration δεν απαιτεί καμία χειροκίνητη διαμόρφωση των κόμβων, ελάχιστη (ή καθόλου) διαμόρφωση των δρομολογητών, και κανένα πρόσθετο server. Ο stateless μηχανισμός επιτρέπει σε έναν κόμβο να παράγει την διεύθυνσή του χρησιμοποιώντας έναν συνδυασμό τοπικά διαθέσιμων πληροφοριών και πληροφοριών που διαφημίζονται από τους δρομολογητές. Οι δρομολογητές διαφημίζουν prefixes που προσδιορίζουν το υποδίκτυο που σχετίζεται την σύνδεση, ενώ οι κόμβοι παράγουν ένα "interface identifier" που χαρακτηρίζει μοναδικά μια διεπαφή σε ένα υποδίκτυο. Μια διεύθυνση διαμορφώνεται με το συνδυασμό των δύο. Ελλείψει δρομολογητών, ένας κόμβος μπορεί μόνο να παραγάγει link-local διευθύνσεις, οι οποίες είναι ικανοποιητικές για την επικοινωνία μεταξύ των κόμβων του ίδιου link.

Στη stateful autoconfiguration, οι κόμβοι λαμβάνουν τις διευθύνσεις διεπαφών ή/και πληροφορίες διαμόρφωσης από έναν κεντρικό υπολογιστή (DHCPv6). Οι κεντρικοί υπολογιστές διατηρούν μια βάση δεδομένων που κρατάν τις ήδη χρησιμοποιούμενες διευθύνσεις. Οι δύο μηχανισμοί αλληλοσυμπληρώνονται. Παραδείγματος χάριν, ένας κόμβος μπορεί να χρησιμοποιήσει τον stateless μηχανισμό για να διαμορφώσει τις διευθύνσεις του, αλλά και τον stateful για να λάβει άλλες πληροφορίες.

Ο stateless μηχανισμός χρησιμοποιείται όταν δεν ενδιαφερόμαστε ιδιαίτερα για την ακριβή ανάθεση διευθύνσεων, εφόσον αυτές είναι μοναδικές και κατάλληλα δρομολογήσιμες. Η stateful προσέγγιση χρησιμοποιείται όταν απαιτείται αυστηρότερος έλεγχος στην ανάθεση των διευθύνσεων.

4.5.3. Διπλότυπη Ανίχνευση Διεύθυνσης (Duplicate Address Detection)

Ας εξετάσουμε τον stateless μηχανισμό λεπτομερέστατα. Ο μηχανισμός αποτελείται από δύο διαδικασίες, την Duplicate Address Detection (DAD), και την Router Discovery. Αρχικά ο κόμβος αποδίδει στο interface την λεγόμενη link-local (τοπική δηλαδή για τη σύνδεση) διεύθυνση. Η διεύθυνση αυτή σχηματίζεται συνενώνοντας το well-known πρόθεμα της σύνδεσης FE80:0:0:0:0:0:0:0/64 με το αναγνωριστικό (identifier) του interface, αντικαθιστώντας τα N τελευταία μηδενικά του προθέματος με τα N ψηφία του αναγνωριστικού. Τυπικά το N θα είναι 64 bits, και θα είναι στις περισσότερες περιπτώσεις η hardware διεύθυνση του κόμβου.

Πριν γίνει η απόδοση της link local διεύθυνσης στο interface ο κόμβος πρέπει να ελέγξει αν αυτή δεν χρησιμοποιείται από άλλον κόμβο στη σύνδεση (DAD). Ο έλεγχος αυτός γίνεται με τη χρήση ενός Neighbor Solicitation μηνύματος όπως αυτό ορίζεται από το NDP χρησιμοποιώντας ως αποδέκτη του μηνύματος την υποψήφια link-local διεύθυνση. Στην περίπτωση που υπάρχει κάποιος άλλος κόμβος στην σύνδεση με την ίδια link-local διεύθυνση θα απαντήσει με ένα Neighbor Advertisement μήνυμα, οπότε η διαδικασία διακόπτεται και το configuration του κόμβου πρέπει να συνεχιστεί χειρονακτικά. Για ευκολία υπάρχει η δυνατότητα να οριστεί και ένα εναλλακτικό αναγνωριστικό για το interface ώστε η διαδικασία να επαναληφθεί με το νέο αναγνωριστικό.

Αν δεν υπάρξει απάντηση σε ένα εύλογο χρονικό διάστημα ο κόμβος μπορεί να υποθέσει ότι η link-local διεύθυνση είναι μοναδική για τη σύνδεση και να προχωρήσει στην απόδοση αυτής στο interface, οπότε και ο κόμβος μπορεί να έχει επικοινωνία IP επιπέδου με τους υπόλοιπους κόμβους της σύνδεσης.

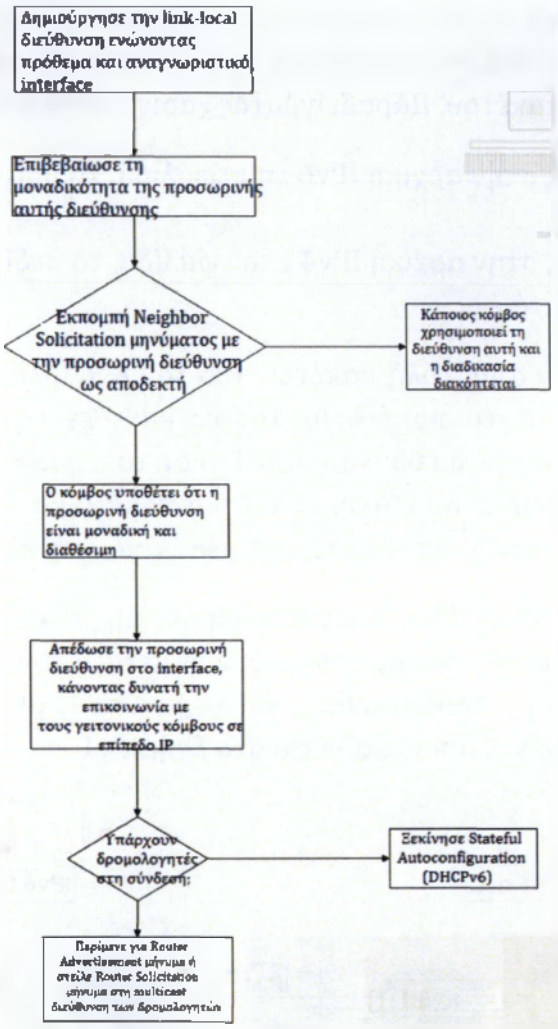
4.5.4. Router Discovery

Το επόμενο βήμα στον stateless μηχανισμό συνίσταται στο να ανιχνεύεται η παρουσία δρομολογητή (Router Discovery). Η λειτουργία του Router Discovery επιτρέπει οι μη-δρομολογητές να ζητήσουν και να επεξεργαστούν λαμβανόμενα Router Advertisements. Οι δρομολογητές

στέλνουν unsolicited RA ανά ένα διάστημα μεταξύ του MIN_RTR_ADV_INT και του MAX_RTR_ADV_INT. Κάθε φορά που ένας router ανακαλύπτεται στο δίκτυο προστίθεται στην Default Routers List (DRL). Η DRL αποθηκεύει τους δρομολογητές που ο κόμβος μπορεί να στείλει off-link8 πακέτα επίσης. Εάν δεν υπάρχει κανένας δρομολογητής στο δίκτυο τότε κάθε διεύθυνση θεωρείται on-link9. Κατά την παραλαβή ενός RA από ένα κόμβο, τα προθέματα που διαφημίζονται από το δρομολογητή αναζητούνται και εάν το flag on-link έχει τεθεί για αυτό το πρόθεμα, τότε το πρόθεμα προστίθεται στην prefix list του κόμβου.

Αυτά τα προθέματα συγκρίνονται με τις διευθύνσεις προορισμού όλων των πακέτων που στέλνονται. Αν οι διευθύνσεις ταιριάζουν με το πρόθεμα, τότε είναι on-link και άρα τα πακέτα μπορούν να σταλούν άμεσα σε έναν γειτονικό κόμβο χωρίς την επέμβαση του δρομολογητή.

Οι κατάλογοι DRL και on-link prefixes θεωρούνται Conceptual Data Structures (CDS) και χρησιμοποιούνται στον αλγόριθμο αποστολής. Είναι ένας αλγόριθμος που όλοι οι κόμβοι χρησιμοποιούν για να καθορίσουν πώς να διαβιβάσουν ή να στείλουν ένα πακέτο. Παρακάτω παρουσιάζεται σχηματικά η Stateless Address Autoconfiguration τεχνική.



Σχήμα 40 : Stateless Address Autoconfiguration

4.6. IPV6 Tunneling και Encapsulation

Το IPv6 tunneling είναι μια τεχνική για την δημιουργία ενός "virtual link" μεταξύ δύο IPv6 κόμβων για τη διαβίβαση ολόκληρων πακέτων σαν περιεχόμενο άλλων πακέτων (Σχήμα 41). Από την άποψη των δύο κόμβων, αυτό το "virtual link", αποκαλούμενο IPv6 tunnel, δεν είναι τίποτα παραπάνω από μία point-to-point σύνδεση. Στην όλη διαδικασία παίρνουν μέρος τέσσερις κόμβοι. Οι A, B είναι η αντίστοιχοι αποστολέας και δέκτης, ενώ οι C και D είναι οι κόμβοι εισόδου και εξόδου του τούνελ (tunnel entry point, tunnel exit point).

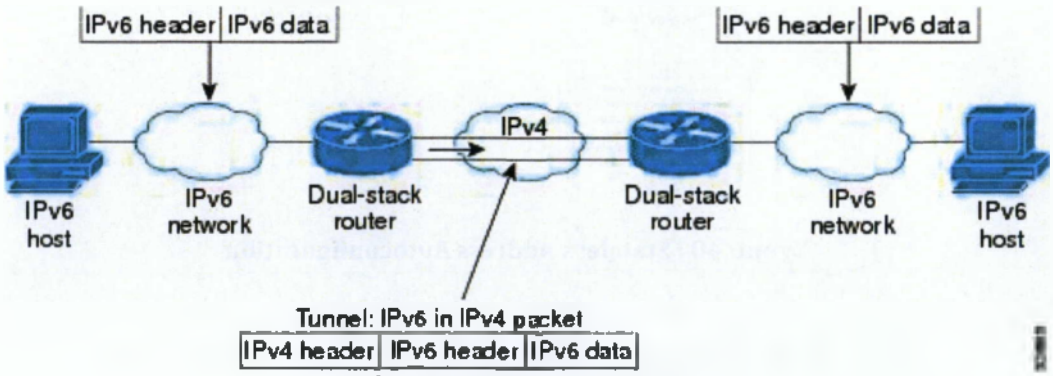
Η IPv6 encapsulation (ενθυλάκωση) ορίζεται σαν η εισαγωγή σε ένα πακέτο μιας επιπλέον επικεφαλίδας, ή πολύ συχνά ένα σετ επικεφαλίδων επέκτασης, οι οποίες καλούνται tunnel headers. Η ενθυλάκωση

πραγματοποιείται σε ένα tunnel entry point, ως αποτέλεσμα της αποστολής του αρχικού πακέτου επάνω στο "virtual link". Το αρχικό πακέτο επεξεργάζεται κατά τη διάρκεια της διαβίβασης σύμφωνα με τους συγκεκριμένους κανόνες του πρωτοκόλλου του πακέτου. Παραδείγματος χάριν εάν το αρχικό πακέτο είναι:

- πακέτο IPv6, στην αρχική IPv6 επικεφαλίδα, το hop limit μειώνεται κατά ένα.
- πακέτο IPv4, στην αρχική IPv4 επικεφαλίδα, το πεδίο Time To Live (TTL) μειώνεται κατά ένα.

Σε μία λοιπόν αποστολή πακέτου από τον A, ο C λαμβάνει το πακέτο. Το ενθυλακώνει σε ένα νέο πακέτο με source address την διεύθυνσή του και destination address την διεύθυνση του D και το προωθεί στον D μέσω του τούνελ. Ο D με τη σειρά του εξάγει το αρχικό πακέτο και το προωθεί στον B, ο οποίος δεν γνωρίζει ότι το πακέτο πέρασε μέσα από τούνελ.

Ένα IPv6 τούνελ ένας κατευθυνόμενος μηχανισμός - η ροή πακέτων πραγματοποιείται μόνο προς μια κατεύθυνση μεταξύ των κόμβων εισόδου και εξόδου. Αμφίδρομη επικοινωνία επιτυγχάνεται με την χρήση δύο κατευθυνόμενων τούνελ όπως φαίνεται στο Σχήμα 41.



Σχήμα 41 : IPv6 Encapsulation

4.7. Mobile IPv6

Το Mobile IPv6 σχεδιάστηκε με βάση το MIP, χωρίς όμως τα μειονεκτήματα του. Έτσι περιληπτικά, το MIPv6 επιτρέπει σε έναν κινητό κόμβο να κινηθεί από μια σύνδεση προς άλλη χωρίς αλλαγή της Home Address του. Τα πακέτα μπορούν να δρομολογηθούν χρησιμοποιώντας αυτήν την διεύθυνση ανεξαρτήτως από το τρέχον σημείο σύνδεσης του κινητού κόμβου στο

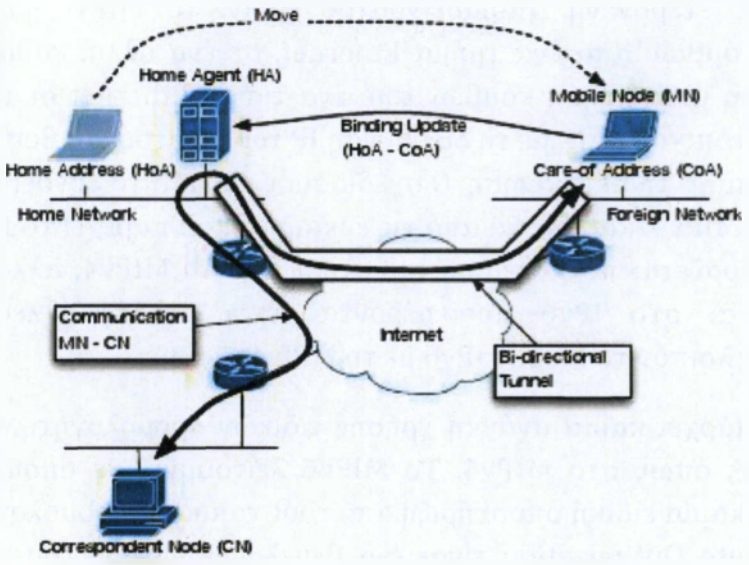
Διαδίκτυο. Ο κινητός κόμβος μπορεί επίσης να συνεχίσει να επικοινωνεί με άλλους κόμβους (στάσιμους ή κινητούς) μετά την κίνηση του σε ένα νέο link. Η μετακίνηση ενός κινητού κόμβου μακριά από το home network του είναι έτσι διαφανής για τα πρωτόκολλα υψηλότερου επιπέδου και τις εφαρμογές.

Το Mobile IPv6 είναι εξίσου κατάλληλο για κίνηση σε ομοιογενή δίκτυα, όπως και σε ετερογενή. Παραδείγματος χάριν, το MIPv6 διευκολύνει τη μετακίνηση κόμβων από ένα τμήμα Ethernet, σε ένα άλλο, καθώς επίσης και διευκολύνει τη μετακίνηση κόμβων από ένα τμήμα Ethernet σε ένα ασύρματο κύτταρο του τοπικού LAN, με τη διεύθυνση IP του κινητού κόμβου να παραμένει αμετάβλητη παρά τη μετακίνηση. Ο σχεδιασμός του MIPv6 ευνοείται και από το ήδη υπάρχον MIPv4, καθώς και από τις ευκαιρίες που παρέχει το IPv6. Συνεπώς το MIPv6 μοιράζεται πολλά χαρακτηριστικά από το MIPv4, αλλά ταυτόχρονα ενσωματώνεται στο IPv6 προσφέροντας έτσι πολλές άλλες βελτιώσεις. Συγκρίνοντας λοιπόν το Mobile IPv6 με το MIPv4 έχουμε:

- Δεν υπάρχει καμία ανάγκη χρήσης ειδικών δρομολογητών σαν "foreign agents", όπως στο MIPv4. Το MIPv6 λειτουργεί σε οποιαδήποτε θέση χωρίς καμία ειδική υποστήριξη από τους τοπικούς δρομολογητές.
- Το Route Optimization είναι ένα θεμελιώδες μέρος του πρωτοκόλλου, παρά μία μη τυποποιημένη επέκταση.
- Το Route Optimization στο MIPv6 μπορεί να λειτουργήσει με ασφάλεια ακόμη και χωρίς την ύπαρξη προκαθορισμένων τροποποιήσεων.
- Στο MIPv6 υπάρχει ενσωματωμένη υποστήριξη χρήσης Route Optimization ακόμα και για δρομολογητές που εκτελούν "ingress filtering".
- Η τεχνική IPv6 Neighbor Unreachability Detection επιβεβαιώνει συμμετρική προσπελασιμότητα μεταξύ του κινητού κόμβου και του δρομολογητή στην τρέχουσα θέση.
- Τα περισσότερα πακέτα που στέλνονται σε έναν κινητό κόμβο ενώ βρίσκεται μακριά από το home network του στέλνονται χρησιμοποιώντας μια IPv6 επικεφαλίδα, παρά με IP ενθυλάκωση μειώνοντας έτσι το overhead σε σχέση με το MIPv4.
- Το MIPv6 δεν εξαρτάται από κανένα link-layer επίπεδο, δεδομένου ότι χρησιμοποιεί IPv6 Neighbor Discovery, αντί για ARP. Αυτό βελτιώνει επίσης την ευρωστία του πρωτοκόλλου.
- Η χρήση της IPv6 ενθυλάκωσης (και του Routing header) απαλείφει την ανάγκη διαχείρισης του "tunnel soft state".
- Ο μηχανισμός αυτόματης home agent address discovery επιστρέφει ένα μόνο reply στον κινητό κόμβο. Η broadcast προσέγγιση του IPv4 επιστρέφει χωριστά reply από κάθε home agent.

Η επικοινωνία στο MIPv6 γίνεται με έναν από τους δύο ακόλουθους τρόπους. Ο default τρόπος χρησιμοποιεί τούνελ μέσω του HA, ενώ ο

προτιμημένος τρόπος είναι μια άμεση διαδρομή που καθιερώνεται μετά από Route Optimization. Και οι δύο τρόποι φαίνονται στο Σχήμα 42. Αντίθετα από το MIPv4, η τριγωνική δρομολόγηση δεν είναι πια μέθοδος επικοινωνίας αν και αυτό μπορεί εμφανιστείτε στιγμιαία κατά τη διάρκεια της φάσης μετάβασης μεταξύ των δύο αναφερθέντων τρόπων.



Σχήμα 42 : Τρόποι επικοινωνίας στο MIPv6

4.7.1. MIPv6 Δρομολόγηση με χρήση Tunneling

Όσο ο MN βρίσκεται μακριά από το σπίτι ο HA λειτουργεί σαν proxy. Αυτό σημαίνει πως οποιαδήποτε πακέτα απευθύνονται στον MN θα καταλήξουν στον HA, καθώς αυτός θα ανταποκριθεί σε όλα Neighbor Solicitation requests για τον MN. Μόλις ο HA παραλάβει ένα πακέτο θα το προωθήσει στον MN στην τρέχουσα θέση του μέσω της CoA που βρει στην binding cache του. Η εγγραφές στην binding cache του δημιουργούνται όταν ο MN εγγράφηκε στον HA και ανανεώνονται με κάθε Binding Update (BU) από τον MN. Όπως και στο κλασσικό IPv6 ο HA θα ενθυλακώσει το αρχικό πακέτο σε ένα νέο. Η tunnel επικεφαλίδα θα έχει μια διεύθυνση προέλευσης την IP διεύθυνση του HA και διεύθυνση προορισμού την CoA διεύθυνση του MN. Ο MN απομονώνει το αρχικό πακέτο, το οποίο πια φαίνεται λες και ο CN το είχε στείλει απευθείας στον MN.

Στην περίπτωση που ο MN δεν έχει δημιουργήσει binding με τον CN, θα πρέπει να στείλει όλα τα πακέτα που προορίζονται για τον CN μέσω του HA χρησιμοποιώντας reverse tunneling. Το αρχικό πακέτο έχει διεύθυνση προέλευσης την HoA και διεύθυνση προορισμού τον CN, ενώ η tunneling επικεφαλίδα θα έχει διεύθυνση προέλευσης την CoA του MN και προορισμό την

διεύθυνση του HA. Μόλις ο HA λάβει το πακέτο θα ελέγξει αν η διεύθυνση προέλευσης της tunneling επικεφαλίδας είναι η CoA που αντιστοιχεί στην HoA του αρχικού πακέτου, εμποδίζοντας έτσι άλλους κόμβους να μεταμφιέζονται σαν MN. Κατά συνέπεια όταν το πακέτο φτάσει στον CN μοιάζει σαν ο MN να το είχε στείλει από τον home network του.

4.7.2. MIPv6 Δρομολόγηση με χρήση Route Optimization

Αυτός ο τρόπος παράδοσης πακέτων δεν απαιτεί τη μεσολάβηση του HA, και συνεπώς επιτρέπει γρηγορότερη και πιο αξιόπιστη μετάδοση. Αυτό επιτυγχάνεται με_χρήση του πεδίου home address destination και της type-2 επικεφαλίδας. Η χρήση αυτών των δύο εξομοιώνει τους μηχανισμούς ενθυλάκωσης της_προηγούμενης μεθόδου, αλλά επιφέρει ελάχιστο overhead. Το πεδίο home address_destination του MN περιέχει τη HoA. Αυτό επιτρέπει σε ένα κινητό κόμβο να στείλει_πακέτα με διεύθυνση προέλευσης την CoA, πράγμα που είναι τοπολογικά ορθό, και συνεπώς περνάει τους ingress filtering κανόνες του ξένου δρομολογητή. Όταν το πακέτο φτάσει, ο CN θα αντιστρέψει το *home address destination* με την διεύθυνση προέλευσης του πακέτου. Το τροποποιημένο πακέτο μεταφέρεται στο transport layer και έτσι η εφαρμογή δεν αντιλαμβάνεται καν ότι επικοινωνεί με ένα κινητό κόμβο.

Μια παρόμοια διαδικασία εμφανίζεται και όταν ο CN στέλνει δεδομένα στον MN. Η εφαρμογή απευθύνει το πακέτο στην HoA του MN. Στο network layer ο CN θα ελέγξει την binding cache του προκειμένου να ανακαλύψει την τρέχουσα θέση του MN, δηλαδή την CoA που ανέφερε ο MN με το BU του. Θα προσθέσει μια type-2 επικεφαλίδα στον πακέτο και θα αντικαταστήσει τη διεύθυνση προέλευσης με την CoA. Το πακέτο θα ταξιδέψει μέσω του δικτύου χρησιμοποιώντας κανονικές διαδικασίες και φθάνει στον MN. Ο MN θα επεξεργαστεί την type-2 επικεφαλίδα ανταλλάσσοντας τα περιεχόμενα του με τη διεύθυνση προέλευσης του πακέτου. Κατά συνέπεια το τελικό πακέτο που περνά στο transport layer έχει ως διεύθυνση προέλευσης την HoA. Αυτό κρατά τις εφαρμογές ανίδεες της μετακίνησης του κόμβου.

Για να καθιερωθεί μια άμεση διαδρομή, ο MN πρέπει να στέλνει BU με την τρέχουσα CoA του στον CN, ο οποίος την αποθηκεύει στην bonding cache του. Προκειμένου να αποτραπεί από κακόβουλους κόμβους να μεταμφιέζονται σαν MNs στέλνοντας BUs με την HoA του MN, χρησιμοποιείται η διαδικασία return routability για να ελεγχθεί η αυθεντικότητα των κόμβων. Σαν πρώτο βήμα ο MN στέλνει ένα Home Test Init μήνυμα στον CN για να αρχίσει τη διαδικασία return routability. Ο CN τότε θα στείλει ένα πακέτο δοκιμής σε κάθε μια από τις δύο διαφορετικές διαδρομές, μια χρησιμοποιώντας την HoA σαν προορισμό και μία χρησιμοποιώντας την CoA σαν προορισμό. Τα δύο πακέτα δοκιμής περιέχουν τα

μέρη ενός time cookie που συναρμολογούνται στον MN και στέλνονται πίσω στον MN. Μόνο αν και οι δύο διευθύνσεις δείχνουν στον ίδιο κόμβο, θα μπορεί να λάβει ολόκληρο το time cookie. Αυτό βασίζεται στην υπόθεση ότι ο HA έχει πιστοποιήσει την ταυτότητα του MN. Αυτή είναι μια έγκυρη υπόθεση καθώς το MIPv6 έχει υιοθετήσει την χρήση της IPSec πιστοποίησης στα BU του MN στον HA. Κατά συνέπεια ο μηχανισμός του Return Routability θα προσθέσει ενάμισι round trip ανά CN για τον οποίο η διαδρομή θα βελτιστοποιηθεί.

Όσο αναφορά τον χειρισμό real-time κυκλοφορίας στο MIPv6, έχει εμφανώς καλύτερη συμπεριφορά καθώς αφενός δεν γίνεται τριγωνική δρομολόγηση καθόλου, και αφετέρου μπορεί πάντα να εφαρμοστεί Route Optimization εκτός και αν ο CN το έχει απαγορέψει. Και οι δύο τρόποι δρομολόγησης φαίνονται στο Σχήμα 42.

4.8. Ασφάλεια της Mobile IP

Το πρωτόκολλο του Internet (IP) θα είναι το κυρίαρχο πρωτόκολλο για οποιαδήποτε μελλοντική επικοινωνία. Στο κινητό κόσμο, όμως, η Mobile IP δεν χρησιμοποιείται ακόμα πολύ συχνά, αλλά με την αυξανόμενη δημοτικότητα των ασύρματων τοπικών δικτύων αυτό μάλλον θα αλλάξει. Από τότε που οι άνθρωποι των επιχειρήσεων είναι η κινητήρια δύναμη της αγοράς για υπηρεσίες κινητών επικοινωνιών, η ασφάλεια γίνεται εξαιρετικά σημαντική σε αυτά τα ασύρματο LAN / Mobile IP σενάρια. Οι επιτιθέμενοι μπορούν να εξαπατήσουν με πακέτα που μεταδίδονται μέσω ασύρματων συνδέσεων κινητής τηλεφωνίας και οι χρήστες θα πρέπει να είναι ασφαλείς επικυρωμένοι κατά την περιαγωγή από ένα ασύρματο σημείο πρόσβασης για άλλο. Ένας φυσικός τρόπος για να παρέχεται ασφάλεια στους χρήστες της Mobile IP, είναι να χρησιμοποιήσουν το πρωτόκολλο IP Security protocol suite . Ένα ιδιαίτερο πρόβλημα κατά τη χρήση της Mobile IP είναι το πρόβλημα firewall traversal. Σε αυτή την περίπτωση, ένα πανεπιστημιακό δίκτυο ή ένα εικονικό ιδιωτικό δίκτυο (VPN), ενός οργανισμού όπως ένα πανεπιστήμιο ή μια εταιρεία που προστατεύεται από ένα τείχος προστασίας από το παγκόσμιο Internet. Μόνο εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση για το ιδιωτικό δίκτυο.

Στην ενότητα αυτή προτείνονται λύσεις που αναπτύχθηκαν από ερευνητές και παρουσιάζεται η αρχιτεκτονική της SecMIP, περιγράφεται η εφαρμογή και εξετάζονται οι επιδόσεις μετρήσεων.

4.8.1. Σχετικά

Οι Zao και Condell εξηγούν τη χρήση του IPSec για κινητά IP για HA-MN, HA-FA, CN-HA, CN-FA, και MN-CN συνδέσεις. Η IPSec χρησιμοποιείται για να αντικαταστήσει την IP-IP-tunneling. Τα προσαρμοσμένα μηνύματα στην Mobile IP που προτείνονται για την αντιγραφή της εγκατάστασης του IPSec tunnel. Προστίθενται Ειδικές επεκτάσεις του IPSec tunnel για διαφημίσεις και μηνύματα εγγραφής.

Οι Binkley και Richardson περιγράφουν πως ένα ασφαλής firewall σε προστατευόμενη περιοχή μπορεί να ανεχθεί την Mobile IP ή το κινητό συστήματα χρησιμοποιώντας μόνο DHCP και να παραμένουν ασφαλή. Αυτοί πρότειναν να χρησιμοποιούν IPSec tunnel διπλής κατεύθυνσης μεταξύ των HA ως ένα κλασικό προπύργιο host και του MN. Μια ασφαλής έννοια της κινητής δικτύωσης προτείνεται και βασίζεται σε ad-hoc δικτύωση και ασφαλή IPSec tunnels διπλής κατεύθυνσης. Το πρότυπο σενάριο Mobile IP θεωρείται ως ειδική περίπτωση ad-hoc δρομολόγησης όπου οι HA και MN έχτισαν ένα ασφαλή ad-hoc δίκτυο. Λαμβάνοντας υπόψη το πρόβλημα της κινητικότητας IP ως ειδική περίπτωση του γενικού ad-hoc προβλήματος δικτύωσης είναι μια ωραίο ιδέα, αλλά μπορεί να είναι υπερβολικά πολύπλοκη για το στόχο να εξασφαλιστεί μόνο ένα Mobile IP περιβάλλον.

Οι Gupta και Montenegro περιγράφουν βελτιώσεις που επιτρέπουν τη λειτουργία Mobile IP σε ένα δίκτυο, το οποίο είναι προστατευμένο από ένα συνδυασμό source-filtering routers, εξελιγμένα firewalls, και ιδιωτικό χώρο διευθύνσεων. Αυτές οι βελτιώσεις θα πρέπει να επιτρέπουν στον χρήστη κινητού στο Δημόσιο Internet να διατηρήσει μια ασφαλή εικονική παρουσία στο προστατευόμενο firewall δίκτυο του γραφείου. Οι συντάκτες προτείνουν να χρησιμοποιηθεί SKIP για τη διαχείριση κλειδών, αυθεντικοποίησης και κρυπτογράφηση. Ο λόγος για τον οποίο επέλεξε SKIP αντί του ISAKMP / Oakley, είναι η ικανότητά του SKIP να κοιτάζει προς τα πάνω το δημόσιο κλειδί του αποστολέα που βασίζεται σε εναλλακτικά ονόματα, ενώ αυτό γίνεται με τις διευθύνσεις πηγής στην περίπτωση των ISAKMP / Oakley. Η έννοια της ασφαλούς Mobile IP φαίνεται να είναι ένας εύκολος και αποτελεσματικός τρόπος για την επίλυση προβλημάτων ασφάλειας της Mobile IP, αλλά απαιτεί την εισαγωγή νέων πρωτόκολλων.

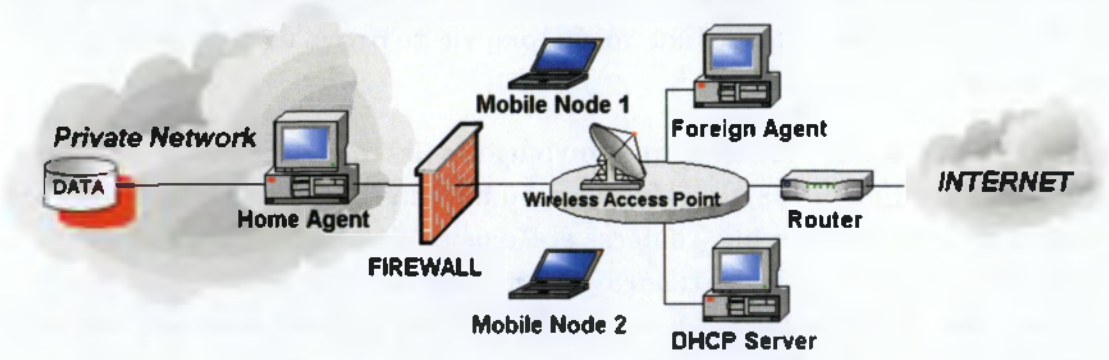
Ο Pahlke, τέλος, προτείνει την ανάπτυξη ειδικών πυλών που δεν περιλαμβάνουν ασφάλεια (π.χ., firewall) και ξένη λειτουργικότητα παράγοντα στο ίδιο κόμβο. Τα IPSec tunnels είναι εγκατεστημένα μεταξύ των κόμβων για την επίτευξη της ασφάλειας. Η προσέγγιση αυτή, αφήνει τους κινητούς κόμβους αμετάβλητους αλλά απαιτεί την παρουσία των εν λόγω κόμβων σε οποιοδήποτε επισκεπτόμενο δίκτυο. Επιπλέον, η ασφάλεια ενός ασύρματου σύνδεσμο απαιτεί

σύνδεση σε επίπεδο μηχανισμών που οδηγούν σε ενδεχομένως επανάληψη της κρυπτογράφησης.

4.8.2. Secured Mobile IP (SecMIP)

Σενάριο SecMIP

Έχουμε επιλέξει μια λεγόμενη screened-subnet firewall αρχιτεκτονική, όπου ο οργανισμός του εσωτερικού δικτύου απομονώνεται από το Internet από μια αποστρατικοποιημένη ζώνη (DMZ). Το τείχος προστασίας μεταξύ του DMZ και του εσωτερικού ιδιωτικού δικτύου είναι το μόνο σημείο εισόδου στο ιδιωτικό δίκτυο του οργανισμού (Σχήμα 43). Αυτό απλοποιεί σημαντικά τη διαχείριση της ασφάλειας, επειδή όλη η κίνηση πρέπει να περάσει αυτό το τείχος προστασίας. Επιπλέον, οι ιδιωτικές διευθύνσεις που χρησιμοποιούνται για τα ιδιωτικά δίκτυα κρύβουν την τοπολογία του ιδιωτικού δικτύου όταν τα πακέτα διοχετεύονται (π.χ., με το IPSec σε tunnel) μέσα σε ένα δημόσιο δίκτυο. Για να εξασφαλιστεί η προστασία της ιδιωτικής ζωής των εν λόγω εικονικών ιδιωτικών δικτύων (VPN), συνήθως αναπτύσσονται μηχανισμοί κρυπτογράφησης.



Σχήμα 43 : Σενάριο SecMIP

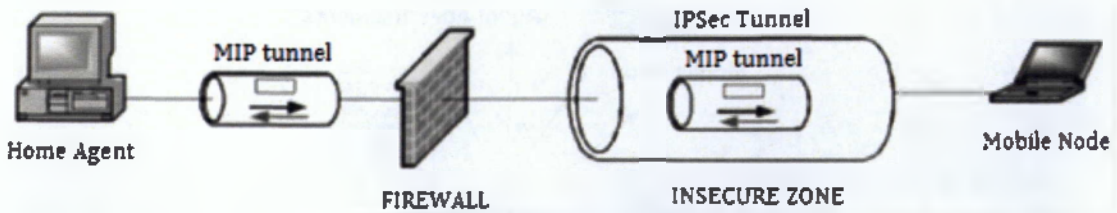
Η κύρια απαίτηση που οδήγησε στην ανάπτυξη της Mobile IP είναι ότι ένα ιδιωτικό εταιρικό δίκτυο δεν πρέπει να είναι εκτεθειμένο σε τυχόν νέες απειλές για την ασφάλεια. Ο πιο εύκολος και αποτελεσματικός τρόπος για την εκπλήρωση αυτής της απαίτησης είναι να τοποθετήσετε όλες τις Mobile IP συσκευές (εκτός από τη δική σας στο σπίτι), έξω από το ιδιωτικό δίκτυο, δηλαδή την τοποθέτησή τους στο DMZ. Αυτή η τοποθέτηση των ξένων πρακτόρων επιτρέπει μη-περιορισμένη πρόσβαση στο Internet από κινητούς κόμβους πελατών, επειδή μπορεί να αντιμετωπίζονται όπως και κάθε host στο δημόσιο Internet. Φυσικά, ο κινητός κόμβος μόνος του θα πρέπει να προστατεύεται από επιθέσεις που προέρχονται από άλλους κόμβους Διαδικτύου, π.χ. με ένα firewall λογισμικό συστήματος τέλους στο κινητό κόμβο.

Υποθέτουμε ότι οι κινητοί κόμβοι λαμβάνουν τι; IP διευθύνσεις τους από διακομιστές DHCP. Όλα οι κινητοί κόμβοι είναι πάντα έξω από το τείχος προστασίας, δηλαδή το DMZ, ακόμα και αυτά που ανήκουν στην εταιρεία. Αυτό σημαίνει ότι ενώ είναι συνδεδεμένοι με ένα ασύρματο LAN, οι κινητοί κόμβοι δεν βρίσκονται ποτέ στο υποδίκτυο του HA και ποτέ δεν καταγράφονται στο σπίτι. Οι κινητοί κόμβοι που επισυνάπτονται στο φυσικά προστατευμένο ενσύρματο ιδιωτικό δίκτυο σταματούν στο Mobile IP tunneling.

Παρά τους περιορισμούς που προκύπτουν από την ταχύτητα αυθεντικοποίησης και κρυπτογράφησης των δεδομένων που αποστέλλονται από το DMZ του οργανισμού μας για το firewall, τα οφέλη της ασφάλειας δικαιολογούν αυτή την έννοια. Είναι ακόμη δυνατό να μειωθεί η κίνηση στο εσωτερικό ιδιωτικού δικτύου, επειδή δεν απαιτούνται πια οι διαφημίσεις των HA. Εάν οι πολιτικές ασφάλειας του οργανισμού επιτρέπουν στους MNs του να συνδεθούν εντός του εσωτερικού δικτύου, όλες οι Mobile IP λειτουργίες θα πρέπει να απενεργοποιηθούν για να εξασφαλιστεί ότι τα σημεία ασύρματης σύνδεσης χρησιμοποιούνται μόνο με ένα ασφαλές Mobile IP.

4.8.3. IPSec σε SecMIP

Δεδομένου ότι οι κινητοί κόμβοι που ανήκουν στην εταιρεία πρέπει να διασχίσουν το τείχος προστασίας για να έχουν πρόσβαση στο ιδιωτικό δίκτυο, πρέπει να αυθεντικοποιηθούν στο firewall με τη χρήση IPSec. Δεδομένου ότι υπάρχει μια πραγματική αυθεντικοποίηση από άκρο-σε-άκρο μεταξύ των κινητών κόμβων της εταιρίας τους και το firewall, μπορούν εύκολα να ρυθμιστούν με μυστική ή δημόσια κλειδιά. Η δημιουργία ενός ασφαλούς IPSec tunnel μεταξύ του κινητού κόμβου και του firewall (Σχήμα 44) επιτρέπει τη χρήση μιας "ελαφριάς" εφαρμογής Mobile IP χωρίς μηχανισμούς ασφάλειας, επειδή όλα τα πακέτα διασχίζουν το δημόσιο δίκτυο κρυπτογραφούνται και επικυρώνονται από το IPSec.



Σχήμα 44 : SecMIP tunneling

Παρόμοια με την πρόταση των Gupta και του Montenegro, η SecMIP χρησιμοποιεί ένα IPSec tunnel για την προστασία του Mobile IP tunnel περνώντας τις πιο επισφαλής περιοχές του Διαδικτύου. Στο ιδιωτικό δίκτυο, ωστόσο, το Mobile IP tunnel είναι επαρκής. Το ISAKMP / Oakley έχει επιλεγεί για

SecMIP. Το ISAKMP / Oakley είναι παρόμοιο με το SKIP, αλλά έχει μερικά πλεονεκτήματα:

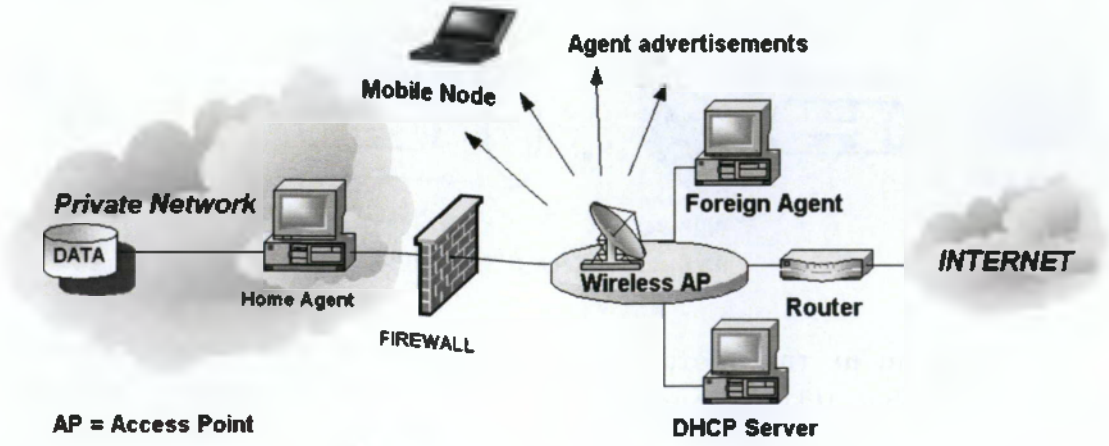
- Αφού ολοκληρώσει τις διαπραγματεύσεις για την εταιρική ασφάλεια του, τα πακέτα δεν περιέχουν ένα κλειδί διαχείρισης header όπως στο SKIP.
- Ο εισβολέας δεν γνωρίζει ποιοί είναι οι αλγόριθμοι που χρησιμοποιούνται για την κρυπτογράφηση και την αυθεντικοποίηση, σε αντίθεση με το SKIP.
- ISAKMP προκαλεί λιγότερες ανταλλαγές των παραμέτρων ασφαλείας. Αν και είναι πολλές οι παράμετροι που περιέχονται σε κάθε πακέτο SKIP, στην περίπτωση της ISAKMP αυτές οι παράμετροι αποθηκεύονται στον τομέα των ασφαλών ενώσεων που έχουν εγκατασταθεί πριν από την ανταλλαγή δεδομένων.

4.8.4. SecMIP Λειτουργία

Σε αυτήν την ενότητα θα περιγράψουμε τη λειτουργία SecMIP λεπτομερειακά. Αυτό γίνεται βήμα-βήμα θεωρώντας ένα κινητό κόμβο να αλλάζει το σημείο της προσάρτησης.

Βήμα 1: Ανίχνευση δικτύου.

Μετά την εισαγωγή μιας νέας δικτυακής περιοχής, ένας κινητός κόμβος πρέπει να συνδέεται μέσω ενός σημείου πρόσβασης ασύρματου δικτύου (Σχήμα 45). Διαφημίσεις εξωτερικών παραγόντων(FA) μεταδίδονται τακτικά σε αυτό το αποστρατικοποιημένο δίκτυο. Με τη λήψη ενός μηνύματος ICMP, ο κινητός κόμβος "μαθαίνει" ότι έχει μόλις εισέλθει σε ένα νέο δίκτυο. Ο κινητός κόμβος μπορεί να στείλει επίσης ένα παράγοντα παράκλησης για να ενεργοποιήσει μια διαφήμιση παράγοντα. Στη συνέχεια, ο κινητός κόμβος σταματά το παλιό IPSec tunnel, που ήταν εγκατεστημένο σε άλλο δίκτυο χρησιμοποιώντας ένα παλιό συνεγκατεστημένο care-of-address.



Σχήμα 45 : Ανίχνευση δικτύου SecMIP

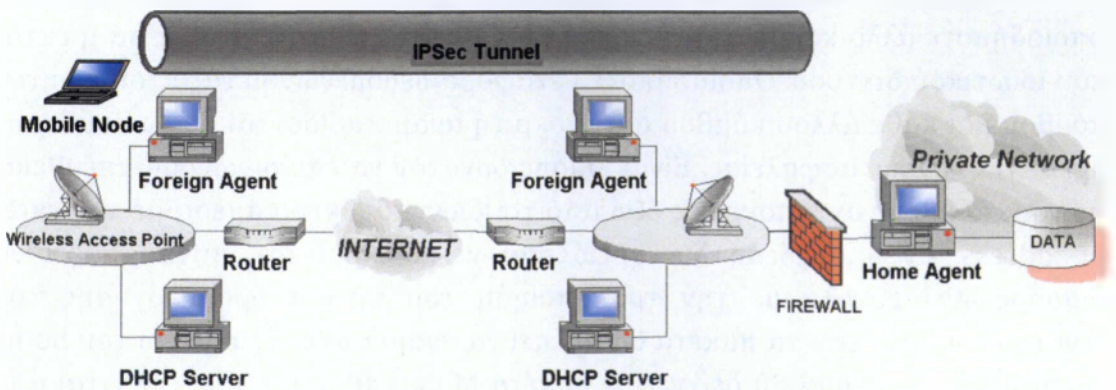
Βήμα 2: Η απόκτηση μιας δρομολογημένης διεύθυνση IP.

Ο κινητός κόμβος πρέπει να αποκτήσει ένα συνεγκατεστημένο care-of-address από DHCP διακομιστές (Σχήμα 46) ή ξένους παραγόντων. Ωστόσο, είναι μάλλον κοινό στις μέρες μας να πάρει care-of-address από DHCP διακομιστές, οι οποίες αναπτύσσονται συνήθως σε ασύρματα LAN περιβάλλοντα. Αυτό αποτρέπει επίσης την ύπαρξη ξένων παραγόντων, η οποία είναι, ούτως ή άλλως, η περίπτωση στο IPv6.

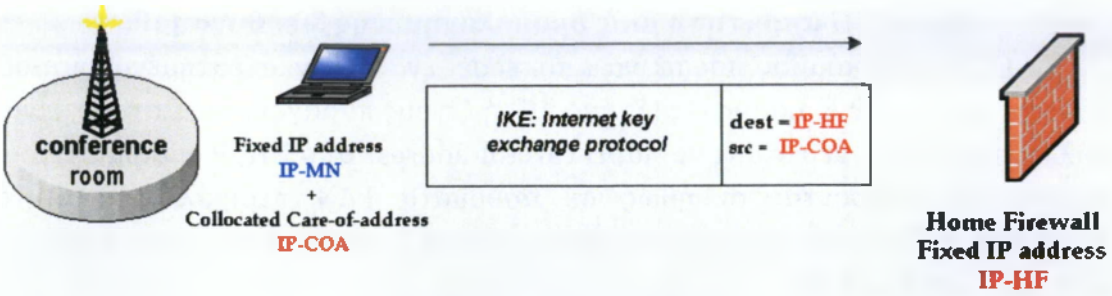
Σχήμα 46 : Απόκτηση μιας συνεγκατεστημένης Care-of-Address

Βήμα 3: Δημιουργία ενός αμφίδρομου IPSec tunnel μεταξύ του κινητού κόμβου και του home firewall.

Όπως φαίνεται στο Σχήμα 47, τα πακέτα δεδομένων πέρασαν ένα ανασφαλές, δημόσιου δικτύου μεταξύ του κινητού κόμβου και του home firewall. Ως εκ τούτου, μια λογική προσέγγιση είναι η δημιουργία ενός IPSec tunnel μεταξύ της care-of-address του κινητού κόμβου και του home firewall πριν από οποιαδήποτε Mobile IP μηνύματα που ανταλλάσσονται μεταξύ του κινητού κόμβου και του οικιακού δικτύου του. Το IPSec tunnel παρέχει αυθεντικοποίηση, ακεραιότητα, και μυστικότητα κάθε πακέτου IP που αποστέλλεται κατά τη διάρκεια της διαδικασία εγγραφής της Mobile IP. Το Σχήμα 48 δείχνει τα πακέτα που ανταλλάσσονται στο βήμα 3 μεταξύ των care-of-address των κινητών κόμβων και το home firewall. Τα πακέτα ωφέλιμου φορτίου μεταφέρουν τις πληροφορίες για την κύρια και γρήγορη λειτουργία του πρωτοκόλλου Internet Key Exchange (IKE).



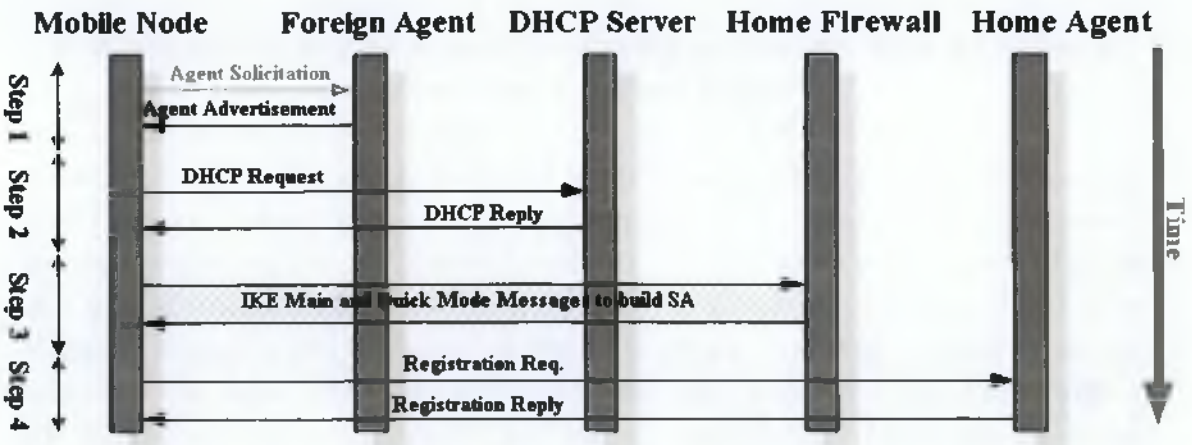
Σχήμα 47 : IPSec Tunnel Mobile Node – Home Firewall



Σχήμα 48 : Πακέτα IPSec

Βήμα 4: Εγγραφή της Mobile IP στο Home Agent.

Σε αυτό το βήμα, ο κινητός κόμβος καταγράφει στο Home Agent. Αφού όλες οι διαπραγματεύσεις της Mobile IP μεταξύ home agent και κινητού κόμβου πέρασαν το IPSec tunnel στο home firewall, δεν υπάρχει ανάγκη για άλλη αυθεντικοποίηση / κρυπτογράφηση στα μηνύματα εγγραφής της Mobile IP. Υποθέτουμε ότι το ιδιωτικό δίκτυο πίσω από το firewall είναι ασφαλής. Στο Σχήμα 49 συνοψίζεται η ανταλλαγή μηνυμάτων κατά τη διάρκεια βήματα 1 έως 4.

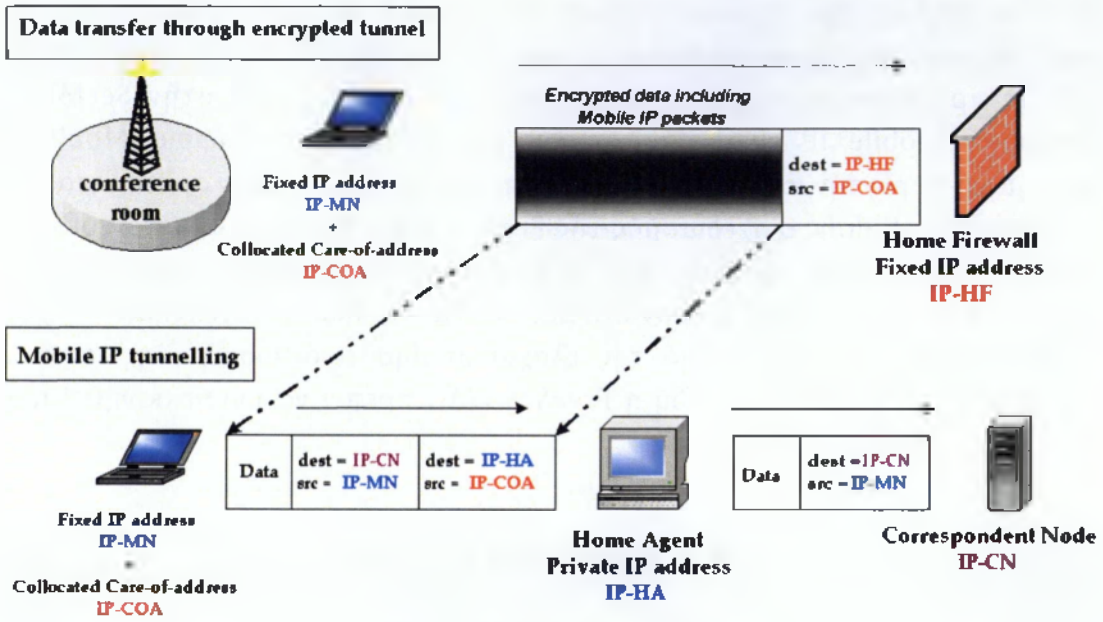


Σχήμα 49 : Ανταλλαγή μηνυμάτων

Βήμα 5: Μεταφορά δεδομένων.

Μέχρι την επόμενη κίνηση, ο κινητός κόμβος μπορεί να επικοινωνεί με οποιοδήποτε άλλο κόμβο ανταποκριτή ανεξάρτητα αν αυτό είναι μέσα ή εκτός του ιδιωτικού δικτύου. Οποιαδήποτε μεταφορά δεδομένων μεταξύ του κινητού κόμβου και κάθε άλλου κόμβου ανταποκριτή αναμεταδίδονται μέσω του home agent για λόγους ασφαλείας. Είναι επίσης δυνατόν να επικοινωνούν απευθείας με τους κόμβους ανταποκριτές έξω από το ιδιωτικό δίκτυο άμεσα με την care-of-address, αν η σύνδεση δεν χρειάζεται να ασφαλίζεται. Αυτό μπορεί να διαμορφωθεί εύκολα με την τροποποίηση του πίνακα δρομολόγησης του κινητού κόμβου, είτε τα πακέτα θα πρέπει να αναμεταδίδονται μέσω του home agent ή όχι. Το Σχήμα 50 δείχνει τα πακέτα Mobile IP που αποστέλλονται από

ένα κινητό κόμβο σε κόμβο ανταποκριτή. Τα κρυπτογραφημένα και επικυρωμένα πακέτα Mobile IP είναι αποκρυπτογραφημένα και απεγκλωβίζονται από το home firewall και παραδίδονται στον home agent. Το home agent τελικά απεγκλωβίζει αυτά τα πακέτα Mobile IP και τα παραδίδει στους κατάλληλους δέκτες, τους κόμβους ανταποκριτές.



Σχήμα 50 : Πακέτα SecMIP

4.9 Εφαρμογή της SecMIP

4.9.1. Η Dynamics Mobile IP και η FreeS/ Wan IPSec

Η SecMIP έχει εφαρμοστεί σε Linux που βασίζονται σε συστήματα τέλους και δρομολογητές. Χρησιμοποιεί δύοtunnels: ένα για υποστήριξη της κινητικότητας και το άλλο για την IPSec.

Η Dynamics Mobile που αναπτύχθηκε από το Helsinki University of Technology (HUT) έχει επιλεγεί για την Mobile IP. Η υλοποίηση αποτελείται από τρία εκτελέσιμα προγράμματα: ένα για κάθε συστατικό Mobile IP, δηλαδή home agent, foreign agent και mobile node. Ο πηγαίος κώδικας είναι διαθέσιμος σε C και όλα τα χαρακτηριστικά του είναι συμβατά με RFC. Η διαμόρφωση των συστατικών είναι σχετικά απλή. Υπάρχει ένα αρχείο διαμόρφωσης για καθένα από αυτά. Κατά την εφαρμογή της SecMIP, η Dynamics Mobile IP χειρίζεται τις διαφημίσεις του agent (εσωτερικών και εξωτερικών), η Mobile IP καθορίζει tunnels μεταξύ home agent και mobile node, συλλαμβάνει και ανακατευθύνει πακέτα για το κινητό κόμβο στο οικιακό δίκτυο.

Η FreeS / Wan (Free Secure WAN) συνεργάζεται με την RSA και για κάθε κόμβο της IPSec ενός ζεύγους κλειδιών RSA πρέπει να δημιουργηθεί. Οι

επιτρεπόμενες συνδέσεις πρέπει να περιγράφεται σε ένα αρχείο ρυθμίσεων. Η FreeS / WAN διαπραγματεύεται κλειδιά μεταξύ κινητών κόμβων και home firewall, εγκαθιστά προστατευμένα tunnels μεταξύ του κινητού κόμβου και home firewall, και κρυπτογραφεί / αυθεντικοποιεί όλα τα δεδομένα μεταξύ του κινητού κόμβου και home firewal.

Η Dynamics Mobile IP και η FreeS / Wan έχουν επιλεγεί λόγω της διαθεσιμότητας του πηγαίου κώδικα τους, αλλά αυτές οι υλοποιήσεις δεν προορίζονται να συγχωνευθούν. Ως εκ τούτου, θα έπρεπε να εκτελέσουμε πολλές προσαρμογές, προτού να εργαστεί με επιτυχώς μαζί στην SecMIP. Η Dynamics Mobile IP είναι πάρα πολύ "βαριά" και μια ελαφριά Mobile IP εφαρμογή χωρίς την ισχυρή υποστήριξη της ασφάλειας θα ήταν αρκετή για τους σκοπούς μας. Επίσης ο σχεδιασμός της FreeS / WAN δεν είναι αρκετά ευέλικτη, επειδή όλες οι IPSec συσκευές που μόλις ξεκίνησαν για πρώτη φορά από την έναρξη λειτουργίας του δαίμονα IPSec. Αυτά τα δύο μειονεκτήματα έχουν συνέπειες για τον περιορισμό της ελαχιστοποίησης καθυστέρησης κατά τη διάρκεια ενός handover, επειδή η FreeS / WAN πρέπει να επανεκκινηθεί μετά από κάθε ενημέρωση θέσης.

4.9.2. Εφαρμογή σεναρίου

Το κύριο μέρος του έργου ήταν η υλοποίηση την επίτευξη της διαλειτουργικότητας μεταξύ της Dynamics Mobile IP, της FreeS / WAN, και του λειτουργικού συστήματος. Για το λόγο αυτό, έχουν αναπτυχθεί τα παρακάτω σενάρια.

Η Αποσύνδεση εκτελεί μια Dynamics Mobile IP API κλήση η οποία στέλνει ένα μήνυμα διαγραφής στο home agent και αποσυνδέει το κινητό κόμβο από το home agent.

Η **Σύνδεση** εκτελεί μια Dynamics Mobile IP API κλήση η οποία στέλνει ένα μήνυμα εγγραφής στο home agent και καθιερώνει ένα άμεσο tunnel μεταξύ του κινητού κόμβου και του home agent.

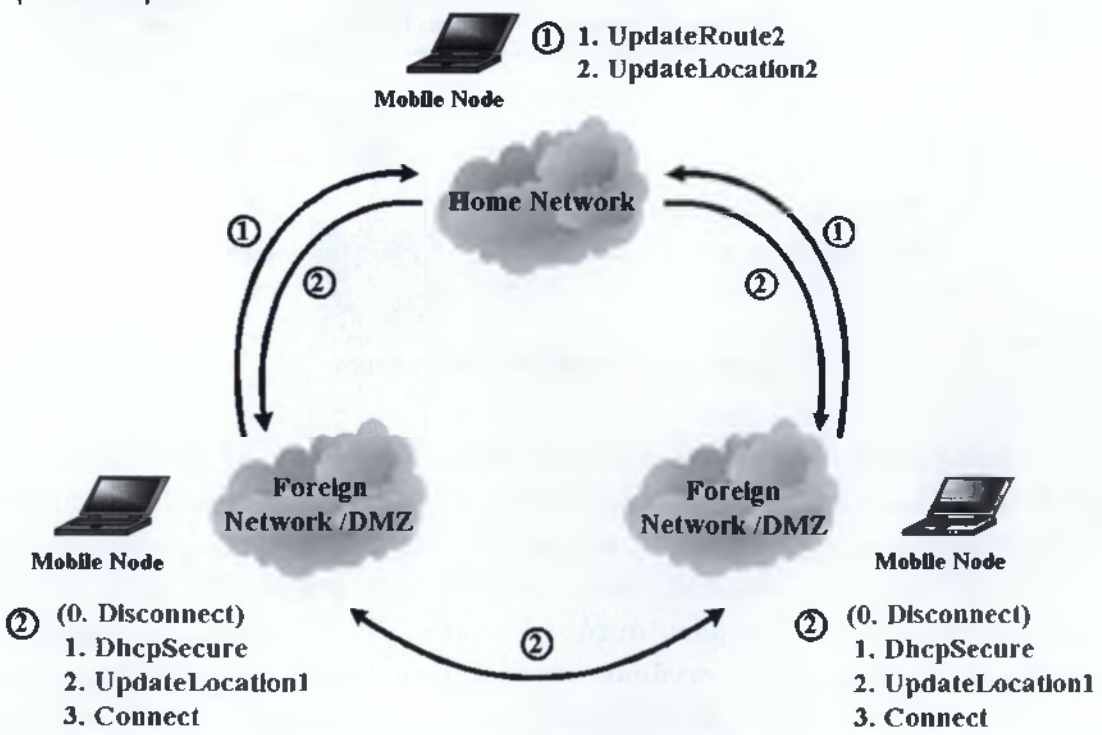
Η **DhcpSecure** στέλνει ένα αίτημα DHCP και τις ενημερώσεις διαμόρφωσης του δικτύου διασύνδεσης και του πίνακα δρομολόγησης. Στη συνέχεια, μια IPSec σύνδεση στο home firewall χτίζεται.

Η **UpdateLocation1** (σε ένα ξένο δίκτυο) και **UpdateLocation2** (στο οικιακό δίκτυο): By the API call 'update interface' the process dynamics_admin can be forced to read the actual IP configuration of the interface. Αν η διαμόρφωση αυτή είναι ταυτόσημη με τη home διαμόρφωση, ο κινητός κόμβος είναι στο home και στέλνει μια διαγραφή μηνύματος στο home agent (UpdateLocation2). Διαφορετικά, επικαλείται μια νέα διαδικασία εγγραφής (UpdateLocation1).

Η **UpdateRoute1** ενημερώνει τον πίνακα δρομολόγησης του κινητού κόμβου, όταν συνδέεται σε ένα ξένο δίκτυο και όταν το Mobile IP tunnel μεταξύ του κινητού κόμβου και του home agent είναι εγκατεστημένο. Όταν ο κινητός κόμβος φθάνει στο home, το IPSec και τα Mobile IP tunnels πρέπει να είναι ανίκανα και ο πίνακας δρομολόγησης πρέπει να ενημερωθεί και πάλι (**UpdateRoute2**).

Το **Firewall.rc**: Για τον έλεγχο των εισερχόμενων και εξερχόμενων κινήσεων στο δίκτυο του κινητού κόμβου, ένα IP-Filter είναι αρχικοποιημένο χρησιμοποιώντας ipchains. Ο κινητός κόμβος έχει μια προεπιλεγμένη firewall διαμόρφωση, η οποία προστατεύει ενάντια των εισβολέων. Αυτή η προστασία είναι πάντα ενεργοποιημένη. Όταν δεν συνδέονται με το οικιακό δίκτυο, ο κινητός κόμβος επιτρέπεται μόνο να επικοινωνεί με τους κόμβους του ιδιωτικού δικτύου μέσω μιας ασφαλής συσκευής IPSec. Αυτό εγγυάται το απόρρητο των δεδομένων.

Τα σενάρια τρέχουν στο κινητό κόμβο για να διασφαλίσει Mobile IP που χρησιμοποιεί πάντα ένα ασφαλές περιβάλλον δικτύου για να επικοινωνεί με το οικιακό δίκτυο. Μόλις η Dynamics Mobile IP και η FreeS / Wan της IPSec έχουν ξεκινήσει, τα σενάρια εκτελούνται όπως φαίνεται στο Σχήμα 51. Όλες οι κλήσεις του σεναρίου που τοποθετήθηκαν στο πηγαίο κώδικα της Dynamics Mobile IP. Δεδομένου ότι δεν ήταν αναγκαίες οι αλλαγές με τον πηγαίο κώδικα της FreeS / WAN, μπορούμε επίσης να χρησιμοποιήσουμε εναλλακτικές IPSec υλοποιήσεις. Η χρήση οποιουδήποτε άλλου home agent και πύλης IPSec είναι δυνατή στο οικιακό δίκτυο, επειδή μόνο ο κώδικας του κινητού κόμβου έπρεπε να τροποποιηθεί.

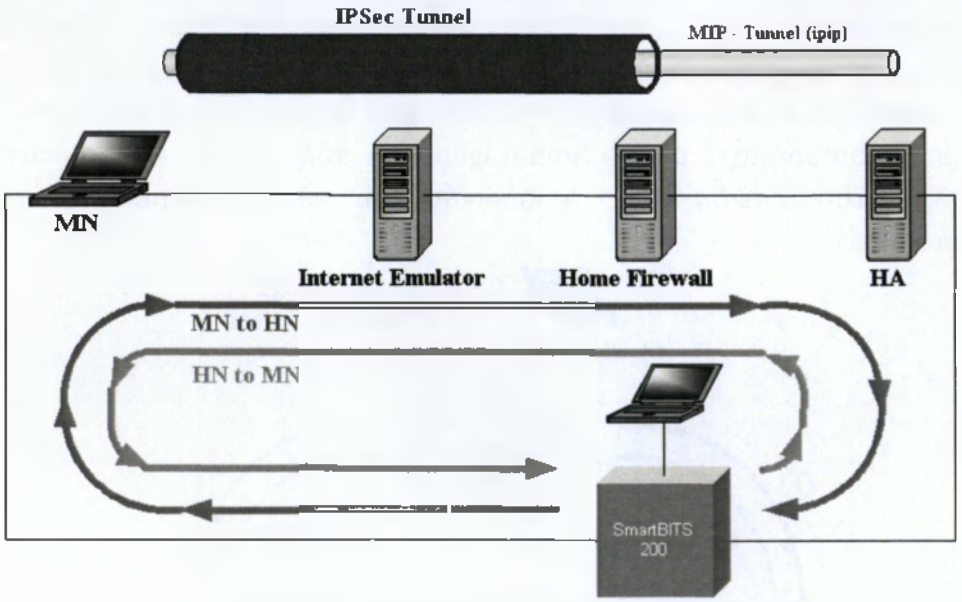


Σχήμα 51 : Σενάρια της SecMIP

4.9.3. Αξιολόγηση των επιδόσεων

Η απόδοση της SecMIP υλοποίησης έχει αξιολογηθεί για να αποδείξει την αποτελεσματικότητα της προτεινόμενη προσέγγισης για επικοινωνίες προστασίας της Mobile IP. Οι δοκιμές που έχουν διεξαχθεί με τη βοήθεια ενός κουτί δοκιμής δικτύου το SMARTBITS 200, το οποίο έχει μέχρι τέσσερις διεπαφές Ethernet στις οποίες η κυκλοφορία μπορεί να παραχθεί και τα στατιστικά στοιχεία μπορούν να αξιολογηθούν. Όλες οι συσκευές Ethernet για τη δοκιμαστική στήριξη της υποδομής των 100 Mbps σε πλήρη λειτουργία εκτύπωσης διπλής όψης.

Η γεννήτρια κίνησης που παράγονται μονής κατεύθυνσης ροές των πακέτων IP μέχρι και 100 Mbps. Το Σχήμα 52 δείχνει το σενάριο του δικτύου που χρησιμοποιείται για τις διάφορες δοκιμές. Κανένα tunnel δεν έχει καθοριστεί για το σενάριο δοκιμής 1, το tunnel της Mobile IP έχει χρησιμοποιηθεί για τα σενάρια 2 και 3, ενώ το tunnel της IPSec έχει καθιερωθεί για το σενάριο 3 μόνο.

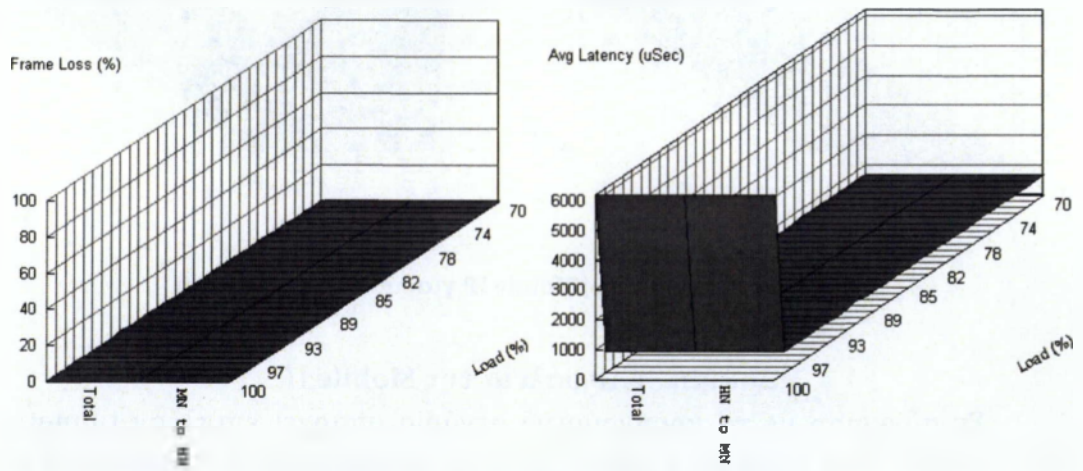


Σχήμα 52 : Δοκιμή ρύθμισης δικτύου

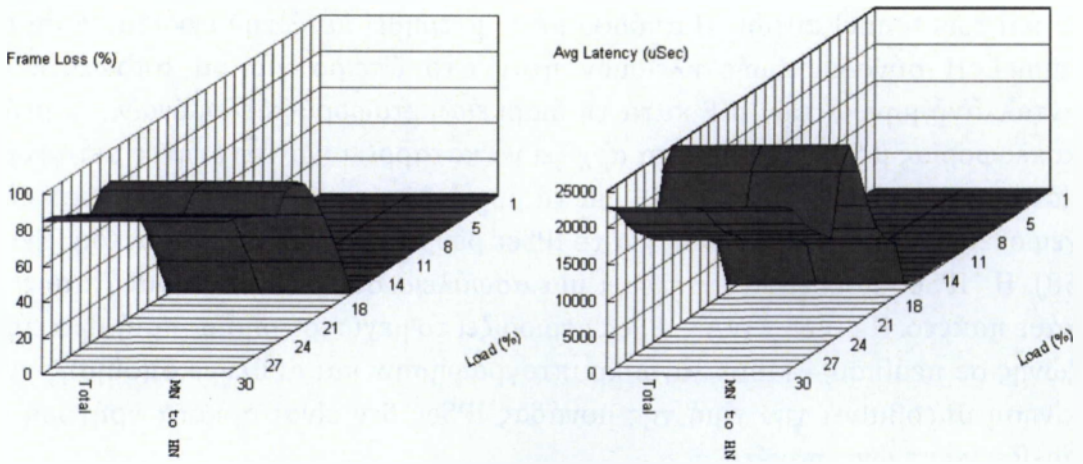
Δύο διαφορετικά μεγέθη πλαισίου έχουν δοκιμαστεί: 64 bytes και 1400 bytes. Τα μικρότερα πακέτα μετέφεραν UDP / IP, όπως συχνά χρησιμοποιείται σε εφαρμογές ροής ή Voice over IP, και τα μεγαλύτερα έχουν χρησιμοποιηθεί για TCP / IP δεδομένα προσομοίωσης μαζικής μεταφοράς δεδομένων. Στα διαφορετικά σενάρια δοκιμών, αυτά τα πακέτα IP στη συνέχεια αλλάζουν συμπεριφορές. Στο πρώτο σενάριο, οι ενδιάμεσοι δρομολογητές έχουν μόλις δρομολογηθεί. Στο δεύτερο σενάριο, τα πακέτα ήταν έγκλειστα από tunnel της Mobile IP (IP σε IP), το οποίο επεκτείνει τα μεγέθη πλαισίου με ένα πρόσθετο IP header(20 bytes). Στο τρίτο σενάριο φέρεται επιπλέον πληροφορία IPSec.

Δοκιμή 1: Απόδοση χωρίς SecMIP

Στο πρώτο σενάριο, η απόδοση χωρίς tunneling ή πρόσθετη επεξεργασία οφείλεται στη Mobile IP ή στην IPSec που έχει μετρηθεί (Σχήμα 53). Η μόνη επεξεργασία από τους ενδιάμεσους δρομολογητές είναι προώθηση πακέτων. Αυτό επιτρέπει την αξιολόγηση της απόδοσης της δοκιμασίας υποδομή. Τα διαγράμματα δείχνουν την καθυστέρηση και την απώλεια πλαισίου που εξαρτάται από την κίνηση από τον κινητό κόμβο στο οικιακό δίκτυο. Μετρήσεις για την αντίθετη κατεύθυνση ήταν παρόμοια. Δεν είναι έκπληξη το γεγονός ότι η απόδοση εξαρτάται σε μεγάλο βαθμό από το παραγόμενο μέγεθος του πακέτου της κυκλοφορίας του. Ο αντίκτυπος για τις επιδόσεις των δρομολογίων είναι πολύ ισχυρότερος για μικρότερα πακέτα (Σχήμα 54).



Σχήμα 53 : Απόδοση για πακέτα των 1,4kB

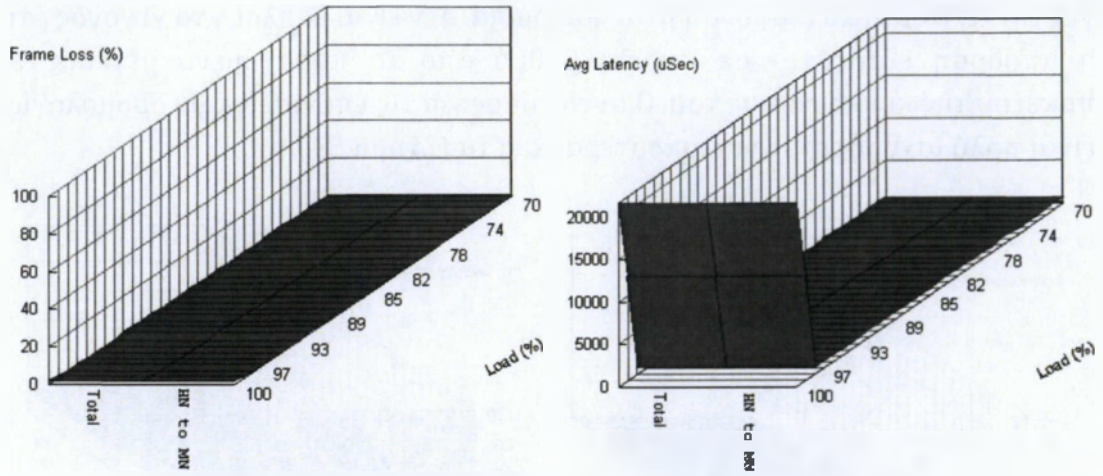


Σχήμα 54 : Απόδοση για πακέτα των 64 bytes

Δοκιμή 2: Mobile IP Tunneling

Το δεύτερο σενάριο δοκιμής ιδρύθηκε για να εκτιμήσει την επίδραση στην απόδοση του tunnel Mobile IP μεταξύ των κινητών κόμβων συνεγκατεστημένης της care-of-address και του home agent. Οι agents της

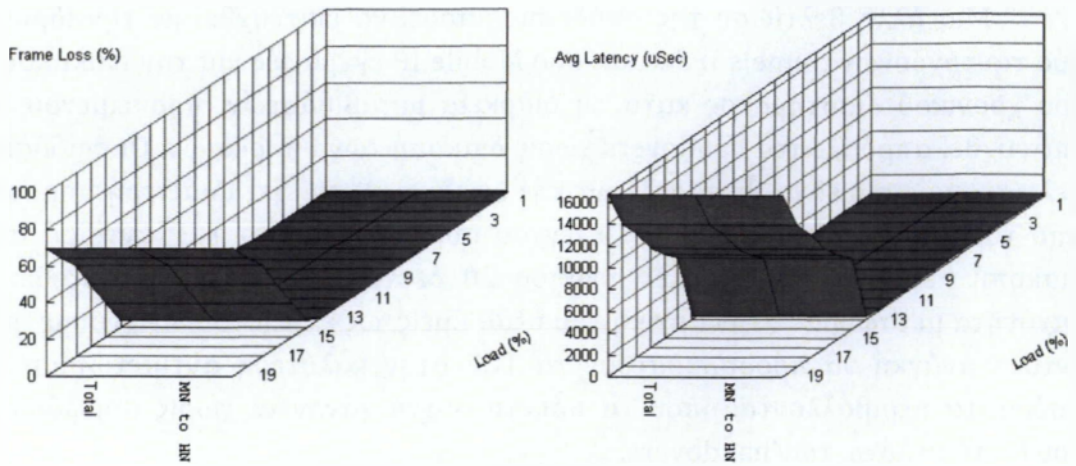
Dynamics Mobile IP ξεκίνησαν πάνω στο κινητό κόμβο και στο home agent. Ο κινητός κόμβος είναι πάλι επισυναπτόμενος σε ένα ξένο δίκτυο και χρησιμοποιεί την συνεγκατεστημένη care-of-address που απέκτησε όπως το τελικό σημείο του tunnel της Mobile IP. Η IP-in-IP ενθυλάκωση και απεγκλωβισμός είναι οι μόνες πρόσθετες επεξεργασίες. Δεν υπάρχει σχεδόν καμία επίδραση στην απόδοση λόγω του tunnel της IP-in-IP (Σχήμα 55). Και πάλι, ο μέγιστος ρυθμός δεδομένων είναι δραματικά χαμηλότερος για μικρά μεγέθη πακέτου (Σχήμα 56).



Σχήμα 55 : Απόδοση της Mobile IP για πακέτα των 1.4 Kb

Δοκιμή 3: Ασφάλεια της Mobile IP

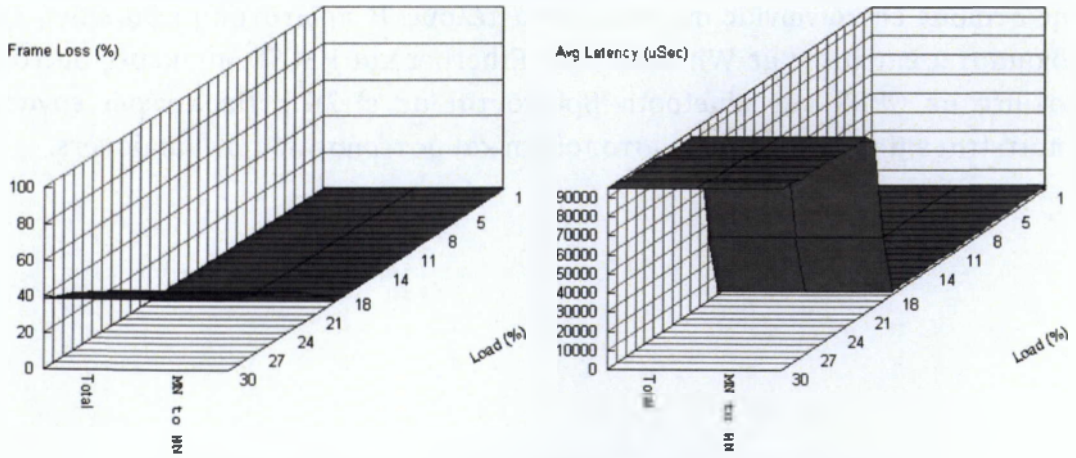
Σε σύγκριση με το προηγούμενο σενάριο υπάρχει επιπλέον tunnel της IPSec μεταξύ του κινητού κόμβου και του home firewall, προκειμένου να καταστεί δυνατή η SecMIP. Ο home firewall και ο κινητός κόμβος πρέπει να κωδικοποιήσουν και να αποκωδικοποιήσουν τα πακέτα των tunnel της Mobile IP και των tunnel αυτών. Η απόδοση έχει μετρηθεί μετά την εγκατάσταση IKE tunnel. Η σύνοδος ζωής κλειδιών ήταν στο άπειρο για να αποφευχθεί η ανταλλαγή μηνυμάτων IKE κατά τη διάρκεια μεταφοράς δεδομένων. Το ρεύμα κυκλοφορίας με μεγάλα πακέτα αρχίζει να καταρρέει για ταχύτητες μεταφοράς πάνω από 18 Mbps (Σχήμα 57). Για τα μικρά πακέτα 64 byte, η απόδοση είναι χειρότερη, διότι η επιβάρυνση για το IPSec ρεύμα είναι πολύ μεγαλύτερη (Σχήμα 58). Η IPSec πρέπει να εκτελέσει μια ασφάλεια συσχετισμού αναζήτησης για κάθε πακέτο. Η FreeS / WAN IPSec περιορίζει το μέγιστο χρησιμοποιήσιμο εύρος ζώνης σε περίπου 4 Mbps λόγω κρυπτογράφησηw και αυθεντικοποίησης. Αν η κίνηση υπερβαίνει την τιμή της μονάδας IPSec δεν είναι αρκετά γρήγορη και αρχίζει να μειώνει πακέτα.



Σχήμα 56 : Απόδοση της Mobile IP με πακέτα των 64 byte

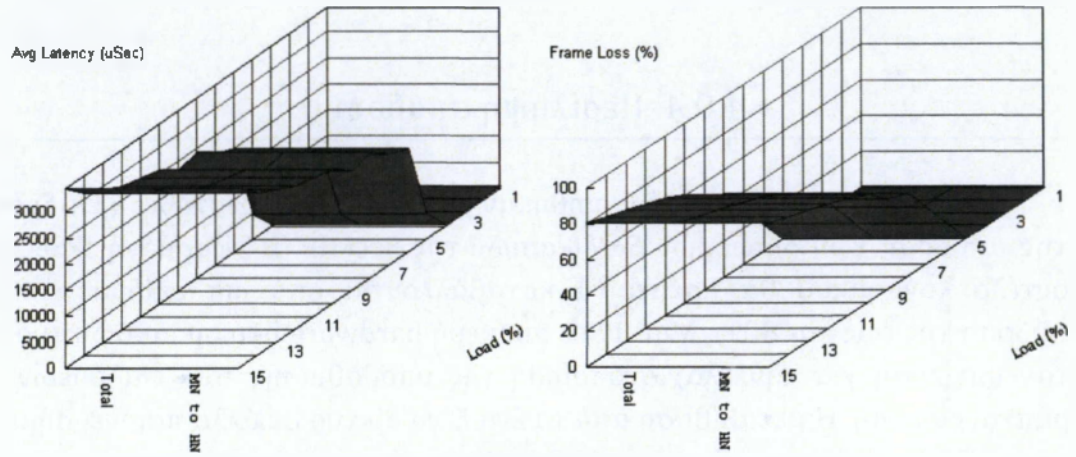
4.9.4. Περίληψη απόδοσης

Οι δοκιμές που πραγματοποιήθηκαν με σκοπό να διερευνηθεί η επίδραση στην απόδοση των διαφόρων διαδικασιών της SecMIP. Η εφαρμογή IPSec ως μοντέλο λογισμικού θα πρέπει να καταβάλλονται από μια επίδραση στην απόδοση της έως και 80%. Μια IPSec συσκευή hardware στο οικιακό δίκτυο θα ήταν μια λύση για την ελαχιστοποίηση της υποβάθμισης των επιδόσεων με κρυπτογράφηση. Η μεταβίβαση από το ένα ξένο δίκτυο σε άλλο παίρνει σήμερα έως και 7 δευτερόλεπτα. Η περισσότερη από αυτή την καθυστέρηση προέρχεται από το μοντέλο IPSec της FreeS / Wan, επειδή η παραγόμενη IPSec συσκευή πρέπει να κλείσει και να ξαναρχίσει μετά εκμάθηση μιας νέας διεύθυνσης IP. Η επανεκκίνηση του μοντέλου IPSec διαρκεί περίπου 4 δευτερόλεπτα πάνω σε δοκιμαστικούς υπολογιστές. Χρησιμοποιώντας μια πιο δυναμική μονάδα IPSec θα μπορούσε να μειώσει τη καθυστέρηση του handover στο max. 3 δευτερόλεπτα. Η καθυστέρηση οφείλεται από το DHCP για να ρυθμίσει το δίκτυο να εργαστεί σε νέο δικτυακό περιβάλλον.



Σχήμα 57 : Απόδοση της vSecMIP με πακέτα των 1.4 kB

Μια άλλη βελτίωση της απόδοσης μπορεί να επιτευχθεί με την ίδρυση δύο ταυτόχρονων tunnels IPSec και δύο Mobile IP εγγραφές για την επικάλυψη του χρονικού διαστήματος κατά τη διάρκεια μεταβιβάσεων, προκειμένου να επιτευχθεί απρόσκοπτα handovers χωρίς διακοπή των υπηρεσιών. Οι επιδόσεις βελτιστοποίησης είναι θέμα μελλοντικής έρευνας. Αυτό έχει ιδιαίτερη σημασία από τότε που ο αλγόριθμος του έλεγχου συμφόρησης του TCP αντιδρά στη διακοπή handover και διαρκεί περίπου 20 δευτερόλεπτα για να αυξηθεί η ταχύτητα μεταφοράς στην αρχική του αξία. Εμείς, ως εκ τούτου, δείχνουμε μια έντονη ανάγκη να προσαρμοστούν τα TCP στην καλύτερη αντιμετώπιση με ασύρματα περιβάλλοντα, όπου τα πακέτα συχνά χάνονται χωρίς συμφόρηση του δικτύου λόγω των handovers.



Σχήμα 58 : Απόδοση της SecMIP με πακέτα των 64 byte

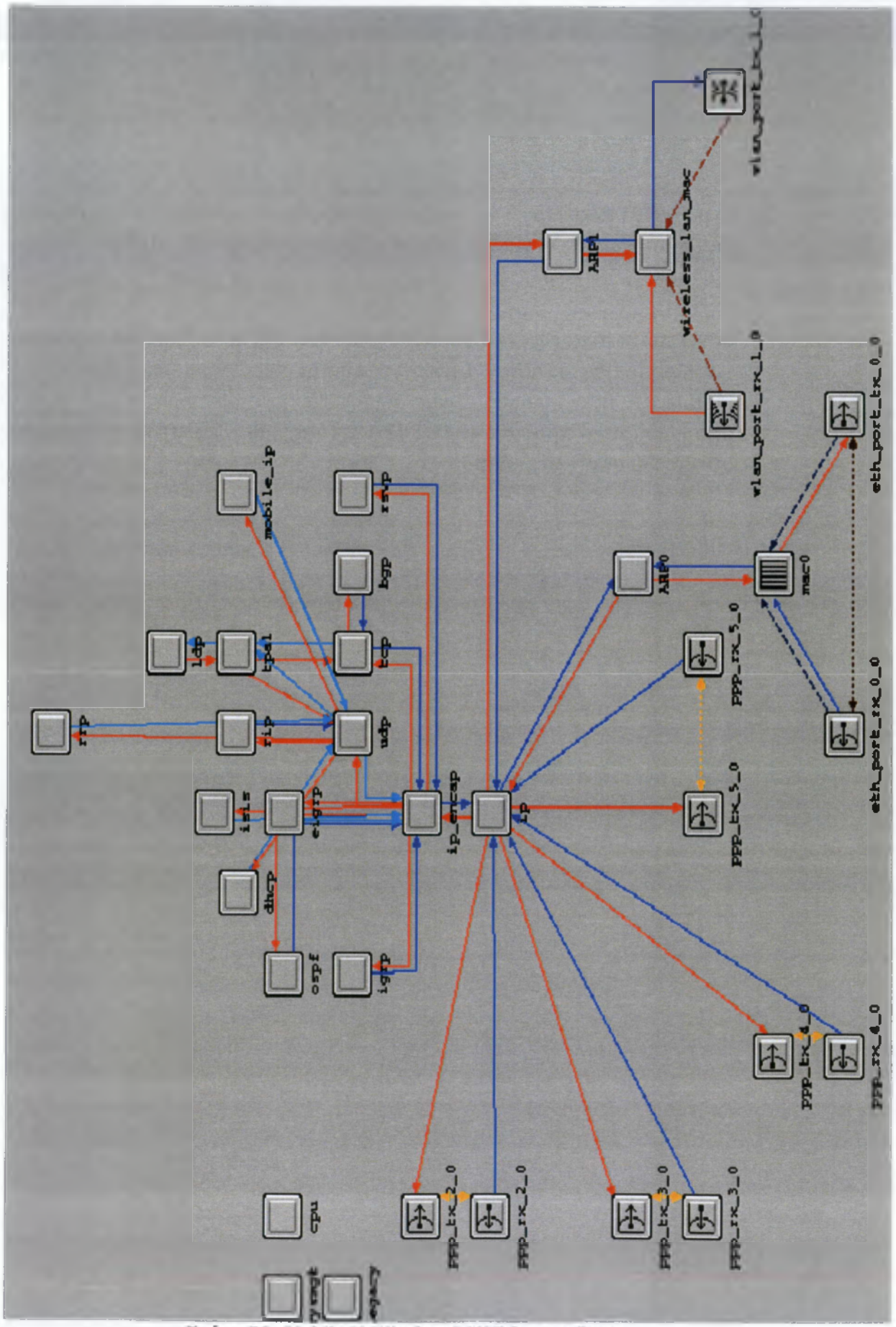
4.9.5. Συμπεράσματα

Παρουσιάσαμε μια προσέγγιση που θα επιτρέψει στους χρήστες της Mobile IP να έχουν πρόσβαση σε προστατευμένα firewall VPNs. Η λύση βασίζεται στα διαθέσιμα πρότυπα και τις απαιτούμενες μικρές τροποποιήσεις της στοίβας επικοινωνίας σε συστήματα τέλους. Η πρωτότυπη εφαρμογή έχει δοκιμαστεί επιτυχώς με Wireless LAN, Ethernet και HSCSD συσκευές δικτύου. Δοκιμές με GPRS και Bluetooth βρίσκονται σε εξέλιξη. Περαιτέρω εργασία απαιτείται επίσης για την ελαχιστοποίηση καθυστερήσεων των handovers.

Κεφάλαιο 5. Μοντέλα OPNET για την Mobile IP σε ασύρματα τοπικά δίκτυα

5.1. Μοντέλα κόμβων

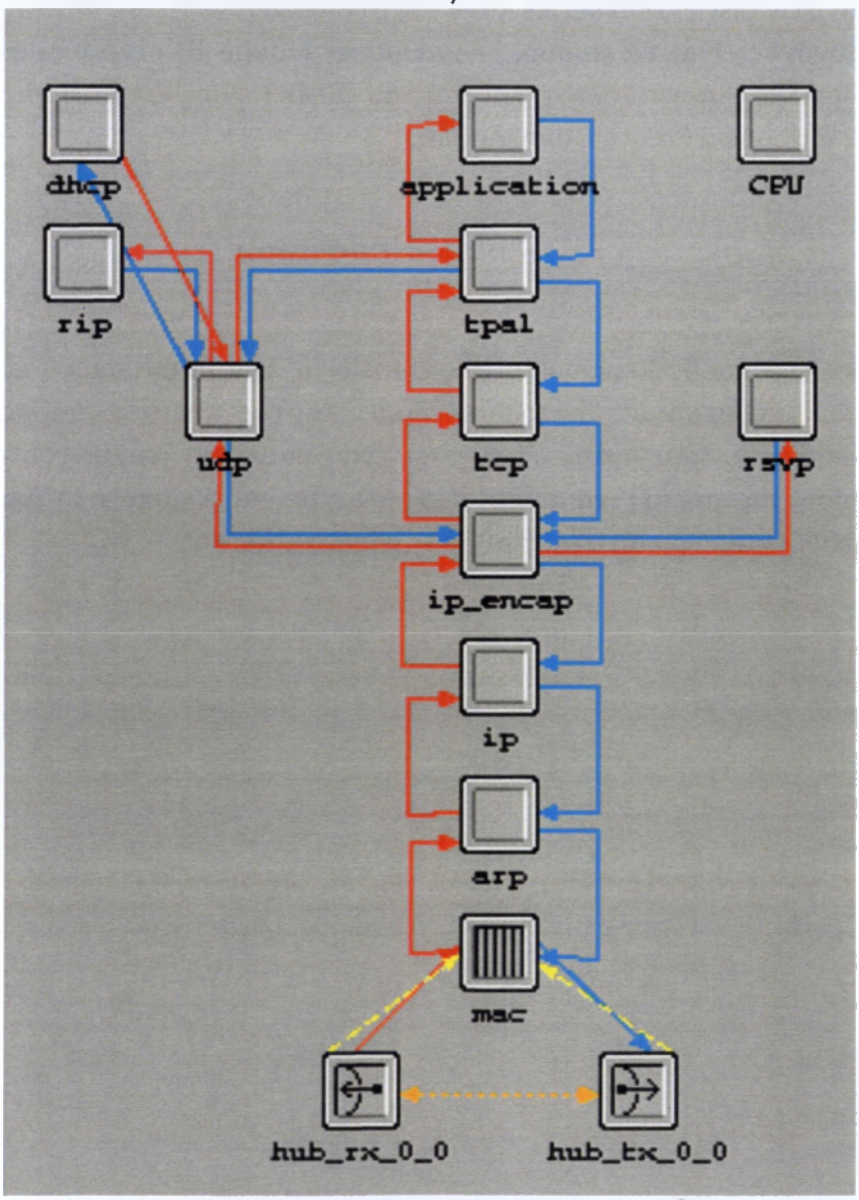
- Στο OPNET Modeler 14.5, υπάρχουν πάνω σε συνιστώμενους κόμβους και διαμορφώσεις για τα σενάρια της Mobile IP. Το σχέδιο είναι να εξηγήσει λεπτομερώς πώς το Mobile IPv4 προσομοιώνεται στο OPNET 14.5. Πρώτον, οι κόμβοι που χρησιμοποιούνται, έχουν εισαχθεί στη συνέχεια οι στάσεις τους θα διευθυνσιοδοτούνται. Για την προσομοίωση της Mobile IP στο OPNET 14.5, απαιτούνται οι ακόλουθοι κόμβοι.
- Mobile IP ικανό router για WLAN με μια διεπαφή Ethernet που υποστηρίζει το πρότυπο IEEE 802.11. Το σχήμα δείχνει τη λεπτομέρεια αυτού του μοντέλου κόμβου.



Σχήμα 59 : Mobile IP Wireless LAN Ethernet Rout

Ένα κινητό subnet μπορεί να κινηθεί με τη χαρακτηριστική τροχιά του OPNET. Μια τροχιά είναι η διαδρομή που ο κινητός κόμβος ακολουθεί μέσα στο χώρο σαν μία συνάρτηση του χρόνου. Ο χρήστης μπορεί να βρει περισσότερες λεπτομέρειες για το πώς να κάνει την επιθυμητή τροχιά σε OPNET tutorial.

Ένας σταθμός εργασίας Ethernet ανάμεσα σε client - server που εκτελούνται σε TCP / IP ή UDP / IP. Αυτός ο σταθμός εργασίας υποστηρίζει μία σύνδεση Ethernet σε 10.100 και 1000 Mb / s.



Σχήμα 60 : OPNET Ethernet σταθμού εργασίας μοντέλου κόμβου

Μια σειρά Cisco-7000 router χρησιμοποιείται στην προσομοίωση ως πύλη κόμβου για την διασύνδεση των home agent και foreign agent routers στο FTP server. Το subnet mobile αποτελείται από ένα κινητό router και ένα Ethernet σταθμού εργασίας που είναι συνδεδεμένοι μέσω ενός διπλού συνδέσμου 100BaseT που θα εξηγηθεί λεπτομερώς αργότερα.

5.2. Χαρακτηριστικά κόμβου

Σε αυτήν την ενότητα εξηγούμαι τον τρόπο με τον οποίο ο χρήστης έχει ρυθμίσει και ποιες παράμετροι έχουν οριστεί για το σενάριο της Mobile IP στους κόμβους. Είναι σημαντικό να γνωρίζουμε ότι δεν υπάρχει καμία ρύθμιση που να απαιτείται στις Cisco 7000 series και στον FTP server.

Ο στόχος είναι να προσομοιώσουμε τη Mobile IP σε ασύρματα τοπικά δίκτυα, ώστε με βάση το οδηγό χρήστη του OPNET Wireless LAN, οι κόμβοι θα πρέπει να διαμορφωθούν ως ακολούθως.

5.2.1. Mobile Node Router

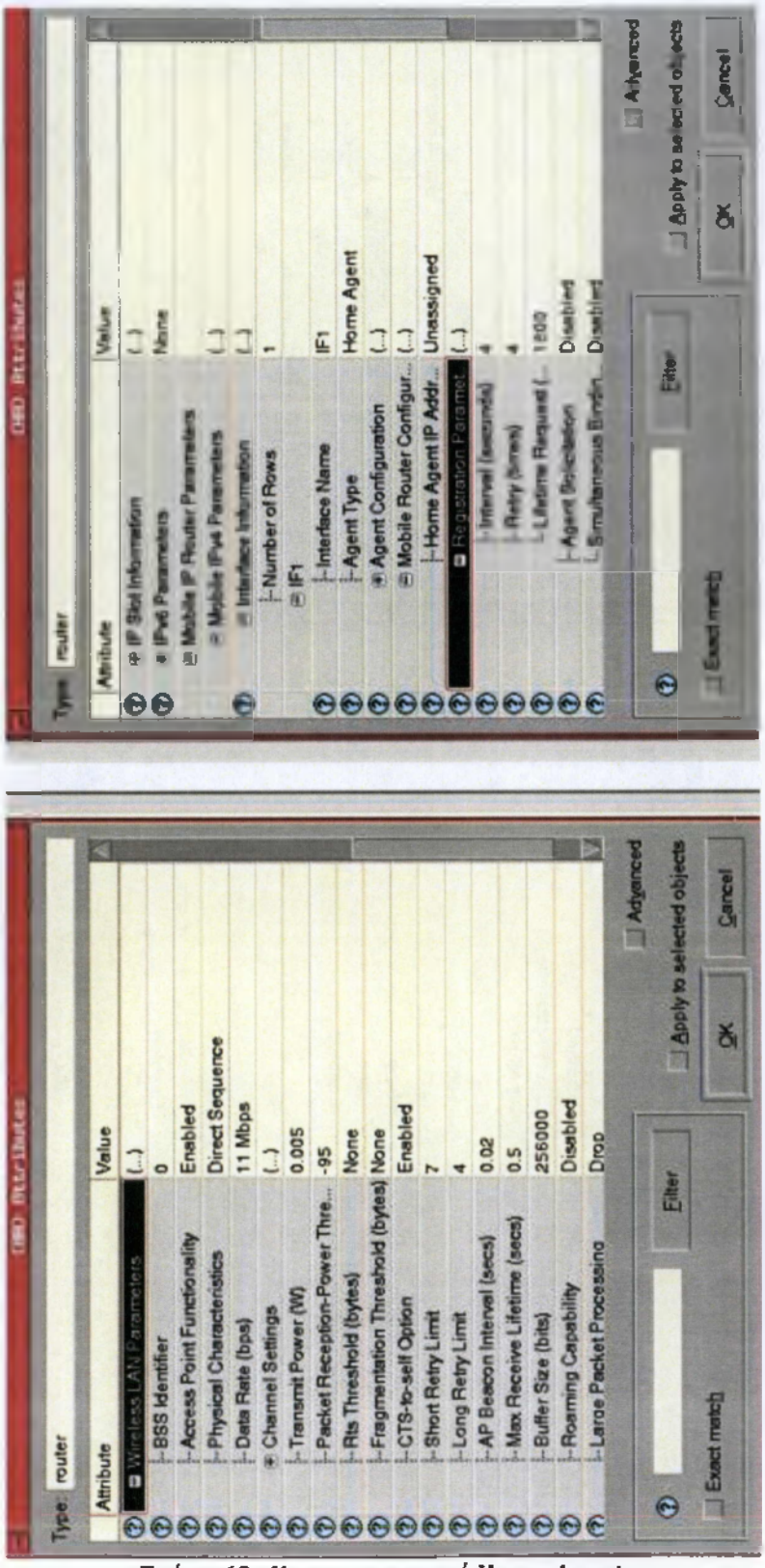
Αυτός ο κόμβος είναι στο ίδιο δίκτυο με τον home agent και κινείται μεταξύ των διαφόρων υποδικτύων. Δεδομένου ότι ο κινητός κόμβος είναι ένα κινητό υποδίκτυο που αποτελείται από έναν ικανό κινητό IP router, τότε η διαμόρφωση θα πρέπει να είναι σύμφωνα με το Σχήμα 61. Δεν υπάρχει απαιτούμενη διαμόρφωση στο σταθμό εργασίας Ethernet.

Σχήμα 61 : Χαρακτηριστικό Mobile Router


(MR) Attributes
Type router
Attribute
Value
IPv6 Parameters
None
Mobile IP Router Parameters
Mobile IPv4 Parameters
(...)
Interface Information
( )
Number of Rows
1
IF1
Interface Name
IF1
Agent Type
Mobile Router
Agent Configuration
( )
Home Agent IP Addr
192.0.8.1
Registration Paramet
( )
Agent Solicitation
Disabled
Simultaneous Bindin
Disabled
Registration Processing Del
0.0
Mobile IPv6 Parameters
( )
NAT Parameters
Not Configured
Security
Advanced
Filter
Apply to selected objects
Exact match
OK
Cancel

5.2.2. Home Agent κόμβοι

Αυτός ο κόμβος είναι ένα ικανό σταθερό Mobile IP router με τα διαμορφωμένα ακόλουθα χαρακτηριστικά που παρουσιάζονται στο Σχήμα 62.



Σχήμα 62 : Χαρακτηριστικά Home Agent

Σύμφωνα με το Σχήμα 62, ο κόμβος πρέπει να στηριχθεί στη πρόσβαση λειτουργικότητας σημείου και έχει την ίδια BSS ID ως κινητός κόμβος. Είναι πολύ σημαντικό να σημειωθεί ότι αν ο χρήστης καθορίζει το BSS ID ως " Auto Assigned", ολόκληρο το υποδίκτυο OPNET θα πρέπει να θεωρείται ως ένα ενιαίο υποδίκτυο. Στην περίπτωση αυτή, ο χρήστης ορίζει διαφορετικά BSS ID για τον home agent και τον foreign agent ώστε να έχουν διαφορετικά υποδίκτυα για τα σενάρια της Mobile IP. Επίσης, ο χρήστης δεν χρειάζεται να ορίσει κάθε διεύθυνση IP στο home agent.

5.2.3. Foreign Agent

Ο κόμβος αυτός διαμορφώνεται όπως ο home agent, εκτός από το ID BSS για κάθε foreign agent είναι διαφορετική από το home agent και foreign agent. Το Σχήμα 63 δείχνει τις παραμέτρους που έχουν τεθεί σε σημεία πρόσβασης foreign agent.

Σχήμα 63 : Χαρακτηριστικά Foreign Agent

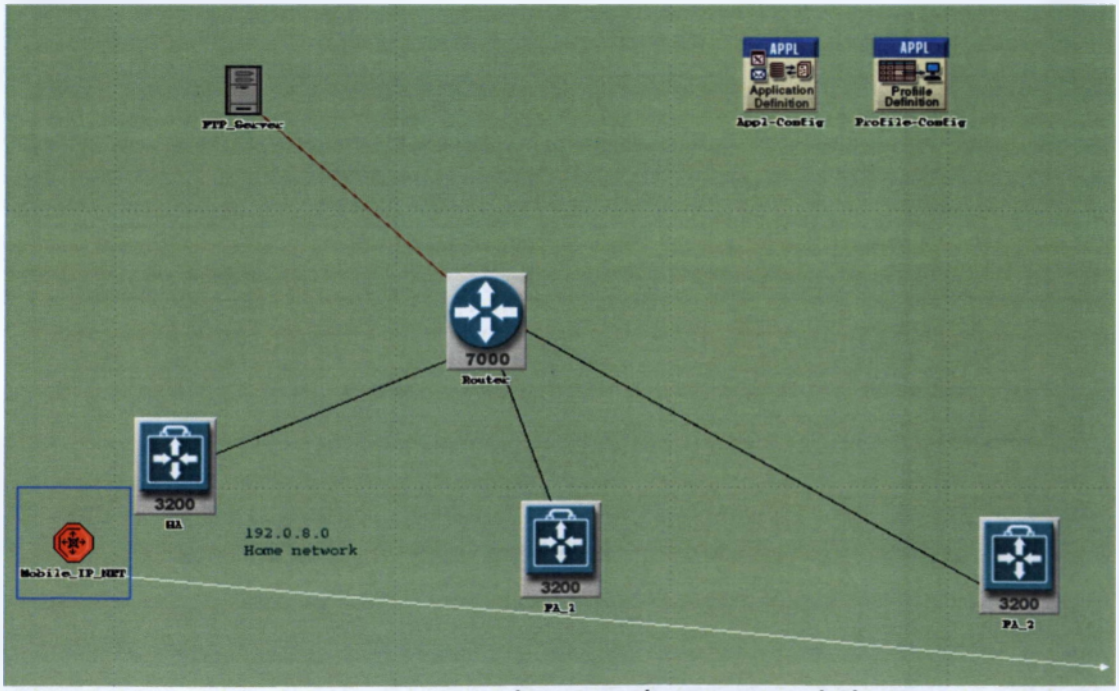

(FA_1) Attributes
Type
router
Attribute
Value
IP Slot Information
(...)
IPv6 Parameters
None
Mobile IP Router Parameters
Mobile IPv4 Parameters
(...)
Interface Information
(...)
Number of Rows
1
IF1
Interface Name
IF1
Agent Type
Foreign Agent
Agent Configuration
(...)
Home Agent IP Addr...
Unassigned
Registration Paramet...
(...)
Agent Solicitation
Disabled
Simultaneous Bindin...
Disabled
Registration Processing Del...
0.0
Mobile IPv6 Parameters
Not Configured
Advanced
Filter
Apply to selected objects
Exact match
OK
Cancel

5.3. Υλοποίηση του έργου στο OPNET Modeler 14.5

Στην ενότητα αυτή θα παρουσιάσουμε πώς το μοντέλο OPNET Mobile IP μπορεί να χρησιμοποιηθεί για την προσομοίωση του σεναρίου Mobile IPv4 σε ασύρματα τοπικά δίκτυα.

Το Σχήμα 64 δείχνει την αρχιτεκτονική του δικτύου το οποίο έχει σχεδιαστεί για την προσομοίωση. Η Cisco 7000 σειρά router χρησιμοποιείται για να κάνει μια σύνδεση μεταξύ των σταθερών κόμβων. Επίσης, μια εφαρμογή FTP-Heavy Load χρησιμοποιείται για την πραγματοποίηση της κυκλοφορίας μεταξύ FTP server που είναι ο αντίστοιχος κόμβος και του κινητού κόμβου. Ο home agent και ο foreign agent είναι ασύρματα LAN routers που έχουν σχεδιαστεί για την Mobile IP από το OPNET 14.5.

Για να παρακολουθείτε μέσω αριθμού «φάρου» που έλαβε από το home agent, ο χρήστης πρέπει να ενεργοποιήσει δυνατότητες περιαγωγής στα κινητά router στο κινητό υποδίκτυο. Όταν το κινητό υποδίκτυο αρχίζει να κινείται πάνω σε χαρακτηριστική πορεία, η οποία υλοποιείται σε αυτό το OPNET Modeler, ο αριθμός «φάρος» που λαμβάνεται από το σημείο πρόσβασης του home agent θα πέσει και στη συνέχεια οι κινητοί διακόπτες δρομολογητών με το σημείο πρόσβασης του foreign agent σημαίνει ότι μια πραγματική μεταβίβαση συμβαίνει σε αυτό το σημείο.

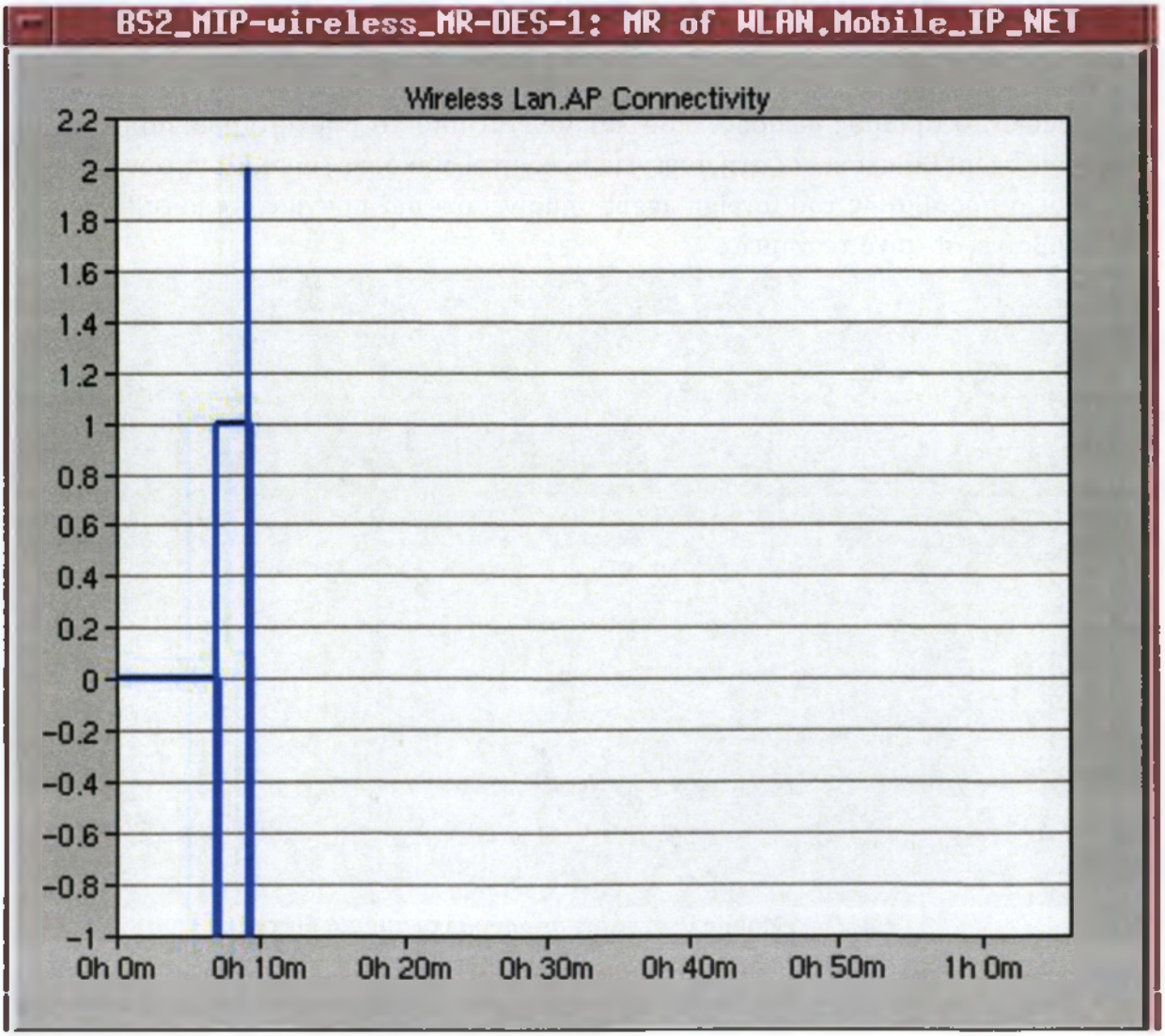


Σχήμα 64 : Mobile IP σενάριο σε ασύρματα τοπικά δίκτυα

5.4. Τα αποτελέσματα της προσομοίωσης

5.4.1. Πρόσβαση Σημείου Συνδεσιμότητας

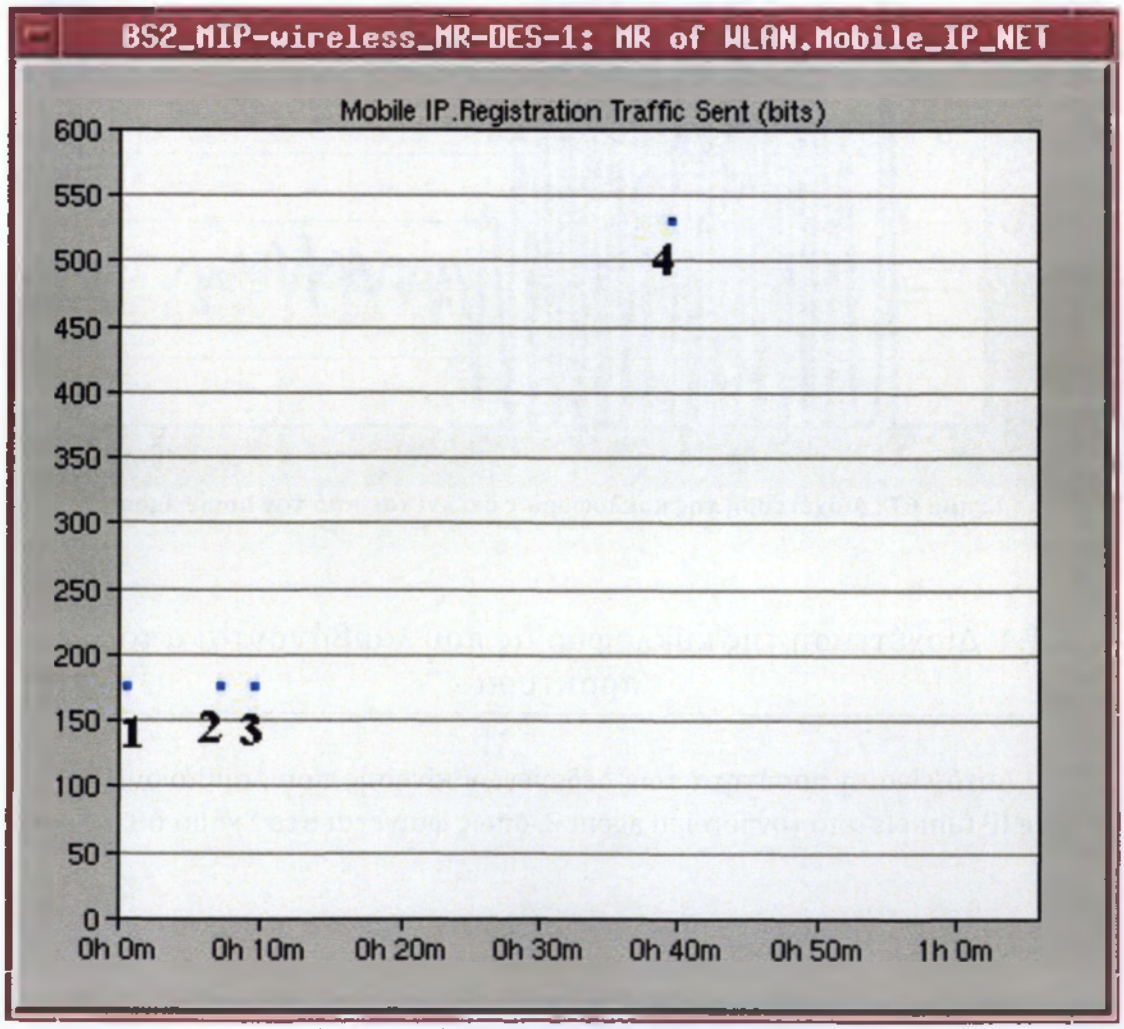
Ένα από τα ενδιαφερόμενα στατιστικά στοιχεία που ο χρήστης ψάχνει μετά είναι, η πρόσβαση στο χαρακτηριστικό γνώρισμα συνδεσιμότητας σημείου. Αυτό το χαρακτηριστικό δείχνει αν ο κινητός κόμβος συνδέεται με ένα σημείο πρόσβασης ή όχι. Σύμφωνα με το Σχήμα 65 όταν η MAC address του κινητού κόμβου έχει αποσυνδεθεί από το τρέχον σημείο πρόσβασης (Home Agent) μια τιμή "-1" είναι γραμμένη σε αυτό το στατιστικό στοιχείο, και όταν συνδέεται με ένα νέο σημείο πρόσβασης (Foreign Agent), τότε το «ID BSS» από το νέο σημείο πρόσβασης καταγράφεται. Η διεύθυνση MAC υποτίθεται ότι έχει αποσυνδεθεί ενώ βρίσκεται σε λειτουργία σάρωσης, κατά την οποία ψάχνει για ένα σημείο πρόσβασης με ικανοποιητική ποιότητα σύνδεσης.



Σχήμα 65 : Συνδεσιμότητα Mobile Node AP

5.4.2. Εγγραφή Κινητού κόμβου

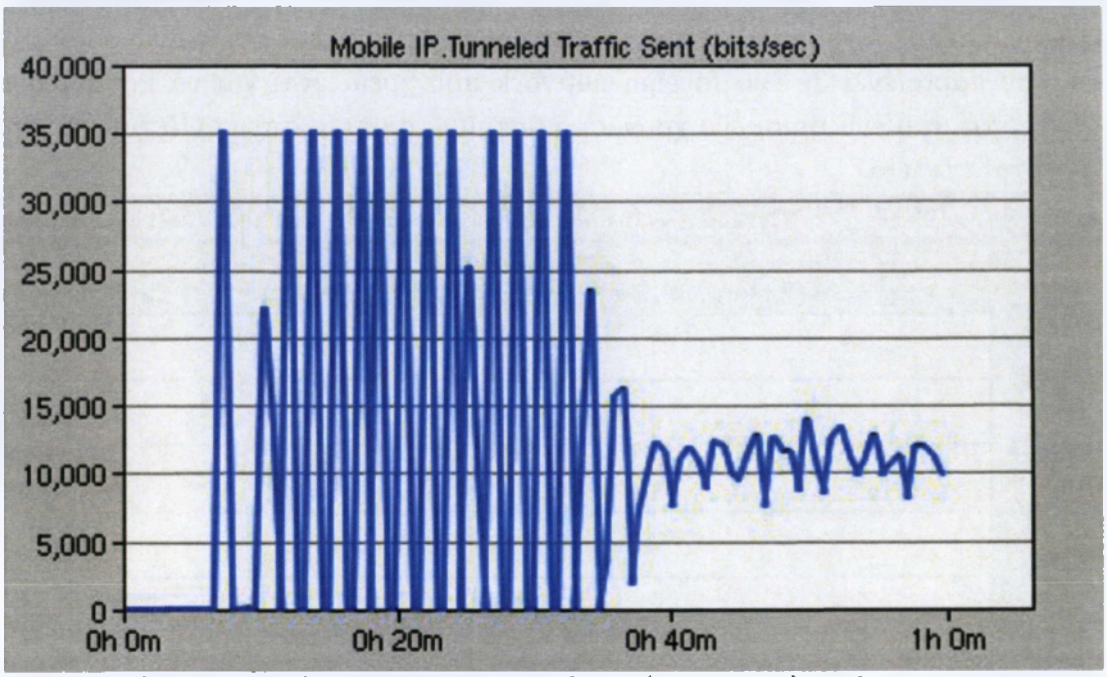
Τα στοιχεία αυτά δείχνουν το πρώτο βήμα που ο κινητός κόμβος γνωρίζει τη διεύθυνση IP του στο σημείο προσάρτησης του και στη συνέχεια καταγράφει με τον home agent. Όταν ο κινητός κόμβος είναι μακριά από το home network, καταγράφει η care-of address της με το home agent του μέσω του foreign agent. Η πρώτη κουκίδα στο Σχήμα 66 δείχνει ότι ο κινητός κόμβος καταγράφει με το home agent του. Η δεύτερη και η Τρίτη κουκίδα δείχνουν όταν ο κινητός κόμβος καταγράφει με foreign agents, μετά κινείται προς το μέρος τους. Ενώ ο κινητός κόμβος παραμένει σε ένα foreign network που χρειάζεται για να καταγράψει ξανά μετά από ένα ορισμένο χρονικό διάστημα το οποίο απεικονίζεται από την τελευταία τελεία.



Σχήμα 66 : Βήματα εγγραφής κινητού κόμβου

5.4.3. Διοχέτευση της κυκλοφορίας αποστέλλονται από τον εκπρόσωπο σπίτι

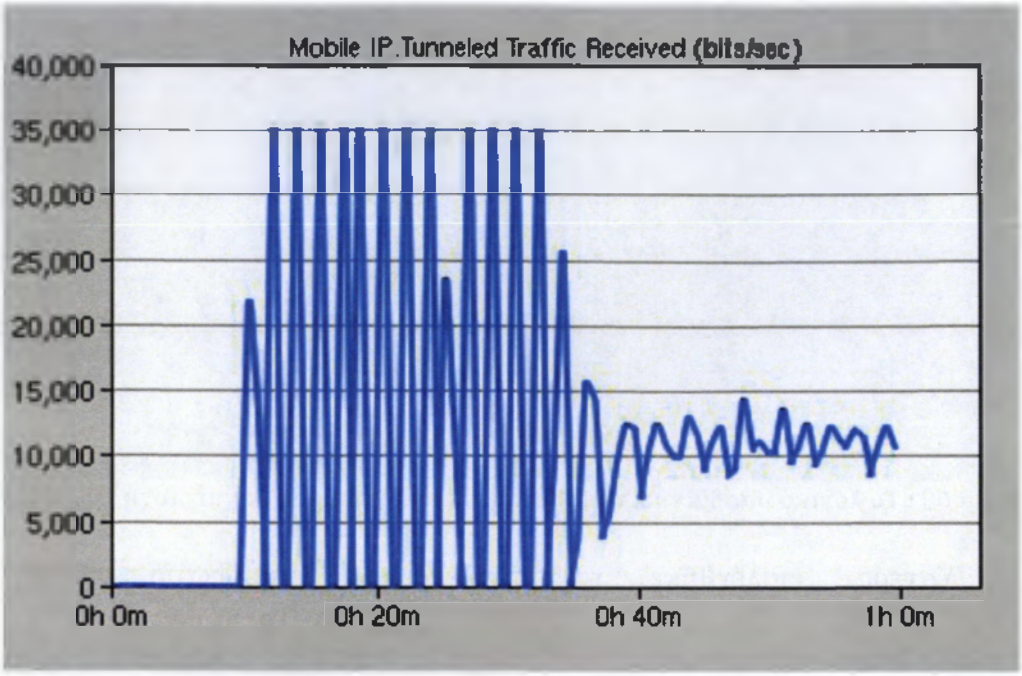
Όπως φαίνεται στο Σχήμα 67, αυτή είναι η ποσότητα των δεδομένων που αποστέλλονται μέσω Mobile IP tunnels από το home agent. Η κυκλοφορία που προορίζεται για κινητούς κόμβους όταν είναι μακριά από το home network τους διοχετεύεται από το κόμβο home agent και αποστέλλονται σε foreign agent.



Σχήμα 67 : Διοχέτευση της κυκλοφορίας στέλνεται από τον home agent

5.4.4. Διοχέτευση της κυκλοφορίας που λαμβάνονται από ξένο πράκτορα

Αυτό είναι η ποσότητα των δεδομένων κίνησης που λαμβάνονται μέσω Mobile IP tunnels από τον foreign agent 2, όπως φαίνεται στο Σχήμα 68.



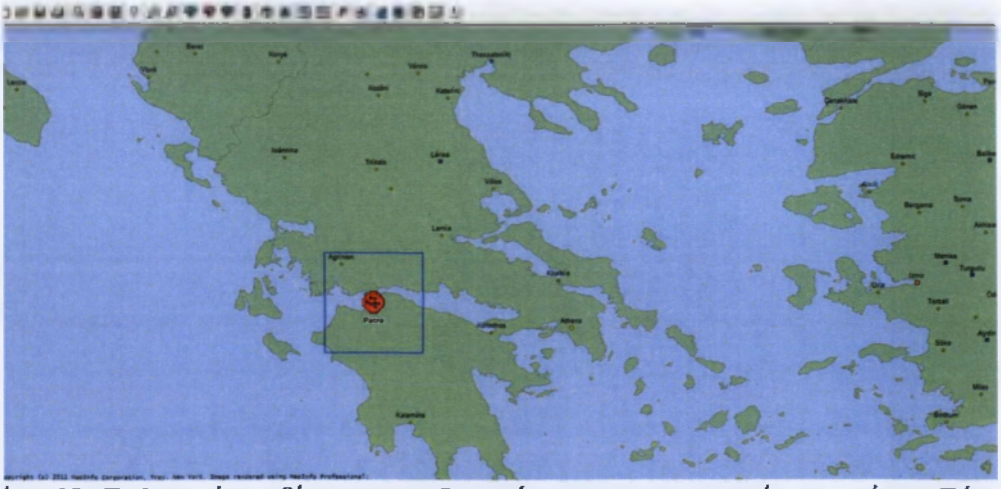
Σχήμα 68 : Διοχετευμένη κυκλοφορία που λαμβάνεται από τον foreign agent

5.5. Handoff Optimization

Εάν τα home και foreign network αλληλεπικαλύπτονται, πράγμα που σημαίνει ότι ο κινητός κόμβος είναι στη κοινή περιοχή τους και μπορεί να λάβει διαφήμιση και από τα δύο δίκτυα. Μόλις ο κινητός κόμβος λάβει τη care-of-address από τον foreign agent, ο κινητός κόμβος στέλνει αίτηση εγγραφής στο home agent του απ 'ευθείας χωρίς να περάσει από τον υποψήφιο foreign agent του, που ονομάζεται άμεση καταχώριση. Η μέθοδος αυτή μπορεί να μειώσει σημαντικά το χρόνο της διαδικασίας καταχώρησης, αλλά έχει υψηλότερη απαίτηση της τοπολογίας του δικτύου, όπως η τέλεια επικάλυψη που αναφέραμε πριν.

5.6. ΚΑΤΑΣΚΕΥΗ ΜΟΝΤΕΛΩΝ

Κατά την εκκίνηση του πρώτου project, δημιουργήθηκε ένα λογικό υποδίκτυο (logical subnet) στη γεωγραφική περιοχή της Πάτρας, όπως φαίνεται στο Σχήμα 69.



Σχήμα 69 : Το λογικό υποδίκτυο, τοποθετημένο στη γεωγραφική περιοχή της Πάτρας

Ύστερα, επιλέχθηκε το συγκεκριμένο υποδίκτυο, ώστε να κατασκευαστούν εντός αυτού τα διάφορα μοντέλα. Το πρώτο μοντέλο που δημιουργήθηκε ήταν αυτό του απλού δικτύου UMTS με 1 τερματική συσκευή συνδεδεμένη. Σε αυτό το μοντέλο, χρησιμοποιήθηκαν συνολικά οι εξής έτοιμοι κόμβοι, χωρίς να υποστούν καμία περαιτέρω τροποποίηση με το συντάκτη κόμβων:

- 1 κινητή τερματική συσκευή UMTS, τύπου umts_wkstn_adv (Mobile Node)
- 1 Node-B, τύπου umts_node_b_adv
- 1 RNC, τύπου umts_rnc_ethernet_atm_slip_adv
- 1 SGSN, τύπου umts_sgsn_ethernet_atm_slip9_adv
- 1 GGSN, τύπου umts_ggsn_ethernet8_atm8_slip8_adv
- 1 επαναλήπτης (hub), τύπου ethernet16_hub
- 4 εξυπηρετητές (servers), τύπου ethernet_server_adv

Μετά την εισαγωγή όλων των παραπάνω, σχεδιάστηκε η περιοχή ασύρματης εμβέλειας του Node-B, με μια τυπική ακτίνα της τάξεως μεγέθους του 1 km, ενώ για τη διασύνδεση των υπόλοιπων κόμβων χρησιμοποιήθηκαν διάφορα είδη ενσύρματων τεχνολογιών και συγκεκριμένα:

- η τεχνολογία ATM
- η τεχνολογία του Διασημειακού Πρωτοκόλλου (Point-to-Point Protocol – PPP), που αποτελεί μετεξέλιξη της τεχνολογίας του Διαδικτυακού Πρωτοκόλλου Σειριακής Γραμμής (Serial Line Internet Protocol – SLIP)
- η τεχνολογία του προτύπου IEEE 802.3, το οποίο περιγράφει την ενσύρματη δικτύωση Τοπικών Δικτύων (Local Area Networks – LANs), υιοθετώντας πλήρως το πρωτόκολλο Ethernet της XEROX Corporation

Παρακάτω καταγράφεται ενδεικτικά ο τρόπος εφαρμογής των συνδέσεων στο μοντέλο αυτό:

- τερματική συσκευή ↔ Node-B: ασύρματη ζεύξη

- Node-B ↔ RNC: ζεύξη ATM, τύπου ATM_OC3
- RNC ↔ SGSN: ζεύξη ATM, τύπου ATM_OC3
- SGSN ↔ GGSN: ζεύξη PPP, τύπου PPP_DS3
- GGSN ↔ hub: ζεύξη Ethernet, τύπου 10baseT_adv
- hub ↔ servers: ζεύξη Ethernet, τύπου 10baseT_adv

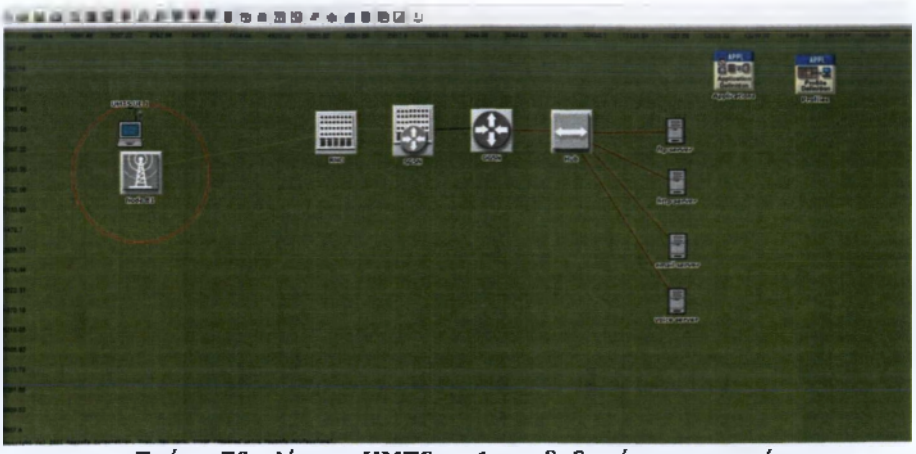
Οι servers συνδέθηκαν με την υποστήριξη των εξής εφαρμογών (ένας για κάθε εφαρμογή):

- ανταλλαγή αρχείων με βάση το Πρωτόκολλο Μεταφοράς Αρχείων (File Transfer Protocol – FTP)
- ανταλλαγή δεδομένων για περιήγηση σε σελίδες με βάση το Πρωτόκολλο Μεταφοράς ΥπερΚειμένου (HyperText Transfer Protocol – HTTP)
- ανταλλαγή δεδομένων ηλεκτρονικής αλληλογραφίας
- υπηρεσία φωνής

Τέλος, εισήχθη μία μονάδα διαμόρφωσης προφίλ χρηστών του συστήματος (Profile Config) και μία μονάδα διαμόρφωσης προφίλ χρήσης εφαρμογών (Application Config). Πρέπει να σημειωθεί εδώ ότι μία στρατηγική επιλογή γι' αυτό το project ήταν η ρεαλιστική διαμόρφωση των προφίλ. Αποφασίσθηκε δηλαδή η εισαγωγή των δεδομένων να βασιστεί σε υπάρχοντα στατιστικά τηλεπικοινωνιακής κίνησης δικτύων κινητής τηλεφωνίας, με τρόπο τέτοιο ώστε η συμπεριφορά του φορτίου στο μοντέλο αυτό να προσεγγίζει κατά το δυνατόν το φορτίο που διαμορφώνεται σε πραγματικές συνθήκες.

Όπως είναι γνωστό από τη θεωρία της τηλεπικοινωνιακής κίνησης και τη στατιστική γενικότερα, η αρνητική εκθετική (negative exponential) κατανομή φαίνεται ότι προσεγγίζει αποτελεσματικά την πιθανότητα ενδιάμεσου χρόνου διαδοχικών αφίξεων κλήσεων (call inter-arrival time probability). Επιπλέον, χρησιμεύει και στην προσέγγιση της πιθανότητας διάρκειας κλήσης (call duration probability), αν και οι περισσότερες σύγχρονες μελέτες συγκλίνουν στη διαπίστωση ότι η λογαριθμική κανονική (logarithmic normal) κατανομή είναι σαφώς καταλληλότερη γι' αυτήν την περίπτωση.

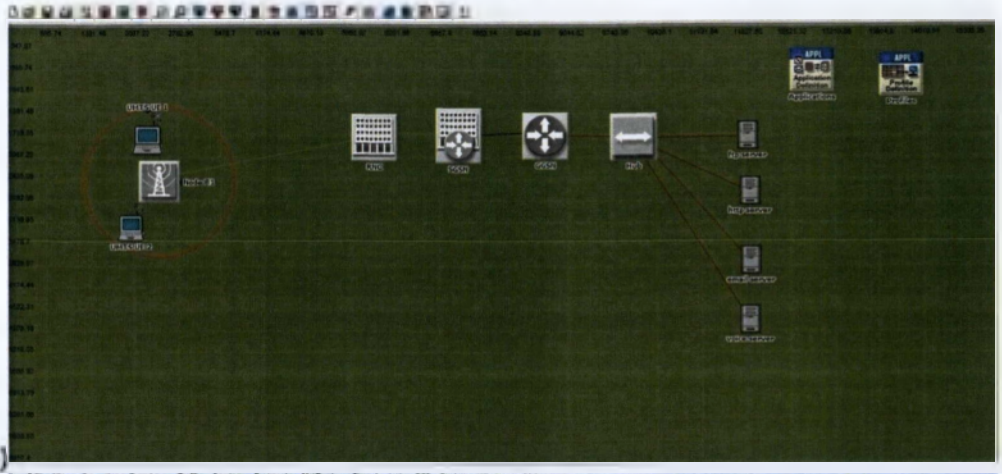
Πράγματι, κατά τη διαμόρφωση των προφίλ αυτής της σειράς σεναρίων ακολουθήθηκαν οι παραπάνω προτάσεις και μάλιστα όχι μόνο για την υπηρεσία φωνής. Όμως, επειδή επρόκειτο να καθοριστεί η διάρκεια της προσομοίωσης στη 1 ώρα, οι μέσες τιμές των συναρτήσεων των παραπάνω μεγεθών συμπτύχθηκαν κατά τέτοιο τρόπο ώστε να είναι εφικτή η εξαγωγή συμπερασμάτων από τα αποτελέσματα μιας τέτοιας προσομοίωσης. Μία γενική άποψη του δικτύου που δημιουργήθηκε, φαίνεται στο Σχήμα 70.



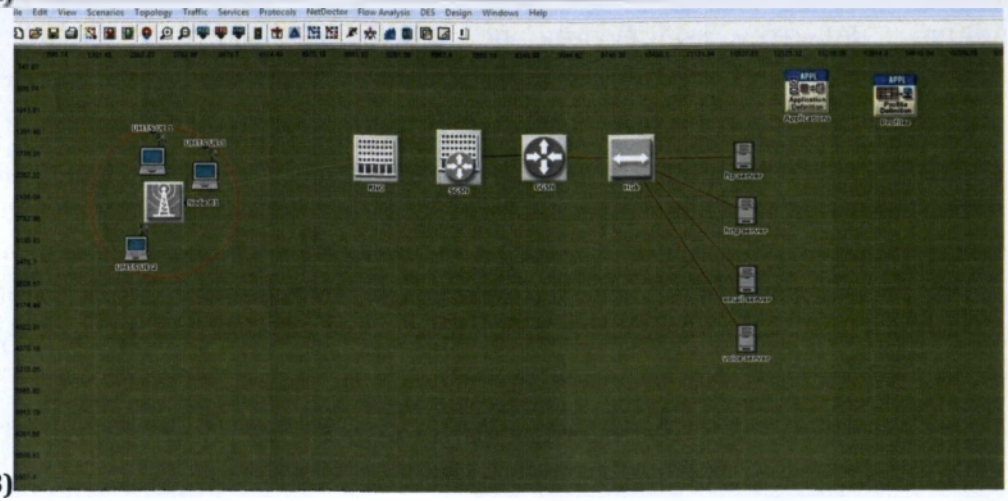
Σχήμα 70 : Δίκτυο UMTS με 1 συνδεδεμένη συσκευή

Εκτός όμως από αυτό το απλό σενάριο, δημιουργήθηκαν και άλλα σενάρια UMTS δικτύου, με περισσότερες συσκευές, αρχικά όλες συνδεδεμένες στον ίδιο Node-B, και στη συνέχεια μοιρασμένες σε 2 Node-Bs. Τα σενάρια αυτά στο σύνολό τους παρατίθενται στο Σχήμα 71 και 72.

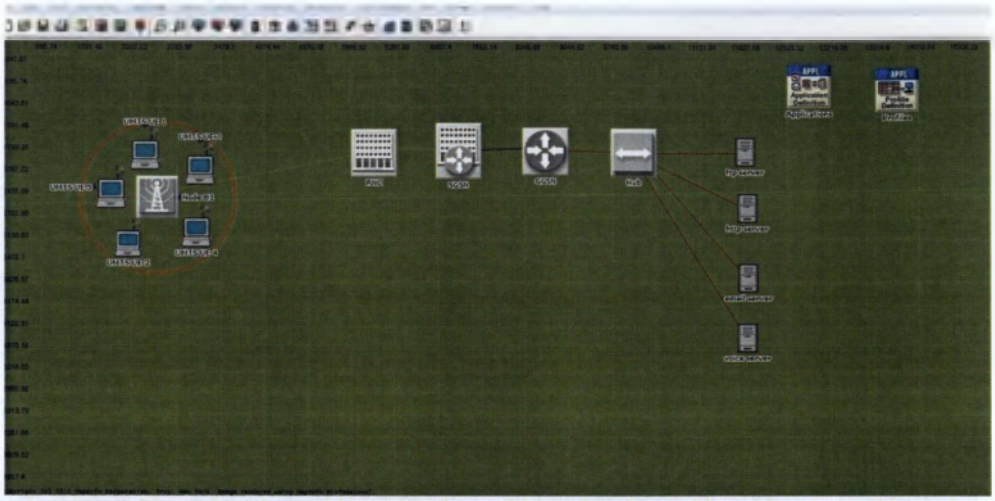
(α)



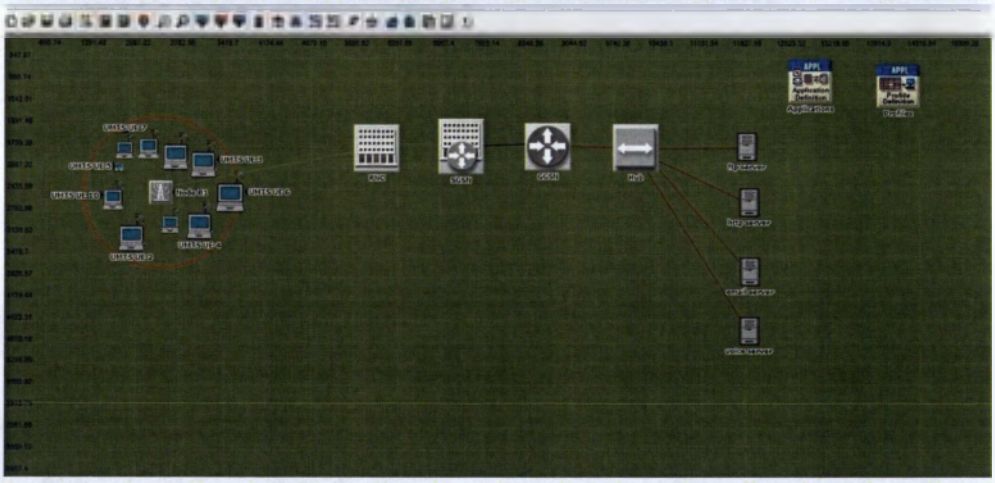
(β)



(γ)

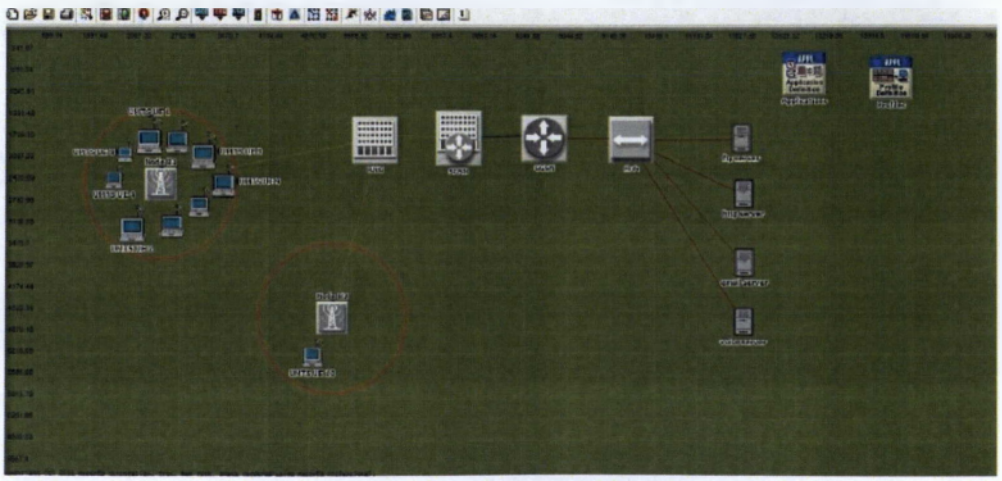


(δ)

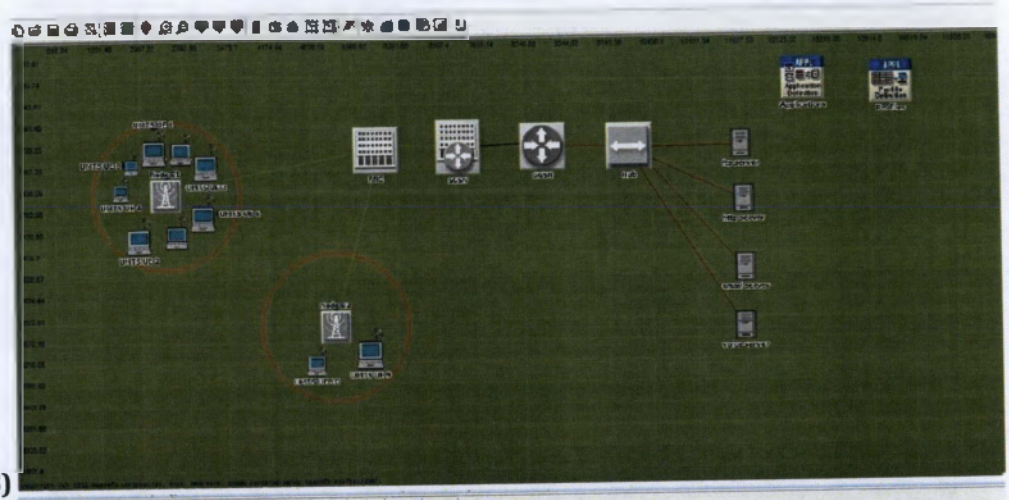


Σχήμα 71 : Δίκτυο UMTS με (α) 2 συνδεδεμένες συσκευές, (β) 3 συνδεδεμένες συσκευές, (γ) 5 συνδεδεμένες συσκευές, (δ) 10 συνδεδεμένες συσκευές

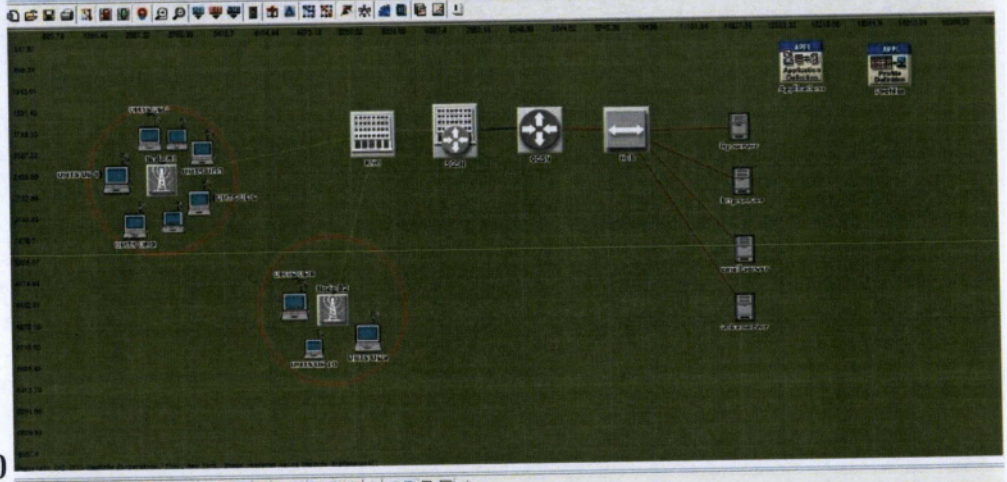
(α)



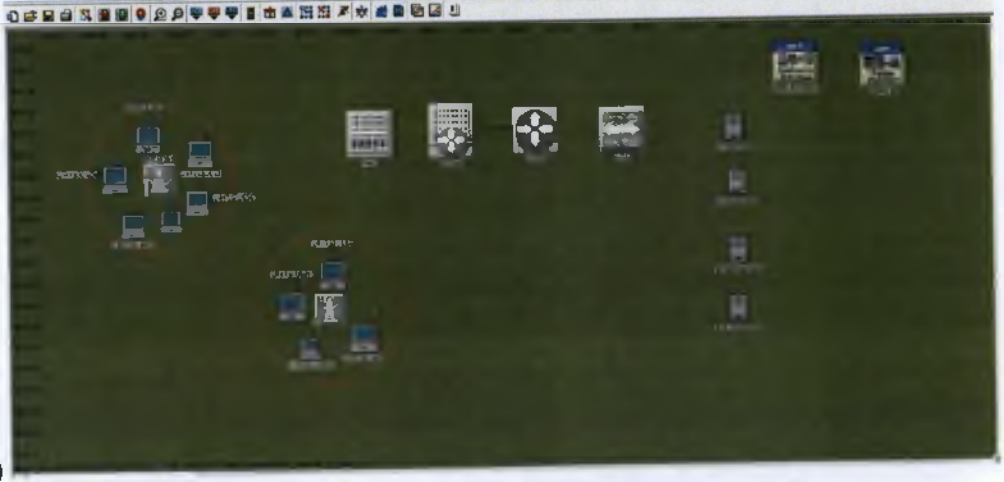
(β)

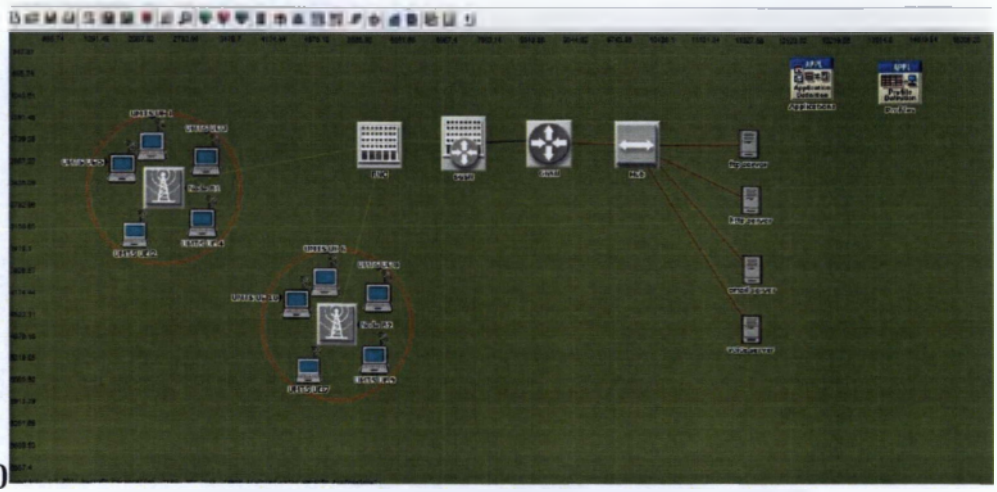


(γ)



(δ)





(ε)

Σχήμα 72 : Δίκτυο UMTS με (α) 9+1 συνδεδεμένες συσκευές, (β) 8+2 συνδεδεμένες συσκευές, (γ) 7+3 συνδεδεμένες συσκευές, (δ) 6+4 συνδεδεμένες συσκευές, (ε) 5+5 συνδεδεμένες συσκευές

Μετά την ολοκλήρωση της κατασκευής των διαφόρων μοντέλων UMTS, δημιουργήθηκε κατ' αντιστοιχία ένα σύνολο από μοντέλα WLAN. Το πρώτο μοντέλο είναι το μοντέλο ενός απλού WLAN με 1 συνδεδεμένη συσκευή. Για το μοντέλο αυτό χρησιμοποιήθηκαν οι εξής κόμβοι:

- 1 κινητή τερματική συσκευή WLAN, τύπου wlan_wkstn_adv (Mobile Node)
- 1 δρομολογητής (router) WLAN, τύπου wlan_ethernet_slip4_adv
- 1 επαναλήπτης (hub), τύπου ethernet16_hub
- 4 εξυπηρετητές (servers), τύπου ethernet_server_adv

Κατά τ' άλλα, οι ενσύρματες συνδέσεις του δικτύου ήταν τύπου Ethernet:

- τερματική συσκευή ↔ router, ασύρματη ζεύξη
- router ↔ hub: ζεύξη Ethernet, τύπου 10baseT_adv
- hub ↔ servers: ζεύξη Ethernet, τύπου 10baseT_adv

Όσο για τα προφίλ των χρηστών και των εφαρμογών, θεωρήθηκε λογικό να μην τροποποιηθούν καθόλου, σε σχέση με αυτά που είχαν ετοιμαστεί για τα UMTS μοντέλα, ώστε να μπορεί να γίνει σύγκριση ανάμεσα στα δύο είδη δικτύων με ίσους όρους. Το στοιχειώδες αυτό σενάριο του WLAN με τη 1 τερματική συσκευή παρουσιάζεται στο Σχήμα 73.

Σχήμα 73 : Δίκτυο WLAN με 1 συνδεδεμένη συσκευή

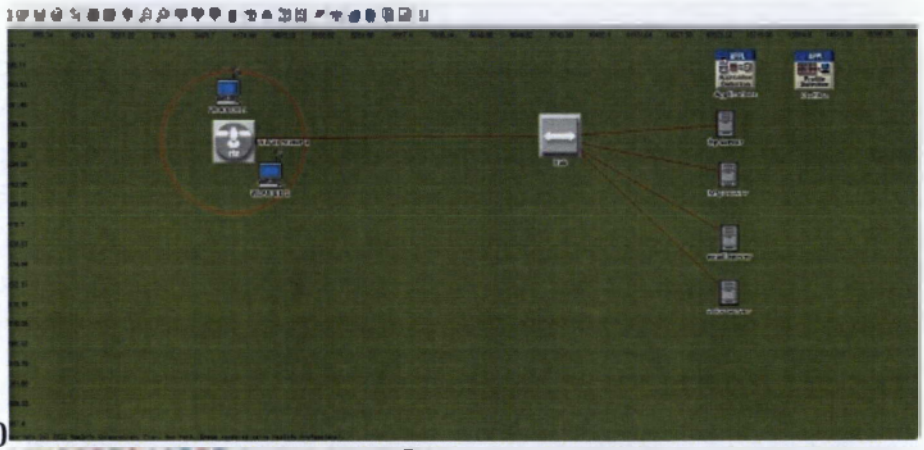
Η σχεδίαση του κύκλου που αντιπροσωπεύει την εμβέλεια του router στηρίχθηκε σε συγκεκριμένους υπολογισμούς. Καταρχήν, τόσο για το router, όσο και για την τερματική συσκευή, χρησιμοποιήθηκε η προκαθορισμένη ισχύς εκπομπής, που είναι ίση με 5 mW, και αντίστοιχα το προκαθορισμένο κατώφλι ευαισθησίας, που βρίσκεται στα -95 dB. Επομένως, με δεδομένο ότι το πρόγραμμα λειτουργεί με βάση το μοντέλο ελευθέρου χώρου, η εμβέλεια του router υπολογίζεται από τον τύπο που φαίνεται στο Σχήμα 74.

$$FSPL[dB] = 20 \cdot \log_{10}(d\,[km]) + 20 \cdot \log_{10}(f\,[MHz]) + 32.45[dB]$$
$$P_t[dB] - P_r[dB] = 20 \cdot \log_{10}(d\,[km]) + 20 \cdot \log_{10}(f\,[MHz]) + 32.45[dB]$$
$$P_t[dBm] - P_r[dBm] = 20 \cdot \log_{10}(d\,[km]) + 20 \cdot \log_{10}(f\,[MHz]) + 32.45[dB]$$
$$20 \cdot \log_{10}(d\,[km]) = P_t[dBm] - P_r[dBm] - 20 \cdot \log_{10}(f\,[MHz]) - 32.45[dB]$$
$$d[km] = 10^{\left(\frac{P_t[dBm] - P_r[dBm] - 20\log_{10}(f[MHz]) - 32.45[dB]}{20}\right)}[km] = 10^{\left(\frac{(10\log_{10}5) - (-95) - (20\log_{10}2400) - (32.45)[dB]}{20}\right)}[km] \approx 1.25[km]$$

Σχήμα 74 : Τύπος για τον υπολογισμό της εμβέλειας του router

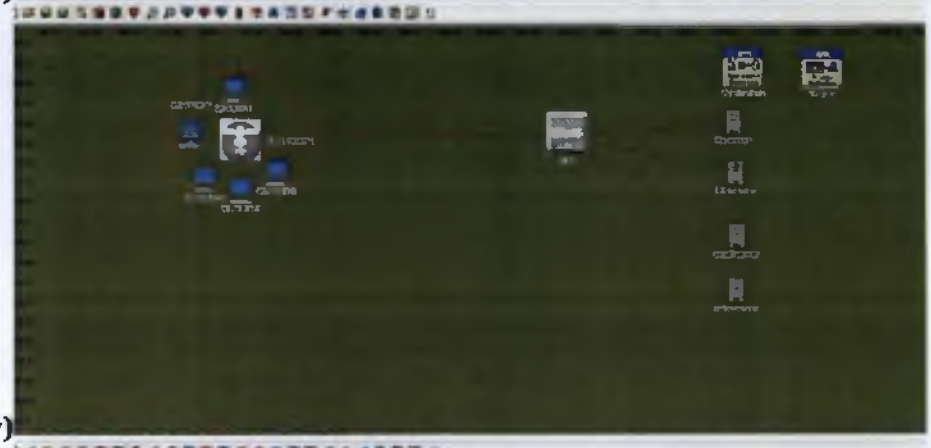
Η ακτίνα της εμβέλειας του router λοιπόν είναι περίπου ίση με 1250 m, στο συγκεκριμένο WLAN μοντέλο. Τέλος, μετά την ολοκλήρωση του πρώτου μοντέλου ακολουθεί η κατασκευή ορισμένων ακόμα σεναρίων, με σταδιακή αύξηση των συνδεδεμένων συσκευών. Τα σενάρια αυτά είναι συγκεντρωμένα στο Σχήμα 75 που ακολουθεί:

(α)

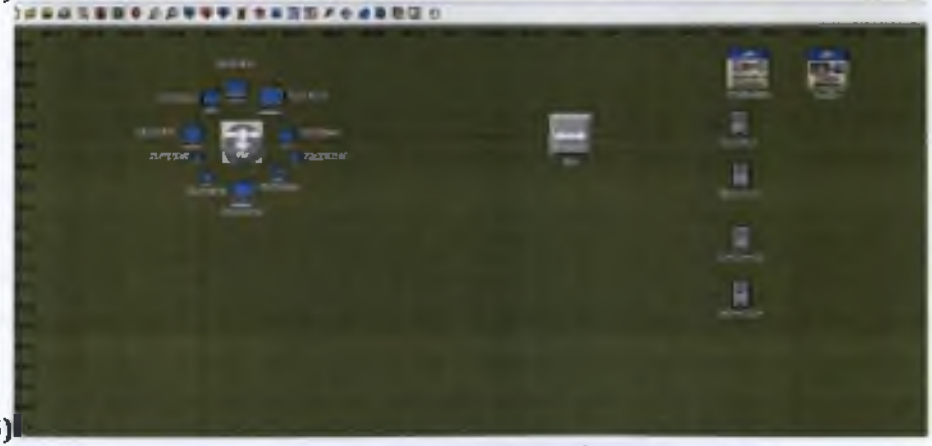


(β)

(γ)



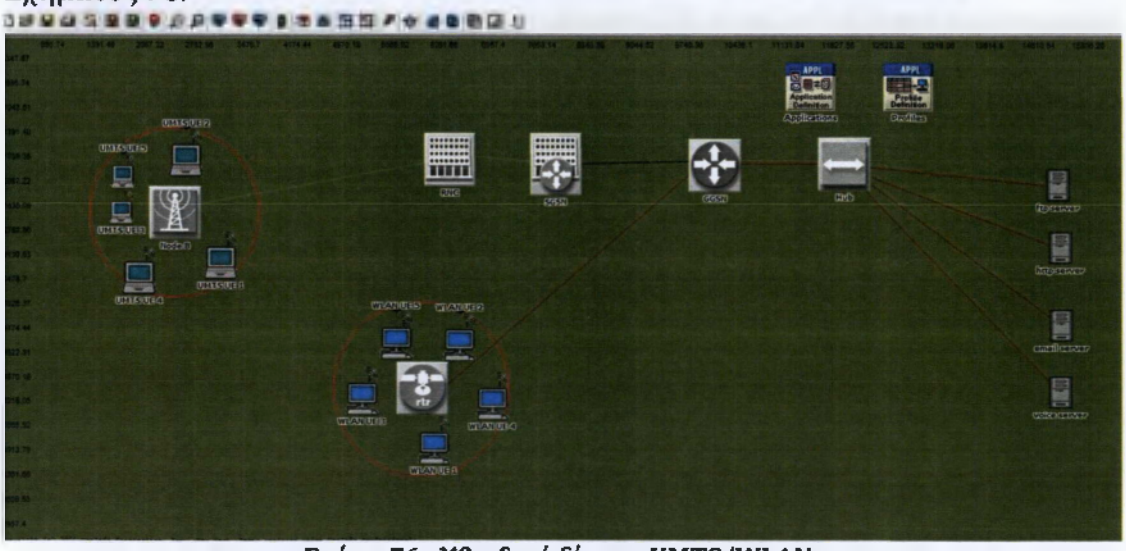
(δ)



Σχήμα 75 : Δίκτυο WLAN με α) 2 συνδεδεμένες συσκευές, β) 3 συνδεδεμένες συσκευές, γ) 5 συνδεδεμένες συσκευές, δ) 10 συνδεδεμένες συσκευές

Το επόμενο βήμα (το οποίο είναι εξάλλου το ουσιαστικότερο της διαδικασίας των προσομοιώσεων) είναι η σχεδίαση ενός υβριδικού δικτύου που προκύπτει από τη συγχώνευση των κόμβων του UMTS και του WLAN. Για το σκοπό αυτό, διατηρήθηκε πρακτικά η εκδοχή του UMTS με τις 5 τερματικές συσκευές, και στον GGSN του δικτύου αυτού συνδέθηκε με Ethernet ζεύξη τύπου 10_baseT_adv ένας router WLAN, με 5 τερματικές συσκευές WLAN γύρω από αυτόν. Κατά τ' άλλα, παρέμειναν και οι 4 servers, για την υποστήριξη των ίδιων 4 εφαρμογών (FTP μεταφοράς, HTTP περιήγησης, ανταλλαγής e-mail, φωνής), ενώ καμία αλλαγή δεν έγινε ούτε στο προφίλ των χρηστών, αφού σε όλες τις συσκευές του υβριδικού δικτύου ενσωματώθηκε το wireless profile που είχε δημιουργηθεί κατά τη διάρκεια της κατασκευής των αρχικών στοιχειωδών δικτύων.

Ίσως είναι σημαντικό να επισημανθεί το γεγονός ότι, όπως σε όλα τα προηγούμενα δίκτυα δεν υφίστανται ενδοσυστημικές μεταπομπές, έτσι και στο παραπάνω υβριδικό δίκτυο δεν έχει προβλεφθεί η υποστήριξη διασυστημικών μεταπομπών. Το υβριδικό δίκτυο που κατασκευάστηκε τελικά είναι αυτό του Σχήματος 76.



Σχήμα 76 : Υβριδικό δίκτυο UMTS/WLAN

Εκτός των άλλων, σε όλα τα παραπάνω δίκτυα οι κινητές τερματικές συσκευές δεν είναι καν κινούμενες. Δεν έχουν καθοριστεί τροχιές κίνησης και ως εκ τούτου οι συσκευές παραμένουν στις θέσεις τους, χωρίς να μεταφέρονται εντός ή εκτός της εμβέλειας των κόμβων με τους οποίους επικοινωνούν, και παραμένοντας επομένως συνδεδεμένες σε όλη τη διάρκεια της προσομοίωσης.

Στο επόμενο μοντέλο, οι συσκευές εξακολουθούν να παραμένουν ακίνητες, επιχειρείται όμως η υποστήριξη "εικονικής" μεταπομπής μεταξύ των δύο δικτύων, με την αποσύνδεση UMTS τερματικών από το UMTS δίκτυο και την ταυτόχρονη κάθε φορά σύνδεση WLAN τερματικών στο WLAN. Συγκεκριμένα, αυτό το μοντέλο, του οποίου η προσομοίωση διαρκεί 30 λεπτά, περιλαμβάνει 5 τερματικά UMTS, τα οποία ξεκινάνε όλα σε κατάσταση λειτουργίας, και 5

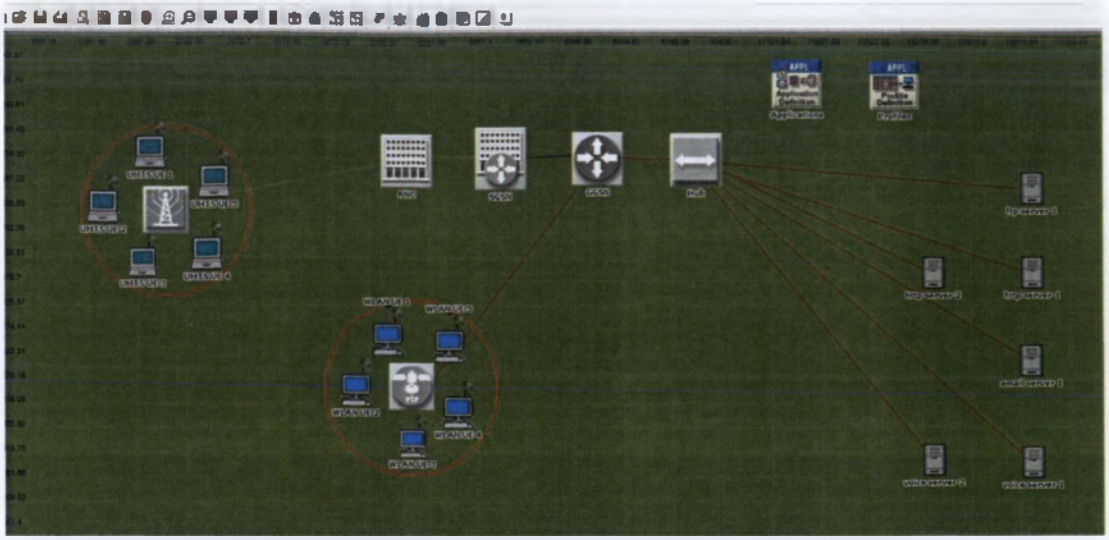
τερματικά WLAN, που ξεκινάνε σε κατάσταση μη λειτουργίας. Κάθε 5 λεπτά, μία συσκευή σταματάει να λειτουργεί στο UMTS, ενώ μία άλλη αρχίζει να λειτουργεί στο WLAN. Το γεγονός αυτό επαναλαμβάνεται μέχρι να λειτουργούν όλες οι συσκευές του WLAN και καμία του UMTS. Αυτό το σενάριο δηλαδή συνεισφέρει στη μελέτη των αποτελεσμάτων των μεταπομπών, χωρίς την ανάγκη πραγματοποίησης τους.

Για να είναι ορατά καθαρότερα τα αποτελέσματα αυτά, θεωρήθηκε καλύτερο να χρησιμοποιηθούν σταθερές τιμές για τα μεγέθη των χρόνων και των φορτίων δεδομένων των εφαρμογών. Έτσι, χρειάστηκαν κάποιες τροποποιήσεις στα προφίλ των εφαρμογών, με εξαίρεση την υπηρεσία φωνής, η οποία παρέμεινε ποιότητας PCM με καταστολή σιγής. Επίσης, δημιουργήθηκαν καινούρια προφίλ χρηστών, ώστε να υλοποιείται αυτού του είδους η εναλλαγή των καταστάσεων λειτουργίας και μη λειτουργίας σε συγκεκριμένες στιγμές. Όλες οι συσκευές UMTS ξεκινάνε τη λειτουργία τους άμεσα και η καθεμία λειτουργεί για καθορισμένο χρόνο, ώστε να διακόπτεται η λειτουργία μίας κάθε 5 λεπτά. Αντίθετα, όλες οι συσκευές WLAN ξεκινάνε σε κατάσταση μη λειτουργίας, και καθεμία εξ αυτών ξεκινάει τη λειτουργία της μετά από καθορισμένο χρόνο, ώστε να γίνεται εκκίνηση της λειτουργίας μίας κάθε 5 λεπτά, και να λειτουργούν ως το τέλος.

Μία ακόμη διαφορά που έχει το υβριδικό δίκτυο "εικονικής" μεταπομπής σε σχέση με το προηγούμενο υβριδικό δίκτυο, είναι ότι έχουν προστεθεί 2 ακόμα servers, διότι κατά τη διάρκεια των πρώτων δοκιμών των προσομοιώσεων, κατέστη προφανές ότι ο μεγάλος όγκος του φορτίου (λόγω της ύπαρξης σταθερής συνιστώσας ως προς το χρόνο για όλες τις εφαρμογές και άρα συνεχόμενης λειτουργίας) δεν μπορούσε να διεκπεραιωθεί ικανοποιητικά από τους προϋπάρχοντες servers. Άλλωστε, το υβριδικό δίκτυο "εικονικής" μεταπομπής θα αποτελούσε αντικείμενο μελέτης από μόνο του και όχι σε συνδυασμό με τα προηγούμενα, επομένως το γεγονός ότι θα άλλαζε ο τρόπος με τον οποίο οι servers θα αντιστοιχίζονταν σε εφαρμογές δεν επρόκειτο να επηρεάσει την εξαγωγή συμπερασμάτων από συγκρίσεις.

Από τους δύο servers που προστέθηκαν, ο ένας αφιερώθηκε στην υπηρεσία φωνής, συμπληρωματικά του προϋπάρχοντος, και ο άλλος στην εξυπηρέτηση της HTTP περιήγησης, επίσης συμπληρωματικά με τον αντίστοιχο προϋπάρχοντα, καθώς σε αυτές τις δύο εφαρμογές είχε παρατηρηθεί το μεγαλύτερο πρόβλημα.

Η γενική άποψη του δικτύου αυτού είναι τελικά ορατή στο Σχήμα 77.



Σχήμα 77 : Υβριδικό δίκτυο "εικονικής" μεταπομπής

Συνοψίζοντας, κατασκευάστηκαν συνολικά 17 σενάρια:

- 5 σενάρια WLAN (με διαφορετικό αριθμό συνδεδεμένων τερματικών συσκευών)
- 10 σενάρια UMTS (με διαφορετικό αριθμό ή διαφορετική ομαδοποίηση των τερματικών συσκευών)
- 2 υβριδικά σενάρια UMTS/WLAN (1 καθολικά ταυτόχρονης λειτουργίας και σταδιακής "εικονικής" μεταπομπής)

Όσον αφορά το δεύτερο project, αυτό με το Mobile IP, η μοντελοποίηση περιορίστηκε σε ένα απλό σενάριο. Το σενάριο αυτό υλοποιήθηκε πάλι εντός ενός λογικού υποδικτύου εγκατεστημένου στη γεωγραφική περιοχή της Πάτρας, και για το σκοπό της δημιουργίας του χρειάστηκε η εισαγωγή των παρακάτω κόμβων:

- 1 κινητή τερματική συσκευή WLAN, τύπου wlan_wkstn_adv (Mobile Node)
- 2 δρομολογητές (routers) WLAN, τύπου wlan_ethernet_slip4_adv
- 1 σύννεφο IP (IP cloud), τύπου ip8_cloud_adv
- 1 εξυπηρετητής (server), τύπου ppp_server_adv

Όσο για τις συνδέσεις, έχουν ως εξής:

- τερματική συσκευή ↔ routers: ασύρματη ζεύξη
- routers ↔ IP cloud: ζεύξη PPP, τύπου PPP_DS3
- IP cloud ↔ server: ζεύξη PPP, τύπου PPP_DS3

Αφού σχεδιάστηκε και εδώ η εμβέλεια του κάθε router (οι οποίοι τοποθετήθηκαν σε σχετικά κοντινά σημεία, ώστε να υφίσταται και περιοχή κοινής εμβέλειας), ορίστηκε μία τροχιά κίνησης για τη συσκευή, με τέτοιο τρόπο ώστε να μεταφέρεται από την περιοχή εξυπηρέτησης του ενός router σε αυτήν του άλλου, μέσω της περιοχής κοινής εμβέλειας. Τα προφίλ εφαρμογών και

χρήστη γι' αυτήν την τερματική συσκευή είναι ακριβώς ίδια με αυτά που χρησιμοποιήθηκαν στο υβριδικό δίκτυο "εικονικής" μεταπομπής (με τις σταθερές συνιστώσες για τα φορτία, κλπ.), με τη μόνη διαφορά ότι προφανώς η συσκευή λειτουργεί από την αρχή μέχρι το τέλος της προσομοίωσης, χωρίς να διακόπτει ποτέ. Βέβαια, χρειάστηκε να οριστούν κατάλληλα συγκεκριμένες παράμετροι που αφορούν ιδιότητες των κόμβων, ώστε το σύστημα να μπορεί να χρησιμοποιεί Mobile IP για την αδιάλειπτη περιήγηση της συσκευής από τη μία BSA στην άλλη. Επίσης, στο δίκτυο αυτό έχουμε μόνο έναν εξυπηρετητή, γι' αυτόν το λόγο καθορίστηκε να διεκπεραιώνει αυτός όλη την κίνηση του δικτύου, δηλαδή να σχετίζεται και με τις 4 εφαρμογές. Μία γενική άποψη του δικτύου αυτού φαίνεται στο Σχήμα 78.

Σχήμα 78 : Ασύρματο δίκτυο με Mobile IP

5.7. Συμπεράσματα προσομοίωσης

Η εργασία αυτή είχε ως στόχο τη μελέτη ορισμένων τύπων ασύρματων δικτύων που θα απαρτίζουν τα Δίκτυα Επόμενης Γενιάς και σ' αυτό το πλαίσιο παρουσιάστηκαν τα δίκτυα UMTS και WLAN, καθώς και το Mobile IP, που υπόσχεται την υποστήριξη της περιαγωγής των ασύρματων χρηστών ακόμα και σε απαιτητικές περιπτώσεις.

Εκτός από τη θεωρητική προσέγγιση των παραπάνω, κρίθηκε χρήσιμη η μοντελοποίηση ορισμένων σεναρίων τέτοιων συστημάτων με κάποιο πρόγραμμα εξομοίωσης. Το πρόγραμμα που χρησιμοποιήθηκε γι' αυτόν το σκοπό ήταν το OPNET modeler. Πρόκειται για ένα λογισμικό ιδιαίτερα χρήσιμο και ιδιαίτερα δημοφιλές, που επιτρέπει το σχεδιασμό και την προσομοίωση της λειτουργίας τηλεπικοινωνιακών δικτύων.

Για την εργασία αυτή, κατασκευάστηκαν δύο projects με το OPNET modeler, ένα για την επισκόπηση και τη σύγκριση των τεχνολογιών UMTS και WLAN και

τη μελέτη ενδεχόμενης συνεργατικής λειτουργίας τους, και ένα για την περιαγωγή με τη βοήθεια του Mobile IP.

Το πρώτο project αποτελείται από 17 σενάρια: 5 σενάρια WLAN (διαφορετικού πλήθους χρηστών), 10 σενάρια UMTS (διαφορετικού πλήθους ή κατανομής χρηστών) και 2 υβριδικά σενάρια UMTS/WLAN (1 παράλληλης λειτουργίας και 1 "εικονικών" μεταπομπών). Τα 15 πρώτα σενάρια δημιουργήθηκαν για τη μελέτη των επιδόσεων των δύο ειδών δικτύων και την απευθείας σύγκριση τους, ώστε να είναι δυνατόν να αποφανθούμε κατά πόσον θα μπορούσε να είναι χρήσιμη μία απόπειρα συνένωσής τους.

Το 16ο σενάριο αποτελεί αυτήν ακριβώς την απόπειρα, η εξέταση των αποτελεσμάτων της οποίας αναμενόταν να είναι πλούσια σε συμπεράσματα. Πάντως, στο συγκεκριμένο σενάριο οι ασύρματοι χρήστες παραμένουν ακίνητοι και δε λαμβάνουν χώρα μεταπομπές ανάμεσα στα δύο διαφορετικά μέρη του συστήματος.

Γι' αυτόν το λόγο, δημιουργήθηκε το 17ο σενάριο, στο οποίο πραγματοποιούνται "εικονικές" μεταπομπές, δίχως και πάλι να υπάρχουν αληθινές μετακινήσεις χρηστών στο χώρο, με στόχο την εξέταση της χρονικής αμεσότητας της εμφάνισης των πλεονεκτημάτων της μεταφοράς χρηστών από το ένα δίκτυο στο άλλο, χωρίς να χρειαστεί να επιβαρυνθεί η σχεδίαση του μοντέλου με ειδικούς μηχανισμούς υποστήριξης διασυστημικών μεταπομπών και διαχείρισης της σηματοδοσίας παράδοσης κλήσεων ή την ενσωμάτωση των πρωτοκόλλων του κάθε δικτύου στο άλλο δίκτυο, κινήσεις που θα απαιτούσαν αρκετά πολύπλοκους χειρισμούς. Άλλωστε, ο στόχος των προσομοιώσεων ήταν να καταστούν εμφανή τα πλεονεκτήματα μιας τέτοιας υβριδικής λύσης.

Σε όλα τα σενάρια του πρώτου project, εκτός από το τελευταίο, τα προφίλ των εφαρμογών και των χρηστών διαμορφώθηκαν με τρόπο όσο το δυνατόν ρεαλιστικότερο, σύμφωνα με τα πορίσματα της σύγχρονης θεωρίας τηλεπικοινωνιακής κίνησης των ασύρματων δικτύων. Στο τελευταίο σενάριο του project, αντίθετα, προτιμήθηκαν σταθερές τιμές για τα περισσότερα μεγέθη, ώστε να γίνονται ευκολότερα αντιληπτές οι σταδιακές (λόγω των τακτικών μεταπομπών) μεταβολές των υπό μελέτη μεγεθών.

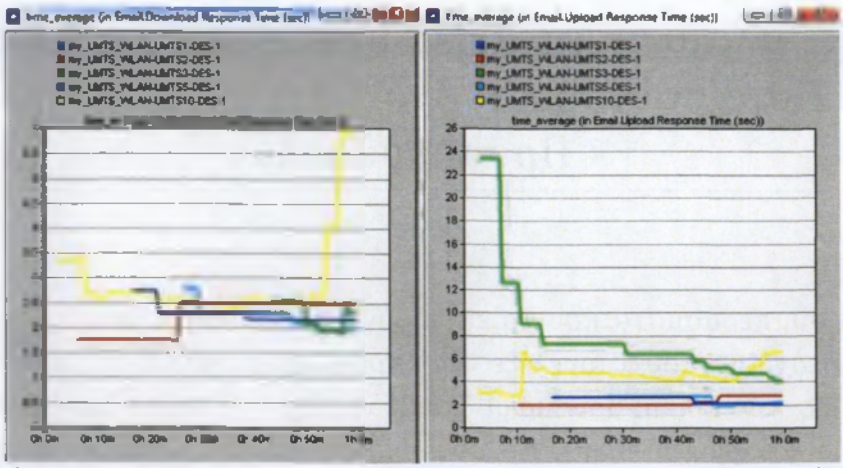
Τέλος, το 2ο project αποτελείται από 1 μόλις σενάριο, που παρουσιάζει ένα WLAN στο οποίο ο ασύρματος χρήστης επιχειρεί να περιηγηθεί ανάμεσα σε δύο BSAs που ανήκουν η καθεμία σε διαφορετικό ESS, με τη βοήθεια του Mobile IP.

Κεφάλαιο 6. Αποτελέσματα Προσομοίωσης
6.1. Παρουσίαση και Ανάλυση Αποτελεσμάτων Προσομοίωσης

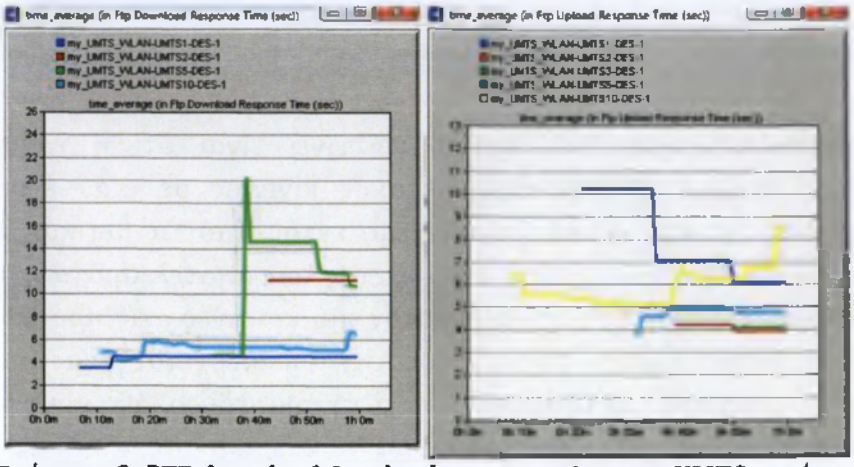
Τα συμπεράσματα που θα εκτεθούν παρακάτω βασίστηκαν κυρίως στα εξής στατιστικά που συνέλεξε το πρόγραμμα κατά τη διάρκεια των προσομοιώσεων: e-mail download & upload response times (χρόνοι απόκρισης αποστολής & λήψης e-mail), ftp download & upload response times (χρόνοι απόκρισης αποστολής & λήψης FTP δεδομένων), http object & page response times (χρόνοι απόκρισης αντικειμένων & σελίδων κατά την HTTP περιήγηση), voice packet end-to-end delays & packet delay variation (διατερματικές καθυστερήσεις πακέτων φωνής & διακύμανση καθυστερήσεων πακέτων). Μία σημαντική παρατήρηση που πρέπει να γίνει είναι ότι η χρησιμοποίηση ρεαλιστικών δεδομένων τηλεπικοινωνιακής κίνησης σε μία τέτοιου είδους προσομοίωση έχει και αρνητικά στοιχεία, εκτός από τα θετικά. Στα θετικά συγκαταλέγεται βέβαια η δυνατότητα μελέτης των αποτελεσμάτων λειτουργίας των δικτύων σε συνθήκες όσο το δυνατόν πιο κοντινές στις πραγματικές. Στα αρνητικά συγκαταλέγεται το γεγονός ότι υπεισέρχεται ένας παράγοντας τυχαιότητας, ο οποίος αναγκαστικά διέπει τη συμπεριφορά των μοντέλων που έχουν σχεδιαστεί κατ' αυτόν τον τρόπο.

Πάντως, το διάστημα της 1 ώρας, το οποίο χρησιμοποιήθηκε στις περισσότερες προσομοιώσεις, κρίνεται ως αρκετά ικανοποιητικό ώστε να επιτρέπει την εξαγωγή ασφαλών συμπερασμάτων. Εκτός αυτού, αποφασίστηκε στις περισσότερες απεικονίσεις να γίνει χρήση της επιλογής time_average του προγράμματος, ώστε να αποτυπώνεται ο μέσος όρος των υπό εξέταση χαρακτηριστικών ως προς το συνολικό χρόνο πραγματικής λειτουργίας των υπηρεσιών. Κατ' αυτόν τον τρόπο, καθώς οι γραφικές παραστάσεις τείνουν προς τα δεξιά, οι τιμές των υπό εξέταση χαρακτηριστικών προσεγγίζουν την τελική μέση τιμή τους, προσφέροντας ένα αρκετά σημαντικό στοιχείο για την αξιολόγηση των αποτελεσμάτων.

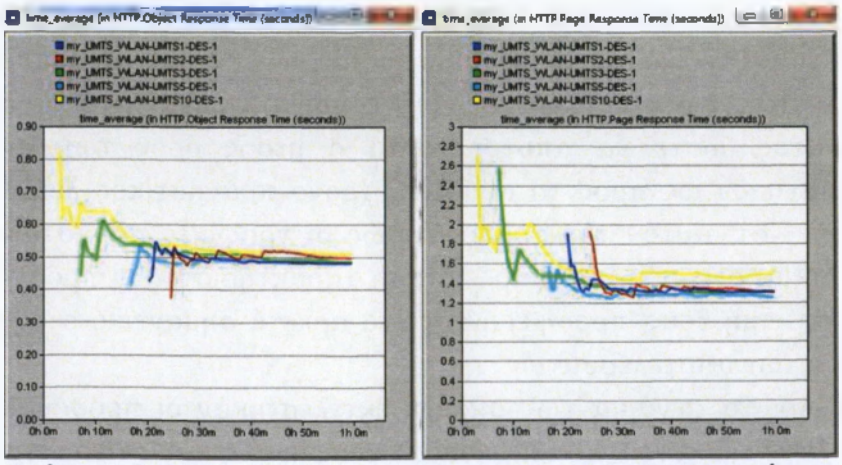
Τα πρώτα σενάρια των οποίων εκτελέστηκαν οι προσομοιώσεις ήταν αυτά του UMTS δικτύου. Στα παρακάτω γραφήματα καθίσταται προφανές ότι, ενώ δεν παρουσιάζονται εντυπωσιακές διαφορές ανάμεσα στα αποτελέσματα των απλούστερων και λιγότερο συνωστισμένων σεναρίων του δικτύου, αντιθέτως στο πολυπληθές δίκτυο με τις 10 συνδεδεμένες κινητές συσκευές παρατηρήθηκαν σαφώς μεγαλύτεροι χρόνοι. Μοναδική εξαίρεση αποτελούν τα αποτελέσματα των χρόνων απόκρισης λήψης FTP δεδομένων, τα οποία παρουσίασαν αστάθεια σε κάποιες περιπτώσεις, ενώ ειδικά όσον αφορά την υπηρεσία φωνής η λειτουργία του πολυπληθούς δικτύου φαίνεται να εμφανίζει πολύ μεγάλες καθυστερήσεις.



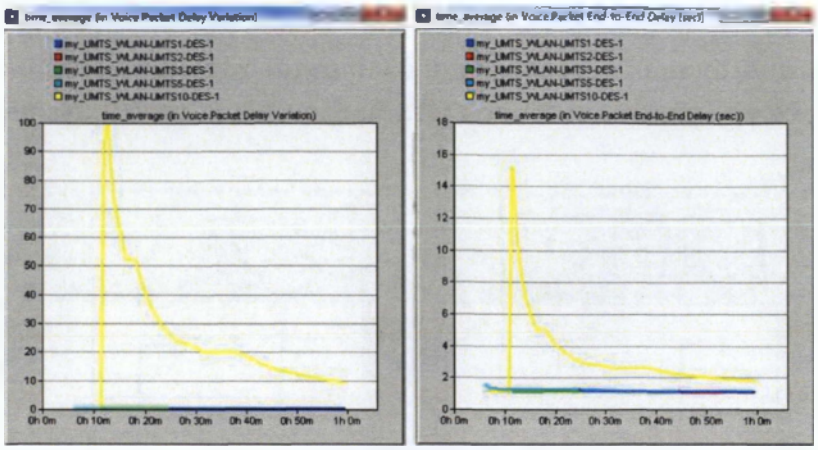
Γράφημα 1: E-mail download & upload response times σε UMTS σενάρια



Γράφημα 2: FTP download & upload response times σε UMTS σενάρια



Γράφημα 3: HTTP object & page response times σε UMTS σενάρια

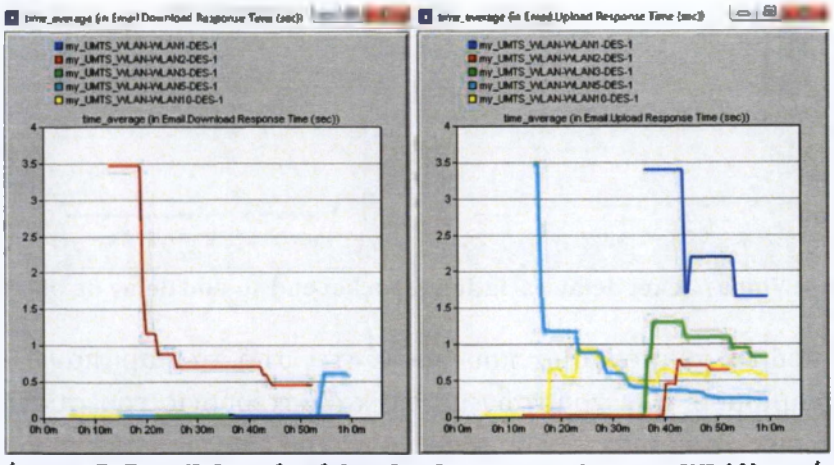


Γράφημα 4: Voice packet delay variation & packet end-to-end delay σε UMTS σενάρια

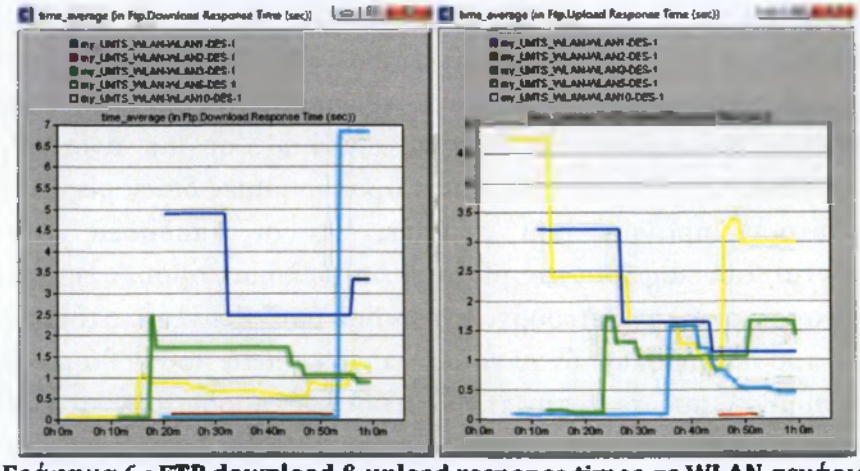
Το πρώτο συμπέρασμα που προκύπτει από τα παραπάνω είναι ότι η σχέση του αριθμού των χρηστών με τις καθυστερήσεις του συστήματος δεν είναι καθόλου γραμμική, αφού στα λιγότερο συνωστισμένα σενάρια δεν υφίσταται κανενός είδους αναλογία ανάμεσα στα δύο μεγέθη. Αυτό πρακτικά υποδηλώνει ότι η χωρητικότητα ενός τέτοιου συστήματος σε χρήστες εγγυάται τη διατήρηση των χρόνων διεκπεραίωσης σε φυσιολογικά επίπεδα παρά την αύξηση του αριθμού των χρηστών, όσο αυτός παραμένει σχετικά περιορισμένος. Με την αύξηση του αριθμού των χρηστών όμως σε μια ανώτερη στάθμη, αρχίζουν να κάνουν την εμφάνισή τους παρατηρήσιμες διαφορές ως προς τους χρόνους αυτούς, πράγμα που σημαίνει ότι οι αποδόσεις του δικτύου επιδεινώνονται, συνεισφέροντας μία αιτία προβληματισμού, στην κατεύθυνση της βελτιστοποίησης της λειτουργίας του δικτύου. Εξάλλου, στόχος αυτής της σειράς των προσομοιώσεων ήταν να διερευνηθεί κατά πόσον θα μπορούσαν τα WLANs να συμβάλλουν σε αυτήν την κατεύθυνση, προσφέροντας εναλλακτικές για την αποσυμφόρηση του UMTS δικτύου. Για το λόγο αυτό, τα επόμενα αποτελέσματα που συνελέχθησαν ήταν αυτά των προσομοιώσεων των μοντέλων WLAN.

Στην περίπτωση των WLANs, τα αποτελέσματα των προσομοιώσεων διαφέρουν με αυτά του UMTS, ως προς το ότι το πολυπληθές δίκτυο των 10 τερματικών συσκευών δεν παρουσιάζει πάντα τους μεγαλύτερους χρόνους. Αντιθέτως, δε φαίνεται να υπάρχει καμία προφανής σύνδεση ανάμεσα στους χρόνους που μελετώνται και στο πλήθος των συνδεδεμένων χρηστών. Τα υπό εξέταση μεγέθη παρουσιάζουν μεγάλη αστάθεια στην πλειονότητα των περιπτώσεων, γεγονός που μπορεί εν μέρει να ερμηνευτεί σύμφωνα με όσα σχολιάστηκαν παραπάνω : εάν ο κάθε χρήστης δεν αντιπροσωπεύει ένα σχεδόν σταθερό φορτίο και τα στατιστικά και πιθανοτικά μεγέθη που σχετίζονται με τον τρόπο με τον οποίο χρησιμοποιεί τις υπηρεσίες χαρακτηρίζονται από μεγάλη εντροπία, τότε υπεισέρχεται ένας παράγοντας τυχαιότητας, ο οποίος ενδεχομένως να είναι ορατός στα αποτελέσματα, εάν δε συντρέχει άλλος λόγος που να προκαλεί την εμφάνιση ουσιαστικότερων διαφορών, για διακριτές περιπτώσεις. Τα δεδομένα της απεσταλμένης και της ληφθείσας κίνησης των

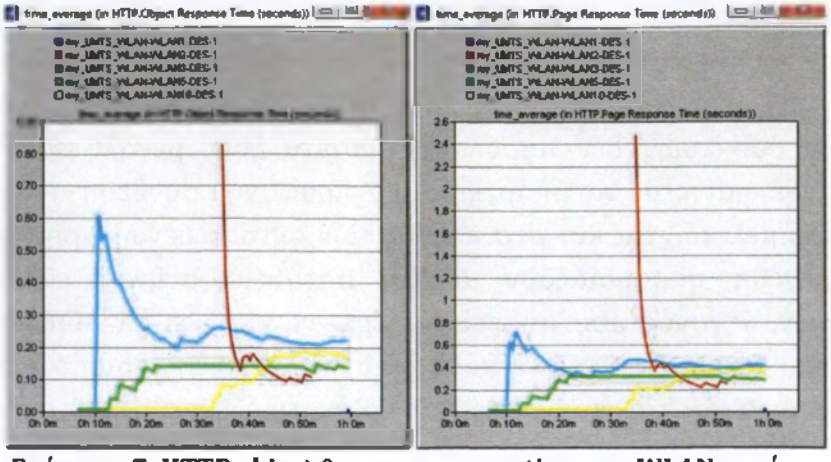
κόμβων κατά τη διάρκεια των προσομοιώσεων αυτών επιβεβαιώνουν τον παραπάνω συλλογισμό, εντούτοις παραλείπονται χάριν εποπτικής απλότητας. Αντιθέτως, τα γραφήματα των υπό εξέταση χρόνων για τα WLANs παρατίθενται παρακάτω.



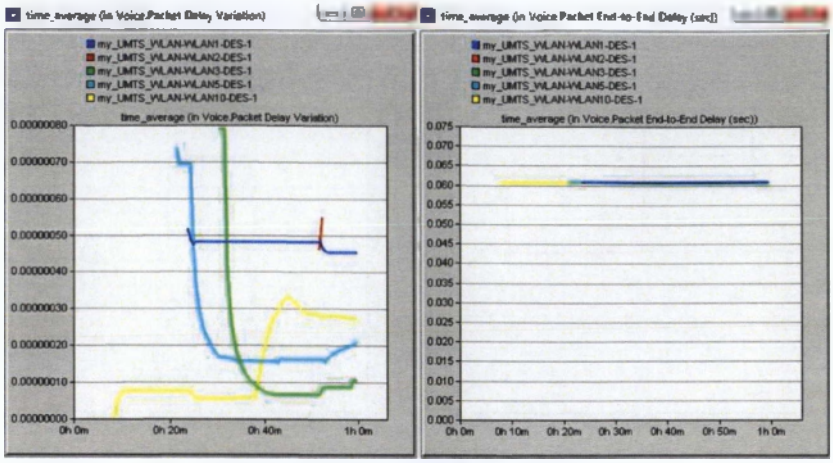
Γράφημα 5: E-mail download & upload response times σε WLAN σενάρια



Γράφημα 6 : FTP download & upload response times σε WLAN σενάρια



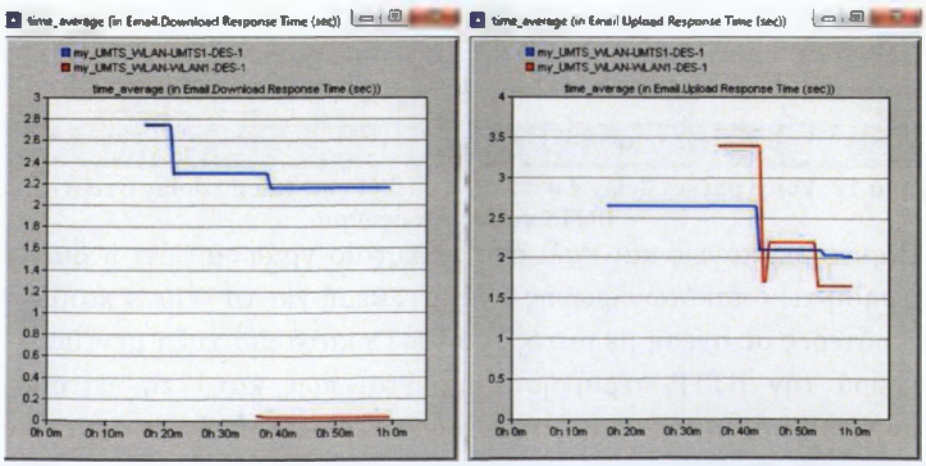
Γράφημα 7: HTTP object & page response times σε WLAN σενάρια



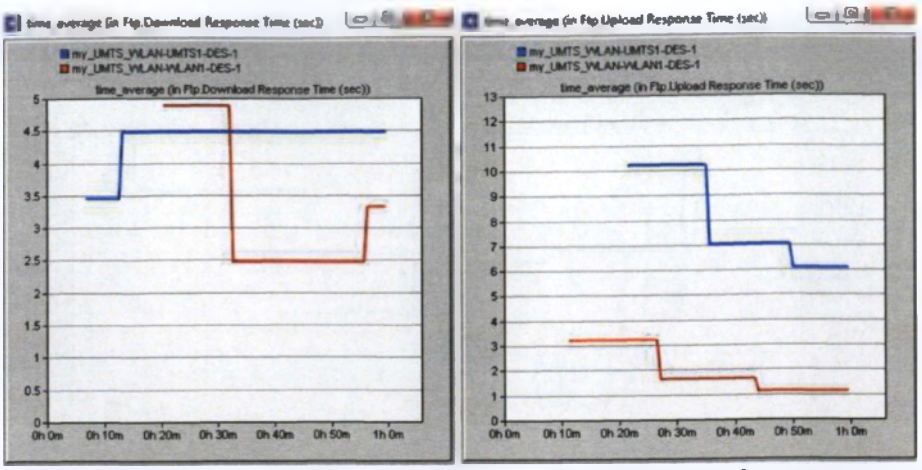
Γράφημα 8: Voice packet delay variation & packet end-to-end delay σε WLAN σενάρια

Μπορεί κανείς να παρατηρήσει στο τελευταίο γράφημα ότι οι διατερματικές καθυστερήσεις των πακέτων της υπηρεσίας φωνής παρουσιάζουν απόλυτη ομοιογένεια σε όλα αυτά τα σενάρια. Κατά τ' άλλα, γεγονός είναι πως τα παραπάνω γραφήματα δεν απεικονίζουν αποτελέσματα αξιολογήσιμα και δεν είναι σε θέση να προσφέρουν χρήσιμα συμπεράσματα. Ένα απλοϊκό σχόλιο θα μπορούσε να είναι ότι η χωρητικότητα ενός WLAN με αυτά τα χαρακτηριστικά είναι τέτοια ώστε να εξασφαλίζει παρόμοιους χρόνους παρά τις αυξομειώσεις του αριθμού των χρηστών, τουλάχιστον όσο αυτός παραμένει στα χαμηλά επίπεδα της συγκεκριμένης παραμετροποίησης.

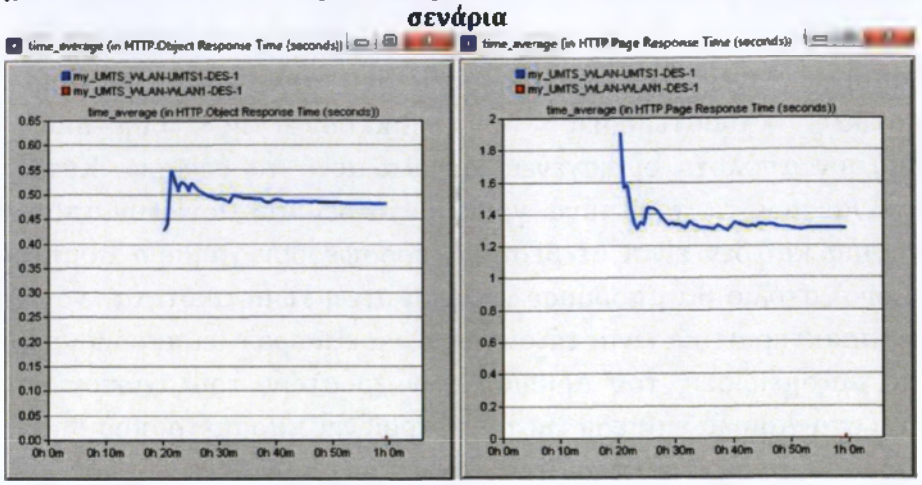
Ωστόσο, είναι χαρακτηριστικό ότι οι τιμές των μεγεθών που μελετώνται είναι κατά κανόνα αρκετά μικρότερες στο WLAN σε σύγκριση με το UMTS. Η διαπίστωση αυτή, αν και αναμενόμενη, αποτελεί τον ακρογωνιαίο λίθο της λογικής της μοντελοποίησης που επιχειρείται σε αυτήν την εργασία, μιας και επιβεβαιώνει τη δυνητική (τουλάχιστον) χρησιμότητα των WLANs στην κατεύθυνση της βελτίωσης της απόδοσης του UMTS. Για να είναι η σύγκριση αυτή καλύτερα αντιληπτή, παρατίθενται στη συνέχεια σε κοινούς άξονες τα γραφήματα του στοιχειώδους UMTS δικτύου 1 συσκευής και του αντίστοιχου WLAN.



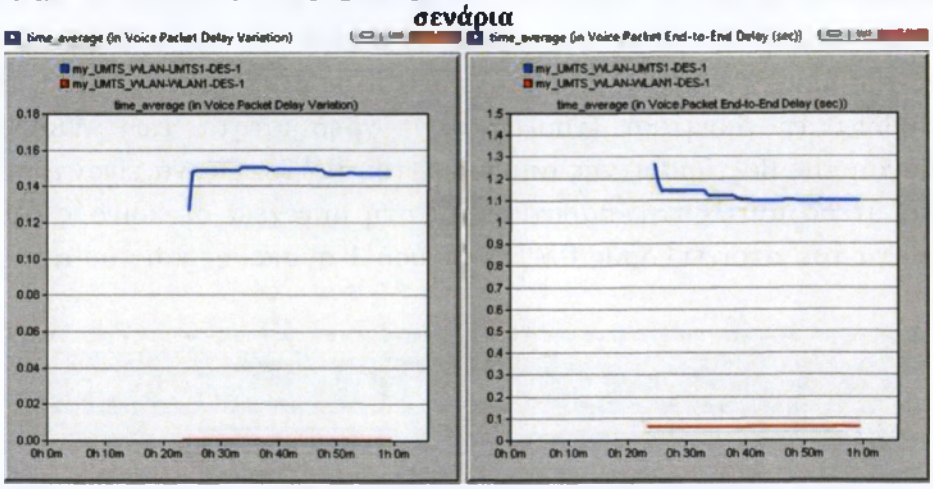
Γράφημα 9: E-mail download & upload response times στα στοιχειώδη UMTS και WLAN σενάρια



Γράφημα 10: FTP download & upload response times στα στοιχειώδη UMTS και WLAN σενάρια



Γράφημα 11: HTTP object & page response times στα στοιχειώδη UMTS και WLAN σενάρια

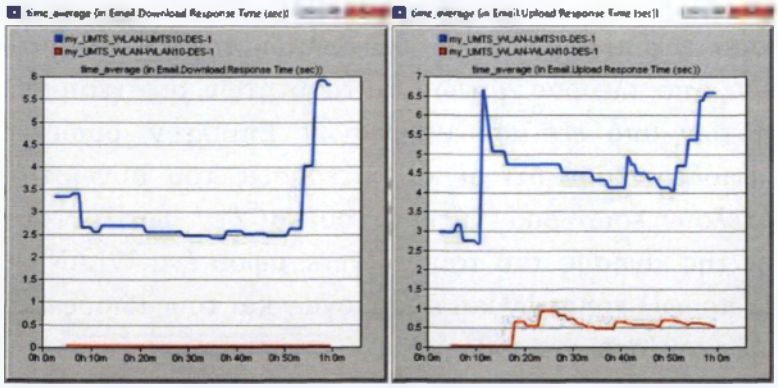


Γράφημα 12: Voice packet delay variation & packet end-to-end delay στα στοιχειώδη UMTS και WLAN σενάρια

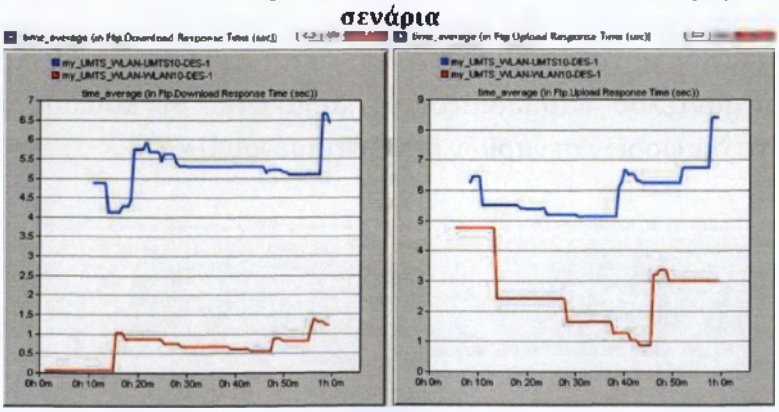
Παρατηρεί κανείς και πάλι στο τελευταίο γράφημα ότι η διατερματική καθυστέρηση των πακέτων φωνής είναι σταθερή για το WLAN και μάλιστα σε τιμές μικρότερες σε σχέση με αυτές του UMTS κατά μία τάξη μεγέθους. Ακόμα, όσον αφορά την HTTP περιήγηση, φαίνεται πως κατά τη λειτουργία του μοντέλου του WLAN η τερματική συσκευή δεν έκανε χρήση της υπηρεσίας παρά μόνο λίγο πριν τη λήξη του χρονικού διαστήματος της προσομοίωσης, με αποτέλεσμα να μην προσφέρεται επαρκής ποσότητα μετρήσεων, χωρίς αυτό

βέβαια να αναιρεί τη γενικότητα του συμπεράσματος της σύγκρισης των δύο δικτύων.

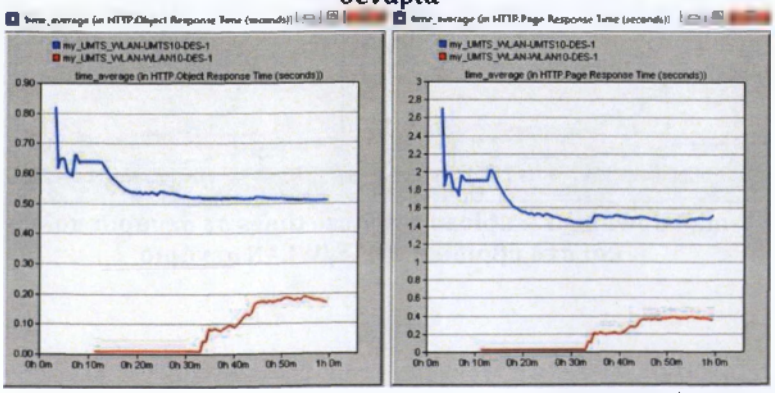
Το συμπέρασμα αυτό είναι βέβαια ότι το στοιχειώδες UMTS δίκτυο παρουσιάζει σε όλες τις περιπτώσεις χρόνους αρκετά μεγαλύτερους σε σχέση με το στοιχειώδες WLAN. Εν είδει επαλήθευσης του συμπεράσματος αυτού, απεικονίστηκαν επίσης σε κοινούς άξονες τα γραφήματα του UMTS δικτύου των 10 συσκευών και του αντίστοιχου WLAN. Βέβαια, οι αποδόσεις του πολυπληθούς αυτού WLAN δεν είναι ανάμεσα στις σημαντικότερες παραμέτρους διερεύνησης της εργασίας αυτής, σκοπός όμως της συγκεκριμένης απεικόνισης είναι να επιβεβαιώσει ότι, ακόμα και σε μια τέτοια περίπτωση αριθμού χρηστών, το WLAN είναι ικανότερο να διαχειριστεί την προσφερόμενη κίνηση. Τα γραφήματα αυτά ακολουθούν παρακάτω:



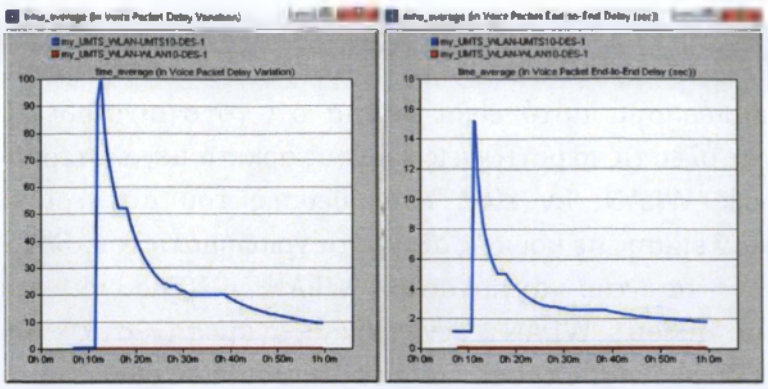
Γράφημα 13: E-mail download & upload response times στα πολυπληθή UMTS και WLAN σενάρια



Γράφημα 14: FTP download & upload response times στα πολυπληθή UMTS και WLAN σενάρια



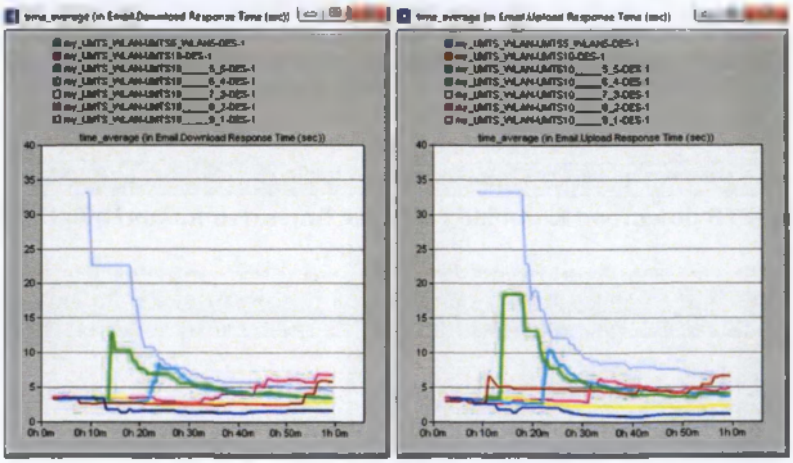
Γράφημα 15: HTTP object & page response times στα πολυπληθή UMTS και WLAN σενάρια



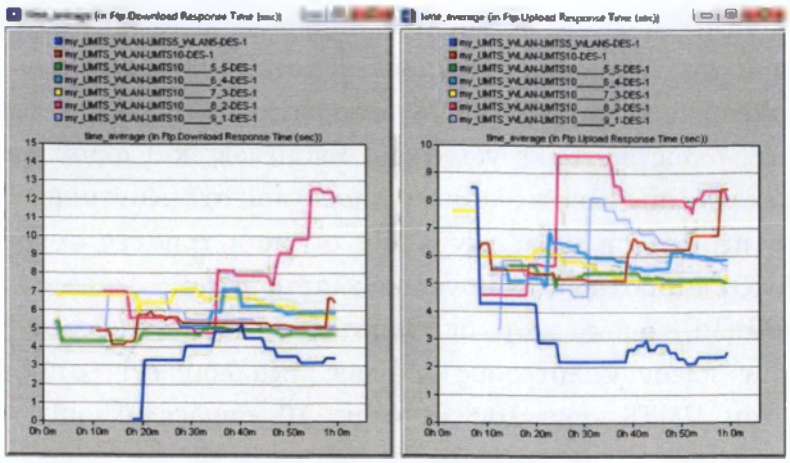
Γράφημα 16: Voice packet delay variation & packet end-to-end delay στα πολυπληθή UMTS και WLAN σενάρια

Σ' αυτήν τη σειρά των γραφημάτων αποτυπώνεται με τρόπο σαφέστερο το συμπέρασμα της προηγούμενης, ότι δηλαδή τα WLANs ανταποκρίνονται πολύ καλύτερα, από πλευράς χρόνων και ταχυτήτων, σε σχέση με το UMTS, για όλα τα είδη των υπό εξέταση υπηρεσιών. Επιπλέον, όμως, τα τελευταία γραφήματα αποδεικνύουν ότι οι καθυστερήσεις του συνωστισμένου UMTS δικτύου αποτελούν εσωτερικό ζήτημά του και δεν οφείλονται σε αδυναμία εξυπηρέτησης της κίνησης από τους servers, αφού ένα WLAN με ίδιο αριθμό χρηστών, ίδια προφίλ χρηστών και εφαρμογών και τους ίδιους ακριβώς servers δεν παρουσιάζει αντίστοιχο πρόβλημα.

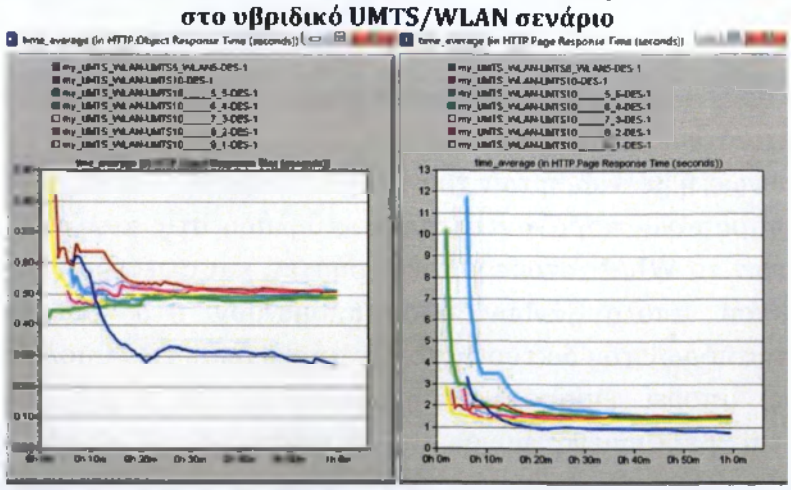
Τα παραπάνω υποδεικνύουν ότι μία ενδιαφέρουσα λύση αποσυμφόρησης του UMTS θα μπορούσε να προσφερθεί από τη συνεργατική λειτουργία των δύο αυτών ειδών δικτύων. Τα αποτελέσματα της προσομοίωσης ενός τέτοιου μοντέλου παρουσιάζονται παρακάτω, σε κοινούς άξονες με τα αποτελέσματα διαφόρων σεναρίων συνωστισμένου UMTS.



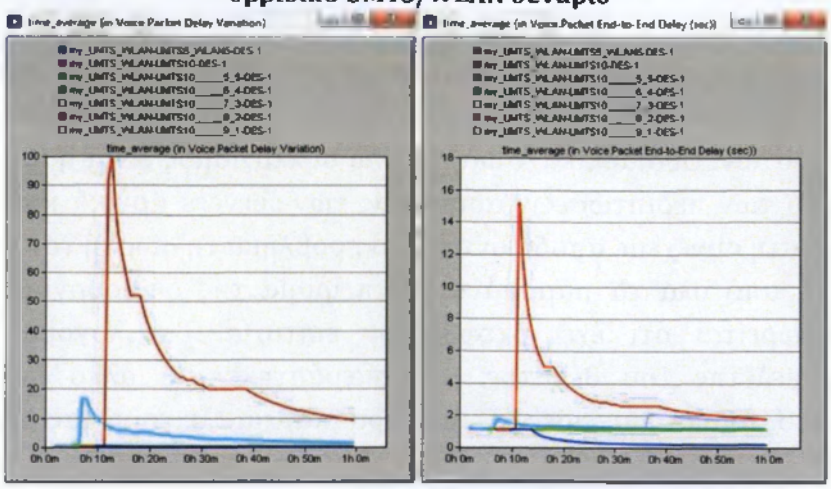
Γράφημα 17: E-mail download & upload response times σε σενάρια πολυπληθούς UMTS και στο υβριδικό UMTS/WLAN σενάριο



Γράφημα 18: FTP download & upload response times σε σενάρια πολυπληθούς UMTS και στο υβριδικό UMTS/WLAN σενάριο



Γράφημα 19: HTTP object & page response times σε σενάρια πολυπληθούς UMTS και στο υβριδικό UMTS/WLAN σενάριο



Γράφημα 20: Voice packet delay variation & packet end-to-end delay σε σενάρια πολυπληθούς UMTS και στο υβριδικό UMTS/WLAN σενάριο

Τα παραπάνω αποτελέσματα είναι ασφαλώς ιδιαίτερα ικανοποιητικά, αφού σε όλα ανεξαιρέτως τα γραφήματα διακρίνεται ότι οι επιδόσεις του υβριδικού δικτύου είναι μακράν καλύτερες, σε σχέση με όλα τα υπόλοιπα σενάρια. Το γεγονός αυτό μπορεί να αναλυθεί με διάφορους τρόπους. Ο πρώτος και προφανής είναι ότι, μετά τη μεταφορά ορισμένων χρηστών από το UMTS σε

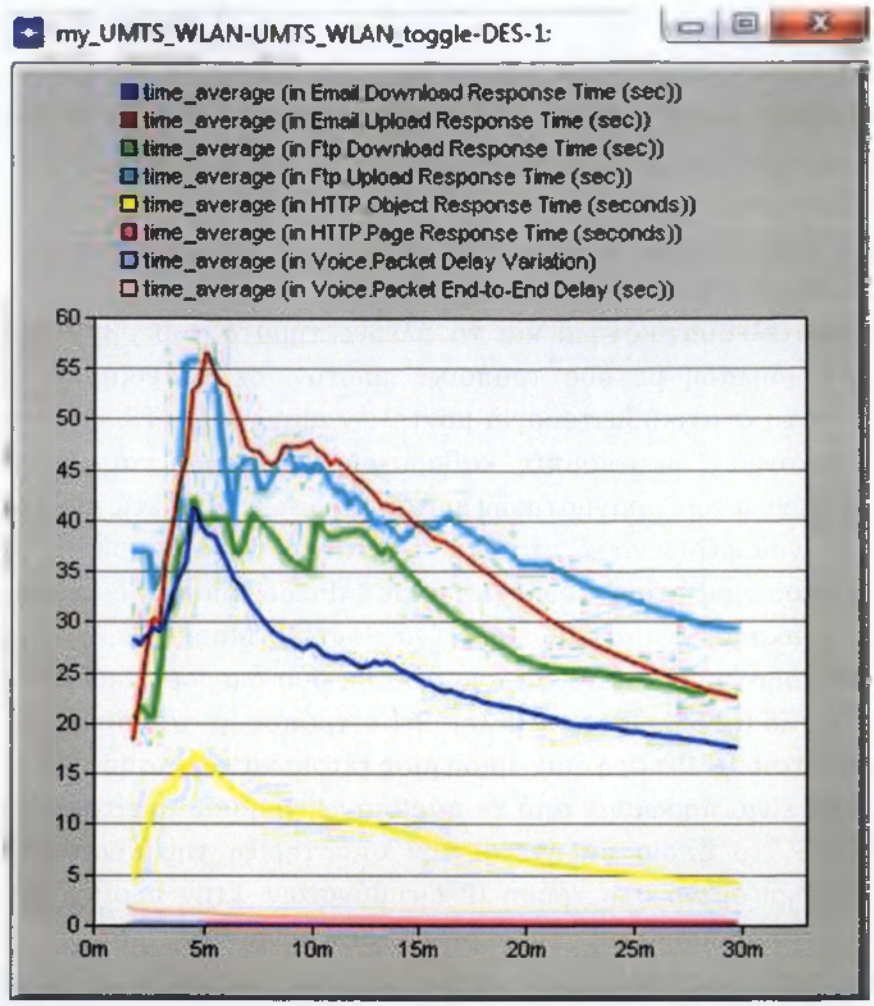
κάποιο WLAN (πράγμα που ουσιαστικά συμβαίνει κατά τη μετάβαση από το UMTS σενάριο στο υβριδικό), οι χρήστες αυτοί απολαμβάνουν καλύτερους χρόνους σε σχέση με αυτούς του UMTS, δεδομένου ότι τα WLANs είναι ταχύτερα από το UMTS, όπως δείχθηκε νωρίτερα. Επομένως, και αφού τα παραπάνω γραφήματα εκφράζουν όλες τις καθυστερήσεις που σχετίζονται με την εκάστοτε εφαρμογή, η περίπτωση κατά την οποία οι μισοί χρήστες συνδέονται μέσω WLAN εμφανίζει καθυστερήσεις συνολικά ελαττωμένες.

Παράλληλα, όμως, και οι χρήστες που παραμένουν στο UMTS απολαμβάνουν πλέον καλύτερους χρόνους. Εξάλλου, έχει αποδειχθεί ότι η λειτουργία του UMTS μοντέλου με τους 10 συνδεδεμένους χρήστες έχει μειωμένες επιδόσεις σε σχέση με αυτές του μοντέλου με τους 5 χρήστες και μάλιστα ότι αυτό αφορά κυρίως το UMTS και όχι τους servers. Όταν λοιπόν μεταφέρονται 5 χρήστες στο WLAN, αυτοί που παραμένουν στο UMTS αντιμετωπίζουν μικρότερες καθυστερήσεις, αφού αξιοποιούνται πλέον αποτελεσματικότερα οι πόροι του δικτύου.

Επομένως, η βελτίωση των χρόνων για το υβριδικό σενάριο οφείλεται και στους δύο παραπάνω παράγοντες, αφενός δηλαδή στις καλύτερες ταχύτητες που προσφέρει το WLAN στους μισούς χρήστες, και αφετέρου στις καλύτερες ταχύτητες που απολαμβάνουν όσοι απομένουν στο UMTS, λόγω της αποδέσμευσης πόρων του δικτύου από την αποχώρηση των υπολοίπων.

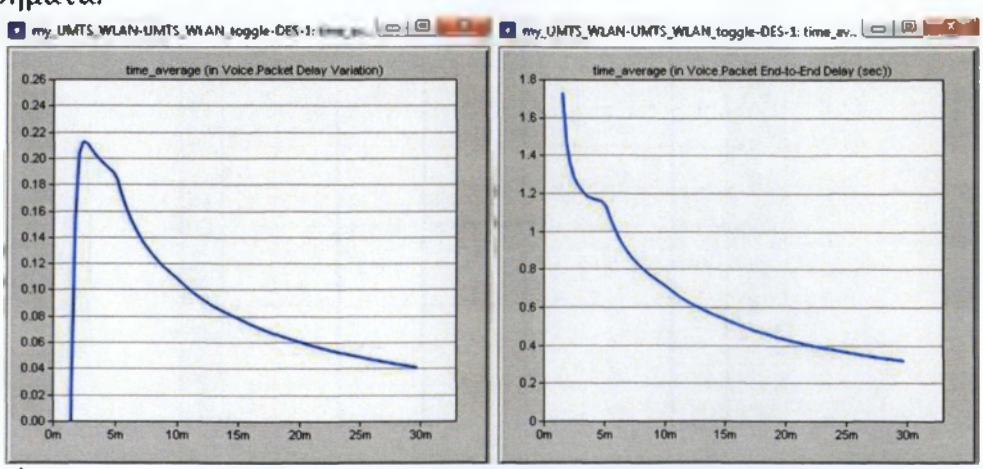
Τέλος, μπορεί επίσης να σημειωθεί ότι το υβριδικό δίκτυο δεν παρουσιάζεται βελτιωμένο μόνο σε σύγκριση με το απλό σενάριο του συνωστιμένου UMTS, αλλά γενικότερα σε σύγκριση με όλα τα κατασκευασμένα UMTS σενάρια αυτού του πλήθους χρηστών. Αυτός άλλωστε ήταν και ο λόγος της δημιουργίας τους: να φανεί ότι το πρόβλημα της συμφόρησης στο UMTS δεν αφορά απλώς συμφόρηση στον τελικό κόμβο του επίγειο δικτύου, αλλά υπάρχει γενικότερο ζήτημα συνωστισμού του δικτύου, κατά τη σύνδεση μεγάλου αριθμού χρηστών. Ουσιαστικά, ο παραπάνω συλλογισμός είναι η κατάληξη του αποκλεισμού των περιπτώσεων αδυναμίας των servers αρχικά και αδυναμίας του Node-B στη συνέχεια, αποδίδοντας στο πρόβλημα τη σωστή του διάσταση.

Μετά από όλα τα παραπάνω, το πείραμα της δημιουργίας υβριδικού δικτύου θεωρείται ότι έχει στεφθεί με επιτυχία. Για λόγους καλύτερης εποπτικής μελέτης του θέματος, κατασκευάστηκε και άλλο ένα υβριδικό σενάριο, στο οποίο επιχειρείται μία προσπάθεια λειτουργίας ενός είδους "εικονικής" μεταπομπής.. Τα αποτελέσματα της προσομοίωσης αυτού του δικτύου παρουσιάζονται συγκεντρωτικά για όλες τις εφαρμογές στο παρακάτω γράφημα:



Γράφημα 21: E-mail & FTP download & upload response times, HTTP object & page response times και voice packet delay variation & packet end-to-end delay στο υβριδικό σενάριο "εικονικής" μεταπομπής

Επειδή τα δύο μεγέθη που σχετίζονται με την υπηρεσία φωνής κυμαίνονται σε τάξεις μεγέθους πολύ χαμηλότερες από αυτές των υπολοίπων, το παραπάνω γράφημα δεν είναι κατάλληλο για την παρατήρησή τους. Γι' αυτόν το λόγο, επαναπαρουσιάζονται παρακάτω σε δύο ξεχωριστά αφιερωμένα γραφήματα.

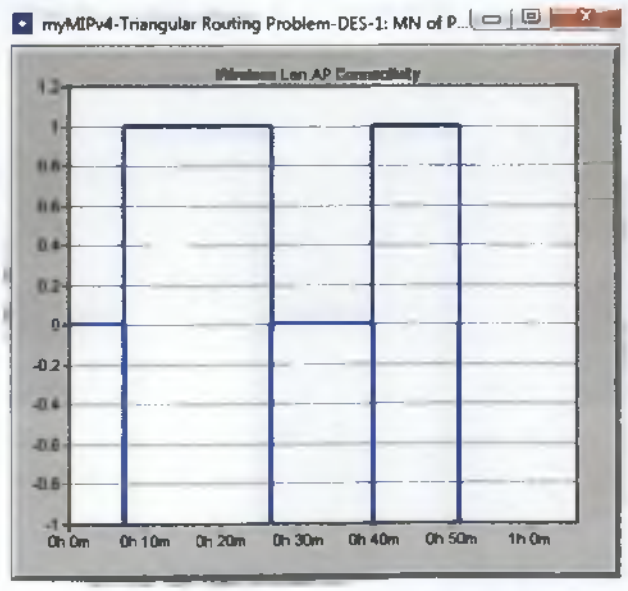


Γράφημα 22: Voice packet delay variation & packet end-to-end delay στο υβριδικό σενάριο "εικονικής" μεταπομπής

Παρατηρούμε λοιπόν μία εξομάλυνση των χρόνων με το πέρασμα της ώρας. Αυτό αποτελεί συνέπεια των "εικονικών" μεταπομπών που επιτυγχάνονται, αφού αρχικά το δίκτυο βρίσκεται σε κατάσταση UMTS λειτουργίας αποκλειστικά και, με την τακτική αποχώρηση των UMTS συσκευών από το δίκτυο και την παράλληλη προσχώρηση WLAN συσκευών σε αυτό, η λειτουργία του μετατρέπεται σταδιακά σε υβριδική και στο τέλος καταλήγει να είναι αποκλειστικά WLAN.

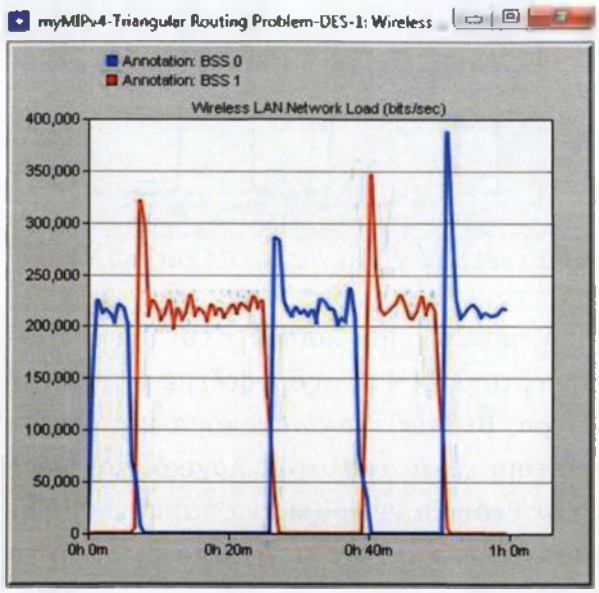
Η αποτελεσματικότητα και τα πλεονεκτήματα του υβριδικού δικτύου εξετάστηκαν δηλαδή με δύο τρόπους: πρώτον, σε στατική λειτουργία, σε σύγκριση με τη στατική λειτουργία μοντέλων αμιγούς UMTS, και δεύτερον, με τακτικές "εικονικές" μεταπομπές, καθαρά ως συνάρτηση του χρόνου. Επειδή όμως η διενέργεια των πραγματικών μεταπομπών είναι αρκετά πιο πολύπλοκη, θεωρήθηκε ενδιαφέρον να εξεταστεί η δυνατότητα χρησιμοποίησης του Mobile IP για την υποστήριξή τους, τουλάχιστον σε επίπεδο τοπικών δικτύων. Γι' αυτόν ακριβώς το σκοπό, κατασκευάστηκε ένα μοντέλο Mobile IP, στο οποίο ένας ασύρματος χρήστης μετακινείται ανάμεσα σε δύο διαφορετικές BSAs που δεν ανήκουν στο ίδιο ESS, ώστε να μελετηθεί ο τρόπος με τον οποίο το σύστημα μπορεί να ανταπεξέλθει στη διαχείριση μιας τέτοια κατάστασης.

Όπως είναι προφανές από τα παραπάνω, χρησιμοποιείται συγκεκριμένα το Mobile IP, το οποίο υπόσχεται την υποστήριξη της κινητικότητας των χρηστών, στηριζόμενο στη χρήση IP διευθύνσεων. Στην περίπτωση αυτή, τα μεγέθη που παρουσιάζουν ενδιαφέρον δεν είναι τα ίδια με αυτά των προηγούμενων προσομοιώσεων, αφού το σημαντικότερο είναι να αποδειχθεί ότι το πρωτόκολλο επιτυγχάνει τη διευθέτηση αυτού του είδος των καταστάσεων, αλλά και να δειχθούν τυχόν μειονεκτήματα που σχετίζονται με αυτό. Το πρώτο γράφημα που θα παρουσιαστεί σχετικά με αυτό το μοντέλο είναι το παρακάτω, στο οποίο εμφανίζεται η συνδεσιμότητα με Access Points (AP connectivity) του MN ως προς το χρόνο, με βάση το αναγνωριστικό BSS (BSS identifier) του κάθε AP:



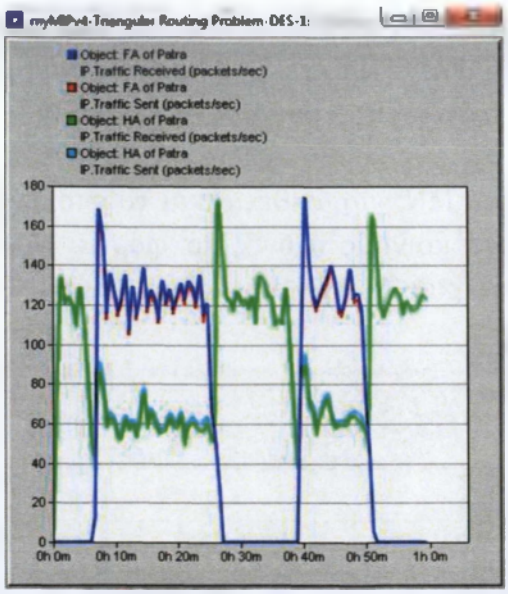
Γράφημα 23: AP connectivity για τον MN στο Mobile IP μοντέλο

Το γράφημα αυτό δείχνει ουσιαστικά πότε ο MN ήταν συνδεδεμένος με τον HA και πότε με τον FA. Ο HA έχει BSS identifier ίσο με 0 και ο FA ίσο με 1. Φαίνεται λοιπόν ότι, λόγω της συνεχούς μετακίνησής του, ο MN συνδέεται εναλλάξ με τους δύο αυτούς κόμβους. Για την καλύτερη εποπτική απεικόνιση της συνδεσιμότητας του MN, παρατίθεται και το επόμενο γράφημα, στο οποίο έχει αναπαρασταθεί σε κοινούς άξονες το φορτίο (load) στα δύο APs του δικτύου, δηλαδή στον κόμβο HA και στον κόμβο FA, με βάση το BSS αναγνωριστικό τους:



Γράφημα 24: Load για τον FA και τον HA στο Mobile IP μοντέλο

Και εδώ, επομένως, είναι δυνατή η παρατήρηση των μεταβάσεων του MN ανάμεσα στην περιοχή κάλυψης του HA και αυτήν του FA. Τα δύο τελευταία γραφήματα είναι ενδεικτικά της λειτουργίας αυτού του συστήματος, και με βάση αυτά μπορεί να εξαχθεί το συμπέρασμα ότι το σύστημα είναι σε θέση να ανταποκριθεί στις ESS μεταβάσεις του MN, με τη βοήθεια του Mobile IP. Για να συσχετιστούν καλύτερα τα παραπάνω δεδομένα με τη θεωρία του Mobile IP, ακολουθεί ένα ακόμα γράφημα, στο οποίο έχουν αποδοθεί σε κοινούς άξονες η απεσταλμένη IP κίνηση (IP traffic sent) και η ειλημμένη IP κίνηση (IP traffic received) για τους κόμβους HA και FA του μοντέλου:

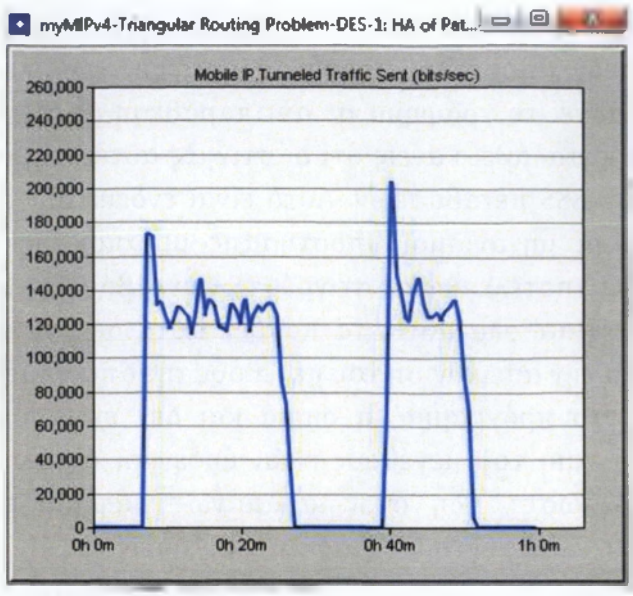


Γράφημα 25: *IP* traffic sent & received για τον *FA* και τον *HA* στο *Mobile IP* μοντέλο

Μία σημαντική παρατήρηση λοιπόν είναι ότι ενώ ο FA αποστέλλει και λαμβάνει πακέτα μόνο όταν ο MN είναι συνδεδεμένος με αυτόν, ο HA αποστέλλει και λαμβάνει (λιγότερα, βέβαια) πακέτα ακόμα και όταν ο MN βρίσκεται σε ξένιο δίκτυο. Κάτι τέτοιο είναι απολύτως λογικό για ένα Mobile IP σύστημα, αφού ο CN δεν είναι σε θέση να γνωρίζει ανά πάσα στιγμή την τοπολογική θέση του MN και έτσι αποστέλλει πάντοτε τα πακέτα με βάση τη home address του παραλήπτη, με αποτέλεσμα να διέρχονται από τον HA όλα τα πακέτα αυτής της κατεύθυνσης της κίνησης. Στη συνέχεια, εάν ο MN είναι εντός του πάτριου δικτύου, ο HA του προωθεί τα πακέτα, ενώ εάν βρίσκεται σε κάποιο ξένιο δίκτυο, ενθυλακώνει τα πακέτα και τα αποστέλλει με βάση τη CoA, την οποία ο HA γνωρίζει, σε αντίθεση με το CN.

Στην αντίστροφη διαδρομή, όμως, δηλαδή στα πακέτα που κατευθύνονται προς το CN, ο HA δεν εμπλέκεται καθόλου όταν ο MN βρίσκεται σε ξένιο δίκτυο, και γι' αυτόν το λόγο, όπως φαίνεται στο γράφημα, ο αριθμός των συνολικών πακέτων που διέρχονται από τον HA στην περίπτωση αυτή είναι περίπου ο μισός (που αντιπροσωπεύει τη 1 από τις 2 διαδρομές) σε σχέση με την περίπτωση κατά την οποία ο MN βρίσκεται στο πάτριο δίκτυό του και κατά την οποία ο HA συνδέεται και με τις δύο κατευθύνσεις της κίνησης.

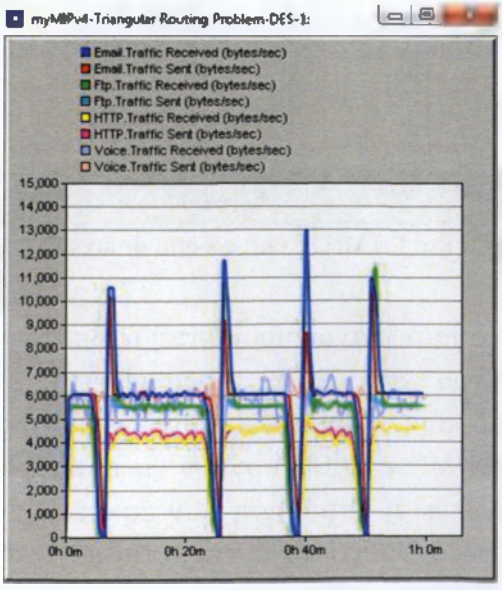
Αυτό μπορεί να αποδειχθεί και με τη βοήθεια του επόμενου γραφήματος, όπου αναπαρίσταται η ενθυλακωμένη και προωθημένη σε σήραγγα IP κίνηση (IP tunneled traffic sent) από τον HA:



Γράφημα 26: *IP tunneled* traffic sent για τον *HA* στο *Mobile IP* μοντέλο

Αντιπαραβάλλοντας το γράφημα αυτό με τα προηγούμενα, είναι προφανές πως ο HA ενθυλακώνει πακέτα όσο ο MN βρίσκεται συνδεδεμένος με τον FA, ακριβώς όπως ορίζει το Mobile IP, ενώ φυσικά δεν υπάρχει ανάγκη ενθυλάκωσης όσο ο MN είναι συνδεδεμένος στον ίδιο τον HA, όπως άλλωστε εξηγήθηκε νωρίτερα.

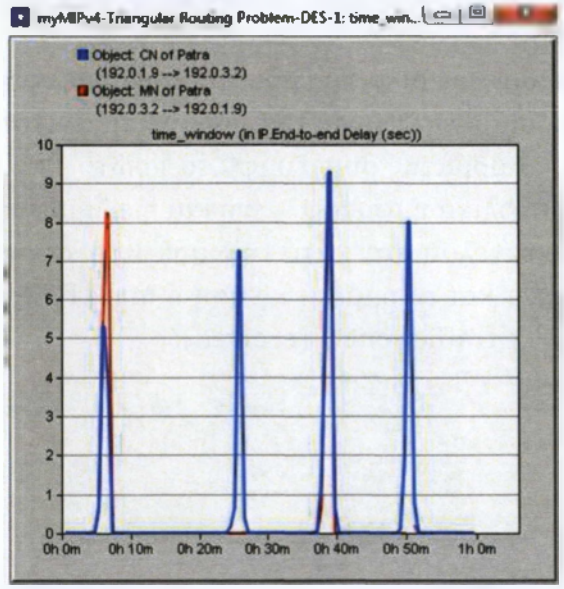
Τέλος, ακολουθούν μερικά γραφήματα για τη μελέτη των επιδόσεων του συστήματος κατά τη διάρκεια των μεταπομπών και γενικότερα της διαδικασίας της περιαγωγής της ασύρματης συσκευής. Στο πρώτο από αυτά τα γραφήματα έχει συγκεντρωθεί συνολικά η απεσταλμένη και η ειλημμένη κίνηση και για τα 4 είδη εφαρμογών που εκτελούνταν κατά τη διάρκεια όλης αυτής της διαδικασίας, δηλαδή η απεσταλμένη και ειλημμένη κίνηση e-mail, FTP, HTTP και φωνής (e-mail, FTP, HTTP & voice traffic sent & received):



Γράφημα 27: E-mail, FTP, HTTP & voice traffic sent & received στο Mobile IP μοντέλο

Παρατηρούμε ότι σε κάποιες στιγμές μηδενίζεται σχεδόν ο αριθμός των πακέτων, τόσο στην αποστολή όσο και στη λήψη, για όλες τις εφαρμογές. Μάλιστα, αν εξεταστεί το γράφημα σε αντιπαράθεση με τα προηγούμενα, δεν είναι δύσκολο να καταλάβει κανείς ότι οι στιγμές αυτές συμπίπτουν ασφαλώς με τις στιγμές των ESS μεταβάσεων. Αυτό είναι ενδεικτικό του γεγονότος ότι στο Mobile IPv4 οι μηχανισμοί υποστήριξης μεταπομπής δεν είναι ακόμα τελειοποιημένοι, με αποτέλεσμα τις στιγμές των μεταβάσεων να παρατηρούνται τέτοια φαινόμενα. Παρ' όλα αυτά, τα πακέτα αυτά δε χάνονται, πράγμα που αποδεικνύεται από την απεικόνιση του μεγέθους της απορριμένης IP κίνησης (IP traffic dropped) στο πρόγραμμα, η οποία και δεν έχει συμπεριληφθεί εδώ, ακριβώς επειδή η τιμή του μεγέθους είναι μηδενική σε όλη τη διάρκεια της προσομοίωσης. Άλλωστε, ήδη στο παραπάνω γράφημα παρατηρεί κανείς ιδιαίτερα απότομες αλλά σύντομης διάρκειας αυξήσεις της κίνησης αμέσως μετά την ολοκλήρωση των μεταβάσεων, πράγμα που οφείλεται στη συσσώρευση πακέτων των οποίων η παράδοση καθυστέρησε (χωρίς όμως να ματαιωθεί) κατά τη διάρκεια αυτών και τελικά εκτελέστηκε μετά την ολοκλήρωσή τους.

Για τη δικαιολόγηση του παραπάνω, ακολουθεί ένα ακόμα γράφημα, το οποίο περιλαμβάνει τις διατερματικές IP καθυστερήσεις (IP end-to-end delays) από τον MN στο CN και από το CN στον MN, ως προς το χρόνο:

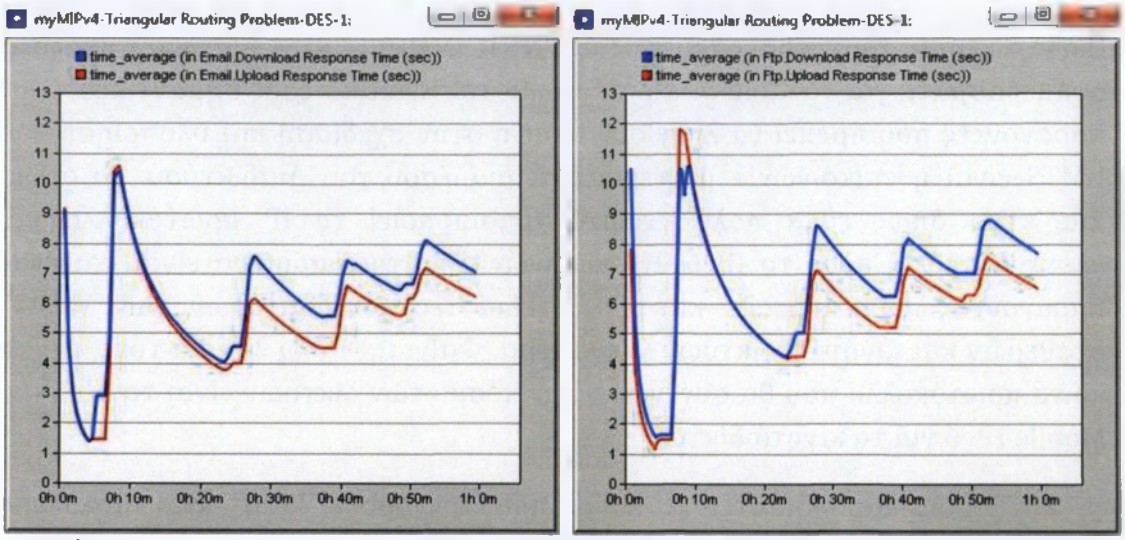


Γράφημα 28: MN CN και CN MN IP end-to-end delays στο Mobile IP μοντέλο

Μετά και από το παραπάνω, προκύπτει ότι κατά τις μεταβάσεις του MN από το ένα υποδίκτυο στο άλλο εμφανίζονται μεγάλες διατερματικές καθυστερήσεις παράδοσης των πακέτων. Ειδικότερα, τα πακέτα που κατευθύνονται από τον MN στο CN αργούν να παραδοθούν κατά τη διάρκεια όλων των μεταβάσεων, ενώ η παράδοση των πακέτων που κατευθύνονται από το CN στον MN καθυστερεί μόνο κατά τις μεταβάσεις του MN από το πάτριο δίκτυο προς το ξένιο δίκτυο. Κάτι τέτοιο είναι λογικό, καθώς όταν ο MN

μετακινείται από το ξένιο δίκτυο στο πάτριο δίκτυο, ο HA εντοπίζει τον MN εύκολα και χωρίς χρονοβόρες διαδικασίες και μπορεί να του παραδώσει αμέσως τα πακέτα που καταφθάνουν συνεχώς από το CN.

Στο επόμενο και τελευταίο γράφημα παρουσιάζονται οι χρόνοι απόκρισης αποστολής και λήψης δεδομένων (download & upload response times) για τις εφαρμογές FTP και HTTP, με χρησιμοποίηση της επιλογής time_average:



Γράφημα 29: *E-mail* & *FTP* download & upload response times στο *Mobile IP* μοντέλο

Εδώ παρατηρούμε και για τις δύο εφαρμογές μία απόκλιση ανάμεσα στις τελικές (και ενδεικτικές) τιμές των μέσων όρων των χρόνων απόκρισης για την ανοδική και την καθοδική ζεύξη, που μπορεί να εξηγηθεί με τη θεωρία του προβλήματος τριγωνικής δρομολόγησης: όσο ο MN βρίσκεται στο ξένιο δίκτυο, τα πακέτα της καθοδικής ζεύξης καθυστερούν περισσότερο, διότι η διαδρομή που πρέπει να διανύσουν είναι διπλάσια από αυτήν της ανοδικής ζεύξης, η οποία δεν περιλαμβάνει καθόλου τον HA.

Με βάση τα τελευταία γραφήματα, μπορεί να υποστηριχθεί ως συμπέρασμα ότι η διαδικασία της μεταπομπής και γενικότερα της περιαγωγής με βάση το Mobile IPv4 επιδέχεται βελτιστοποίηση, εντούτοις η συνολική άποψη για ένα τέτοιο μοντέλο, μετά από το σύνολο των αποτελεσμάτων που προσέφερε η συγκεκριμένη προσομοίωση, είναι θετική.

Κεφάλαιο 7. Συμπεράσματα

Στην πτυχιακή αυτή ασχοληθήκαμε με την ανάπτυξη συστημάτων 3ης γενιάς UMTS. Το UMTS σχεδιάστηκε με τέτοιο τρόπο ώστε να προσφέρει στον μέσο χρήστη τις βασικές υπηρεσίες και να συνδυάζει επίσης πιο ανεπτυγμένες packet – switched και circuit – switched υπηρεσίες κάτω από μια συνενωμένη All – IP αρχιτεκτονική. Στη συνέχεια αναλύσαμε όλα τα σενάρια για τα συστήματα UMTS μέσω του προγράμματος OPNET MODELER 14.5 και βγάλαμε συμπεράσματα για το κάθε σενάριο ξεχωριστά. Ένα από τους σημαντικότερους παράγοντες που πρέπει να ληφθούν υπόψη στην σχεδίαση και υλοποίηση του UMTS είναι η επικοινωνία με τερματικά διαμέσου του Διαδικτύου, το οποίο Διαδίκτυο όπως είναι πολύ γνωστό χρησιμοποιεί το IP πρωτόκολλο και «μεταναστεύει» προς το IPv6. Η επικοινωνία με το Διαδίκτυο είναι και ένας παράγοντας που επηρεάζει και τους σχεδιαστές των διαφόρων LAN, WLAN, σταθερών και κινητών δικτύων γενικότερα. Φαίνεται πολύ λογικό τότε, ότι το κοινό πρωτόκολλο που θα συνενώσει τον κόσμο των δικτύων είναι το IPv6 και Mobile IPv6 για τα κινητά δίκτυα.

Έχουν παρουσιαστεί οι λόγοι που το Mobile IPv6 είναι πολύ πιο αποδοτικό από το Mobile IPv4 και γιατί θα προσφέρει περισσότερα στα τρίτης γενιάς κινητά δίκτυα. Μερικοί από τους λόγους που αναφέρθηκαν είναι: ο μεγαλύτερος αριθμός διαθέσιμων διευθύνσεων, η χρήση του Dynamic Home Agent Discovery, οι 100 ενσωματωμένοι μηχανισμοί ασφάλειας, η χρήση Route Optimization και τα λοιπά. Παρουσιάζονται διάφοροι μηχανισμοί μετάβασης και φαίνεται ότι οι μηχανισμοί αυτοί παρέχουν τα αναγκαία εργαλεία για μετάβαση από το IPv4 στο IPv6. Ο κάθε μηχανισμός έχει και τα δικά του χαρακτηριστικά και μπορεί να επιλύσει διαφορετικά προβλήματα.

Μιλώντας τώρα αποκλειστικά για τα UMTS, έχουν παρουσιαστεί διαφορετικά σενάρια που διαγράφουν κάποιες δυνατές περιπτώσεις λειτουργίας του UMTS και πως επιτυγχάνεται η επικοινωνία με εφαρμογές που τρέχουν σε hosts του Διαδικτύου. Είναι αβέβαιο το αν όντως θα υλοποιηθούν αυτά τα σενάρια ακριβώς όπως έχουν παρουσιαστεί, αλλά το EURESCOM πιστεύει ότι σε κάποια χρονική στιγμή είναι πολύ πιθανή η υλοποίησή τους. Επίσης, λόγο του ότι το UTRAN μέρος του UMTS δικτύου είναι εντελώς απομονωμένο από το κυρίως δίκτυο, μπορεί να λειτουργήσει και με άλλα είδη δικτύων, σαν WLANS.

Κεφάλαιο 8. Βιβλιογραφία και Πηγές

[1] J. Postel, "RFC 791 Internet Protocol", Σεπτέμβριος 1981
[2] Γ. Κοκκινάκης, Τηλεπικοινωνιακά Συστήματα, 3η έκδοση, 1994
[3] T. Rappaport, Wireless Communications – Principles and Practice, 2η έκδοση, Prentice Hall,1996
[4] C. Perkins, "RFC 2002 IP Mobility Support", Οκτώβριος 1996
[5] C. Perkins, "RFC 2003 IP Encapsulation within IP", Οκτώβριος 1996
[6] C. Perkins, D. B. Johnson, "Route Optimization in Mobile IP", Νοέμβριος 1997
[7] John K. Zao, Matt Condell: Use of IPSec in Mobile IP, Νοέμβριος 1997
[8] R. Hinden, M. O'Dell, S. Deering, "RFC 2374 An IPv6 Aggregatable Global Unicast Address Format", Ιούλιος 1998
[9] R. Hinden, S. Deering, "RFC 2373 IP Version 6 Addressing Architecture", Ιούλιος 1998
[10] D. Maughan, M. Schneider, M. Schertler, J. Turner: Internet Security Association and Key Management Protocol (ISAKMP), Νοέμβριος 1998
[11] D. Harkins, D. Carrel: The Internet Key Exchange (IKE), RFC 2409, Νοέμβριος 1998
[12] Jim Binkley, John Richardson: Security Considerations for Mobility and Firewalls, Νοέμβριος 1998
[13] S. Deering, R. Hinden "RFC 2460 Internet Protocol, Version 6 (IPv6) Specification", Δεκέμβριος 1998
[14] M. Crawford, "RFC 2464 Transmission of IPv6 Packets over Ethernet Networks", Δεκέμβριος 1998
[15] A.Conta, S.Deering, "RFC 2473 Generic tunneling in IPv6 specification", Δεκέμβριος 1998
[16] S. Thomson, T. Narten, "RFC 2462 IPv6 Stateless Address Autoconfiguration", Δεκέμβριος 1998
[17] T. Narten, E. Nordmark, W. Simpson, "RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)", Δεκέμβριος 1998
[18] D. Haskin, E. Allen, "RFC 2472 IP Version 6 over PPP", Δεκέμβριος 1998
[19] V. Gupta, G. Montenegro, Secure and mobile Networking, Mobile Networks and Applications 3 (381-390), Baltzer Science Publisher BV, 1998
[20] James R. Binkley, John McHugh, Portland State University: Secure Mobile Networking Final Report, Ιούνιος 1999
[21] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, L. Salgarelli, "IP micro-mobility support using HAWAII", Ιανουάριος 2000
[22] P. Ferguson, D. Senie, "RFC 2827 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", Μάιος 2000
[23] Misra, S. Das, A. Mcauley, A. Dutta, S. K. Das, "IDMP: An Intra-Domain Mobility Management Protocol using Mobility Agents", Ιούλιος 2000
[24] O'Neill, G. Tsirtsis, S. Corson, "Edge Mobility Architecture", Ιούλιος 2000
[25] Charles Perkins, David B. Johnson: Mobility Support in IPv6, Νοέμβριος 2000
[26] Μ. Λογοθέτης, Θεωρία Τηλεπικοινωνιακής Κινήσεως και Εφαρμογές, 2001
[27] Martin, T.; Pütz, S.; Schmitz, R.: On the Security of the UMTS System. Accepted for Verlässliche IT-Systeme (VIS) 2001
[28] F. Pählke, G. Schäfer, J. Schiller, Paketfilter- und Tunnelkonfiguration zur Firewall-verträglichen Mobilitätsunterstützung in IP-Netzen, KiVS 2001, Hamburg, Φεβρουάριος 2001
[29] M. Danzeisen, Secure Mobile IP Communication, Diploma Thesis, Institute of Computer Science and Applied Mathematics, University of Bern, Μάιος 2001
[30] A. Conta, "RFC 3122 Extensions to IPv6 Neighbor Discovery for Inverse Discovery", Ιούνιος 2001
[31] M. Danzeisen, T. Braun: Access of Mobile IP Users to Firewall Protected VPNs, Mobile Communication over Wireless LAN, Workshop at Informatik 2001, Vienna, Σεπτέμβριος 2001
[32] Ahonen και Barrett (editors), Υπηρεσίες για το UMTS, Wiley, 2002
[33] Perkins, "RFC 3220 IP Mobility Support for IPv4", Ιανουάριος 2002
[34] B. Johnson, C. E. Perkins, J. Arkko, "Mobility Support in IPv6", Ιούνιος 2002
[35] K. Kawano, K. Kinoshita, K. Murakami, "Multilevel Hierarchical Distributed IP Mobility Management Scheme for Wide Area Networks", in Proceedings of IEEE ICCCN, 2002
[36] Laiho, Wacker και Novosad, Radio Σχεδιασμού Δικτύου και Βελτιστοποίηση για το UMTS, Wiley, 2002
[37] J. Proakis, M. Salehi, Communication Systems Engineering, 2η έκδοση, Prentice Hall, 2002
[38] Horn, G.; Howard, P.: Review of Third Generation Mobile System Security. Proc. Information Security Solutions Europe (ISSE) 2000

[39] A. Tanenbaum, Computer Networks, 4η έκδοση, 2003
[40] V. Thing, H. Lee, Y. Xu, "A Local Mobility Agent Selection Algorithm for Mobile Networks", IEEE International Conference on Communications, 2003
[41] T. Narten, E. Nordmark, W. Simpson, H. Soliman, J. Tatuya, "Neighbor Discovery for IP version 6 (IPv6)", Οκτώβριος 2003
[42] Γ. Κοκκινάκης, Εισαγωγή στις Επικοινωνίες, 2004
[43] H. Jung, S. Koh, "Fast handover support in hierarchical mobile IPv6", 6th International Conference on Advanced Communication Technology, 2004, Volume 2, Issue , 2004
[44] J. Lai, "Performance Evaluation of Mobility Management Protocols for the Next Generation Internet (IPv6)", Master Thesis, Monash University, Ιανουάριος 2004
[45] Vogt, R. Bless, M. Doll, T. K'fner, "Early Binding Updates for Mobile IPv6", Φεβρουάριος 2004
[46] J. Kempf, M. M. Khalil, "IPv6 Fast Router Advertisement", Ιούλιος 2004
[47] J. Arkko, V. Devarapalli, F. Dupont, "RFC 3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", Ιούνιος 2004
[48] Johnson, C. Perkins, J. Arkko "RFC 3775 Mobility Support in IPv6", Ιούνιος 2004
[49] H. Soliman, C. Catelluccia, K. El Malki, L. Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)", Ιούνιος 2004
[50] J. Kempf, M. Khalil, "IPv6 Fast Router Advertisement", , Οκτώβριος 2004
[51] S. Pack, M. Nam, T. Kwon, Y. Choi, "An adaptive mobility anchor point selection scheme in hierarchical Mobile IPv6 networks", Computer Communications, 2005
[52] Balanis, Antenna Theory, 3η έκδοση, Wiley, 2005
[53] Vogt, "Early Binding Updates for Mobile IPv6", Φεβρουάριος 2005
[54] H. Jung, H. Soliman, S. Koh, "Fast Handover for Hierarchical MIPv6 (FHMIPv6)", Οκτώβριος 2005
[55] R. Koodli, "RFC 4068 Fast Handovers for Mobile IPv6", Ιούλιος 2005
[56] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier, "RFC 4140 Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", Αύγουστος 2005
[57] H. Jung, E. Kim, J. YI, H. Lee, "A Scheme for Supporting Fast Handover in Hierarchical Mobile IPv6 Networks", ETRI Journal, vol.27, no.6, Δεκέμβριος 2005
[58] Σ. Κωτσόπουλος, Συστήματα Ευρείας Εκπομπής, 2006
[59] A. Conta, S. Deering, M. Gupta, "RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)", Μάρτιος 2006
[60] N. Moore, "RFC 4429 Optimistic Duplicate Address Detection (DAD) for IPv6", Απρίλιος 2006
[61] V. Devarapalli, F. Dupont , "RFC 4877 Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", Απρίλιος 2007
[62] Kreher και Ruedebusch, UMTS Σηματοδότηση: Διεπαφές UMTS, πρωτόκολλα, Ροές και διαδικασίες αναλύονται και εξηγούνται, Wiley, 2007
[63] Σ. Κωτσόπουλος, Δορυφορικές και Κινητές Επικοινωνίες, Πανεπιστήμιο Πατρών, 2007
[64] Δ. Λυμπερόπουλος, Τηλεπικοινωνιακά Δίκτυα Επόμενης Γενιάς NGN, Πανεπιστήμιο Πατρών, 2007
[65] Δ. Λυμπερόπουλος, Επικοινωνίες Πολυμέσων, Πανεπιστήμιο Πατρών, 2008