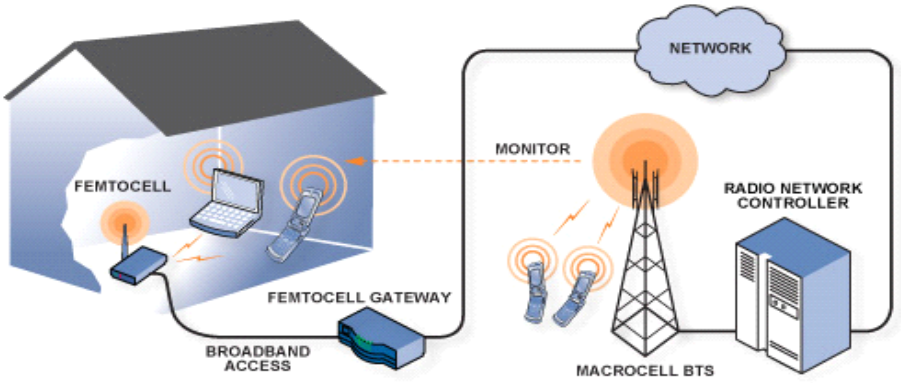
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Ψηφιακών Συστημάτων

Διπλωματική Εργασία

Αξιολόγηση Ασφάλειας 3GPP LTE - Femtocell Home evolved Node B - (HeNB)



Ονοματεπώνυμο: Μαρμαράς Γεώργιος

Επιβλέπων: Κ. Ξενάκης Χρήστος, Επίκουρος Καθηγητής

ΠΕΙΡΑΙΑΣ, ΜΑΙΟΣ 2014

Περίληψη

Η ασφάλεια των κινητών επικοινωνιών στα πρώτα της βήματα δεν ήταν κάτι που απασχολούσε άμεσα τους παρόχους, καθώς το κόστος ήταν μεγάλο και η οποιαδήποτε κακόβουλη ενέργεια θεωρούταν δύσκολη στα ιδιόκτητα δίκτυα φωνής. Αυτό έχει αλλάξει, τα κινητά δίκτυα γίνονται τα πιο επικρατέστερα δίκτυα δεδομένων, με την σταδιακή κατάργηση των ιεραρχικών αρχιτεκτονικών και στην σύγκληση της αρχιτεκτονικής IP, με την χρήση εξελιγμένων τεχνολογικά προτύπων όπως το LTE και LTE/Advanced. Η σύγκληση αυτή παράλληλα με την διείσδυση των "έξυπνων" μικροσυσκευών στην αγορά των κινητών επικοινωνιών, είχαν ως συνέπεια την αλματώδη ανάπτυξη κακόβουλου λογισμικού και επιθέσεων έναντι στα ευπαθή σημεία των δικτύων με σκοπό την υποκλοπή συνομιλιών, την παρεμπόδιση των επικοινωνιών την τροποποίηση διαπιστευτηρίων αλλά και άλλων τύπων επιθέσεων.

Το ενδιαφέρον της παρούσας διπλωματικής εργασίας, εστιάζεται στις αδυναμίες και ευπάθειες που εντοπίζονται στην αρχιτεκτονική ασφάλειας της LTE Φεμτοκυψέλης. Αναφερόμαστε δηλαδή στο κομμάτι εκείνο της αρχιτεκτονικής που χαρακτηρίζεται μη έμπιστο και είναι εκτεθειμένο σε απειλές ή συνδυασμός απειλών. Σκοπός είναι να εντοπιστούν οι ευπάθειες/απειλές, αλλά και οι διαδικασίες που αποτελούν τα αντίμετρα για την αντιμετώπιση και προστασία από αυτές. Ακόμα γίνεται μια προσπάθεια ώστε να ομαδοποιηθούν οι πιθανές απειλές, να χαρακτηριστούν σε σχέση με την επικινδυνότητα τους και να προταθούν ειδικοί τρόποι αντιμετώπισης τους.

Η δομή της εργασίας διαμορφώνεται ως εξής:
Στο κεφάλαιο ένα γίνεται μια εισαγωγική χρονική προσέγγιση στα κινητά δίκτυα από τη πρώτη γενιά κινητών επικοινωνιών (1G), μέχρι και τη σημερινή εποχή που διανύουμε, με την εξέλιξη της τέταρτης γενιάς κινητών επικοινωνιών (4G) να είναι στο τεχνολογικό προσκήνιο. Σημαντικό ιστορικά πρότυπο είναι το GSM (Δεύτερης γενιάς - 2G) το οποίο στιγμάτισε και αποτέλεσε την αρχή της τόσο διαδεδομένης ανάπτυξης των κινητών τηλεπικοινωνιών. Τα σκήπτρα της δεύτερης γενιάς παίρνει το πρότυπο UMTS (Τρίτης γενιάς - 3G) όπου νέες δυνατότητες προστέθηκαν

βελτιώνοντας τα ήδη υπάρχοντα δίκτυα. Αποτέλεσε βάση για το πρότυπο στο οποίο βασίζεται η παρούσα εργασία και είναι το LTE (Long Term Evolution).

Γίνεται μια αναφορά στα βασικά χαρακτηριστικά σημεία της ασφάλειας των προγενέστερων τεχνολογιών GSM, UMTS, εμμένοντας στις αδυναμίες που έπρεπε να αντιμετωπιστούν αλλά και στα δυνατά σημεία που συνέχισαν την λειτουργία τους και στο LTE. Τέλος επισημαίνεται πόσο απαραίτητη και επιτακτική είναι η ανάγκη για την ασφάλεια των δικτύων τόσο από την πλευρά των παρόχων και των υπηρεσιών που αυτοί προσφέρουν, όσο και από την πλευρά των πελατών/χρηστών.

Στο κεφάλαιο δύο γίνεται μια αναφορά στο πρότυπο LTE – (Long Term Evolution), με έμφαση στην αρχιτεκτονική ασφάλειας του. Εντοπίζονται τα σημαντικότερα στοιχεία του συστήματος (κορμού και πρόσβασης) και εξετάζονται από την σκοπιά της ασφάλειας, που είναι πιο επιτακτική ανάγκη από κάθε άλλη φορά στο παρελθόν λόγο των μεγάλων απαιτήσεων της αγοράς και των συνδρομητών για νέες υπηρεσίες.

Το τρίτο κεφάλαιο αναφέρεται στον όρο της φεμτοκυψέλης (Femtocell), στους λόγους που γίνεται πόλος έλξης για όλο και περισσότερους παρόχους, ποια είναι τα πλεονεκτήματα αλλά και οι δυσκολίες που αντιμετωπίζονται στην χρήση τους και γιατί είναι απαραίτητη η ξεχωριστή μελέτη των θεμάτων ασφάλειας που προκύπτουν. Τέλος, γίνεται μια αναφορά στις βασικές αρχές της ασφάλειας και των μεθόδων αντιμετώπισης των απειλών που παρουσιάζονται σε μια φεμτοκυψέλη, αλλά και ένας διαχωρισμός των αρχιτεκτονικών ασφάλειας του 3G UMTS Femtocell και του LTE Femtocell.

Το τέταρτο κεφάλαιο εστιάζει εκτενώς στην αρχιτεκτονική ασφάλειας της LTE φεμτοκυψέλης, καλύπτοντας όλες τις οντότητες που συμμετέχουν με σκοπό την ανάδειξη των μη έμπιστων στοιχείων, δηλαδή τα ευπαθή μέρη τα οποία κάποιος μπορεί να εκμεταλλευτεί και να ωφεληθεί ανάλογα. Περιγράφονται τα χαρακτηριστικά, οι διαδικασίες και οι μηχανισμοί ασφάλειας αλλά και οι απαιτήσεις που είναι ποικίλες, γι’ αυτό και καταγράφονται σε κατηγορίες.

Το πέμπτο κεφάλαιο εστιάζει με μεγαλύτερη λεπτομέρεια στις απειλές ενάντια στο HeNB, ενώ παράλληλα αξιολογείται η επικινδυνότητα τους στο δίκτυο από την πλευρά του παρόχου, αλλά και του χρήστη.

Θεματική Περιοχή: Ασφάλεια στο 3GPP LTE - Femtocell.

Λέξεις Κλειδιά: Φεμτοκυψέλη, LTE, EPS, SAE, EPC, HeNB, GSM, UMTS, Αρχιτεκτονική Ασφάλειας, Μηχανισμοί Ασφάλειας.

Abstract

The safety of mobile communications in its infancy was not something that directly employed providers, the cost was great and any malicious action be considered difficult on proprietary voice networks. This has changed, the mobile networks are becoming the most dominant data networks, with the gradual elimination of hierarchical architectures and the convening of the IP architecture, using sophisticated technological standards such as LTE and LTE-Advanced. The convening of this alongside the penetration of "smart" widgets on the mobile communications market, have led to the rapid growth of malware and attacks against vulnerabilities of networks with a view to tapping conversations, preventing credential modification but communications and other types of attacks.

The interest of this thesis focuses on weaknesses and vulnerabilities identified in the security architecture of LTE Femtocells. Talking about the piece of architecture that is untrustworthy and is exposed to threats or combination of threats. The aim is to identify threats/vulnerabilities, but also the processes which form the countermeasures for treating and protecting against them. Even an attempt to group the potential threats, be classified in relation to their risk and to propose specific ways to tackle them.

The structure of the work is as follows:
In chapter one becomes an introductory time approach to mobile networks from the first generation (1G) mobile communications, up to the present time, with the development of the fourth generation (4G) mobile communications to be at the technological forefront. Important historical model is GSM (second generation-2G) which marked the beginning of the widespread development of mobile telecommunications. The scepters of second generation takes the UMTS (third generation-3G) where new features were added by improving existing networks. Formed the basis for the template on which this paper is based and is LTE (Long Term Evolution).

Makes a reference to the basic features of earlier points of technologies GSM, UMTS, insisting on weaknesses that needed to be addressed but also the advantages that have continued their operation and in LTE. End note how necessary and urgent is the need for network security both on the part of providers and the services they offer, as well as from the side of customers/users.

In chapter two it becomes a reference to standard LTE – (Long Term Evolution), with emphasis on the security architecture. Identify the major components of the system (trunk and access) and examined from the standpoint of security.

The third chapter refers to the condition of Femtocell, on the grounds that becomes an attraction for more and more providers, what are the advantages and the difficulties encountered in using them and why it is necessary to separate study of safety issues that arise. Finally, there is a reference to the basic principles of security and methods of dealing with threats presented in a Femtocell, and a separation of the 3G UMTS security architectures Femtocell and LTE Femtocell.

The fourth chapter focuses extensively on security architecture of LTE Femtocell, covering all entities involved in the emergence of non-trusted data, i.e. the affected parties that anyone can take advantage and benefit accordingly. Describes the characteristics, processes and security mechanisms and requirements.

The fifth chapter focuses in greater detail on threats against HeNB, while assessing the danger posed by the network from the perspective of the provider, and the user.

Thematic Area: Safety in 3GPP LTE-Femtocell.

Keywords: Femtocell, LTE, EPS, SAE, EPC, GSM, UMTS, HeNB, Security Architecture, Security Mechanisms.

Ευχαριστίες

Θερμές ευχαριστίες προς τον επιβλέποντα Επίκουρο Καθηγητή κύριο Χρήστο Ξενάκη, για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα αντικείμενο μελέτης που πραγματικά με ενδιαφέρει, αλλά και τόσο τεχνολογικά επίκαιρο και εξελισσόμενο τομέα στον χώρο των τηλεπικοινωνιών.

Περιεχόμενα

Περίληψη III

Abstract V

Ευχαριστίες VII

Περιεχόμενα VIII

Κατάλογος Εικόνων X

Κατάλογος Πινάκων IXX

Εξέλιξη Ασφάλειας Κινητών Επικοινωνιών 1

1.1 Εξέλιξη προτύπων κινητών επικοινωνιών 2

1.1.1 Γενιές πριν την Εξέλιξη του LTE 2

1.2 Ασφάλεια στο AMPS - (1G) 9

1.3 Βασικά Στοιχεία Ασφάλειας του GSM - (2G) 10

1.3.1 Αυθεντικοποίηση Συνδρομητή στο GSM 12

1.3.2 Κρυπτογράφηση στο GSM 13

1.3.3 Εμπιστευτικότητα της ταυτότητας του συνδρομητή στο GSM 14

1.4 Βασικά Στοιχεία Ασφάλειας του UMTS - (3G) 14

1.4.1 Αμοιβαία αυθεντικοποίηση και συμφωνία κλειδιών (authentication and key agreement) στο UMTS 17

1.4.2 Κρυπτογράφηση στο UMTS 18

1.4.3 Προστασία Ακεραιότητας στο UMTS 19

1.4.4 Εμπιστευτικότητα Ταυτότητας Χρηστών στο UMTS 20

1.4.5 Αλγόριθμοι Ασφάλειας στα Τρίτης Γενιάς Δίκτυα 20

1.5 Ευπάθειες στο UMTS 21

1.6 Ανάπτυξη Ασφάλειας B3G (Beyond 3G) - Πρότυπο LTE 22

Αρχιτεκτονική Ασφάλειας στο LTE 24

2.1 Εισαγωγή στο Σύστημα LTE 25

2.1.1 Δίκτυο πρόσβασης (Access Network) 26

2.1.2 Δίκτυο Κορμού (Core Network) 27

2.2 Αρχιτεκτονική Ασφάλειας EPS (LTE/SAE) 28

2.3 Απειλές και Επιθέσεις στο EPS 32

Ασφάλεια Φεμτοκυψελών 34

3.1 Ορισμός φεμτοκυψέλης 35
3.2 Λειτουργίες φεμτοκυψέλης 36
3.2.1 Πολιτικές Πρόσβασης 37
3.3 Πλεονεκτήματα Φεμτοκυψέλης από τη πλευρά των χρηστών 38
3.4 Πλεονεκτήματα Φεμτοκυψέλης από τη πλευρά των παρόχων 40
3.4.1 Self Organizing Network 40
3.4.2 Γεωγραφικό Στίγμα Φεμτοκυψέλης 41
3.5 Μειονεκτήματα και Τεχνικές Δυσκολίες Φεμτοκυψέλης 43
3.6 Αρχιτεκτονικές Ασφάλειας Φεμτοκυψελών 45
3.6.1 2G Femtocells - GSM 48
3.6.2 3G Femtocells - UMTS 49
3.6.3 LTE Femtocells 51
3.7 Γενικές Αρχές Ασφάλειας στα Femtocells και Επιθέσεις 52
Αρχιτεκτονική Ασφάλειας H(e)NB 63
4.1 Αρχιτεκτονική Ασφάλειας H(e)NB 64
4.2 Στοιχεία H(e)NB Αρχιτεκτονικής 64
4.3 Ευπάθειες στο H(e)NB 69
4.4 Απαιτήσεις Ασφάλειας 72
4.5 Χαρακτηριστικά και Διαδικασίες Ασφάλειας 73
4.5.1 Τοπική & Φυσική Ασφάλεια - (Local & Physical Security) 73
4.5.2 Διαδικασίες Ασφάλειας του HeNB και του SeGW 75
4.5.3 Διαδικασίες Ασφάλειας του HeNB και του HeMS 80
4.5.4 Διαδικασίες Ασφαλείας Άμεσης Διασύνδεσης μεταξύ HeNBs 83
Απειλές ενάντια στο H(e)NB και η Επικινδυνότητα τους 84
5.1 Κατηγοριοποίηση Απειλών 85
5.2 Περιγραφή και Επικινδυνότητα Απειλών 87
Επίλογος - Συμπεράσματα 105
Παράρτημα - Ακρώνυμα 113

Κατάλογος Εικόνων

ΚΕΦΑΛΑΙΟ 1

Εικόνα 1.1: Παγκόσμια εκτίμηση συνδρομητών το 2013 και εκτίμηση το 2018 [3]. 1
Εικόνα 1.2: Η εξέλιξη των κινητών επικοινωνιών από τα 1G στα 4G συστήματα....2
Εικόνα 1.3: Χρονική εξέλιξη LTE και LTE Advanced προτύπων. 8
Εικόνα 1.4: Διαδικασία Αυθεντικοποίησης στο GSM.....12
Εικόνα 1.5: Διαδικασία κρυπτογράφησης στο GSM. 13
Εικόνα 1.6: Αρχιτεκτονική ασφάλειας UMTS. 16
Εικόνα 1.7: Διαδικασίες Ασφάλειας στο UMTS. 16
Εικόνα 1.8: Διαδικασία αυθεντικοποίησης στο UMTS. 18
Εικόνα 1.9: Διαδικασία κρυπτογράφησης στο UMTS.....19
Εικόνα 1.10: Διαδικασία ακεραιότητας στο UMTS. 20
Εικόνα 1.11: Αλγόριθμος KASUMI. 22
Εικόνα 1.12: Εξέλιξη των αρχιτεκτονικών ασφάλειας. 23

ΚΕΦΑΛΑΙΟ 2

Εικόνα 2.1: 3GPP Οργανισμοί στο Παγκόσμιο Χάρτη. 25
Εικόνα 2.2: Αρχιτεκτονική LTE. 26
Εικόνα 2.3: Αρχιτεκτονική ασφάλειας του EPS. 28
Εικόνα 2.4: Πρωτόκολλα δεδομένων σηματοδοσίας EPS. 30
Εικόνα 2.5: Πρωτόκολλα δεδομένων χρήστη EPS. 30
Εικόνα 2.6: EPS Key hierarchy.....31
Εικόνα 2.7: EPS authentication and key agreement (AKA). 32

ΚΕΦΑΛΑΙΟ 3

Εικόνα 3.1: Κλίμακα Φεμτοκυψέλης.....35
Εικόνα 3.2: Πολιτικές πρόσβασης Femtocells, (a) Closed (b) Open (c) Hybrid. 38
Εικόνα 3.3: Self Organizing Network.....41
Εικόνα 3.4: GPS Jammer. 43
Εικόνα 3.5: Σημεία αναφοράς ενός Femtocell όπως ορίζεται από το Femto Forum. 45
Εικόνα 3.6: Αρχιτεκτονική ασφάλειας Femtocell [4]. 47
Εικόνα 3.7: Αρχιτεκτονική UMTS Femtocell Network.....51
Εικόνα 3.8: Δίκτυο LTE Femtocell.....52
Εικόνα 3.9: Τρόποι προσέγγισης μιας φεμτοκυψέλης από επιτιθέμενους [13]. 53
Εικόνα 3.10: Χρήση του IPsec σε ένα δίκτυο IP. 59

ΚΕΦΑΛΑΙΟ 4

Εικόνα 4.1: Αρχιτεκτονική HeNB [12]. 64
Εικόνα 4.2: Λειτουργία (LIPA) - Local Internet Protocol Access. 65
Εικόνα 4.3: Στοιχεία αρχιτεκτονικής ασφάλειας HeNB. 68
Εικόνα 4.4: Διαδικασία αυθεντικοποίησης με χρήση διαπιστευτηρίων [1]. 77
Εικόνα 4.5: EAP-AKA αυθεντικοποίηση συσκευής και EAP-AKA HP. 78
Εικόνα 4.6: Αρχιτεκτονική Διαχείρισης HeMS [46]. 81
Εικόνα 4.7: Initial HeMS και Serving HeMS. 82

Κατάλογος Πινάκων

ΚΕΦΑΛΑΙΟ 1

Πίνακας 1.1: Πρώτης γενιάς πρότυπα.....4
Πίνακας 1.2: Δεύτερης γενιάς πρότυπα. 5
Πίνακας 1.3: 2.5 γενιάς πρότυπα. 6
Πίνακας 1.4: Τρίτης γενιάς πρότυπα.....7
Πίνακας 1.5: Διαφορές Χαρακτηριστικών LTE & LTE-Advanced.....9
Πίνακας 1.6: Βελτιώσεις στοιχείων ασφάλειας από το GSM στο UMTS. 15

ΚΕΦΑΛΑΙΟ 2

Πίνακας 2.1: Απειλές στο EPS.....33

ΚΕΦΑΛΑΙΟ 3

Πίνακας 3.1: Διαφορές Φεμτοκυψέλης - Μακροκυψέλης. 36
Πίνακας 3.2: Σύγκριση ανοιχτού και κλειστού τύπου πρόσβασης [42].....44
Πίνακας 3.3: Αντιστοιχίες ορολογίας ανάμεσα στο πρότυπο του Femto Forum και των UMTS, LTE. 50
Πίνακας 3.4: Τρόποι αυθεντικοποίησης χρήστη.....61

ΚΕΦΑΛΑΙΟ 4

Πίνακας 4.1: Κατηγορίες Επιθέσεων (Ομαδοποίηση). 70
Πίνακας 4.2: Συνδυασμοί Αυθεντικοποίησης.....79

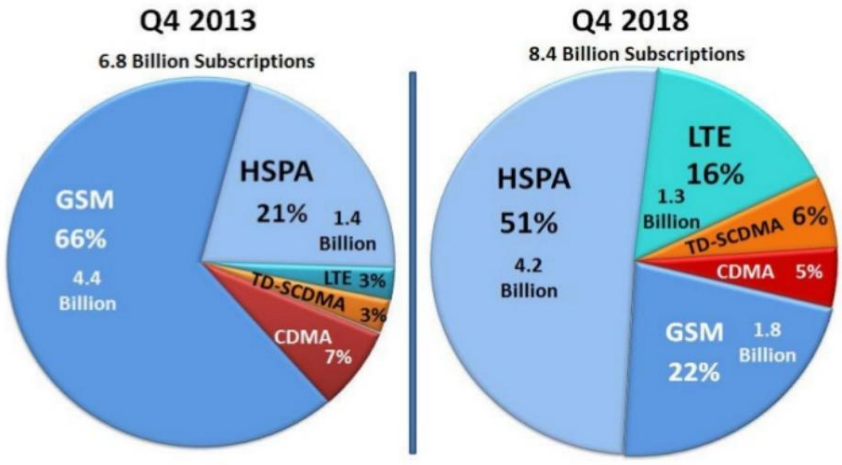
ΚΕΦΑΛΑΙΟ 5

Πίνακας 5.1: Λίστα απειλών στο HeNB. 85
Πίνακας 5.2: Στοιχεία που επηρεάζονται ανά απειλή [4]. 103
Πίνακας 5.3: Πιθανότητα & Επικινδυνότητα Απειλών [4].....104

ΚΕΦΑΛΑΙΟ

Εξέλιξη Ασφάλειας Κινητών Επικοινωνιών 1

Οι ασύρματες κινητές επικοινωνίες αναπτύσσονται συνεχώς και η ανάγκη για μεγαλύτερους ρυθμούς μετάδοσης δεδομένων είναι επιτακτική. Όσο αναπτύσσονται όμως τα δίκτυα και η κίνηση σε αυτά τόσο πιο δύσκολο είναι και να προστατευτούν. Η στροφή προς τα IP κινητά δίκτυα σε συνδυασμό με την τεχνολογικά εξελισσόμενη αγορά των "έξυπνων" μικροσυσκευών (smartphones, tablets, netbooks) με προχωρημένες δυνατότητες, έχουν αλλάξει τον τρόπο με τον οποίο αντιμετωπίζουμε την ασφάλεια, δίνοντας της την απαιτούμενη προτεραιότητα, με μεγαλύτερες απαιτήσεις να εμφανίζονται στην σχεδίαση των αρχιτεκτονικών ασφάλειας των προτύπων που χρησιμοποιούνται.

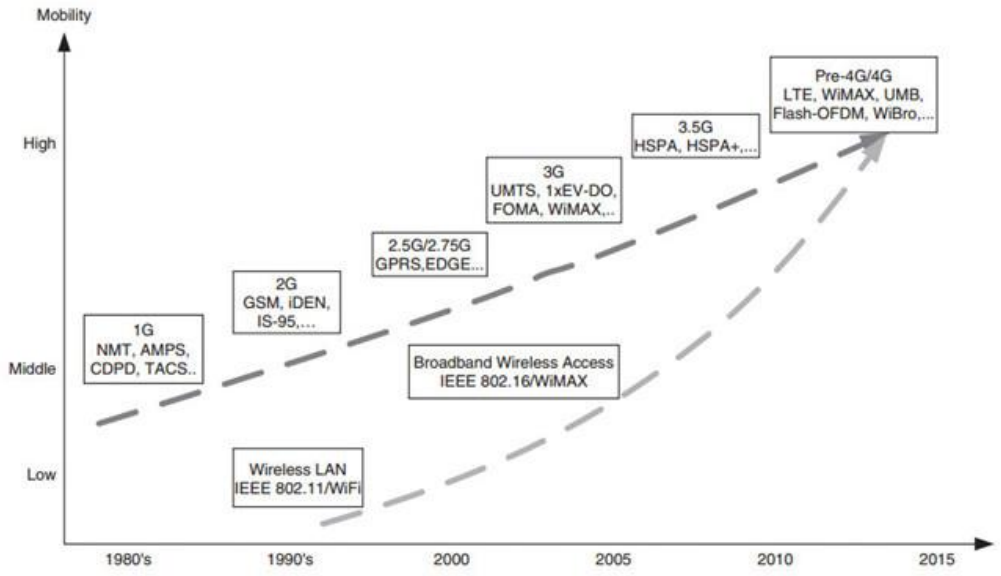


Εικόνα 1.1: Παγκόσμια καταγραφή συνδρομητών ανά τεχνολογία πρόσβασης το έτος 2013 και εκτίμηση το έτος 2018 [3].

Οι συνδρομητές των κινητών επικοινωνιών ολοένα και αυξάνονται (Εικόνα 1.1), απαιτώντας γρήγορες υπηρεσίες, αξιόπιστες και ασφαλείς. Το αίσθημα αυτό της ασφάλειας από τους χρήστες είναι καθοριστικός παράγοντας για τη συνέχιση των συμβολαίων που έχουν με τους παρόχους, κάτι που οι πάροχοι δείχνουν να γνωρίζουν καλά, ειδικά όταν πρόκειται για εταιρικά συμβόλαια στον επιχειρησιακό τομέα.

1.1 Εξέλιξη προτύπων κινητών επικοινωνιών

Η πορεία των δικτύων κινητής επικοινωνίας ξεκινά χρονολογικά τη δεκαετία του 1980. Κάθε δεκαετία χαρακτηρίζεται από μια νέα τεχνολογία που φέρνει αλλαγές στις υπάρχουσες υποδομές, η ακόμα και αντικατάσταση με τη πλήρη αναβάθμιση των προτύπων (Εικόνα 1.2).



Εικόνα 1.2: Η εξέλιξη των κινητών επικοινωνιών από τα 1G στα 4G συστήματα.

1.1.1 Γενιές πριν την Εξέλιξη του LTE

Πρώτη Γενιά Δικτύων - 1G Networks

Η εμφάνιση των πρώτων κυψελωτών συστημάτων έγιναν στην Βόρεια Αμερική, την Ευρώπη και την Ιαπωνία το 1980 με τη χρήση αναλογικών τεχνικών μετάδοσης.

Κάποια από τα πρότυπα που χρησιμοποιήθηκαν είναι τα επόμενα [48]:

- Advanced Mobile Phone Service (AMPS)
- Total Access Communication System (TACS)
- Nordic Mobile Telephone (NMT)
- European Total Access Communication System (ETACS)
- US Digital Cellular Standard IS-54 (USDC)
- Nippon Telegraph (NTT)
- Radio Telefono Mobile Intergrato (RTMI)

Ήταν συστήματα που υποστήριζαν μόνο υπηρεσίες φωνής, βασισμένα σε αναλογική διαμόρφωση FM. Οι δυνατότητες τους ήταν περιορισμένες, με μικρή χωρητικότητα και χωρίς τη δυνατότητα μεταπομπών (Handover) από μια κυψέλη σε κάποια γειτονική, με αποτέλεσμα τη διακοπή των κλήσεων και την παρεμπόδιση της κινητικότητας των χρηστών. Χαμηλός ρυθμός μετάδοσης, μικρή υποστηρικτική ικανότητα χρηστών και κακή ποιότητα φωνής, ογκώδεις κεραίες χωρίς τη δυνατότητα πολλών βελτιώσεων, η χρησιμοποίηση FDMA (Frequency Division Multiple Access) ήταν τα χαρακτηριστικά τους.

Κάποια από τα πρότυπα αυτά καθώς και τα χαρακτηριστικά τους παρουσιάζονται στον παρακάτω πίνακα (Πίνακας 1.1):

Πρότυπο	**AMPS**	**NMT 450**	**NMT 900**	**ETACS**	**NTACS**
Περιοχή	ΗΠΑ	Φινλανδία, Σουηδία, Δανία, Νορβηγία	Φινλανδία, Σουηδία, Δανία, Νορβηγία	Μ. Βρετανία	Μ. Βρετανία
Φάσμα Συχνοτήτων MHz	Tx 824-849 Rx 869-894	Tx 453-458 Rx 463-468	Tx 890-915 Rx 935-960	Tx 871-904 Rx 916-949	Tx 915-925 Rx 860-870
Εύρος ζώνης καναλιού KHz	30	25	12,5	25	12,5
Αριθμός καναλιών	666/832	200	1999	1000	400
Μέθοδος Πολυπλεξίας	FDMA	FDMA	FDMA	FDMA	FDMA

Duplex	FDD	FDD	FDD	FDD	FDD
Μέθοδος διαμόρφωσης	FM	FM	FM	FM	FM

Πίνακας 1.1: Πρώτης γενιάς πρότυπα.

Δεύτερη Γενιά Δικτύων - 2G Networks

Η μεταπήδηση στα δίκτυα Δεύτερης Γενιάς στις αρχές της δεκαετίας του 1990, συνδυάστηκε με την εισαγωγή ψηφιακών τεχνικών. Οι χρήστες μπορούν να χρησιμοποιούν το ίδιο κανάλι αφού αυτό διαιρείται είτε με διαίρεση χρόνου TDMA (Time Division Multiple Access), είτε με διαίρεση κώδικα CDMA (Code Division Multiple Access).

Τα πιο γνωστά 2G συστήματα που δημιουργήθηκαν είναι τα εξής:

- Global System for Mobile communications (GSM)
- Code Division Multiple Access IS-95 (CDMA)
- Personal Digital Cellular (PDC)
- Digital AMPS (D-AMPS)

Το πρότυπο που γνώρισε τη μεγαλύτερη απήχηση είναι το GSM, το οποίο ακόμα και στις μέρες μας χρησιμοποιείται σε παγκόσμιο επίπεδο. Οι λόγοι που το κατέστησαν τόσο δημοφιλές, είναι κυρίως η εξυπηρέτηση πολλών χρηστών σε σχέση με τα προγενέστερα συστήματα και η δυνατότητα αποστολής και λήψης μηνυμάτων (SMS, Short Message Service) αλλά και δεδομένων. Ακόμα, δυνατότητες όπως η περιαγωγή, η δυνατότητα κινητικότητας των χρηστών χωρίς να διακόπτεται η επικοινωνία, η βελτιωμένη ποιότητα μετάδοσης, και η μεγαλύτερη κάλυψη της κυψελωτής τεχνολογίας είχαν ως επακόλουθο την αύξηση της χωρητικότητας του συστήματος. Οι κινητές συσκευές με τη σειρά τους έγιναν μικρότερες, με μικρότερη κατανάλωση ισχύος και παράλληλα μεγαλύτερη διάρκεια μπαταρίας οδηγούμενες προς την κατασκευή μικρών εφαρμογών αλλά και τη δυνατότητα για λήψη πολυμεσικού περιεχομένου. Την ανάπτυξη εφαρμογών μέσω Internet βοήθησε το πρωτόκολλο Wireless Applications Protocol (WAP).

Για τη συνέχιση της λειτουργίας του GSM στην μετέπειτα εποχή τρία συστήματα σχεδιάστηκαν, το (General Packet Radio Services - GPRS) σύστημα που επιτρέπει την μεταγωγή πακέτων, το (Enhanced Data Rates for Global Evolution - EDGE) και το (High-Speed Circuit-Switched Data - HSCSD) συστήματα που επιτρέπουν μεγαλύτερους ρυθμούς μετάδοσης. Η περίοδος αυτή ονομάστηκε 2.5G, δηλαδή εποχή ανάμεσα στα 2G συστήματα και στην εξέλιξη της τρίτης γενιάς κινητών επικοινωνιών. Πρόκειται για αναβαθμίσεις προς την κατεύθυνση των απαιτήσεων που συναντώνται στα 3G συστήματα.

Κάποια από τα πρότυπα αυτά καθώς και τα χαρακτηριστικά τους παρουσιάζονται στους παρακάτω πίνακες (Πίνακες 1.2, 1.3):

Πρότυπο	GSM	GSM 1800	GSM 1900	E_GSM 900
Φάσμα Συχνοτήτων MHz	890-915 935-960	1710-1785 1805-1880	1850-1910 1930-1990	880-915 925-960
Εύρος ζώνης καναλιού KHz	200	200	200	200
Αριθμός καναλιών	125 ανά κατεύθυνση	375 ανά κατεύθυνση	300 ανά κατεύθυνση	175 ανά κατεύθυνση
Μέθοδος Πολυπλεξίας	TDMA	TDMA	TDMA	TDMA
Μέθοδος διαμόρφωσης	GMSK	GMSK	GMSK	GMSK
Duplex	FDD	FDD	FDD	FDD

Πίνακας 1.2: Δεύτερης γενιάς πρότυπα.

	HSCSD	GPRS	IS-95B	EDGE
Year Introduced	1999	1999	1999	1999
Location	Europe	Europe	N. America	Europe
Modulation	GMSK	GMSK	QPSK	8-PSK
Multiple Access	TDMA	TDMA	CDMA	TDMA
Duplex	FDD	FDD	FDD	FDD
Forward channel (uplink) range	935-960 MHz	935-960 MHz	1930-1990 MHz	935-960 MHz
Reverse channel (downlink) range	890-915 MHz	890-915 MHz	1850-1910 MHz	890-915 MHz
Channel Bandwidth	200 KHz	200 KHz	1250 KHz	200 KHz

Channel Separation	45 MHz	45 MHz	n/a	45 MHz
Number of Channels	124	124	n/a	124

Πίνακας 1.3: 2.5 γενιάς πρότυπα.

Τρίτη Γενιά Δικτύων - 3G Networks

Πρόκειται για τις τεχνολογίες προς τη μετάβαση στα δίκτυα τέταρτης γενιάς και τη σημερινή εποχή όπου τα κινητά δίκτυα είναι τα επικρατέστερα είτε μιλάμε για υπηρεσίες φωνής, είτε για υπηρεσίες δεδομένων.

Τα πρότυπα που επικράτησαν στην τρίτη γενιάς δίκτυα είναι τα επόμενα:

- Universal Mobile Telecommunication System (UMTS)
- Code Division Multiple Access (CDMA2000)
- NTT Docomo
- Time Division-Synchronous Code Division Multiple Access (TD-SCDMA)
- Digital Enhanced Cordless Telecommunications (DECT)
- Worldwide Interoperability for Microwave Access (WiMAX)

Τα χαρακτηριστικά των 3G συστημάτων είχαν ως γνώμονα την πλήρη κινητικότητα του χρήστη και παροχή υπηρεσιών παντού, παγκόσμια περιαγωγή, την πρόσβαση στο Internet, την δυνατότητα πολυμέσων όπως και της τηλεδιάσκεψης, κοινές εφαρμογές (fax, e-mail), αλλά και χάρτες πλοήγησης, διαδραστικές εφαρμογές, υψηλής ποιότητας κλήσεων, αυξημένες ταχύτητες μετάδοσης δεδομένων, αυξημένη χωρητικότητα, χρησιμοποίηση του Voice over Internet Protocol (VoIP) και η υποστήριξη QoS, καθώς και η συμβατότητα με υπάρχοντα 2G συστήματα.
Η βελτίωση των 3G συστημάτων άρχισε να γίνεται όταν χρησιμοποιήθηκε για πρώτη φορά η τεχνολογία High Speed Packet Access (HSPA), βελτιωμένο πρότυπο του UMTS. Αυτή η εποχή ονομάστηκε 3.5G. Τεχνολογίες που συνέβαλλαν στα αληθινά χαρακτηριστικά των 3G συστημάτων και έδωσαν τη δυνατότητα στους χρήστες να απολαμβάνουν υπηρεσίες που μέχρι τότε μόνο μια ενσύρματη ευρυζωνική σύνδεση τους παρήχε, είναι τα High Speed Downlink Packet Access (HSDPA) και High Speed Uplink Packet Access (HSUPA), που είχαν ως σκοπό την αύξηση της χωρητικότητας

στο Downlink και το Uplink αντίστοιχα. Το HSPA μπορεί να λειτουργεί παράλληλα με το κλασικό UMTS και χαρακτηρίζεται από πολύ υψηλούς ρυθμούς μετάδοσης, μεγάλες ταχύτητες στον τελικό χρήστη και υψηλή χωρητικότητα.
Περαιτέρω βελτιώσεις στο πρότυπο υλοποιούνται κάτω από την ονομασία (HSPA+) με σημαντικό στοιχείο τη χρησιμοποίηση πολλαπλών κεραιών MIMO (Multiple Input Multiple Output) [48].

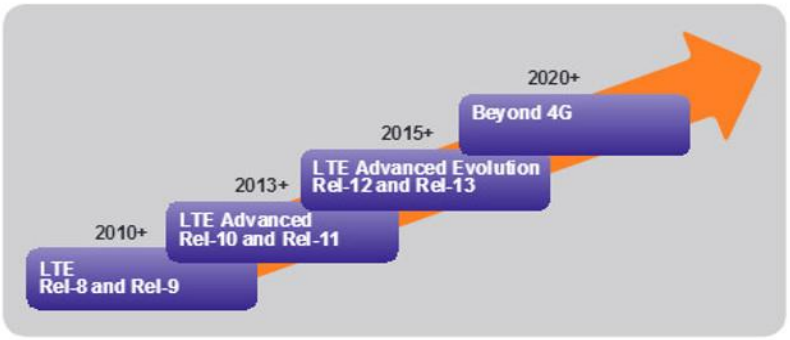
Κάποια από τα πρότυπα αυτά καθώς και τα χαρακτηριστικά τους παρουσιάζονται στον παρακάτω πίνακα (Πίνακας 1.4):

Πρότυπο	**EDGE**	**CDMA2000**	**UMTS W-CDMA**	**UMTS TD-CDMA**	**UMTS TD-STDMA**	**DECT**
Περιοχή Κάλυψης	Παγκόσμια εκτός της Ιαπωνίας και Ν. Κορέας	Αμερική, Ασία	Παγκόσμια	Ευρώπη	Κίνα	Ευρώπη, ΗΠΑ
Bandwidth	EDGE Evolution	EV-DO	HSPA	HSPA	HSPA	-
Μέθοδος Πολυπλεξίας	TDMA	CDMA	CDMA	CDMA	CDMA	FDMA/TDMA
Duplex	FDD	FDD	FDD	TDD	TDD	TDD

Πίνακας 1.4: Τρίτης γενιάς πρότυπα.

Τέταρτη Γενιά Δικτύων - 4G Networks

Η τέταρτη γενιά δικτύων διαδραματίζεται στις μέρες μας και το πρότυπο που δείχνει να επικρατεί είναι βασισμένο στο LTE, διαμορφωμένο με τις προδιαγραφές που πρέπει να τηρεί ένα 4G δίκτυο, με την ονομασία (LTE–Advanced ή IMT-Advanced). Την εξελικτική αυτή πορεία έχει αναλάβει το 3GPP (3rd Generation Partnership Project) με την δημοσίευση εκθέσεων για τις προδιαγραφές που πρέπει να έχουν οι αντίστοιχες εκδόσεις (Εικόνα 1.3).



Εικόνα 1.3: Χρονική εξέλιξη LTE και LTE Advanced προτύπων.

Το LTE σε σχέση με τις υπάρχουσες τεχνολογίες (GSM, GPRS, EDGE, WCDMA, HSPA), αυξάνει την χωρητικότητα του δικτύου, τον ρυθμό μετάδοσης δεδομένων, ενώ ταυτόχρονα μειώνει τις καθυστερήσεις. Σύμφωνα με τις προδιαγραφές του 3GPP στο Release 8, οι ελάχιστοι ρυθμοί μετάδοσης για το LTE είναι τουλάχιστον 100 Mbps για την κάτω ζεύξη και 50 Mbps για την άνω ζεύξη και η μέγιστη καθυστέρηση με επιστροφή υπολογίζεται στα 10 ms [48]. Στο φυσικό επίπεδο χρησιμοποιείται για το Downlink η μέθοδος ορθογώνιας πολυπλεξίας διαίρεσης συχνότητας (Orthogonal Frequency Division Multiple Access - OFDMA) και στο Uplink η μέθοδος Πολλαπλή Πρόσβαση Διαίρεσης Συχνότητας Μονού Φέροντος (Single Carrier Frequency Division Multiple Access – SC-FDMA). Επίσης υποστηρίζει τις τεχνικές διαμόρφωσης Quadrature Phase Shift Keying (QPSK), 16 Quadrature Amplitude Modulation (16QAM), και 64QAM. 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 στο IP πρωτόκολλο (Internet Protocol).

Άλλα πρότυπα που ανταγωνίζονται για μια θέση στα τέταρτης γενιάς δίκτυα, είναι το Mobile WiMax και το Ulta-Mobile Broadband (UMB).

Προδιαγραφές LTE-Advanced

Η σημαντικότερη τεχνολογικά αλλαγή των 4G δικτύων, είναι ο προσανατολισμός προς τα IP δίκτυα (μεταγωγή πακέτων), η δυνατότητα εναλλαγής από δίκτυα 2^{ης} και 3^{ης} γενιάς όπου επιτρέπεται η απρόσκοπτη και συνεχής μετάβαση από το ένα σύστημα στο άλλο, ενώ όλα τα στοιχεία του δικτύου είναι ψηφιακά.

Οι διαφορές του LTE με το LTE Advanced σημειώνονται στον πίνακα που ακολουθεί (Πίνακας 1.5).

Απόδοση Συστήματος	LTE Advanced	LTE
Μέγιστοι Ρυθμοί Ζεύξης Ανόδου	1000 Mbps στα 10 MHz	100 Mbps στα 20 MHz
Μέγιστοι Ρυθμοί Ζεύξης Καθόδου	500 Mbps στα 100 MHz	50 Mbps στα 20 MHz
Καθυστερήσεις του πλάνου ελέγχου Idle to Connected	< 50 ms	< 100 ms
Καθυστερήσεις του πλάνου ελέγχου Dormant to Active	< 10 ms	< 50 ms
Καθυστερήσεις του πλάνου χρήστη	<<<< 5 ms	< 5 ms
Μέγιστη Αποδοτικότητα φάσματος	Κάθοδος: 30 bps/Hz στα <= 8X8, Άνοδος: 15 bps/Hz στα <= 4X4	Κάθοδος: 5 bps/Hz στα <= 2X2, Άνοδος: 2,5 bps/Hz στα <= 1X2
Μέσος όρος αποδοτικότητας φάσματος	Κάθοδος: 3,7 bps/Hz/κυψέλη στα 4X4, Άνοδος: 2 bps/Hz/ κυψέλη στα 2X4	Κάθοδος: 3 με 4 φορές του HSPA R6 στα 2X2, Άνοδος: 2 με 3 φορές του HSPA R6 στα 1X2
Αποδοτικότητας φάσματος στα άκρα της κυψέλης	Κάθοδος: 0,12 bps/Hz/κυψέλη/χρήστη στα 4X4, Άνοδος: 0,7 bps/Hz/ κυψέλη/χρήστη στα 2X4	Δεν προβλέπεται
Κινητικότητα	<= 350 χλμ/ώρα, <= 500 χλμ/ώρα στη συγκεκριμένη μπάντα φάσματος	<= 350 χλμ/ώρα
Ευκαμψία χρήσης φάσματος	Συνεχές φάσμα > 20 MHz με δυνατότητες σύγκλισης φάσματος (spectral convergence)	1.4, 3, 5, 10, 15, 20 MHz

Πίνακας 1.5: Διαφορές χαρακτηριστικών LTE & LTE-Advanced.

1.2 Ασφάλεια στο AMPS - (1G)

Τα συστήματα κινητών επικοινωνιών της πρώτης γενιάς, χαρακτηρίζονταν από πολλαπλά προβλήματα λειτουργίας όπως και θέματα ασφάλειας. Το AMPS (προηγμένο σύστημα κινητής τηλεφωνίας), ήταν το πρώτο σύστημα που εμφανίστηκε το 1978 και εφαρμόστηκε το 1983 στις Η.Π.Α. Γνώρισε στην εποχή του μεγάλη

εμπορική ανάπτυξη κυρίως στην Αμερική, το Ισραήλ και Αυστραλία. Είχε να αντιμετωπίσει σοβαρά προβλήματα ασφάλειας, όπως το ότι η επικοινωνία δεν προστατευόταν από κάποια κρυπτογράφηση, με αποτέλεσμα να είναι ευάλωτη σε υποκλοπές με την κατοχή μόνο ενός κατάλληλου ραδιοδέκτη. Ένα ακόμα τρωτό σημείο του AMPS, ήταν η αδυναμία του στην κλωνοποίηση κινητών συσκευών, διαδικασία που ο επιτιθέμενος υποδύεται τον νόμιμο κάτοχο της πραγματικής συσκευής με μια τροποποιημένη συσκευή, κάνοντας κλήσεις και χρεώνοντας τον νόμιμο κάτοχο. Ακόμα, τα αναλογικά σήματα μπορούν εύκολα να επηρεάζονται από παρεμβολές, με συνέπεια μειώσεις στην ποιότητα των κλήσεων.

Το AMPS αντικαταστάθηκε αργότερα το 1990 από το D-AMPS (Digital AMPS), σημαίνοντας και το τέλος των αναλογικών προβλημάτων.

1.3 Βασικά Στοιχεία Ασφάλειας του GSM - (2G)

Την διαδοχή της αναλογικής εποχής κατέλαβαν ψηφιακά συστήματα όπως το GSM δεύτερης γενιάς. Στόχος της ασφάλειας του GSM ήταν να μιμηθεί την ασφάλεια των ενσύρματων επικοινωνιών.
Κάποιες από τις εμφανής αδυναμίες του συστήματος είναι οι επόμενες:

- Ενεργές επιθέσεις (Active Attacks), υποδύοντας με κατάλληλο εξοπλισμό κάποιο υπαρκτό στοιχείο του δικτύου (π.χ. Σταθμός βάσης).
- Ευαίσθητα δεδομένα διαχείρισης όπως κλειδιά κρυπτογράφησης, μπορούν να στέλνονται σε διάφορα δίκτυα χωρίς προστασία (Clear Text).
- Ορισμένα μέρη της αρχιτεκτονικής ασφάλειας όπως οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται, δεν ήταν γνωστοί στο ευρύ κοινό με αποτέλεσμα να μην είναι διαθέσιμοι για δοκιμές αντοχής σε νέες απειλές.
- Κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση λόγο του μικρού μήκους τους, είναι σχετικά εύκολο να αποκαλυφτούν με επιθέσεις εξαντλητικής αναζήτησης.
- Δεν παρέχεται ακεραιότητα δεδομένων.
- Έλλειψη ευελιξίας για την βελτίωση και αναβάθμιση της ασφάλειας με το πέρασμα του χρόνου.

- Κρυπτογράφηση σε μερικά δίκτυα δεν χρησιμοποιείται.
- Η κρυπτογράφηση δεν επεκτείνεται αρκετά μακριά από το δίκτυο.
- Το International Mobile Equipment Identity (IMEI) είναι ένα ανασφαλές στοιχείο.

Το μειονέκτημα του GSM ήταν ότι όλες αυτές οι αδυναμίες ήταν γνωστές όταν σχεδιάστηκε, αλλά για λόγους κόστους δεν αποφασίστηκε να βρεθούν τρόποι αντιμετώπισης τους.

Τα σημαντικότερα χαρακτηριστικά ασφάλειας του πιο δημοφιλούς συστήματος στον κόσμο είναι τα ακόλουθα:

- Αυθεντικοποίηση συνδρομητών (Authentication).
- Κρυπτογράφηση της επικοινωνίας (Encryption).
- Χρήση προσωρινών ταυτοτήτων (Temporary Identities).

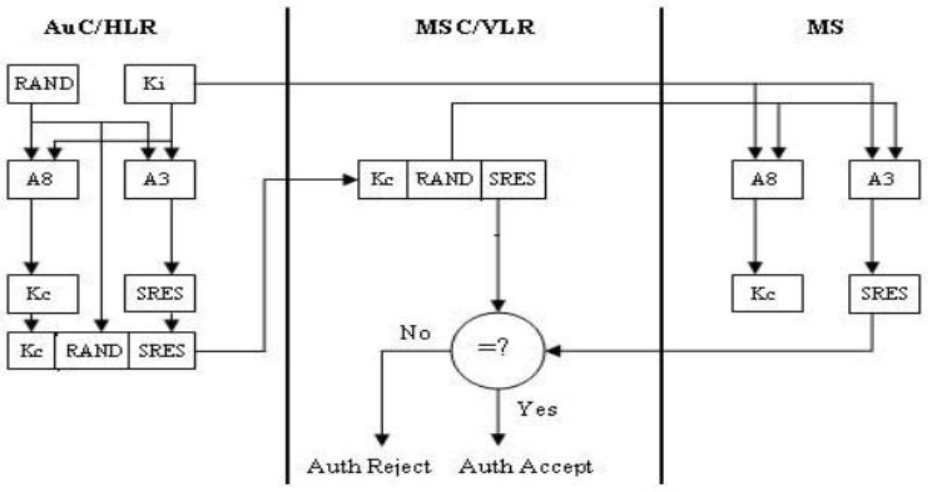
Η καρδιά της ασφάλειας του GSM βασίζεται στη μονάδα ταυτότητας του συνδρομητή Subscriber Identity Module (SIM). Πρόκειται για μια έξυπνη κάρτα η οποία περιέχει την ταυτότητά του συνδρομητή, καθώς και ένα μόνιμο κλειδί Permanent Key (Ki) 128-bit, με το οποίο πραγματοποιείται η διαδικασία της αυθεντικοποίησης. Στις αμέσως επόμενες εκδόσεις η έξυπνη κάρτα ονομάστηκε Universal IC Card (UICC) και η SIM αναφερόταν στο λογισμικό που τρέχει εσωτερικά της κάρτας [26][17]. Η δυσκολία απόσπασης κάποιας χρήσιμης πληροφορίας από την κάρτα, η φορητότητα (ακόμα και η χρησιμοποίηση κάποιας συσκευής από διαφορετική χώρα), η δυνατότητα υποστήριξης διαφορετικών συχνοτήτων, είναι τα χαρακτηριστικά που οδήγησαν στην εμπορική επιτυχία της.
Οι επιθέσεις που γίνονται ενάντια στην SIM κάρτα, απαιτούν την κλωνοποίηση της (Cloning SIM), ή την αντιγραφή της (Lunch-Time Attack) και αν αποκαλυφτεί το μόνιμο κλειδί (Permanent Key - Ki), τότε ο επιτιθέμενος είναι σε θέση να πραγματοποιήσει ελεύθερα κλήσεις. Παρόλο την εφικτή απειλή των παραπάνω επιθέσεων, αν ο επιτιθέμενος προβεί σε επανειλημμένες κλήσεις, τότε είναι εύκολο να ανιχνευτεί η παραβίαση και να απομονωθεί, καθώς μόνο μια συνδρομή μπορεί να υπάρχει για την κάθε SIM κάρτα στο εγγεγραμμένο δίκτυο.

1.3.1 Αυθεντικοποίηση Συνδρομητή στο GSM

Η αυθεντικοποίηση του συνδρομητή γίνεται όταν πιστοποιηθεί ότι ο χρήστης διαθέτει το ίδιο κλειδί με αυτό που είναι αποθηκευμένο στο κέντρο αυθεντικοποίησης (Authentication Centre - AuC). Η διαδικασία έχει ως εξής:

Για να προστατευτεί η επικοινωνία των δύο μερών, του συνδρομητή και του AuC, το σημαντικό στοιχείο που είναι το μόνιμο κλειδί Ki και προϋπάρχει και στις δύο πλευρές, δεν πρέπει να στέλνεται μέσω δικτύου. Το AuC ζητάει από τον συνδρομητή να κάνει έναν υπολογισμό εσωτερικά της SIM, χρησιμοποιώντας τον αλγόριθμο A3 (αλγόριθμος αυθεντικοποίησης) με βάση το κλειδί Ki και έναν τυχαίο 128-bit string αριθμό (RAND) τον οποίο στέλνει το AuC στο συνδρομητή. Το αποτέλεσμα εξάγεται και επιστρέφεται στο AuC με τη μορφή ενός 32-bit μηνύματος απόκρισης (SRES), όπου και ελέγχεται αν ο συνδρομητής είναι έγκυρος η όχι. Το δίκτυο που εξυπηρετεί τη διαδικασία δεν έχει άμεση πρόσβαση στο κλειδί Ki, οπότε το AuC στέλνει τα τρία απαραίτητα στοιχεία (RAND, SRES, Kc) στο Mobile Switching Centre/Visitor Location Register (MSC/VLR) και (SGSN, Serving GPRS Support Node) αντίστοιχα για το GPRS. Τέλος, για να προστατευτεί όλη αυτή η διαδικασία στο δίκτυο, ένα προσωρινό κλειδί δημιουργείται Kc (με παραμέτρους τις τιμές των Ki και RAND), με τη χρήση του αλγορίθμου A8 (αλγόριθμος παραγωγής προσωρινών κλειδιών).

Η εικόνα 1.4 δείχνει τις οντότητες που λαμβάνουν χώρα στην διαδικασία καθώς και τους αλγόριθμους που συμμετέχουν.

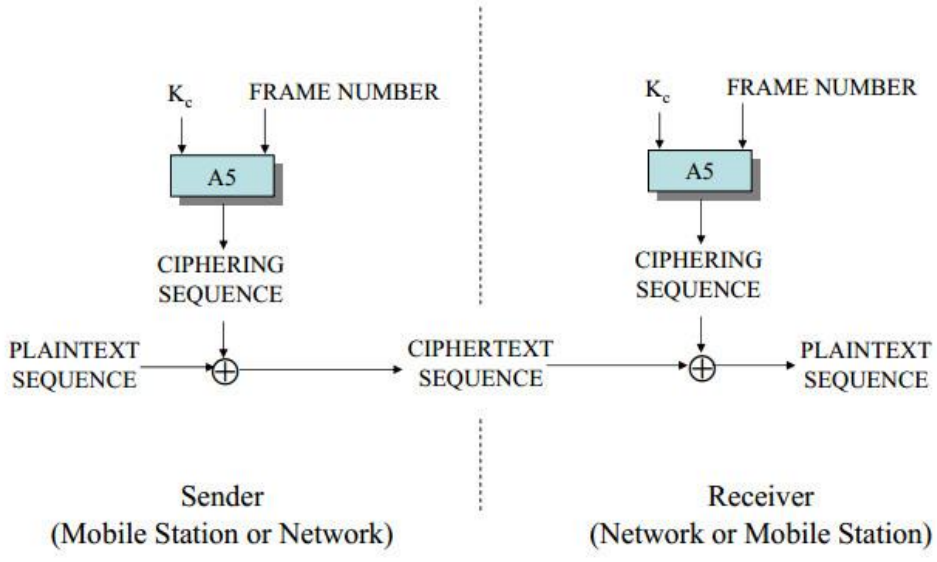


Εικόνα 1.4: Διαδικασία αυθεντικοποίησης στο GSM.

1.3.2 Κρυπτογράφηση στο GSM

Οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται για την κρυπτογράφηση της επικοινωνία ανάμεσα στον χρήστη και το σταθμό βάσης (Base Station), είναι της οικογενείας A5. Το GSM σχεδιάστηκε έτσι ώστε όταν κάποιοι αλγόριθμοι κρίνεται ότι πρέπει να βελτιωθούν ή να αντικατασταθούν με καινούριους, πιο δυναμικούς, αυτό να μπορεί να γίνεται χωρίς να αλλάζει τις υπόλοιπες λειτουργίες ασφάλειας του προτύπου. Για παράδειγμα ο αλγόριθμος A5/2 χρειάστηκε να απομακρυνθεί λόγω αδυναμίας σε μια απειλή όπου ο επιτιθέμενος εκκινούσε την χρήση του A5/2 με το ίδιο κλειδί που ήταν έγκυρο από άλλο A5 αλγόριθμο. Οι A5/1, A5/2, A5/3 υλοποιούνται για 64-bit κλειδιά, ενώ ο A5/4 υλοποιείται για 128-bit κλειδιά. Η δήλωση A5/0 δηλώνει πως δεν χρησιμοποιείται κανένας αλγόριθμος κρυπτογράφησης.

Στο GPRS οι αλγόριθμοι A5 αντικαταστάθηκαν από τους GEA (GPRS Encryption Algorithm) αλγορίθμους και η διαδικασία της κρυπτογράφησης μεταφέρθηκε από το φυσικό επίπεδο (Physical Layer) στο Logical Link Control (LLC), υπό-επίπεδο του Data Link Layer (DLL). Αντίστοιχη κατάργηση του GEA1 έγινε όπως και στο A5/2.



Εικόνα 1.5: Διαδικασία κρυπτογράφησης στο GSM.

1.3.3 Εμπιστευτικότητα της ταυτότητας του συνδρομητή στο GSM

Η εμπιστευτικότητα της ταυτότητας του χρήστη προστατεύεται από τους ωτακουστές (Eavesdroppers) με το International Mobile Subscriber Identity (IMSI). Επειδή όμως το να στέλνεται σε συνεχή βάση το IMSI δεν είναι καλή τεχνική, ένα προσωρινό αναγνωριστικό Temporary Mobile Subscriber Identity (TMSI) χρησιμοποιείται. Αντίστοιχα για το GPRS χρησιμοποιείται το Packet Temporary Mobile Subscriber Identity (P-TMSI), το οποίο είναι ανεξάρτητα κατανεμημένο από το TMSI.

1.4 Βασικά Στοιχεία Ασφάλειας του UMTS - (3G)

Αντίθετα με το GSM, το κόστος έναντι μιας καλύτερης και ακριβότερης ασφάλειας για τα κινητά δίκτυα τρίτης γενιάς (3G) κρίθηκε αναγκαία. Τα δυνατά στοιχεία του GSM υιοθετήθηκαν και στα τρίτης γενιάς δίκτυα όπως το UMTS, αλλά και το LTE όπως θα δούμε και στη συνέχεια της εργασίας.

Στόχος του UMTS ήταν να κρατηθούν τα ισχυρά στοιχεία της ασφάλειας του GSM (2G), να βελτιωθούν και μαζί με νέες δυνατότητες να αποτελέσει ένα πρότυπο ασφάλειας τρίτης γενιάς (3G). Στα προγενέστερα πρότυπα, ανάμεσα τους και το GSM, δεν επέτρεπαν τις κινητές συσκευές να αναγνωρίζουν και να αυθεντικοποιούν τις κεραίες κυψελών, με συνέπεια οι επιτιθέμενοι να είναι σε θέση να μιμηθούν τις κυψέλες. Αυτό με τα νέα πρότυπα και το UMTS δεν επιτρέπεται, καθώς η αμοιβαία αυθεντικοποίηση το αποτρέπει. Το δίκτυο δημιουργεί ένα νέο Token αυθεντικοποίησης, που βασίζεται σε έναν αριθμό ακολουθίας και κοινόχρηστο συμμετρικό κλειδί, το οποίο αποθηκεύεται στο κεντρικό δίκτυο αλλά και στη κάρτα SIM του χρήστη και έτσι για κάθε αυθεντικοποίηση ο χρήστης γνωρίζει και συνδέεται μόνο αν η κυψέλη εκπέμπει το σωστό Token αυθεντικοποίησης [17].

Τα ήδη υπάρχοντα στοιχεία βελτιώθηκαν στο UMTS όπως φαίνονται και στον παρακάτω πίνακα (Πίνακα 1.6).

Ταυτότητα του συνδρομητή :	Αμοιβαία αυθεντικοποίηση (mutual authentication)

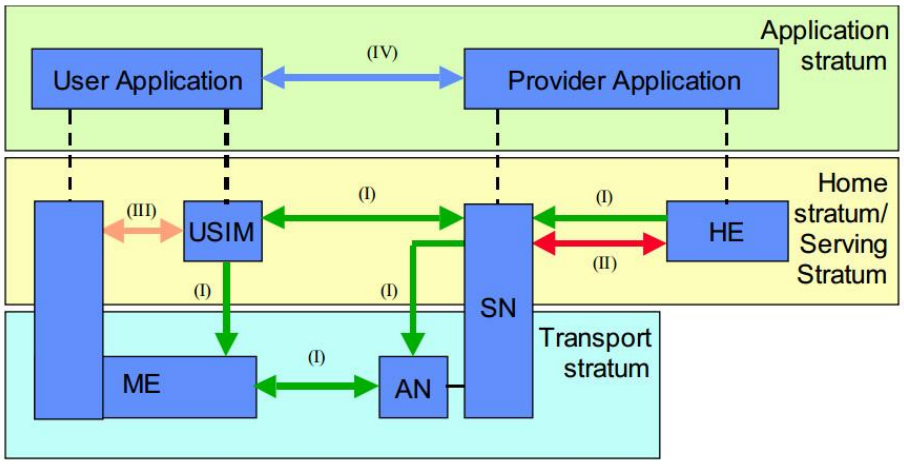
Κρυπτογράφηση :	Μεγαλύτερη έκταση κρυπτογράφησης καθώς και μεγαλύτερο μήκος κλειδιών
Subscriber Identity Module (SIM) :	Universal Subscriber Identity Module (USIM) και USIM application toolkit

Πίνακας 1.6: Βελτιώσεις στοιχείων ασφάλειας από το GSM στο UMTS.

Η αρχιτεκτονική ασφάλειας στο UMTS χωρίζεται σε πέντε κατηγορίες ασφάλειας (Εικόνα 1.6), που παρέχουν διαφορετικές απαιτήσεις και αντίμετρα έναντι απειλών που εκμεταλλεύονται αδυναμίες του συστήματος όπως, Eavesdropping, Man-In-The-Middle, Identity Spoofing, Session Hijacking, Repudiation Repley, Denial of Service (DoS). Αντίμετρα που χρησιμοποιούνται: Κρυπτογράφηση, Προσωρινά Κλειδιά, Αμοιβαία Αυθεντικοποίηση, Προστασία της Ακεραιότητας, Εμπιστευτικότητα Ταυτότητας.

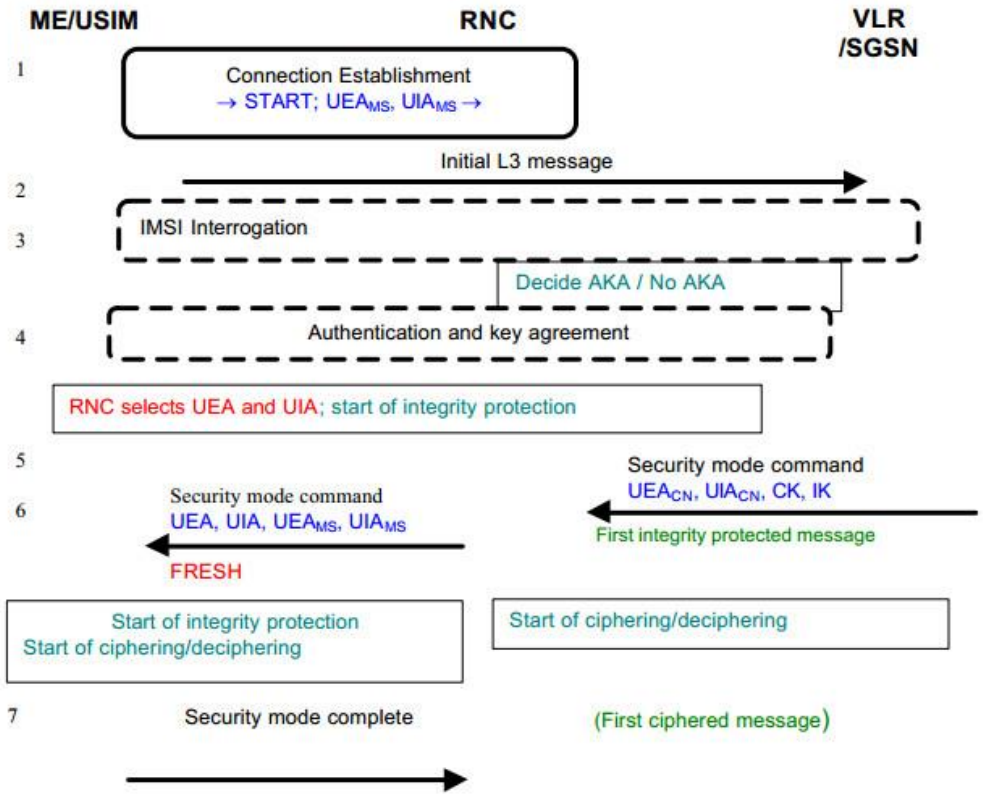
Αυτές οι κατηγορίες ασφάλειας είναι οι:

I. **Network Access Security** - Η ασφάλεια πρόσβασης στο δίκτυο παρέχει στους χρήστες ασφαλή πρόσβαση σε υπηρεσίες 3G και προστατεύει από επιθέσεις κατά την πρόσβαση στο ραδιοδίαυλο.
II. **Network Domain Security** - Δίνει τη δυνατότητα σε κόμβους στον τομέα του παρόχου να ανταλλάσσουν δεδομένα σηματοδοσίας με ασφάλεια.
III. **User Domain Security** - Επιτρέπει στους χρήστες να έχουν ασφαλή πρόσβαση σε κινητούς σταθμούς.
IV. **Application Domain Security** - Επιτρέπει στις εφαρμογές του χρήστη και στον πάροχο να ανταλλάσσουν μηνύματα με ασφάλεια.
V. **Visibility and Configurability of Security** - Ενημερώνει το χρήστη εάν ένα χαρακτηριστικό ασφαλείας είναι σε λειτουργία ή όχι, επιτρέποντας την κατάλληλη χρήση της υπηρεσίας.



Εικόνα 1.6: Αρχιτεκτονική ασφάλειας UMTS.

Τα πιο σημαντικά στοιχεία της ασφάλειας των συστημάτων του UMTS παρουσιάζονται συνοπτικά στις επόμενες υποενότητες σύμφωνα με την διαδικασία που ακολουθείται στην Εικόνα 1.7.



Εικόνα 1.7: Διαδικασίες ασφάλειας στο UMTS.

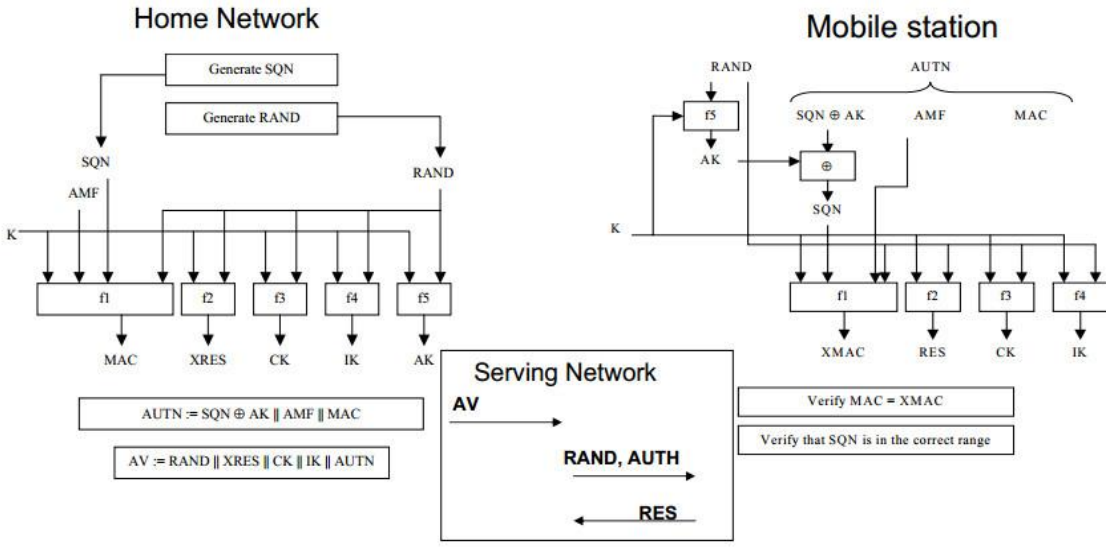
1.4.1 Αμοιβαία Αυθεντικοποίηση και Συμφωνία Κλειδιών στο UMTS (Mutual Authentication and Key Agreement)

Το πρωτόκολλο αυθεντικοποίησης, ή όπως συνήθως αναφέρεται AKA (Authentication and Key Agreement) στο UMTS, υλοποιεί την αμοιβαία αυθεντικοποίηση. Τα στοιχεία που συμμετέχουν στην διαδικασία είναι ο χρήστης (Universal Subscriber Identity Module - USIM), το δίκτυο (Serving Network - SN) και το δίκτυο στο χώρο του χρήστη (Home Environment - HE). Όπως και στο GSM, έτσι και στο UMTS το AuC και ο χρήστης μοιράζονται ένα κοινό μόνιμο κλειδί K (128-bits), το οποίο δεν έχει τη δυνατότητα διαμοιρασμού στο δίκτυο. Υπολογισμοί γίνονται και πάλι εσωτερικά της κάρτας USIM με διαφορετικούς όμως αλγορίθμους.
Το UMTS AKA αποτελείται από δυο φάσεις λειτουργίας (Εικόνα 1.8) [21].

- **Παραγωγή πίνακα διανυσμάτων για την αυθεντικοποίηση**
  Το SN δίκτυο στέλνει αίτημα αυθεντικοποίησης στο HE/AuC και αυτό με τη σειρά του παράγει έναν πίνακα με n διανύσματα αυθεντικοποίησης, όπου το καθένα από αυτά αποτελείται από τις ακόλουθες πέντε συνιστώσες: Έναν τυχαίο αριθμό (RAND), μια απόκριση απάντησης (XRES), ένα κλειδί κρυπτογράφησης (CK - Ciphering Key), ένα κλειδί ακεραιότητας (IK - Integrity Key) και ένα Token αυθεντικοποίησης (AUTN). Στο AuC υπάρχει το μόνιμο κλειδί του χρήστη βασισμένο στο IMSI ή στο TMSI και με χρήση κρυπτογραφικών αλγορίθμων παράγεται ο παραπάνω πίνακας. Ο πίνακας αυτός στέλνεται στο SN δίκτυο και ακολουθείται η επόμενη διαδικασία.
- **Αυθεντικοποίηση και συμφωνία κλειδιών**
  Η απόκριση από το SN γίνεται διαμέσου του (VLR) ή του (SGSN) για το GPRS και επιλέγοντας ένα διάνυσμα από τον πίνακα, στέλνει έναν τυχαίο αριθμό RAND καθώς και ένα Token αυθεντικοποίησης AUTN στον χρήστη. Ο χρήστης με τη σειρά του και συγκεκριμένα το USIM ελέγχει κατά πόσο το AUTN είναι έγκυρο. Σε περίπτωση που είναι έγκυρο, παράγει μια απάντηση RES και στέλνεται πίσω στο SN όπου και συγκρίνεται με το XRES. Αν οι τιμές είναι ίδιες τότε η αυθεντικοποίηση του χρήστη είναι επιτυχής. Κατά τη διαδικασία της αυθεντικοποίησης η USIM υπολογίζει και δυο κλειδιά CK (Ciphering Key), IK (Integrity Key) τα οποία χρησιμοποιούνται για την

κρυπτογράφηση και την ακεραιότητα της όλης επικοινωνίας. Τα κλειδιά αυτά είναι προσωρινά, (128-bits) και παράγονται κατά την αίτηση για αυθεντικοποίηση συναρτήσει του μόνιμου κλειδιού K. Όπως είπαμε και στο GSM είναι καλή τεχνική να χρησιμοποιούνται προσωρινά κλειδιά.

Η αμοιβαία αυθεντικοποίηση δεν αποτρέπει απειλές τύπου ενεργών επιθέσεων (Active Attacks), αλλά με συνδυασμό κι άλλων στοιχείων είναι ικανή να εμποδίσει τον επιτιθέμενο ώστε να κερδίσει κάτι ουσιαστικό, εκτός ίσως από την παρεμπόδιση της επικοινωνίας (Radio-Jamming), που μπορεί όμως και με άλλα μέσα να πετύχει.

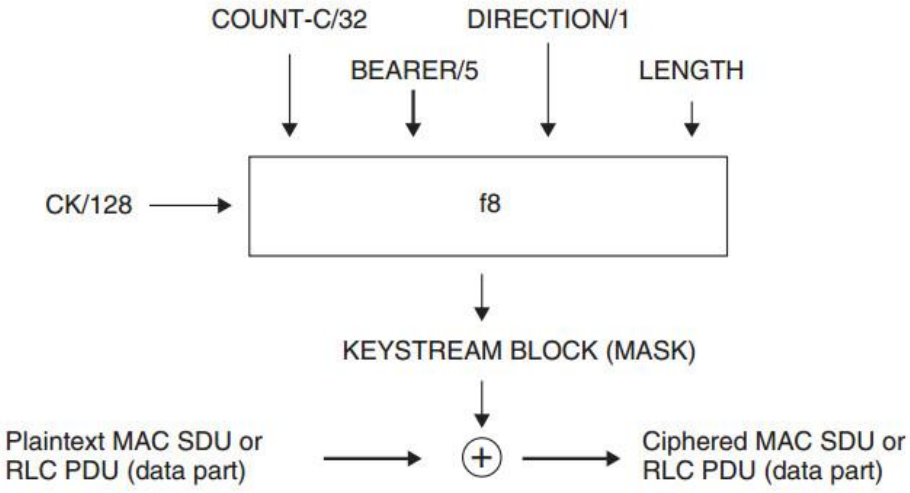


Εικόνα 1.8: Διαδικασία αυθεντικοποίησης στο UMTS.

1.4.2 Κρυπτογράφηση στο UMTS

Μετά την διαδικασία της επιτυχούς αυθεντικοποίησης, οι δύο πλευρές μπορούν να ξεκινήσουν την μεταξύ τους επικοινωνία. Η κρυπτογράφηση όπως και στο GSM, έχει ως σκοπό την εγκαθίδρυση ενός ασφαλούς καναλιού. Επιλέγονται και πάλι κατάλληλοι αλγόριθμοι κρυπτογράφησης, οι οποίοι χρησιμοποιούν το κρυπτογραφικό κλειδί CK. Το κλειδί αυτό πρέπει να μεταφερθεί από το κεντρικό δίκτυο (CN), στο δίκτυο πρόσβασης Radio Access Network (RAN), μεταξύ του τερματικού και του Radio Resource Control (RRC). Αυτή η μεταφορά επιτυγχάνεται με το πρωτόκολλο Radio Access Network Application Protocol (RANAP) και της εντολής (Security Mode Command), η οποία εντολή μετά και την απόκτηση του CK από το RRC

μπορεί να ενεργοποιήσει την κρυπτογράφηση. Στο 3G η διαδικασία της κρυπτογράφησης (Εικόνα 1.9), γίνεται είτε στο επίπεδο Medium Access Control layer (MAC), είτε στο επίπεδο Radio Link Control layer (RLC).

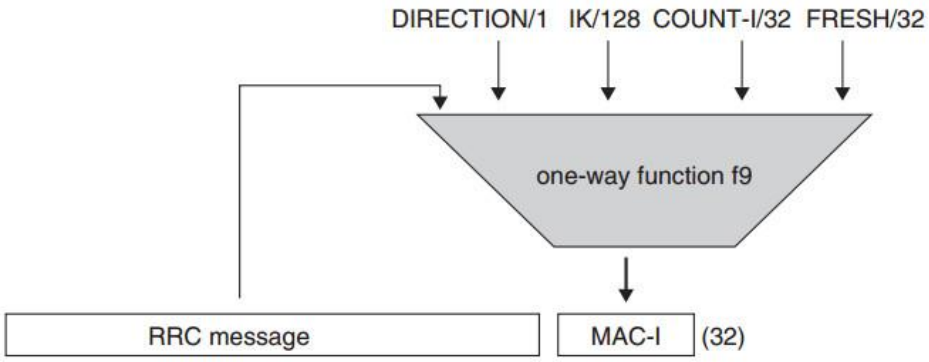


Εικόνα 1.9: Διαδικασία κρυπτογράφησης στο UMTS.

1.4.3 Προστασία Ακεραιότητας στο UMTS

Η προστασία ακεραιότητας στο UMTS είναι σημαντική λειτουργία για την ασφάλεια και ένας τρόπος θωράκισης της επικοινωνίας μετά την επιτυχή αυθεντικοποίηση. Η αυθεντικοποίηση από μόνη της δεν αρκεί, καθώς επιθέσεις τύπου "man-in-the-middle" μπορούν να περιμένουν μέχρι να τελειώσει η διαδικασία της αυθεντικοποίησης και μετά να αρχίσουν να αλλάζουν τα μηνύματα. Με την ακεραιότητα κάθε μήνυμα προστατεύεται ξεχωριστά, κάτι που δυσκολεύει την εξάπλωση τέτοιων τεχνικών επίθεσης.

Η προστασία ακεραιότητας υλοποιείται στο επίπεδο RRC μεταξύ του τερματικού και του RNC, όπως και η κρυπτογράφηση (Encryption) και το κλειδί που μοιράζονται είναι το IK (128-bit), το οποίο μεταφέρεται μαζί με το CK στο RNC (Εικόνα 1.10). Είναι βασισμένο στο MAC (Message Authentication Code), μια μονόδρομη συνάρτηση (One-Way Function) που ελέγχεται από το κλειδί IK. Η συνάρτηση αυτή ονομάζεται f9 και η έξοδος αυτής MAC-I (32-bit), η οποία έξοδος υπολογίζεται για κάθε μήνυμα RRC τόσο στην μεριά του αποστολέα όσο και στη μεριά του παραλήπτη.



Εικόνα 1.10: Διαδικασία ακεραιότητας στο UMTS.

1.4.4 Εμπιστευτικότητα Ταυτότητας Χρηστών στο UMTS

Η κύρια ταυτότητα του χρήστη, όπως και στο GSM είναι το IMSI. Στο δίκτυο όμως χρησιμοποιείται το προσωρινό αναγνωριστικό ταυτότητας TMSI στο τομέα CS (Circuit-Switched) ή το P-TMSI στο PS τομέα (Packet-Switched), κάτι που προστατεύει την εμπιστευτικότητα της ταυτότητας των χρηστών σχεδόν πάντα από τους παθητικούς ωτακουστές. Προσωρινή ταυτότητα δεν μπορεί να χρησιμοποιηθεί στην αρχική περίπτωση εγγραφής, όπου στο δίκτυο δεν είναι ακόμα γνωστό το IMSI.

1.4.5 Αλγόριθμοι Ασφάλειας στα Τρίτης Γενιάς Δίκτυα

Για την αρχιτεκτονική ασφάλειας UMTS πολλοί είναι οι αλγόριθμοι που απαιτούνται, οι οποίοι έχουν προταθεί από το 3GPP. Οι αλγόριθμοι AKA υλοποιούνται στο USIM και στο HE/AuC, τα οποία και τα δύο ανήκουν στον ίδιο πάροχο δικτύου. Αν ο πάροχος δικτύου επιθυμεί να χρησιμοποιήσει αλγορίθμους που ο ίδιος έχει αναπτύξει μπορεί να το κάνει, σε αντίθεση με τους αλγορίθμους της κρυπτογράφησης και της ακεραιότητας (Cipher and Integrity) όπου είναι υποχρεωτικό να χρησιμοποιούνται μόνο οι πρότυποι αλγόριθμοι και οι οποίοι υλοποιούνται στο τερματικό και στο SN δίκτυο μέσου του Radio Network Controller (RNC).

Μια καλή τεχνική είναι η λήψη προληπτικών μέτρων για τη χρησιμοποίηση δύο αλγορίθμων κρυπτογράφησης ταυτόχρονα, έτσι ώστε αν ο ένας αποτύχει να τεθεί σε λειτουργία, ένας άλλος να αναλάβει την κρυπτογράφηση.

Ο αλγόριθμος UMTS AKA αποτελείται από επτά λειτουργίες/συναρτήσεις, f1, f1*, f2, f3, f4, f5, f5* και ονομάζεται MILENAGE. Οι αλγόριθμοι κρυπτογράφησης και ακεραιότητας βασίστηκαν στον αλγόριθμο KASUMI και είναι οι f8 (αλγόριθμος κρυπτογράφησης) και f9 (αλγόριθμος ακεραιότητας). Οι αντίστοιχες ονομασίες τους είναι UEA1 (f8) και UIA1 (f9), οι οποίοι αλγόριθμοι αργότερα εξελίχτηκαν σε UEA2 και UIA2 χρησιμοποιώντας ως βάση τους τον αλγόριθμο SNOW 3G, εξέλιξη η οποία με τη πάροδο του χρόνου έπρεπε να γίνει για λόγους επιθέσεων τύπου εξαντλητικής αναζήτησης στον KASUMI, κάνοντας εφικτή την απόσπαση κλειδιών.

ΑΛΓΌΡΙΘΜΟΣ KASUMI

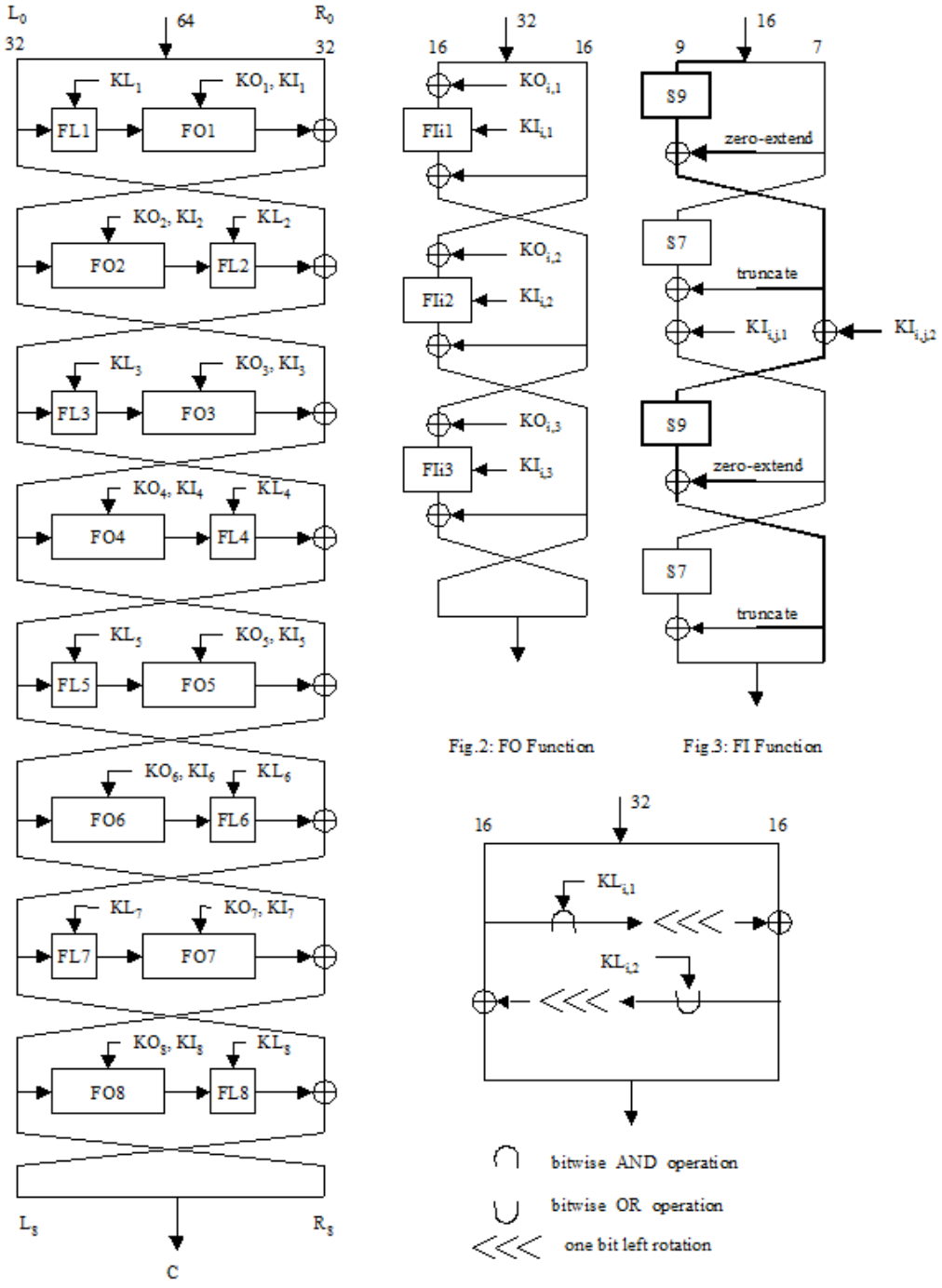
Ο αλγόριθμος KASUMI (Εικόνα 1.11), ή αλλιώς A5/3, είναι ένας Block Cipher αλγόριθμος, βασισμένος στον αλγόριθμο MISTY και λειτουργεί σε ένα μπλοκ δεδομένων 64-bit, χρησιμοποιώντας ένα κλειδί 128-bit. Είναι βασισμένο σε μια δομή Feistel και περιέχει οχτώ γύρους (Rounds) [9].

1.5 Ευπάθειες στο UMTS

Οι ευπάθειες στο UMTS μπορεί να είναι λιγότερες συγκριτικά με το προκάτοχο του GSM, όμως υπάρχουν και κάποιες από αυτές είναι οι επόμενες:

- Χωρίς την κρυπτογράφηση ενεργοποιημένη, η υποκλοπή είναι υπαρκτή απειλή.
- Η πρώτη εγγραφή στο δίκτυο με την ταυτότητα του χρήστη (IMSI), αποστέλνεται υπό μορφή απλού κειμένου (Clear Text) επιτρέποντας επιθέσεις παθητικού τύπου (περιμένοντας για πιθανές εκπομπές απροστάτευτων IMSI) και Man-In-The-Middle (MITM) επιθέσεις.
- Επιτιθέμενοι που εφαρμόζουν παθητικές (Passive) ή ενεργητικές (Active) μεθόδους, μπορούν να υποκλέψουν διανύσματα (Vectors) αυθεντικοποίησης.
- Προστασία στο επίπεδο εφαρμογής παρέχεται από το πρωτόκολλο Wireless Transport Layer Security (WTLS), το οποίο χρησιμοποιεί WAP πύλη (Gateway) η οποία θεωρείται ανασφαλής και δεν εξασφαλίζει end-to-end επικοινωνία. Επιπλέον επιτρέπει τη χρησιμοποίηση αδύναμων (Weak) αλγορίθμων κρυπτογράφησης και διαθέτει χαρακτηριστικά, τα οποία

επιτρέπουν την ανάπτυξη επιθέσεων του τύπου επιλεγμένου αρχικού κειμένου (Chosen-Plaintext) και εξαντλητικής αναζήτησης (Brute Force).

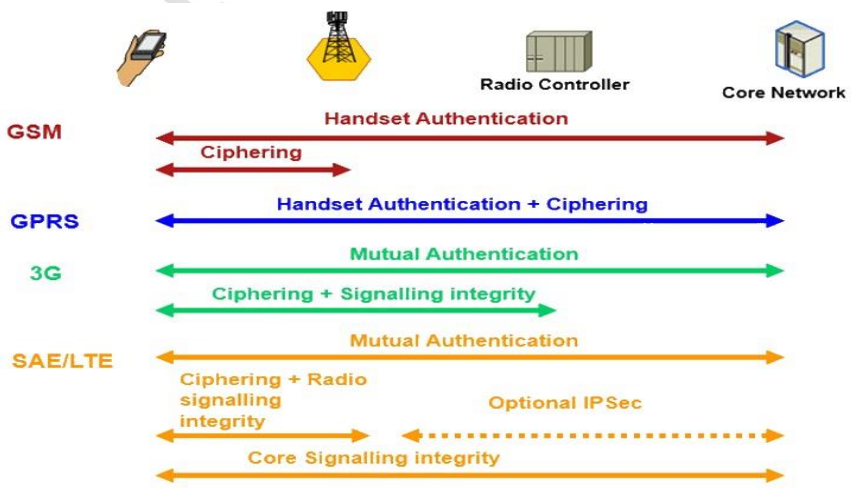


Εικόνα 1.11: Αλγόριθμος KASUMI.

1.6 Ανάπτυξη Ασφάλειας B3G (Beyond 3G) - Πρότυπο LTE

Η εξέλιξη των βασικών στοιχείων ασφάλειας που είδαμε μέχρι τώρα, αποτέλεσαν τις βάσεις για την ανάπτυξη της ασφάλειας του LTE συστήματος, τα προβλήματα που έπρεπε να αντιμετωπίσει το νέο πρότυπο, τα κοινά στοιχεία με τα προγενέστερα πρότυπα, τη δια-λειτουργικότητα με άλλα συστήματα, τις μέχρι τώρα ευπάθειες αλλά και τις απειλές που κλήθηκαν να αντιμετωπιστούν.
Μαθαίνοντας λοιπόν από τα θετικά και αρνητικά στοιχεία των προγενέστερων προτύπων, το LTE προσπαθεί να κρατήσει τα δυνατά χαρακτηριστικά και να βελτιώσει η να εξαλείψει τα προβλήματα των προηγούμενων προτύπων (Εικόνα 1.12).

Ασφάλεια μέσω της εναέριας διεπαφής του LTE παρέχεται μέσω ισχυρών κρυπτογραφικών τεχνικών. Για την ασφάλεια της σύνδεσης Backhaul από το eNB προς το κεντρικό δίκτυο, γίνεται χρήση του πρωτοκόλλου ανταλλαγής κλειδιών IKE και το πρωτόκολλο ασφαλείας IPsec, όταν χρειάζεται κρυπτογραφική προστασία. Ισχυρές κρυπτογραφικές τεχνικές παρέχουν από άκρο σε άκρο προστασία για σηματοδοσία μεταξύ του κεντρικού δικτύου και των UEs. Το κεντρικό σημείο λοιπόν όπου τα δεδομένα του χρήστη είναι εκτεθειμένα, είναι στις βάσεις eNBs.
Εκτενέστατη περιγραφή της ασφάλειας στο LTE και των βασικών αρχών ασφάλειας, γίνεται στο επόμενο κεφάλαιο όπου και αποτελεί την βασική τεχνολογία (RAN) για την κύρια μελέτη της παρούσας εργασίας που είναι η ασφάλεια της LTE Φεμτοκυψέλης (LTE - Femtocell).



Εικόνα 1.12: Εξέλιξη των αρχιτεκτονικών ασφάλειας.

ΚΕΦΑΛΑΙΟ

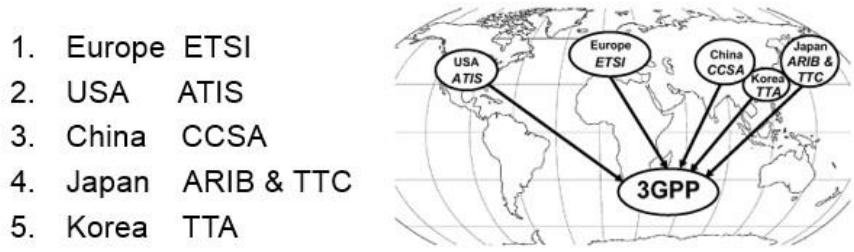
Αρχιτεκτονική Ασφάλειας στο LTE (Βασικές Αρχές) 2

Η ανάγκη για εξέλιξη των 3G προτύπων τη τελευταία δεκαετία, έγινε η αφορμή για την δημιουργία μιας τεχνολογίας όπου τα κινητά τηλέφωνα σταδιακά μετατρέπονται σε ισχυρές συσκευές, με δυνατότητες υπολογιστών, με πρόσβαση στο διαδίκτυο οπουδήποτε κι αν οι χρήστες βρίσκονται, με μεγάλες ταχύτητες και χωρίς καμία διακοπή σύνδεσης λόγω μεταπομπών σε διαφορετικά δίκτυα. Οι προδιαγραφές αυτές συγκεντρώθηκαν στο LTE πρότυπο.

Η μακροπρόθεσμη εξέλιξη της Κινητής Τηλεφωνίας LTE (Long Term Evolution), δημιουργήθηκε κάτω από τις εργασίες του 3rd Generation Partnership Project (3GPP) το Νοέμβριο του 2004, με το σύνολο έξι οργανισμών (Standards Development Organizations - SDOs), European Telecommunications Standards Institute (ETSI), Alliance for Telecommunications Industry Solutions (ATIS), China Communications Standards Association (CCSA), Association of Radio Industries and Businesses (ARIB), Telecommunication Technology Committee (TTC), Telecommunications Technology Association (TTA), (Εικόνα 2.1) και στόχος ήταν η βελτίωση του συστήματος 3G UMTS παρόλα τα ελάχιστα κοινά σημεία που έχει με το LTE. Οι βελτιώσεις του προτύπου (HSPA, HSPA+) δεν ήταν αρκετές για μια εποχή που απαιτεί πλήρη κινητικότητα του χρήστη, αυξανόμενες ανάγκες διαδικτύωσης και απαιτήσεων παράλληλων με αυτών των Broadband Συνδέσεων.

Η εξέλιξη του νέου προτύπου και η προτυποποίηση του από το 3GPP ακολούθησε μια πορεία από εκδόσεις τεχνικών προδιαγραφών (Technical Specification Groups -

TSGs), τα οποία αποτελούνται από ομάδες (Working Groups - WGs) η κάθε μια επικεντρωμένη σε διαφορετικό κομμάτι του συστήματος.



Εικόνα 2.1: 3GPP οργανισμοί στο παγκόσμιο χάρτη.

2.1 Εισαγωγή στο Σύστημα LTE

Το UMTS αποτελεί τον πρόδρομο για το πρότυπο LTE και η αρχιτεκτονική του είναι σαφώς επηρεασμένη από αυτό.
Το UMTS RAN (Radio Access Network) αποτελείται από δύο μέρη,

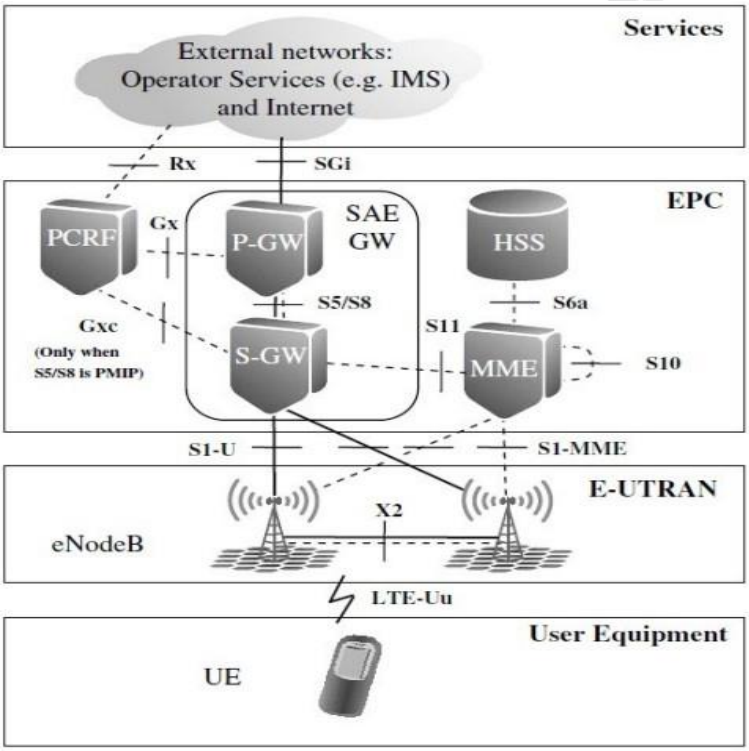
- **UMTS Terrestrial Radio Access (UTRA)**
  - Το οποίο είναι το air interface, περιλαμβάνοντας τον εξοπλισμό του χρήστη (UE) ή κάποιο κινητό τηλέφωνο.
- **UMTS Terrestrial Radio Access Network (UTRAN)**
  - Το οποίο περιλαμβάνει το Radio Network Controller (RNC) και τον σταθμό βάσης που είναι γνωστό ως Node B (NB).

Ισοδύναμα με τα παραπάνω για το RAN του LTE έχουμε τα αντίστοιχα δύο μέρη:

1. **Evolved UTRA (E-UTRA)**
2. **Evolved UTRAN (E-UTRAN)**

Ορίζοντας ολόκληρο το σύστημα του LTE παράλληλα με το RAN, υπάρχει και ένα άλλο 3GPP πρόγραμμα ονομαζόμενο System Architecture Evolution (SAE), το οποίο ορίζει όλα τα νέα IP πακέτα του Core Network (CN), γνωστό ως Evolved Packet Core

(EPC). Το RAN (E-UTRA, E-UTRAN) μαζί με το SAE (EPC) προσδιορίζουν ολόκληρο το σύστημα που ονομάζεται Evolved Packet System (EPS). Το όραμα του LTE, ήταν η δημιουργία μιας επίπεδης all IP Packet Core Network αρχιτεκτονικής και την πλήρη δυνατότητα συνεργασίας με άλλες τεχνολογίες πρόσβασης Radio Access Technologies (RATs). Το EPS λοιπόν αποτελείται από το δίκτυο πρόσβασης E-UTRAN, από το δίκτυο κορμού EPC, από το υλικό των χρηστών και τον τομέα υπηρεσιών. Το δίκτυο πρόσβασης αποτελείται από ένα μοναδικό στοιχείο, το evolved NodeB (eNodeB) που επικοινωνεί με τους Users (UEs) και το δίκτυο κορμού που αποτελείται από αρκετά στοιχεία όπως θα δούμε και παρακάτω (Εικόνα 2.2) [19].



Εικόνα 2.2: Αρχιτεκτονική LTE.

2.1.1 Δίκτυο πρόσβασης (Access Network)

Το E-UTRAN διαχειρίζεται την επικοινωνία του σταθμού βάσης με το EPC [45].

- **Evolved NodeB (eNodeB)**
  Αποτελείται από ένα σύνολο σταθμών βάσεων (eNodeBs ή eNBs). Ο eNodeB

είναι ένας σταθμός βάσης που ελέγχει όλες τις ραδιολειτουργίες με το κεντρικό δίκτυο. Αποτελεί μια γέφυρα επιπέδου 2 μεταξύ των UEs και του EPC. Άλλες λειτουργίες του eNodeB είναι, κρυπτογράφηση/ αποκρυπτογράφηση των δεδομένων των χρηστών, συμπίεση/αποσυμπίεση των IP κεφαλίδων (Header Compression), Radio Resource Management (RRM), μετρήσεις Radio Signal.

2.1.2 Δίκτυο Κορμού (Core Network)

Το EPC παρέχει υπηρεσίες μεταγωγής, δρομολόγησης, μετάδοσης και ασφάλειας για τη σηματοδοσία. Αποτελείται από τις παρακάτω οντότητες [45]:

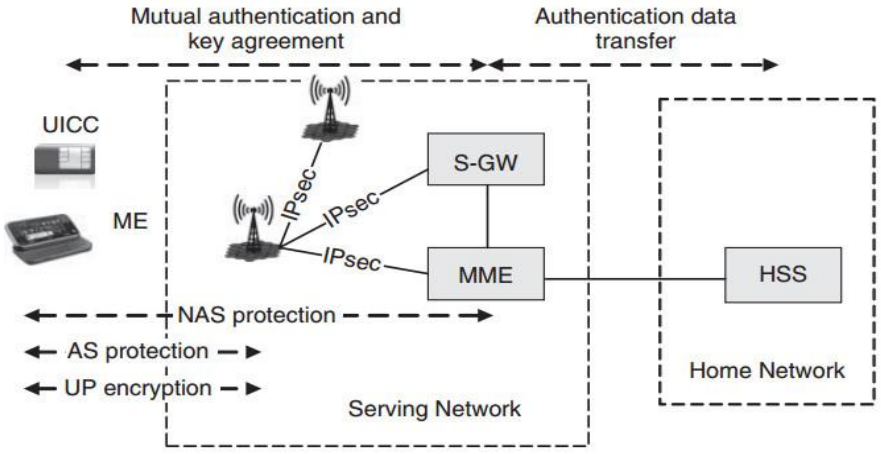
- **Serving Gateway (S-GW)**
  Το S-GW συμπεριφέρεται σαν ένα Router που προωθεί και δρομολογεί δεδομένα μεταξύ του σταθμού βάσης και το PDN Gateway.
- **Packet Data Network Gateway (P-GW)**
  Το P-GW είναι το στοιχείο που είναι υπεύθυνο για την επικοινωνία των UEs με εξωτερικά δίκτυα πακέτων, αποτελώντας τα σημεία εισόδου και εξόδου για την κίνηση που προορίζεται για τα UEs, αλλά και το σημείο στο οποίο γίνεται η διανομή και ανάθεση των IP διευθύνσεων στα UEs.
- **Mobility Management Entity (MME)**
  Το MME ελέγχει τη λειτουργία του δικτύου, αλλά και την πρόσβαση των χρηστών μέσω των μηνυμάτων σηματοδοσίας και του Home Subscription Server (HSS).
- **Policy and Charging Resource Function (PCRF)**
  Το PCRF είναι υπεύθυνο για τη λήψη αποφάσεων σχετικά με την πολιτική και έλεγχο χρέωσης.
- **Home Subscription Server (HSS)**
  Το HSS είναι μια βάση δεδομένων που περιέχει όλες τις πληροφορίες των συνδρομητών του δικτύου του διαχειριστή.

2.2 Αρχιτεκτονική Ασφάλειας EPS (LTE/SAE)

Οι ασύρματες κινητές τηλεπικοινωνίες πρέπει να μπορούν να ανταποκρίνονται στις αυξημένες απαιτήσεις τόσο του χρηστών, όσο και των δικτύων παροχής υπηρεσιών, προσδοκώντας παράλληλα την εμπιστοσύνη και προστασία της ιδιωτικής ζωής. Εκτός από την προφανή ανάγκη για την πιστοποίηση της ταυτότητας και κρυπτογράφησης, οι νέες αρχιτεκτονικές απαιτούν πιο εξελιγμένους μηχανισμούς προστασίας.

Το Evolved Packet System (EPS), κάνει την εμφάνιση του στο 3G περιβάλλον με δύο νέες τεχνολογίες, το Evolved Universal Terrestrial Radio Access Network (E-UTRAN) με νέα διεπαφή ραδιοσυχνοτήτων και το Evolved Packet Core (EPC), κεντρικό δίκτυο βασισμένο στο πρωτόκολλο IP. Από την σκοπιά της ασφάλειας, το σύστημα EPS έχει τις βάσεις του στις προγενέστερες μεθόδους και τεχνικές που εφαρμόστηκαν τόσο στο GSM όσο και στα 3G συστήματα. Η διαλειτουργικότητα με διαφορετικά συστήματα, έκανε εμφανή την ανάγκη για νέες δυνατότητες και επεκτάσεις που έπρεπε να εφαρμοστούν στη νέα αρχιτεκτονική.

Η αρχιτεκτονική ασφάλειας του EPS (LTE/SAE), παρουσιάζεται παρακάτω (Εικόνα 2.3).



Εικόνα 2.3: Αρχιτεκτονική ασφάλειας του EPS.

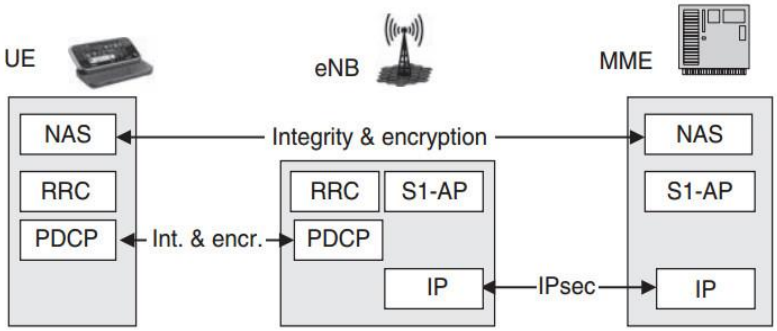
Τα σημαντικότερα σημεία ασφάλειας για το EPS σύστημα, απαιτήσεις ασφάλειας, απειλές και επιθέσεις ενάντια στο EPS, καθώς και οι σημαντικότερες διαδικασίες ασφάλειας, είναι ζητήματα τα οποία πραγματεύονται παρακάτω.

Σύμφωνα με την αρχιτεκτονική του EPS στην Εικόνα 2.3, οι κυριότερες λειτουργίες ασφάλειας λαμβάνονται με την εξής σειρά.

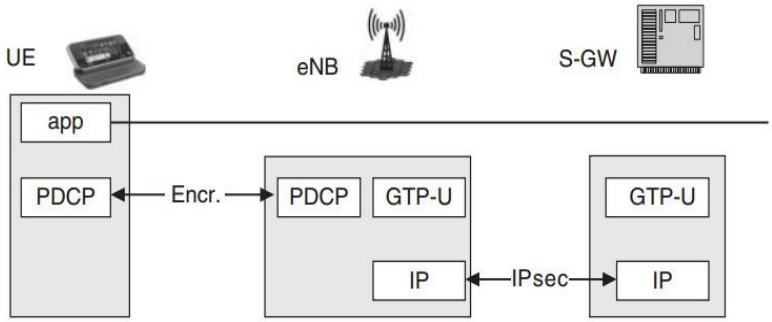
Αφού προσδιοριστεί ο εξοπλισμός του χρήστη (UE), ο φορέας διαχείρισης κινητικότητας MME στο δίκτυο, λαμβάνει δεδομένα αυθεντικοποίησης από το οικείο δίκτυο. Στη συνέχεια το MME εκκινεί το πρωτόκολλο AKA (Authentication and Key Agreement) με τον χρήστη. Μετά την επιτυχή εκτέλεση του πρωτοκόλλου, το MME με τον χρήστη UE μοιράζονται ένα κοινό μυστικό κλειδί K_{ASME}, όπου το ακρώνυμο ASME παραπέμπει στο Access Security Management Entity. Στο EPS το ρόλο του ASME αναλαμβάνει το MME. Τώρα το MME και το UE είναι σε θέση να αντλήσουν περαιτέρω κλειδιά από το K_{ASME}. Από τα κλειδιά που αντλούνται, δύο κλειδιά χρησιμοποιούνται για την εμπιστευτικότητα και την ακεραιότητα της προστασίας των δεδομένων σηματοδοσίας μεταξύ του MME και του UE. Αυτό αναπαρίσταται στην παραπάνω εικόνα με το βέλος "NAS protection" (Non-Access Stratum). Ένα άλλο κλειδί μεταφέρεται στο σταθμό βάσης (eNB). Τρία ακόμα κλειδιά προορίζονται για το MME και το UE, εκ των οποίων δύο από αυτά χρησιμοποιούνται για την εμπιστευτικότητα και την ακεραιότητα της προστασίας των δεδομένων σηματοδοσίας μεταξύ του eNB και του UE (βέλος με "AS προστασίας" (Access Stratum) και το τρίτο κλειδί χρησιμοποιείται για την προστασία της εμπιστευτικότητας των δεδομένων των χρηστών μεταξύ του eNB και του UE (βέλος "UP[1] encryption"). Εκτός από την προστασία των δεδομένων σηματοδοσίας και του χρήστη (UP), παρέχεται επίσης προστασία εμπιστευτικότητας και ακεραιότητας για τα δεδομένα σηματοδοσίας και του χρήστη τα οποία μεταφέρονται μέσω διασύνδεσης μεταξύ του σταθμού βάσης και του κεντρικού δικτύου (EPC). Τα δεδομένα σηματοδοσίας μεταφέρονται μεταξύ του UE και του MME μέσω της διασύνδεσης S1- MME, ενώ τα δεδομένα του χρήστη μεταφέρεται μεταξύ του UE και της πύλης (S-GW), μέσω της διασύνδεσης S1–U. Εάν χρησιμοποιείται κρυπτογραφική προστασία στις S1 διεπαφές, τότε ο μηχανισμός προστασίας που χρησιμοποιείται είναι το IPsec. Η X2 διεπαφή μεταξύ δύο σταθμών βάσης είναι παρόμοια και προστατεύεται επίσης από το

[1] User Plane data.

IPsec. Στις επόμενες δύο εικόνες (2.4, 2.5) απεικονίζονται τα δεδομένα σηματοδοσίας και χρήστη στο EPS [23].



Εικόνα 2.4: Πρωτόκολλα δεδομένων σηματοδοσίας EPS.



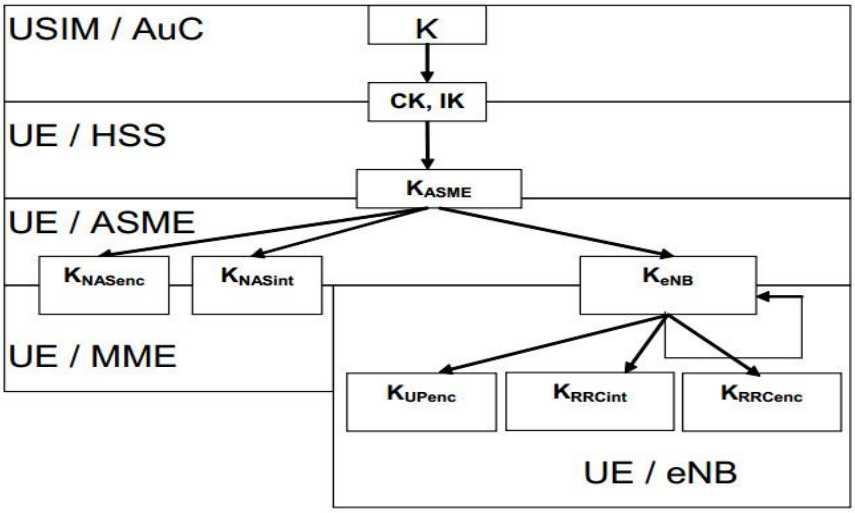
Εικόνα 2.5: Πρωτόκολλα δεδομένων χρήστη EPS.

Αυθεντικοποίηση Χρήστη - (EPS Authentication and Key Agreement)

Ο αλγόριθμος αυθεντικοποίησης στο LTE είναι βασισμένος στο UMTS-AKA (UMTS Authentication and Key Agreement) πρωτόκολλο. Παρέχει αμοιβαία αυθεντικοποίηση ανάμεσα στον χρήστη και το κεντρικό δίκτυο. Οι ταυτότητες των συνδρομητών (SIM) του GSM, δεν επιτρέπεται στο LTE καθώς δεν παρέχουν επαρκή ασφάλεια.

Το EPS AKA παρέχει ένα κλειδί ρίζας, το οποίο προέρχεται από μια ιεραρχία κλειδιών (Key Hierarchy), Εικόνα 2.6. Τα κλειδιά στην ιεραρχία χρησιμοποιούνται για την προστασία δεδομένων χρήστη και σηματοδοσίας ανάμεσα στο UE και το δίκτυο. Η ιεραρχία κλειδιών προκύπτει από την χρήση κρυπτογραφικών λειτουργιών. Αν ένας επιτιθέμενος γνωρίζει για παράδειγμα ένα από 3 πιθανά κλειδιά (key1, key2,

key3), έστω το key2, τότε δε μπορεί να γνωρίζει τα υπόλοιπα δύο λόγο διαφορετικής ιεραρχίας. Στόχος είναι ο διαχωρισμός των κλειδιών.

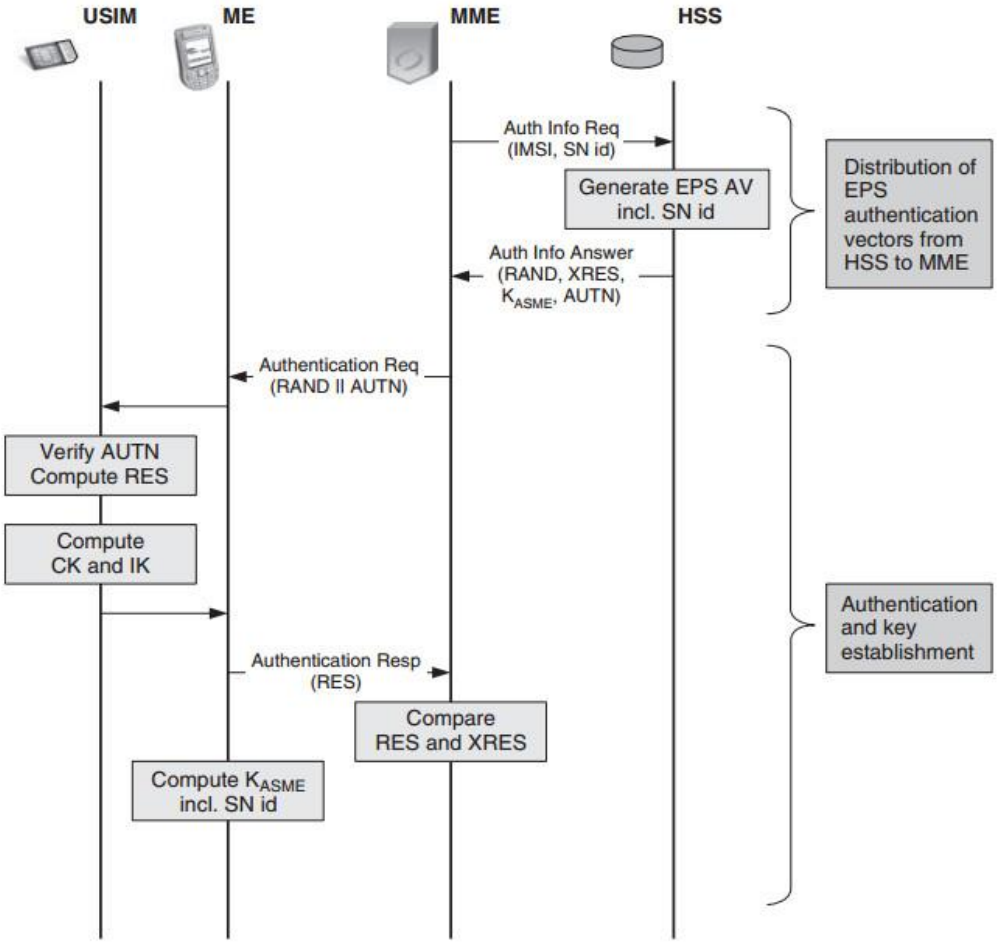


Εικόνα 2.6: EPS key hierarchy.

Η διαδικασία EPS AKA είναι ένας συνδυασμός από τις ακόλουθες διαδικασίες:

- Μια διαδικασία για την παραγωγή EPS διανυσμάτων αυθεντικοποίησης (AVs) στο Home Subscriber Server (HSS), κατόπιν αιτήματος του MME που στέλνονται στο MME.
- Μια διαδικασία για την αμοιβαία αυθεντικοποίηση και την εγκατάσταση ενός νέου κλειδιού ανάμεσα στο UE και το εξυπηρετούμενο δίκτυο (Serving Network - SN).
- Μια διαδικασία για τη διανομή των στοιχείων αυθεντικοποίησης εντός και μεταξύ των SNs.

Η διαδικασία του EPS-AKA (Εικόνα 2.7) αναλύεται στην 3GPP τεχνική αναφορά, (TS 33.401) [54].



Εικόνα 2.7: EPS Authentication and Key Agreement (AKA).

Ασφάλεια Σηματοδοσίας

Το LTE παρέχει ακεραιότητα, προστασία αναπαραγωγής και κρυπτογράφησης μεταξύ του UE και του eNB. Τα πρωτόκολλα IKE/IPsec, μπορούν να παρέχουν προστασία στο Backhaul σύνδεσμο ανάμεσα στα eNB και MME αλλά και στα δεδομένα του χρήστη ανάμεσα στα S-GW και eNB.

2.3 Απειλές και Επιθέσεις στο EPS

Οι σημαντικότερες κατηγορίες απειλών στο EPS σύστημα αποτυπώνονται στον παρακάτω πίνακα (Πίνακας 2.1):

– Απειλές κατά της ταυτότητας των χρηστών.
– Απειλές κατά της ιδιωτικότητας.
– Απειλές ανίχνευσης των UEs.
– Απειλές που σχετίζονται με τις μεταπομπές.
– Απειλές που σχετίζονται με τους σταθμούς βάσης και τις συνδέσεις τελευταίου μίλι (last-mile transport links)
– Απειλές που σχετίζονται με Multicast και Broadcast σηματοδότηση.
– Απειλές που σχετίζονται με την άρνηση υπηρεσίας (DoS).
– Απειλές κατάχρησης των υπηρεσιών δικτύου.
– Απειλές κατά των ραδιοφωνικών πρωτοκόλλων.
– Απειλές που σχετίζονται με τη διαχείριση της κινητικότητας.
– Απειλές κατά της χειραγώγησης του επιπέδου δεδομένων ελέγχου.
– Απειλές από μη εξουσιοδοτημένη πρόσβαση στο δίκτυο.

Πίνακας 2.1: Απειλές στο EPS.

Η πλήρης υποστήριξη από το LTE των οικιακών eNBs (Home eNBs - HeNBs), ή αλλιώς φεμτοκυψέλες (Femtocells) όπως ονομάζονται, είναι μια σχετικά καινούρια τεχνολογία η οποία αποτελεί και αντικείμενο μελέτης της παρούσας διπλωματικής στη συνέχεια.

Μια φεμτοκυψέλη συνδέεται με το EPC μέσω των διεπαφών S1-MME και S1-U. Χρησιμοποιείται μια πύλη HeNB (HeNB Gateway), για να επιτρέψει την ύπαρξη διεπαφής S1 μεταξύ των HeNBs και του EPC. Το HeNB-GW θα εμφανίζεται σε ένα HeNB ως μια MME, ενώ για την MME το HeNB-GW θα εμφανίζεται σαν ένα HeNB.

ΚΕΦΑΛΑΙΟ

Ασφάλεια Φεμτοκυψελών - (Femtocell Security) 3

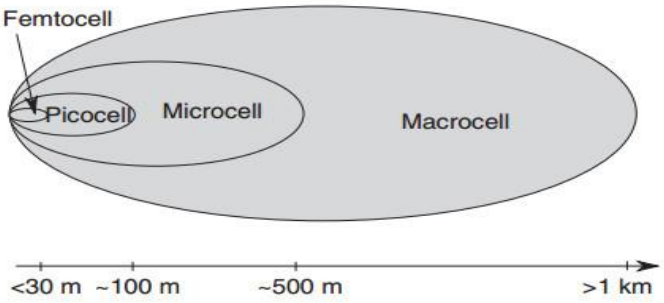
Το μεγαλύτερο ποσοστό της κίνησης στα κινητά δίκτυα επικοινωνών, εκτιμάται πως λαμβάνει χωρα σε εσωτερικούς χώρους (σπίτια, χώροι εργασίας, πανεπιστήμια, αεροδρόμια κ.α.). Το ποσοστό αυτό φτάνει τα 2/3 των κλήσεων και το 90% των δεδομένων και αυξάνεται όλο και περισσότερο με την τεχνολογική εξέλιξη των κινητών μικροσυσκευών όπως tablets, iPads και smartphones [42].

Η κακή κάλυψη όμως που χαρακτηρίζει τους εσωτερικούς χώρους είναι ενα φαινόμενο που βάζει περιορισμούς στην επίτευξη υπηρεσιών φωνής αλλά και δεδομένων υψηλής ταχύτητας. Κάποιες έρευνες δείχνουν ότι το 45% των νοικοκυριών και το 30% των επιχειρήσεων βιώνουν αυτό το φαινόμενο [51]. Οι παραπάνω λόγοι οδήγησαν την ανάγκη της κυψελωτής τεχνολογίας για μικρότερες κυψέλες, στην δημιουργία των Femtocells.

Τα Femtocells είναι μια αναδυόμενη τεχνολογία που έχει στόχο να ενισχύσει τη συνδεσιμότητα 3G συσκευών και να αποσυμφορήσει την αύξηση της κυκλοφορίας δεδομένων από τα Macrocells. Είναι μια μέθοδος αποτελεσματικής αντιμετώπισης της κακής κάλυψης, βελτιστοποίησης της παρεχόμενης ποιότητας υπηρεσιών (QoS), αύξηση της χωρητικότητας αλλά και η πιο οικονομική λύση σε σχέση με προγενέστερες μεθόδους όπως τα κατανεμημένα συστήματα κεραιών DAS (Distributed Antenna Systems), η χρησιμοποίηση πικοκυψελών (Picocells) αλλά και αναμεταδοτών (Relay Nodes)[2]. Στην κλίμακα των μικροκυψελωτών τεχνολογιών η

[2] eNB βάσεις συνδεδεμένες με το EPC δια μέσου του air interface και όχι δια μέσου IP.

φεμτοκυψέλη κατέχει μέχρι σήμερα την μικρότερη θέση, με αμέσως μεγαλύτερη αυτή των πικοκυψελών (Εικόνα 3.1).



Εικόνα 3.1: Κλίμακα φεμτοκυψέλης.

Στις Ηνωμένες Πολιτείες η Sprint Nextel ξεκίνησε τη διανομή φεμτοκυψελών το 2008, με τις Verizon και AT&T να ακολουθούν το 2009 και το 2010 αντίστοιχα. Μέσα στο 2009 πολλές εταιρείες, όπως η Vodafone, AT&T, Softbank Mobile, China Unicom, και η NTT DoCoMo, έστρεψαν το ενδιαφέρον τους προς τις φεμτοκυψέλες και ανακοίνωσαν την εμπορική εκμετάλλευση της τεχνολογίας αυτής μέσα στα κινητά τους δίκτυα [53].

3.1 Ορισμός φεμτοκυψέλης

Οι φεμτοκυψέλες είναι οικιακοί σταθμοί βάσης Home Node B (HNB) χαμηλής ισχύος και χαμηλού κόστους, ή ασύρματα σημεία πρόσβασης FAP's (Femto Access Points) όπως αναφέρονται συχνά, λειτουργούν σε εξουσιοδοτημένο φάσμα συχνοτήτων και παρέχουν κάλυψη από 10 έως 30 μέτρα σε μια οικία. Η κυψελοειδής αυτή βάση τοποθετείται στο χώρο του χρήστη και συνδέεται με τον πάροχο του υπάρχοντος δικτύου μέσω καλωδίωσης, οπτικών ινών ή ευρυζωνικής σύνδεσης DSL[3]. Βοηθάει στην αποσυμφόρηση της μακροκυψέλης και στην μεγιστοποίηση του διαθέσιμου εύρους ζώνης. Μπορεί να υποστηρίξει έως 4 ενεργά κινητά τηλέφωνα για ένα οικιακό δίκτυο και έως 16 ενεργά κινητά τηλέφωνα για ένα επιχειρησιακό δίκτυο. Τα πρότυπα που υποστηρίζει είναι ποικίλα όπως GSM, UMTS, WCDMA, CDMA2000, OFDMA, WiMAX και LTE.

[3] Όλες οι τεχνολογίες DSL περιγράφονται από τον γενικό όρο xDSL.

Τα Femtocells είναι μια μικρογραφία των αντίστοιχων μακροκυψελωτών σταθμών βάσης (Macro Base Stations). Οι μακροκυψέλες τοποθετούνται συνήθως σε ιστούς ή σε στέγες κτιρίων, έτσι ώστε να μην παρεμποδίζεται η λειτουργία τους από εμπόδια καθώς καλύπτουν την μεγαλύτερη περιοχή κάλυψης σε ένα δίκτυο κινητής τηλεφωνίας.

Παρακάτω εντοπίζονται και παρουσιάζονται οι βασικές διαφορές των δύο κυψελωτών τεχνολογιών (Πίνακας 3.1).

	Femtocell	Macrocell
Air Interface	Telecommunication standard	Telecommunication standard
Backhaul	Broadband Internet	Telephony network
Cost	$200/year	$60,000/year
Cell phone Power consumption	low	high
Radio Range	10-15 meters	300-2000 meters

Πίνακας 3.1: Διαφορές φεμτοκυψέλης - μακροκυψέλης.

3.2 Λειτουργίες φεμτοκυψέλης

Όταν ο χρήστης εισέρχεται στην οικία του ή στο χώρο εργασίας του ο οποίος καλύπτεται από την φεμτοκυψέλη, αυτόματα όλες οι κινητές συσκευές του συγχρονίζονται και όλη η τηλεπικοινωνιακή κίνηση (φωνής, δεδομένων), ελέγχεται από το σταθμό βάσης της φεμτοκυψέλης. Παράλληλα η μακροκυψέλη ενημερώνεται ότι η κάλυψη του χρήστη γίνεται από την φεμτοκυψέλη και του οικιακού ISP δικτύου. Με αυτόν τον τρόπο αποδεσμεύονται πόροι οι οποίοι χρησιμοποιούνται από άλλους εξωτερικούς χρήστες της μακροκυψέλης. Για να γίνει αυτό θα πρέπει η κάθε συσκευή όταν εισέρχεται στην εμβέλεια της φεμτοκυψέλης, να εγγράφεται στην υπηρεσία της. Αντίστοιχα όταν η συσκευή απομακρύνεται και βρεθεί εκτός εμβέλειας, εξυπηρετείται και πάλι από την μακροκυψέλη. Στην περίπτωση που οι συσκευές του χρήστη είναι περισσότερες από αυτές που μπορεί να υποστηρίξει η φεμτοκυψέλη, τότε εξυπηρετούνται οι εγγεγραμμένες συσκευές και οι υπόλοιπες που

αποτυγχάνουν να εγγραφούν συνεχίζουν να εξυπηρετούνται από τη δημόσια μακροκυψελωτή βάση. Ο χρήστης μπορεί να ειδοποιείται μέσω κατάλληλης διεπαφής χρήστη (User Interface) και σχετικού μηνύματος από το δίκτυο της εταιρίας όταν εγγράφεται στην υπηρεσία της φεμτοκυψέλης. Τα πρώτα σημεία ζωής της ύπαρξης της φεμτοκυψέλης γίνεται κατόπιν αιτήματος στον πάροχο του δικτύου μέσω μιας ασφαλούς σύνδεσης IPsec όπως θα δούμε και παρακάτω, και ενεργοποιούνται οι εργοστασιακές ρυθμίσεις της συσκευής. Σε αυτό το σημείο είναι σημαντικό να αναφερθούν οι πολιτικές πρόσβασης στην υπηρεσία της φεμτοκυψέλης (Εικόνα 3.2).

3.2.1 Πολιτικές Πρόσβασης

1. Πολιτική Πρόσβασης Ανοιχτού Τύπου (Open Access)

Με την πολιτική πρόσβασης ανοιχτού τύπου, όλοι οι χρήστες που εισέρχονται στην εμβέλεια της φεμτοκυψελωτής βάσης έχουν δικαίωμα στην εγγραφή και την χρησιμοποίηση των υπηρεσιών της. Οι χρήστες επιλέγουν τη σύνδεσή τους με την κυψέλη με το ισχυρότερο σήμα. Θέματα ασφάλειας προκύπτουν κατά την εφαρμογή της πολιτικής αυτής, καθώς και μειώνεται η απόδοση του Femtocell λόγο διαμοιρασμού των πόρων σε πολλούς χρήστες.

2. Πολιτική Πρόσβασης Κλειστού Τύπου (Closed Access ή Closed Subscriber Group - CSG)

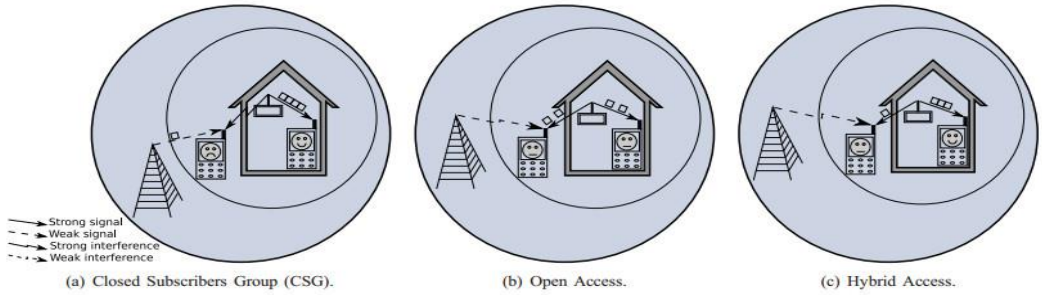
Με την πολιτική πρόσβασης κλειστού τύπου, μόνον οι χρήστες που είναι εγγεγραμμένοι έχουν το δικαίωμα σύνδεσης σε αυτήν. Δηλαδή μια CSG Femtocell διατηρεί μια λίστα ελέγχου πρόσβασης των ταυτοτήτων (IMSIs) που επιτρέπονται να συνδεθούν [17]. Η χρησιμοποίηση αυτού του τύπου πολιτικής είναι και η πιο διαδεδομένη ειδικά σε οικίες και από θέμα ασφάλειας αποτρέπει κακόβουλους χρήστες να συνδέονται διασφαλίζοντας την ιδιωτικότητα των χρηστών.

3. Πολιτική Πρόσβασης Υβριδικού Τύπου (Hybrid Access)

Με την πολιτική πρόσβασης υβριδικού τύπου, οι εγγεγραμμένοι χρήστες που είναι συνδρομητές κλειστού τύπου (CSG) έχουν προτεραιότητα και πλήρη πρόσβαση στην υπηρεσία της φεμτοκυψέλης, ενώ διατίθεται και ένα μέρος των πόρων της σε χρήστες ανοικτού τύπου όπως περιγράφηκε παραπάνω, οι οποίοι έχουν περιορισμένη

πρόσβαση. Οι πόροι προς ανάθεση δεν πρέπει να επηρεάζουν την ποιότητα των υπηρεσιών [42][50].

Η πολιτική πρόσβασης κλειστού τύπου προτιμάται από οικιακούς χρήστες, ενώ η πολιτική πρόσβασης ανοιχτού τύπου χρησιμοποιείται κυρίως στον επιχειρηματικό τομέα, όπου η συχνή μετακίνηση ανάμεσα σε διαφορετικά δίκτυα είναι πιο συχνή. Τέλος η πολιτική πρόσβασης υβριδικού τύπου, προσπαθεί να συγκεντρώσει τα θετικά στοιχεία των δύο προαναφερθέντων πολιτικών προς όφελος της απόδοσης.



Εικόνα 3.2: Πολιτικές πρόσβασης Femtocells, (a) Closed (b) Open (c) Hybrid.

Μια απειλή σχετική με τις πολιτικές πρόσβασης κάνει εφικτή την αλλαγή μιας πολιτικής με κάποια άλλη, συνήθως επιχειρείται η αλλαγή της κλειστής πολιτικής (CSG), σε πολιτική ανοιχτής ή υβριδικής πρόσβασης [21].

Στη συνέχεια δίνονται οι λόγοι που η τεχνολογία της φεμτοκυψέλης κερδίζει το εμπορικό ενδιαφέρον όλο και περισσότερων παρόχων κινητής τηλεφωνίας, αναδεικνύοντας τα πλεονεκτήματα της συγκεκριμένης κυψελωτής τεχνολογίας έναντι των μεγάλων κυψελών αλλά και των υπόλοιπων μικρών κυψελών.

3.3 Πλεονεκτήματα Φεμτοκυψέλης από τη πλευρά των χρηστών

Ολοένα και περισσότεροι χρήστες/συνδρομητές ζητούν και κλείνουν συμβόλαια με τις εταιρίες των παρόχων για εγκατάσταση φεμτοκυψελών στον χώρο τους, καθώς αντιλαμβάνονται τα πολλά πλεονεκτήματα που προσφέρουν στα εξελισσόμενα

τεχνολογικά πρότυπα αλλά και των μικροσυσκευών (δυνατότητες υλικού και λογισμικού) που συνεχώς βελτιώνονται, προτρέποντας τον μέσω χρήστη για ποιοτικές υπηρεσίες.
Τα σημαντικότερα από αυτά τα οφέλη αποτυπώνονται παρακάτω [51]:

- Προσφέρει μεγαλύτερο εύρος ζώνης, γιατί η επαναχρησιμοποίηση του διαθέσιμου φάσματος είναι μεγαλύτερη.
- Άρα και καλύτερη κάλυψη.
- Μεγαλύτερη χωρητικότητα.
- Υψηλότεροι ρυθμοί μετάδοσης δεδομένων στον χρήστη.
- Χαμηλότερη ισχύς εκπομπής.
- Μεγαλύτερη αυτονομία της μπαταρίας.
- Μεταφερισιμότητα σε άλλο χώρο ακόμα και εκτός κατοικίας.
- Μεγαλύτερους χρόνους αναμονής και ομιλίας.
- Υψηλότερη αναλογία σήματος προς θόρυβο και παρεμβολή (SINR).
- Χαμηλό κόστος που σταδιακά μειώνεται.
- Δυνατότητα αυτόματης ενημέρωσης ρυθμίσεων και αναβαθμίσεων.
- Καινούριες καινοτόμες εφαρμογές.
- Μεγαλύτερη συμβατότητα συσκευών.
- Απλή εγκατάσταση του εξοπλισμού (Plug and Play).
- Δυνατότητες αυτορρύθμισης (Self-Ρύθμιση), αυτοβελτίωσης (Self-Optimization) αυτό-τροφοδότησης (Self-Provisioning) και Self-Healing.
- Έλεγχος προσβασιμότητας χρηστών.

Το μειονέκτημα της μακροκυψέλης η οποία χάνει ένα ποσοστό της ισχύς που εκπέμπει προσκρούοντας σε τοίχους και εμπόδια κτιρίων γίνεται πλεονέκτημα και απόλυτα επιθυμητό στην περίπτωση της φεμτοκυψέλης για την καλύτερη κάλυψη εσωτερικά μιας οικίας, με την επίτευξη της μειωμένης εκπομπής προς τα έξω.

3.4 Πλεονεκτήματα Φεμτοκυψέλης από τη πλευρά των παρόχων

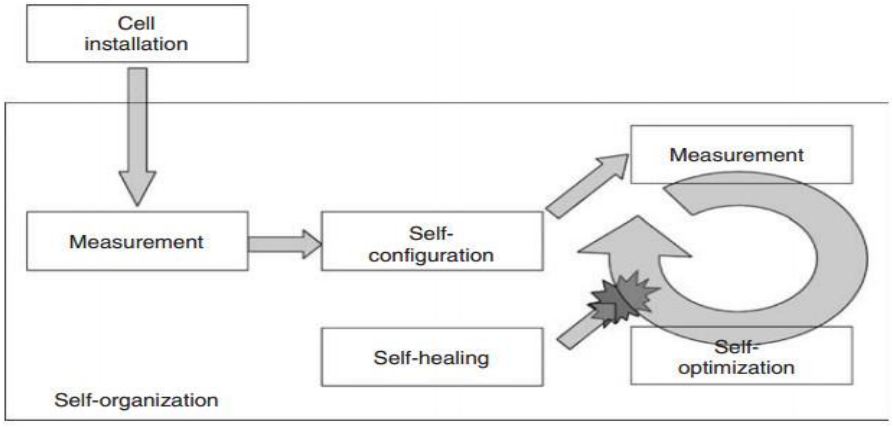
Από την πλευρά τους οι πάροχοι επωφελούνται από πολλά θετικά στοιχεία που παρουσιάζονται παρακάτω και επιτυγχάνοντας αξιόπιστες και ποιοτικές υπηρεσίες, οι ευχαριστημένοι συνδρομητές αυξάνονται και μαζί με την αύξηση αυτή προβλέπεται και μεγαλύτερη αύξηση του κέρδους από την πλευρά των εταιριών [51][31].

- Η αύξηση της φασματικής απόδοσης περιοχής.
- Αποσυμφόρηση της κυκλοφορίας δεδομένων από τα Macrocell Base Stations (BSs).
- Βελτιωμένη αξιοπιστία των Macrocells και αύξηση της χωρητικότητας.
- Μείωση του κόστους του δικτύου των υποδομών (μείωση των Base Stations)
- Αύξηση εσόδων.
- Λειτουργούν σε εξουσιοδοτημένο φάσμα συχνοτήτων.
- Ευκολότερος τρόπος διαχείρισης και χρέωσης.
- Self Organizing Networks (SONs).
- Ανταγωνισμός με άλλες τεχνολογίες.
- Μείωση για ανάγκη περισσότερων μακροκυψελωτών βάσεων.
- Καλύτερη ποιότητα υπηρεσιών.

3.4.1 Self Organizing Network

Σημαντικό χαρακτηριστικό των Femtocells είναι η δυνατότητα τους για αυτορρύθμιση (Auto-Configuring), κάτι που το 3GPP αποκαλεί αυτο-οργανούμενο δίκτυο (Self Organizing Network - SON), (Εικόνα 3.3). Το δίκτυο θα πρέπει να είναι σε θέση να επιτελεί αυτόματα μέσω κατάλληλων εφαρμογών, λειτουργίες και παραμετροποιήσεις. Διαδικασίες όπως αυτόματη εγγραφή (Registration), επαλήθευση ταυτότητας (Authentication), διαχείριση και προμήθευση (Management and Provisioning), ανακάλυψη γειτόνων (Neighbor Discovery), συγχρονισμό, επιλογή ID κυψέλης και βελτιστοποίησης δικτύου, αυτόματο κλείσιμο και άνοιγμα των σταθμών βάσης για εξοικονόμηση ενέργειας, αυτόματη επιλογή καναλιού και ρύθμιση ισχύος, ενημέρωση των χρηστών, είναι κάποιες από αυτές που είναι απαραίτητες

λόγο της μη άμεσης πρόσβασης του παρόχου στη συσκευή για βελτιώσεις και αλλαγή παραμέτρων [24][53].



Εικόνα 3.3: Self Organizing Network - SON.

3.4.2 Γεωγραφικό Στίγμα Φεμτοκυψέλης

Ο πάροχος πρέπει να γνωρίζει ανά πάσα στιγμή την ακριβή θέση της φεμτοκυψέλης, καθώς οι συχνότητες στις οποίες εκπέμπει πρέπει να είναι οι προβλεπόμενες και οι νόμιμες. Έξω από αυτές τις συχνότητες ο πάροχος δεν έχει δικαίωμα να εκπέμψει. Σε μερικές χώρες το φάσμα που χρησιμοποιείται είναι διαφορετικό και για αυτό το λόγο μια φεμτοκυψέλη δεν μπορεί να λειτουργήσει παρά μόνο μέσα στα εθνικά της σύνορα. Για την γνωστοποίηση της ακριβούς θέσης, δηλαδή των γεωγραφικών συντεταγμένων, χρησιμοποιείται κυρίως η τεχνική του Global Positioning System (GPS), οι διευθύνσεις IP αλλά και η λίστα των κοντινών γειτονικών κυψελών (μακροκυψέλες). Το GPS χρησιμοποιείται ακόμα σε περίπτωση κάποιας επείγουσας κλήσης. Σε περίπτωση που η φέμτο-βάση έχει μεταφερθεί σε κάποια άλλη χώρα, τότε και οι υπηρεσία έκτακτης ανάγκης παρουσιάζει πρόβλημα λειτουργίας. Θέματα ασφάλειας και επιθέσεων προκύπτουν και για τις τρείς αυτές τεχνικές. Για την μέθοδο του GPS ο επιτιθέμενος χρησιμοποιεί Jammers (συσκευές χαμηλού κόστους), για να μπλοκάρει το GPS σήμα και να ξεγελάσει το Femtocell (Εικόνα 3.4), ενώ αντίστοιχες τεχνικές επιθέσεων ακολουθούνται και στις άλλες δύο περιπτώσεις με απώτερο

σκοπό να "πείσουν" την φέμτο-βάση ότι εκπέμπει στην σωστή τοποθεσία [4]. Ακολουθεί αναλυτικότερη περιγραφή των τριών μεθόδων [21]:

- **Διεύθυνση IP**

  Το Femtocell μόλις συνδεθεί με το υπάρχον δίκτυο του χρήστη (DSL), του ανατίθεται μια IP διεύθυνση με την οποία σε συνδυασμό με στοιχεία αυθεντικοποίησης, ο πάροχος μπορεί να εντοπίσει. Τα δεδομένα της τοποθεσίας της συσκευής με τη χρήση της IP, αποθηκεύονται στον Access point Home Register (AHR) Server. Η μέθοδος αυτή δεν είναι αρκετή για τον πλήρη και σίγουρο εντοπισμό της πραγματικής τοποθεσίας, καθώς επιτιθέμενοι μπορούν να δίνουν λανθασμένο στίγμα για το Femtocell, κάνοντας χρήση εσφαλμένων Proxy Servers.

- **Γειτονικές Μακροκυψέλες**

  Η φεμτοκυψέλη μπορεί να δέχεται πληροφορίες από γειτονικές μακροκυψέλες, όπως PLMN ID (Public Land Mobile Network Identity), LAI (Location Area Identity), ή αναγνωριστικό κυψέλης (Cell ID). Διαθέτει ένα κομμάτι υλικού (chip), με το οποίο σαρώνεται η περιοχή και συλλέγονται οι πληροφορίες που στη συνέχεια αποστέλλονται στο AHR (Home Register of HNB). Για την σάρωση χρησιμοποιείται υλικό δέκτη τεχνολογίας 2G, καθώς τα 3G σήματα παρουσιάζουν αδυναμία σε κλειστούς χώρους [21].

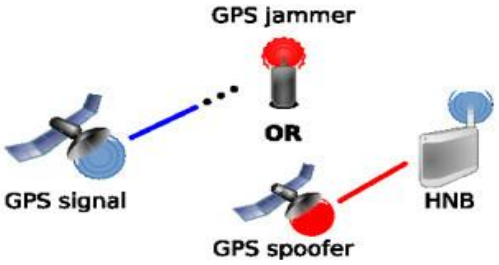
- **GPS**

  Η πληροφορία θέσης μπορεί να ληφθεί χρησιμοποιώντας ένα δέκτη A-GPS[5] (Assisted GPS) ενσωματωμένο στο Femtocell, το οποίο με τη σειρά του μπορεί να λάβει τις πληροφορίες θέσης από τη μονάδα A-GPS και να τις μεταβιβάσει στο AHR για επαλήθευση. Ωστόσο, είναι σημαντικό η εγκατάσταση της φέμτο-βάσης να γίνεται σε μια θέση όπου είναι δυνατόν να ληφθούν δορυφορικά σήματα GNSS (Global Navigation Satellite Systems). Ακόμα GPS πληροφορίες θέσης μπορούν να ληφθούν και από τις τερματικές συσκευές των χρηστών (UE) αν το υποστηρίζουν.

[4] Τοποθεσία που ο επιτιθέμενος έχει ορίσει.

[5] Είναι ένα σύστημα που χρησιμοποιείται για να βελτιώσει την απόδοση εκκίνησης του δορυφορικού συστήματος εντοπισμού θέσης GPS.

Ο διαχειριστής του Femtocell πρέπει να κλειδώσει τη βάση σε μια συγκεκριμένη γεωγραφική θέση για τους ακόλουθους λόγους: 1) για να παρέχει στους χρήστες την δυνατότητα για κλήσεις έκτακτης ανάγκης, 2) να εξασφαλιστεί ότι το Femtocell λειτουργεί σε μια χώρα στην οποία έχει δικαιώματα εκπομπής και λήψης, 3) επαλήθευση της άδειας του φάσματος συχνοτήτων 4) και να παρέχει δεδομένα σε πραγματικό χρόνο για νόμιμη παρακολούθηση της κίνησης των χρηστών από κυβερνητικές υπηρεσίες [16][21].



Εικόνα 3.4: GPS Jammer.

3.5 Μειονεκτήματα και Τεχνικές Δυσκολίες Φεμτοκυψέλης

Πέρα από τα εμφανή πλεονεκτήματα που προσφέρουν στον χρήστη αλλά και στο ίδιο το υπάρχον δίκτυο, οι φεμτοκυψέλες έχουν να αντιμετωπίσουν και κάποια μειονεκτήματα τα οποία έχουν απασχολήσει και χρήζουν την προσοχή για επίλυση. Οι παρεμβολές μεταξύ μιας φεμτοκυψέλης και μιας μακροκυψέλης, ή ακόμα και ανάμεσα σε δύο φεμτοκυψέλες, είναι ένα θέμα που λόγο χρησιμοποίησης της ίδιας συχνότητας και του εύρους ζώνης αποτελεί ένα σημαντικό πρόβλημα. Οι μη εγγεγραμμένοι χρήστες, πρόσβασης κλειστού τύπου όπως είδαμε και παραπάνω, μπορούν να δέχονται ή και να δημιουργούν παρεμβολές από και προς τις κοντινές φεμτοκυψέλες λόγω του ότι δεν έχουν δικαίωμα σύνδεσης και λόγω της διαφοράς στην ισχύ της μακροκυψέλης με αυτήν της φεμτοκυψέλης όταν πλησιάζουν και εισέρχονται στην εμβέλεια της. Στην περίπτωση της πρόσβασης ανοιχτού τύπου που επίσης έγινε λόγος παραπάνω, δεν δημιουργούνται παρεμβολές όπως με τις παρεμβολές του κλειστού τύπου καθώς ο κάθε χρήστης έχει δικαίωμα να εγγραφεί στη φεμτοκυψέλη. Παρόλα αυτά, νέα μειονεκτήματα παρουσιάζονται στην ανοιχτού τύπου πρόσβασης. Ο κάτοχος της φεμτοκυψέλης χρεώνεται για την υπηρεσία που του

προσφέρεται με την εγκατάσταση της, με αποτέλεσμα να μην θέλει να τη μοιράζεται με μη εγγεγραμμένους χρήστες. Οι μεταπομπές είναι πολύ πιο συχνές ανάμεσα στην φεμτοκυψέλη και στις εξωτερικές μακροκυψέλες, με την πιθανότητα της αποτυχημένης μεταπομπής να αυξάνεται λόγω του φόρτου του δικτύου και των μη ενημερωμένων λιστών των υπόλοιπων χρηστών που προσπαθούν παράλληλα για μια θέση στον ενεργό κατάλογο της φεμτοκυψέλης. Χρήστες που κινούνται με μεγάλες ταχύτητες στα όρια της φεμτοκυψέλης, δεν είναι επιθυμητό να κάνουν μεταπομπή σε αυτή αλλά να συνεχίσουν να εξυπηρετούνται από την μακροκυψέλη. Κάποιες διαφορές των δύο τρόπων πρόσβασης στην φεμτοκυψέλη δίνονται επιγραμματικά στον παρακάτω πίνακα (Πίνακας 3.2).

Κλειστή Πρόσβαση	Ανοιχτή Πρόσβαση
Υψηλότερες παρεμβολές	Περισσότερες μεταπομπές
Χαμηλότερη ρυθμαπόδοση συστήματος	Υψηλότερη ρυθμαπόδοση συστήματος
Εξυπηρέτηση μόνο των εσωτερικών χρηστών (indoor users)	Αύξηση χωρητικότητας εξωτερικών χρηστών (increased outdoor capacity)
Home Market	SMEs (Small to Medium – sized Enterprises offices) hotspots
Ευκολότερη τιμολόγηση	Τίθενται θέματα ασφάλειας

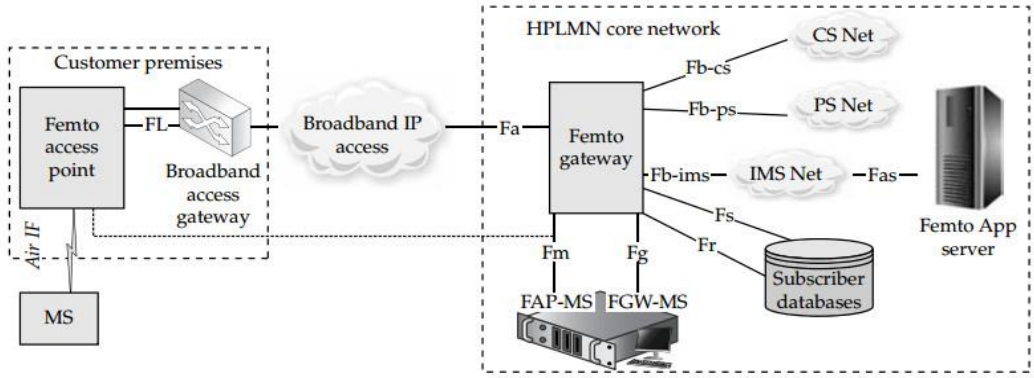
Πίνακας 3.2: Σύγκριση ανοιχτού και κλειστού τύπου πρόσβασης [42].

Το πρόβλημα των παρεμβολών των Cross-tier παρεμβολών [6] ή των Co-tier παρεμβολών, [7] μπορεί να επιλυθεί με την μείωση της εκπομπής ισχύος της φεμτοκυψέλης, προσαρμοζόμενη ανά περίπτωση (δυνατότητα αυτορρύθμισης και αυτοβελτίωσης) είτε πρόκειται για παρεμβολές με τις μακροκυψέλες, είτε για παρεμβολές με κοντινές φεμτοκυψέλες. Γενικά θα λέγαμε πως η καλύτερη μέθοδος προς αποφυγή του προβλήματος των παρεμβολών, είναι η ικανότητα του Femtocell για σωστό και ορθολογικό καταμερισμό των πόρων, καθώς και ο έλεγχος του περιβάλλοντος στο οποίο προσαρμόζεται [35].

[6] Παρεμβολών ανάμεσα σε ένα femtocell και ένα macrocell.
[7] Παρεμβολών ανάμεσα σε ένα femtocell με γειτονικά femtocell.

3.6 Αρχιτεκτονικές Ασφάλειας Φεμτοκυψελών

Στη συνέχεια περιγράφονται οι αρχιτεκτονικές φεμτοκυψελών για τις διάφορες κινητές ασύρματες τεχνολογίες σε λειτουργία σήμερα. Η τεχνολογία των Femtocell μπορεί να χρησιμοποιηθεί για τις περισσότερες, εάν όχι όλες τις κινητές ασύρματες τεχνολογίες, συμπεριλαμβανομένου των GSM, UMTS, CDMA, WiMax και LTE. Για τον λόγο αυτό το Femto Forum[8] έχει δημιουργήσει ένα μοντέλο αναφοράς (Εικόνα 3.5) το οποίο εφαρμόζεται σε όλα τα είδη τεχνολογιών Femtocell.



Εικόνα 3.5: Σημεία αναφοράς ενός Femtocell όπως ορίζεται από το Femto Forum.

Ακολουθεί μια περιγραφή των κύριων συστατικά που υπάρχουν σε ένα Femtocell δίκτυο και τα σημεία αναφοράς τους και στη συνέχεια δίνονται δύο παραδείγματα υλοποίησης φεμτοκυψέλης.

1. **Femto Access Point (FAP)**

   Το FAP είναι μια συσκευή (όπως ένα Router), τοποθετημένη στο χώρο του χρήστη που επικοινωνεί με τις κινητές συσκευές δια μέσου ασύρματης διεπαφής. Το FAP εμφανίζεται σε μια κινητή συσκευή ως μια κοινή Macrocell βάση, με όμως πολύ μικρότερη κατανάλωση ενέργειας και επικοινωνεί με το κεντρικό δίκτυο κινητών (Core Mobile Network) δια-μέσου μιας Broadband διεπαφής όπως καλωδίωσης, οπτικών ινών ή DSL. Μπορεί να υποστηρίξει

[8] Μη-κερδοσκοπική οργάνωση που ιδρύθηκε το 2007 για την προώθηση της ανάπτυξης Femtocell και των υπηρεσιών της σε όλο τον κόσμο και συνεργάζεται με οργανισμούς τυποποίησης όπως 3GPP, 3GPP2 και το Broadband Forum. Σήμερα φέρει την ονομασία Small Cell Forum (SCF). www.femtoforum.org/. [A9].

έναν ποικίλο αριθμό κινητών συσκευών, χαρακτηριστικά από τέσσερα για μια οικία και ως οκτώ για τις μικρές επιχειρήσεις. Η χρησιμοποίηση του FAP για να προσπελάσουμε το κινητό δίκτυο, βελτιώνει σημαντικά την εσωτερική κάλυψη και τη διαθεσιμότητα του εύρους ζώνης για τις φορητές συσκευές.

2. **Femto Gateway (FGW)**

   Το Femto Gateway επικοινωνεί με το FAP μέσω της Broadband σύνδεσης και εκτελεί μετατροπές σηματοδοσίας πρωτοκόλλων (Signaling Protocol), αλλά και λειτουργίες ασφάλειας (Security Gateway), αυθεντικοποίησης και καταχώρηση της συσκευής, προστατεύοντας το διαχειριστή του δικτύου κινητής τηλεφωνίας Mobile Network Operator (MNO) από προσπάθειες επιθέσεων δια μέσου του δημόσιου Broadband δικτύου στο σημείο Fa του παραπάνω σχήματος. Το FGW διασυνδέεται με τα διάφορα τμήματα των MNO ανάλογα με το αν πρόκειται για Circuit-Switched δίκτυο και υπηρεσίες όπως εφαρμογές πραγματικού χρόνου (σημείο Fb-cs) (Real-Time Applications), ή για Packet-Switched δίκτυο και εφαρμογές όπως μηνύματα και e-mails (σημείο Fb-ps). Ακόμα το σημείο Fb-ims στο σχήμα χρησιμοποιείται από το FGW για την επικοινωνία με το κεντρικό IMS[9] δίκτυο.

3. **Subscriber Databases**

   Οι βάσεις δεδομένων των συνδρομητών χρησιμοποιούνται για την αποθήκευση πληροφοριών (FAP Identity και ρυθμίσεις για την τροφοδότηση του FAP) που απαιτούνται για την παροχή υπηρεσιών. Το Femto Gateway αποκτά πρόσβαση στη βάση των συνδρομητών δια μέσου των διεπαφών Fs και Fr.

4. **Femto Management System**

   Το Femto Management System χρησιμοποιείται για την διαχείριση της FAP συσκευής (FAP-MS) μέσω της διεπαφής Fm και την διαχείριση των Femto Gateway συσκευών (FGW-MS) μέσω της διεπαφής Fg. Παρέχει τις απαιτούμενες ενημερωμένες εκδόσεις λογισμικού για το Femtocell και μπορεί να βρίσκονται μέσα στο κεντρικό δίκτυο του παρόχου.

5. **Femto Application Server**

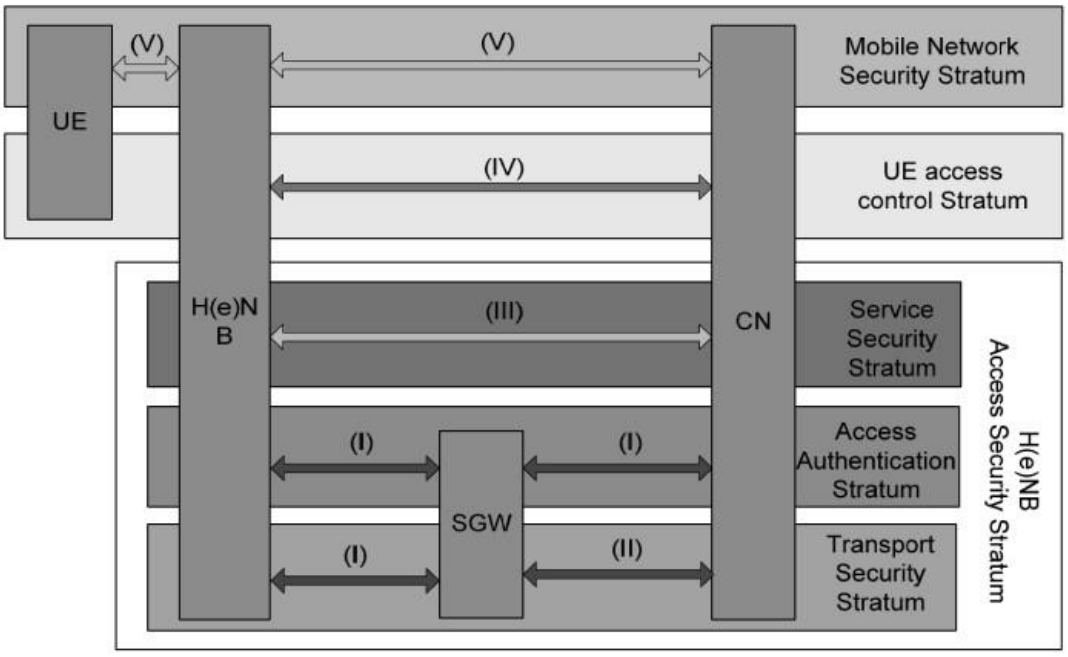
[9] Η διεπαφή IMS χρησιμοποιείται για να μετατρέψει την κίνηση του χρήστη σε μεταγωγής πακέτων (packet switched) Voice Over IP (VoIP).

Το σημείο αναφοράς για το Femto Application Server είναι το Fas και αποτελεί την διεπαφή προς ένα IMS δίκτυο.

Τα παραδείγματα που ακολουθούν περιγράφουν το UMTS Femtocell ή αλλιώς Home NodeB (HNB) και το LTE Femtocell ή αλλιώς Home eNodeB (HeNB). Οι συσκευές των χρηστών (κινητά τηλέφωνα, προσωπικοί υπολογιστές κ.α.), θα πρέπει να υποστηρίζονται από 3G τεχνολογία για να υποστηρίξουν τα παραπάνω πρότυπα. Ο λόγος που επιλέχτηκαν είναι γιατί η στροφή προς τα 3G δίκτυα είναι μεγάλη και οι χρήστες αν και δειλά στην αρχή, αρχίζουν και δείχνουν την προτίμησή τους έναντι των 2G τεχνολογιών.

Η γενική δομή της αρχιτεκτονικής ασφάλειας μιας φεμτοκυψέλης παρουσιάζεται παρακάτω στην Εικόνα 3.6, ξεχωρίζοντας τις ομάδες ασφάλειας που η κάθε μια συγκεντρώνει διαφορετικές απειλές και απαιτήσεις.

Η ασφάλεια της φεμτοκυψέλης διαιρείται σε δύο μέρη, την αυθεντικοποίηση της και την ασφάλεια του μη έμπιστου σημείου (Backhaul Link) ανάμεσα στη συσκευή και το Femtocell-GW [21].



Εικόνα 3.6: Αρχιτεκτονική ασφάλειας Femtocell [4].

- **Femtocell Access Security (I)**

  Αυτή η ομάδα αποτελείται από ένα σύνολο χαρακτηριστικών ασφαλείας που περιλαμβάνει, αμοιβαία αυθεντικοποίηση μεταξύ Femtocell και του δικτύου, ασφαλή εγκατάσταση διόδου (Tunnel) μεταξύ Femtocell και του SeGW, διάφορες άδειες και τεχνικές κλειδώματος της θέσης ενός Femtocell. Επιπλέον, το SeGW εκτελεί αμοιβαία αυθεντικοποίησης ταυτότητας και αδειοδότησης προτού επιτραπεί στα Femtocells να αποκτήσουν πρόσβαση στο κεντρικό δίκτυο.

- **Network Domain Security (II)**

  Παρέχονται μέθοδοι για την ασφαλή σύνδεση με το Core Network. Το SeGW δεν συνδέεται με το κεντρικό δίκτυο μέσω του δημόσιου Internet οπότε και θεωρείται ασφαλής σύνδεση.

- **Femtocell Service Domain Security (III)**

  Εφαρμόζονται χαρακτηριστικά ασφάλειας για τη δημιουργία ασφαλούς επικοινωνίας μεταξύ Femtocell και διαφόρων στοιχείων που βρίσκεται στο κεντρικό δίκτυο. Ειδικότερα, αυτές οι μέθοδοι εξασφαλίζουν ότι το Femtocell θα πρέπει να αλληλοεπιδρά με ασφαλή τρόπο με το Operation Administration and Management (OAM) [10] Server, προκειμένου να χρησιμοποιείται η δυνατότητα αυτορρύθμισης.

- **UE Access Control Domain Security (IV)**

  Αυτή η ομάδα διαθέτει διάφορους μηχανισμούς ελέγχου πρόσβασης που απαιτούνται για την UE. Ο έλεγχος πρόσβασης βασίζεται στην λίστα CSG, που παρέχονται από το χειριστή του δικτύου και αποθηκεύονται τοπικά στο Femtocell ή στο Femtocell-GW.

- **UE Access Security Domain (V)**

  Χαρακτηριστικά ασφαλείας αυτής της ομάδας έχουν σαν στόχο την ασφάλεια της ασύρματης διεπαφής για την πρόσβαση υπηρεσιών κινητής επικοινωνίας.

3.6.1 2G Femtocells - GSM

Η τεχνολογική επικαιρότητα είναι στραμμένη στα επόμενης γενιάς δίκτυα και στην παραγωγή 3G Femtocells, όμως πολλοί χρήστες σε παγκόσμιο επίπεδο

[10] Το OAM Server είναι στοιχείο του Femtocell Management System.

χρησιμοποιούν ακόμα GSM στα δίκτυα τους. Τα στατιστικά αυτά έγιναν ο κινητήριος μοχλός για την μελέτη και ανάπτυξη μιας φεμτοκυψέλης βασισμένης στο πρότυπο του GSM. Το κόστος του GSM σε σχέση με τα σύγχρονα δίκτυα είναι εμφανώς μικρότερο και η κατασκευή GSM Femtocells ακολουθεί την ίδια φτηνή λύση ανταγωνιζόμενη τεχνολογίες όπως Voice Over WiFi ή UMA[11] (Unlicensed Mobile Access).

Παραδείγματα τέτοιων Femtocells υπήρξαν από την Σουηδική εταιρία Ericsson, κολοσσό στον χώρο των τηλεπικοινωνιών και την Hay Systems Ltd (HSL) πάροχο δικτύου της Σκωτίας [51].

Η διαφορά στο κόστος έναντι των πολλών διαφωνιών από μέλη του κλάδου που ισχυρίζονται ότι τα 2G Femtocells δεν πρέπει να αναπτυχτούν, πηγάζουν από μειονεκτήματα σε σύγκριση με τα 3G Femtocells. Για παράδειγμα, ο μηχανισμός ελέγχου ισχύος στα δίκτυα GSM δεν είναι τόσο ευέλικτος όσο αυτό του 3G και αυτό μπορεί να προκαλέσει παρεμβολές και επικάλυψη στα Macrocells. Ένας άλλος σοβαρός λόγος ειδικά σε σύγκριση με τα σημερινά πρότυπα, είναι η χαμηλή διεκπεραιωτική ικανότητα του GPRS, πράγμα που σημαίνει ότι τα 2G Femtocells δεν θα είναι σε θέση να προσφέρουν πολύ περισσότερα, πέρα από μια υψηλή ποιότητα στις υπηρεσίες φωνής.

Το πρότυπο του GSM Femtocell κατά την διαδικασία της αυθεντικοποίησης χρησιμοποιεί την μέθοδο EAP-SIM και διαπιστευτήρια (Certificates) που αναλύεται παρακάτω.

3.6.2 3G Femtocells - UMTS

Η ανάπτυξη των 3G Femtocells ή αλλιώς Home NodeB (HNB) όπως αναφέρονται συχνά, είχαν περισσότερο χρόνο για προετοιμασία πριν αποφασιστεί η προώθηση τους στην αγορά (Release 8, 9), αλλά και καλύτερα χαρακτηριστικά και δυνατότητες τα οποία ενσωματώθηκαν στα Femtocells, με τα κινητά δίκτυα IP να παίζουν καθοριστικό ρόλο στην υλοποίηση τους. Η αρχιτεκτονική του UMTS Femtocell, φαίνεται στην Εικόνα 3.7 και είναι σύμφωνη με τη γενική μορφή της αρχιτεκτονικής του Femto Forum που είδαμε παραπάνω. Το HNB είναι το Femtocell που χρησιμοποιούν οι χρήστες (UE) με τη διεπαφή Uu και για να παρέχει υπηρεσίες

[11] Η αλλιώς Generic Access Network (GAN). Αρχικά είχε σχεδιαστεί για να επιτρέπει την επικοινωνία κινητού τηλεφώνου μέσω του Wi-Fi, επιτρέποντας να συνδεθεί με το δίκτυο του παρόχου μέσω ενός δικτύου IP [21].

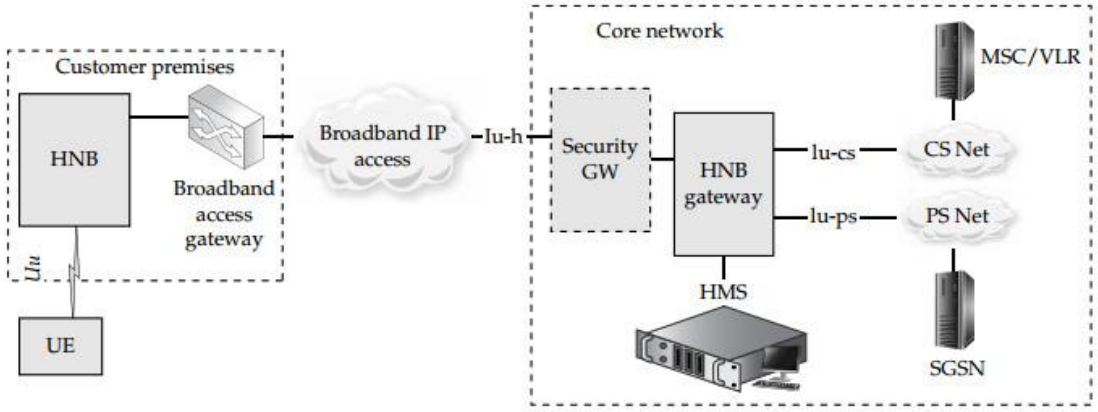
κινητής τηλεφωνίας χρησιμοποιεί τις επόμενες λειτουργίες, 3GPP σηματοδοσία (Signalling), Radio Resource Management, IP Transport functions, Quality of Service (QoS), Management functions, Firewall functions, Network Address Translation (NAT), αυτόματη λειτουργία διαμόρφωσης και λειτουργίες ασφάλειας [21]. Η διεπαφή (UE) πρέπει να υποστηρίζεται από 3G τεχνολογία και επικοινωνεί με το Femtocell κάνοντας χρήση μιας διαδικασίας 3G AKA (Authentication and Key Agreement). Η lu-h διεπαφή επικοινωνεί με το κεντρικό IP δίκτυο, μέσω μιας ασφαλούς IPsec σύνδεσης με τη χρήση του IKEv2. Η επικοινωνία αυτή γίνεται δια μέσου μιας Broadband σύνδεσης και επειδή η σύνδεση αυτή δεν θεωρείται ασφαλής, στην πλευρά του κεντρικού δικτύου ο πάροχος του κινητού δικτύου χρησιμοποιεί το Security Gateway για να προστατέψει το δίκτυο του από ανεπιθύμητες επιθέσεις (ωτακουστές, τροποποίηση της κίνησης). Πρώτα αυθεντικοποιεί με αμοιβαίο τρόπο (Mutual Authentication) τη συσκευή Femtocell με τη μέθοδο EAP-AKA και στη συνέχεια την καταχωρεί. Τα δεδομένα αυθεντικοποίησης του χρήστη βρίσκονται εσωτερικά της φεμτοκυψέλης. Το SeGW μπορεί να είναι ενσωματωμένο στο Femtocell-GW και σε περίπτωση που δεν είναι, τότε η διεπαφή ανάμεσα σε αυτά τα δύο στοιχεία γίνεται με τη χρήση του NDS/IP (Network Domain Security/IP network layer security). Η σύνδεση με το κεντρικό δίκτυο (Core Network) γίνεται με τις διεπαφές lu-cs/lu-ps. Τα στοιχεία είναι κατά αντιστοιχία τα ίδια με αυτά του προτύπου στο Femto Forum με τις παρακάτω αντιστοιχίες (Πίνακας 3.3).

Femto Forum	UMTS / LTE
MS	UE
Femto Access Point (FAP)	HNB / HeNB
Femto Gateway	Security Gateway (GW)
Femto Management Server (FMS)	HMS
HSS	Authentication, Authorization and Accounting (AAA)

Πίνακας 3.3: Αντιστοιχίες ορολογίας ανάμεσα στο πρότυπο του Femto Forum και των UMTS, LTE.

Στη συνέχεια το HNB Gateway προωθεί την αποκρυπτογραφημένη κίνηση μέσα στο Core Network. Το HNB Management System είναι ένας Server που είναι υπεύθυνο

για την διαμόρφωση και τροφοδότηση των δεδομένων του χρήστη σύμφωνα με την πολιτική του παρόχου, αλλά και για την ενημέρωση του λογισμικού του Femtocell. Ο Server AAA (Authentication, Authorization and Accounting) αυθεντικοποιεί τα δεδομένα του χρήστη που διαβάζει από το Home Subscriber Server (HSS), οντότητες που ανήκουν και οι δύο στο κεντρικό δίκτυο του παρόχου. Όπως είπαμε και στην αρχή του κεφαλαίου η φεμτοκυψέλη είναι μια μικρογραφία της μακροκυψέλης που τοποθετείται στον προσωπικό χώρο του συνδρομητή παρέχοντας του ικανοποιητική κάλυψη και ποιοτικές υπηρεσίες φωνής και δεδομένων [31].



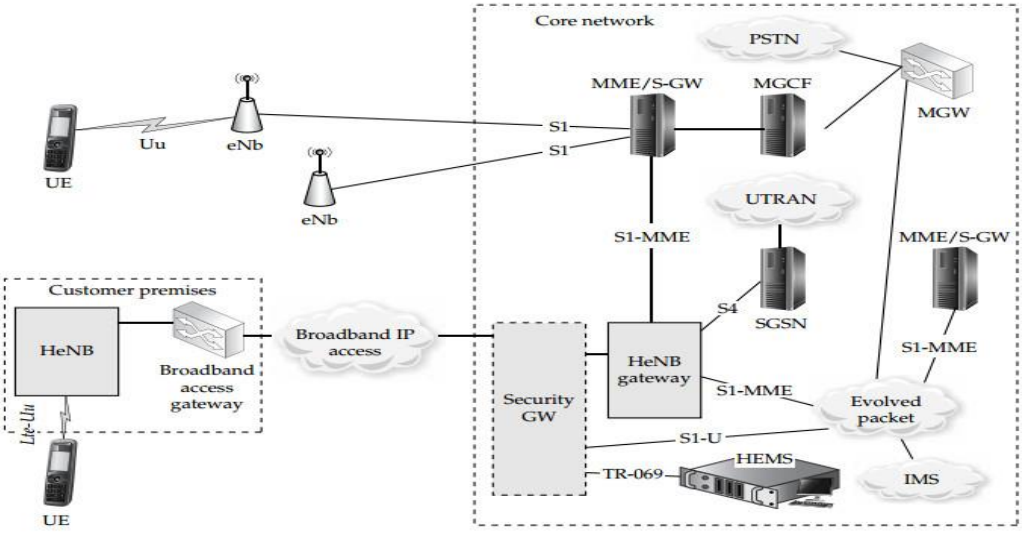
Εικόνα 3.7: Αρχιτεκτονική UMTS Femtocell Network.

3.6.3 LTE Femtocells

Το LTE είναι μια αναδυόμενη ασύρματη τεχνολογία, η οποία χαρακτηρίζεται ως η τεχνολογία της επόμενης γενιάς στο χώρο των κινητών τηλεπικοινωνιών (Next Generation Technology) και που όλο και περισσότεροι φορείς παροχής υπηρεσιών σκοπεύουν να εγκαταστήσουν στα δίκτυα τους. Το γεγονός ότι η τεχνολογία της φεμτοκυψέλης άρχισε να κάνει τα πρώτα της βήματα μετά την δημοσίευση και υλοποίηση των 3G προτύπων, αυτό είχε ως συνέπεια να μείνει εκτός από τις διαδικασίες προτυποποίησης. Αντίθετα, το πρότυπο του LTE συμπεριέλαβε τα Femtocell στην διαδικασία αυτή και η αυξανόμενη χρήση τους δείχνει την απόλυτη συμβατότητα και υποστήριξη από το LTE. Παρόλα αυτά, οι διαφορές των 3G HNB και των LTE HeNB Femtocells είναι μικρές, καθώς τα χαρακτηριστικά ασφάλειας του HNB σχηματίστηκαν παράλληλα με αυτά της ασφάλειας του EPS (LTE).

Όλα ξεκίνησαν με την έκδοση 8 (Release 8) από το 3GPP και τα πρώτα βήματα από κατασκευαστική άποψη έγιναν το 2008 από την εταιρία "picoChip" με την δημιουργία ενός μικροτσίπ που παρέπεμπε στις μέχρι τότε τεχνικές αναφορές του LTE [51]. Η δομή του δικτύου δεν διαφέρει από την δομή που παρουσιάστηκε και στο UMTS Femtocell που επίσης ακολουθεί την δομή του προτύπου του Femto Forum. Οι διαφορές επισημαίνονται στο κεντρικό δίκτυο του LTE όπως φαίνεται και στην Εικόνα 3.8.

Διανύοντας την τέταρτη γενιά κινητών επικοινωνιών (4G), βελτιώσεις σε όλα τα επίπεδα του LTE με νέες δυνατότητες και διεύρυνση των δικτύων και των υπηρεσιών προς τους συνδρομητές, προστέθηκαν και στο 4G LTE Femtocell δυνατότητες, αλλά κυρίως τρόποι αντιμετώπισης προβλημάτων, όπως αυτό των παρεμβολών με μεθόδους όπως: ο συντονισμός που βασίζεται στην οπισθόζευξη (Backhaul-Based Coordination), η δυναμική ορθογωνοποίηση (Dynamic Oorthogonalization), ο χρονοπρογραμματισμός υποζώνης (Subband Scheduling), η προσαρμοστική κλασματική επαναχρησιμοποίηση συχνοτήτων (Adaptive Fractional Frequency Reuse) και ο προσαρμοστικός έλεγχος ισχύος εκπομπής [53].



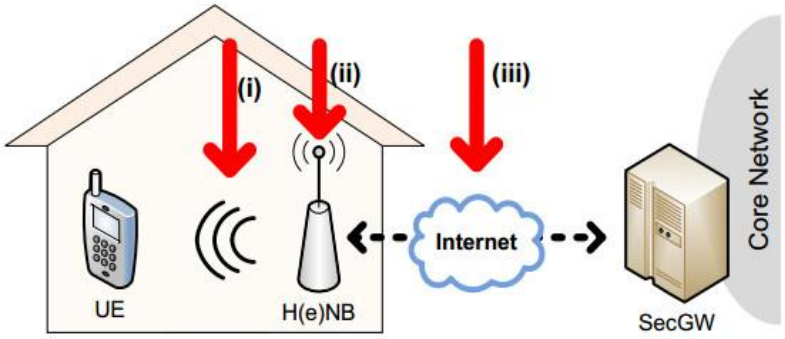
Εικόνα 3.8: Δίκτυο LTE Femtocell.

3.7 Γενικές Αρχές Ασφάλειας στα Femtocells και Επιθέσεις

Τα Femtocells όπως είδαμε και στις προηγούμενες ενότητες μπορούν να υλοποιηθούν με τη χρήση πολλών τεχνολογικά προτύπων πρόσβασης, είτε αυτά ανήκουν στα

δεύτερης γενιάς δίκτυα είτε ανήκουν σε καινούρια πρότυπα (ασύρματα και ενσύρματα) με το καθένα από αυτά να έχει τα δικά του επιπλέον στοιχεία που απαιτούνται για τα Femtocells. Οι τεχνολογίες αυτές απαριθμούν από μόνες τους προβλήματα και αδυναμίες ασφάλειας, με αποτέλεσμα η τεχνολογία της φεμτοκυψέλης να είναι ευάλωτη σε αυτές και πρέπει να λαμβάνονται υπόψιν [17].

Ένα Femtocell είναι ευάλωτο τόσο σε φυσικό επίπεδο (βλέπε Εικόνα 3.9, απειλή (i)), όσο και σε επίπεδο διαδικτύωσης με το Internet (βλέπε Εικόνα 3.9, απειλή (ii), απειλή (iii)). Αυτή η πολλαπλή προσέγγιση ενός Femtocell από τους επίδοξους επιτιθέμενους απαιτεί και την ξεχωριστή μελέτη για την διασφάλιση και προστασία των προσωπικών δεδομένων του συνδρομητή. Μεγαλύτερη επικινδυνότητα παρουσιάζεται στην ανοιχτού τύπου πρόσβασης, όπου ο κάθε χρήστης μπορεί να συνδεθεί, αυξάνοντας έτσι και τις πιθανότητες για κακόβουλες ενέργειες.



Εικόνα 3.9: Τρόποι προσέγγισης μιας φεμτοκυψέλης από επιτιθέμενους [13].

Όπως φαίνεται και στο παραπάνω σχήμα, οι απειλές ενάντια σε ένα Femtocell μπορούν να προκύψουν σε τρία διαφορετικά σημεία:

- **i.** Στην διεπαφή αέρα μεταξύ της κινητής συσκευής (Εξοπλισμός χρηστών) και το Femtocell.
- **ii.** Στο Femtocell το ίδιο.
- **iii.** Στη δημόσια σύνδεση μεταξύ Femtocell και της πύλης ασφάλειας (SecGW), επικοινωνία με το κεντρικό δίκτυο.

Κάθε σημείο της παραπάνω ανάλυσης, αποτελεί και έναν διαφορετικό τρόπο για απόσπαση πληροφοριών με τη χρήση διαφορετικών ή και συνδυασμός επιθέσεων,

κάτι που αναλύεται σε βάθος στο τέταρτο κεφάλαιο της εργασίας για την περίπτωση του LTE-Femtocell [13].

Οι ευπάθειες τις οποίες πρέπει να αντιμετωπίσει το Femtocell και οι απαιτήσεις ασφάλειας περιγράφονται παρακάτω [17]:

- **Ιδιωτικότητα και Εμπιστευτικότητα (Privacy and Confidentiality)**
  Είτε πρόκειται για επικοινωνίες φωνής, είτε δεδομένων, πρέπει να διασφαλίζεται η εμπιστευτικότητα και ιδιωτικότητα των δεδομένων του χρήστη από απειλές όπως ωτακουστών και ενεργών εισβολέων (Eavesdroppers & Active Attackers), που πρέπει να είναι ορατά μόνο στον ίδιο και όχι από τρίτους. Πρέπει να προστατεύεται το IMSI και να μην δίνεται η δυνατότητα από επιθέσεις τύπου (IMSI-Catcher Attacks)[12] να ανακτούν τα αναγνωριστικά με τη μορφή απλού κειμένου (Plaintext). Στα 3G δίκτυα αυτού του είδους η επιθέσεις είναι λιγότερο διαδεδομένες, καθώς η κινητή συσκευή επαληθεύει την ταυτότητα του φορέα δικτύου. Η προσπέλαση των δεδομένων του συνδρομητή από το Femto Gateway πρέπει να προστατεύεται καθώς το Femtocell είναι συνδεδεμένο στο τοπικό δίκτυο στο χώρο του χρήστη. Η νόμιμη παρακολούθηση (Lawful Interception) αποτελεί εξαίρεση [17].
- **Ακεραιότητα (Integrity)**
  Η οποιαδήποτε πληροφορία, πρέπει να διασφαλίζεται ως έχει και να μην μπορεί να τροποποιηθεί από κακόβουλες ενέργειες και μη εγγεγραμμένους χρήστες.
- **Διαθεσιμότητα υπηρεσίας (Service Availability)**
  Το δίκτυο πρέπει να είναι σε θέση να είναι διαθέσιμο στους συνδρομητές προσφέροντας τους υπηρεσίες. Όταν αυτό παραβιάζεται, οι συνδρομητές δεν μπορούν να συνδεθούν στο Femtocell. Επιθέσεις που πετυχαίνουν κάτι τέτοιο είναι γνωστές ως Denial of Service (DoS).

  Οι DoS επιθέσεις που προορίζονται για ένα femtocell μπορούν να υποδιαιρεθούν σε δύο κατηγορίες:
  - Επιθέσεις DoS προς το συνδρομητή

[12] Επιθέσεις ενάντια σε GSM δίκτυα. Πρόκειται για μια ανάμιξη υλικού και λογισμικού με σκοπό να υποδυθούν μια έγκυρη βάση του δικτύου και την υποκλοπή των IMSI των υποψήφιων θυμάτων.

Οι DoS επιθέσεις προς το συνδρομητή είναι δυνατόν, μπλοκάροντας οποιαδήποτε εισερχόμενη ή εξερχόμενη μετάδοση δεδομένων σε ένα Femtocell. Μια άλλη μέθοδος για να εκτελεστεί μια επίθεση DoS είναι η αποστολή ακατάλληλων πακέτων στις συσκευές με σκοπό να θέσουν σε κίνδυνο τη στοίβα Base-Band. Η διεργασία αυτή ονομάζεται Fuzzing, η οποία συνήθως υλοποιείται στα πολύ χαμηλά στρώματα πρωτοκόλλου. Περισσότερο επιρρεπής στην απειλή αυτή είναι το GSM, καθώς στο UMTS δεν έχει σημειωθεί κάτι τέτοιο [17]. Μια άλλη DoS απειλή που είναι εφικτή στο GSM, χρησιμοποιεί πλαστό IMSI με συνέπεια το δίκτυο να θεωρεί πως η συσκευή αυτή είναι απενεργοποιημένη στοιβάζοντας στο συγκεκριμένο δέκτη όλη την εισερχόμενη κίνηση. Όταν ένα κινητό τηλέφωνο απενεργοποιείται στέλνετε στο δίκτυο ένα μήνυμα IMSI DETACH για να σταματήσει η διαδικασία σελιδοποίησης για υπηρεσίες. Επειδή όμως αυτού του είδους τα μηνύματα δεν αυθεντικοποιούνται[13] και η συσκευή δεν λαμβάνει καμία απόκριση είναι εύκολο να σταλεί ψεύτικο IMSI DETACH μήνυμα με συνέπεια το κινητό να "νομίζει" ότι η σύνδεση είναι ακόμα ανοιχτή, παρακολουθώντας το δίκτυο. Παρόλα αυτά, για το Femtocell ο επιτιθέμενος χρειάζεται να γνωρίζει και τη ταυτότητα (IMSI & TMSI) του συνδρομητή που σκοπεύει να επιτεθεί καθώς φέρονται στα μηνύματα IMSI DETACH.

- Επιθέσεις DoS προς τον πάροχο

Οι DoS επιθέσεις προς τον πάροχο στοχεύουν στην αποστολή αιτημάτων για εγκαθίδρυση IPsec συνδέσεων με το SeGW και στην υπερφόρτωση (Overloaded) κάνοντας τη φέμτο-βάση να υπολειτουργεί. Αυτές οι επιθέσεις μπορούν να γενικευτούν και σε άλλες οντότητες του δικτύου του Femtocell όπως AAA/HSS αν και γενικά είναι δύσκολο [17].

- **Κλοπή της υπηρεσίας (Theft of Service)**

  Κανένας μη εγγεγραμμένος χρήστης δε θα πρέπει να αποκτά πρόσβαση στο Femtocell, υποκλέπτοντας την ταυτότητα του νόμιμου συνδρομητή και υποδύοντας τον (Spoofing Attack) με επακόλουθο σκοπό την απρόσκοπτη χρησιμοποίηση των υπηρεσιών και χρεώσεις εις βάρος του.

- **Αυθεντικοποίηση Δικτύου (Network Authentication)**

[13] Τόσο στο GSM όσο και στα 3G δίκτυα.

Προστέθηκε στο πρότυπο του UMTS καλύπτοντας μια σημαντική αδυναμία του GSM. Πρέπει να προστατεύει τους συνδρομητές από ψευδής βάσεις κυψελών και αυτό επιτυγχάνεται με το UMTS-AKA πρωτόκολλο. Το δίκτυο χρησιμοποιεί αποδείξεις για την αποτροπή επαναμεταδόσεων και το κλειδί μιας συσκευής χρήστη (SIM) που γνωρίζει το δίκτυο, δεν είναι ορατό στο Femtocell κάνοντας αδύνατη την απειλή [17].

- **Αυθεντικοποίηση Ταυτότητας Συνδρομητή (Subscriber Identity Authentication)**

  Η πιστοποίηση της ταυτότητας του συνδρομητή πρέπει να διασφαλίζεται ότι είναι μοναδική στο δίκτυο και να προστατεύεται από υποκλοπές. Η διασφάλιση αυτή γίνεται με το πρωτόκολλο αμοιβαίας αυθεντικοποίησης UMTS-AKA. Η διαδικασία της αυθεντικοποίησης δεν λαμβάνει χώρα εσωτερικά του Femtocell αλλά στην μεριά του κεντρικού δικτύου του παρόχου. Επιθέσεις προς αυτή την κατεύθυνση προσπαθούν να παρακάμψουν το πρωτόκολλο UMTS-AKA, όπως στην περίπτωση πού πραγματοποιηθεί μια κλήση ανάγκης (Emergency Call) και αμέσως μετά μια δεύτερη κανονική κλήση, αφήνοντας την πρώτη σε εξέλιξη εκμεταλλευόμενη την μη αυθεντικοποιημένη σύνδεση της πρώτης κλήσης (κλήσης ανάγκης) [17].

- **Προστασία Σηματοδοσίας (Signaling Protection)**

  Τα μηνύματα σηματοδοσίας ανάμεσα στον χρήστη και το δίκτυο πρέπει να είναι εμπιστευτικά και ακέραια. Δεν θα πρέπει να δίνεται η δυνατότητα σε επιθέσεις να αλλάζουν μηνύματα κατά βούληση. Παρόλα αυτά τέτοιες επιθέσεις ελπίζουν σε μηνύματα σηματοδοσίας που στέλνονται εκτός IPsec σύνδεσης [29]. Μηνύματα σηματοδοσίας ανταλλάσσονται ανάμεσα σε διάφορες οντότητες του δικτύου όπως VLR, HLR, AuC και SGSN μέσω του HNB-GW. Υλοποίηση Femtocell Botnets είναι εφικτή.

- **Ιδιωτικότητα της τοποθεσίας του χρήστη**

  Θα πρέπει να αποτρέπεται από επιτιθέμενους η ανίχνευση της τοποθεσίας του χρήστη. Επιθέσεις τέτοιου τύπου προσπαθούν μέσω κατάλληλων μηνυμάτων αυθεντικοποίησης (Authentication Request Message) να λάβουν ένα μήνυμα λάθους από τη κινητή συσκευή και αμέσως μετά ο επιτιθέμενος στέλνει μια προγενέστερη έγκυρη αίτηση αυθεντικοποίησης και με αυτόν τον τρόπο

μπορεί να γνωστοποιηθεί αν η συσκευή του χρήστη βρίσκεται σε συγκεκριμένη κυψέλη [17].

Ο πιο εύκολος τρόπος προσέγγισης του Femtocell είναι δια μέσου της ασύρματης ζεύξης. Οι απειλές σε αυτή την περίπτωση αντιμετωπίζονται με τη χρήση κρυπτογράφησης (αλγόριθμοι κρυπτογράφησης) για την ασφαλή επικοινωνία του χρήστη με τη φεμτοκυψέλη. Οι πιο διαδεδομένοι κρυπτογραφικοί αλγόριθμοι είναι οι Block Ciphers. Η διαδικασία κρυπτογράφησης ξεκινάει στην πλευρά του αποστολέα με την κρυπτογράφηση των δεδομένων προς αποστολή με τη χρήση ενός μυστικού κλειδιού. Στη συνέχεια το κρυπτογραφημένο μήνυμα αποστέλλετε στον παραλήπτη μέσω ενός ασφαλούς καναλιού με τη χρήση των πρωτοκόλλων, Internet Protocol Security (IPsec), Virtual Private Network (VPN) και Transport Layer Security/The Secure Real-time Transport Protocol (TLS/SRTP), αποκρυπτογραφώντας με το ίδιο κλειδί το μήνυμα ώστε να αναπαραχθεί το αυθεντικό αρχικό μήνυμα. Κρίσιμο σημείο στην διαδικασία της κρυπτογράφησης είναι ο τρόπος ανταλλαγής του μυστικού κοινού κλειδιού ανάμεσα στον αποστολέα και τον παραλήπτη αφού τα κλειδιά πρέπει να σταλούν πριν την εγκατάσταση ενός ασφαλούς καναλιού. Για να γίνει η ανταλλαγή αυτή με ασφαλές τρόπο, συνήθως χρησιμοποιείται το πρωτόκολλο Internet Key Exchange (IKE) και IKEv2 η αμέσως επόμενη βελτιωμένη έκδοσή του. Τα κλειδιά μέσα στο Femtocell χρειάζεται να αποθηκεύονται με ασφάλεια, συνήθως με μια έξυπνη κάρτα ή μέσα σε ένα ξεχωριστό υλικό, TPM (Trusted Platform Module).

Η αυθεντικοποίηση (αμοιβαία αυθεντικοποίηση - mutual authentication) γίνεται ανάμεσα στο HNB και το SeGW με τη χρήση X.509 διαπιστευτηρίων - Certificates ή και SIM/UICC (GSM/UMTS). Τα δεδομένα που στέλνονται ανάμεσα στη φεμτοκυψέλη και το κεντρικό δίκτυο είναι δεδομένα χρήστη και δεδομένα σηματοδοσίας [31][17].

Πρωτόκολλο IPsec

Το IPsec χρησιμοποιείται μεταξύ δύο συσκευών που απαιτούν ένα υψηλότερο επίπεδο ασφάλειας με το κεντρικό δίκτυο (Core Network), όταν η επικοινωνία μεταξύ τους γίνεται μέσα από ένα μη ασφαλές δίκτυο IP (Εικόνα 3.10). Χρησιμοποιείται για την αυθεντικοποίηση και κρυπτογράφηση των IP πακέτων τα οποία χωρίζεται σε δύο μέρη, μια κεφαλίδα IP (IP Header) και τα δεδομένα (Data). Το πρωτόκολλο μπορεί να

λειτουργήσει με δύο τρόπους, κατάσταση μεταγωγής (Transport mode) και κατάσταση διόδου (Tunnel mode). Στη λειτουργία Transport μόνο τα δεδομένα που πρόκειται να μεταφερθούν κρυπτογραφούνται και η κεφαλίδα μένει ως έχει, ενώ στη λειτουργία Tunnel όλο το πακέτο (κεφαλίδα και δεδομένα) κρυπτογραφούνται και σχηματίζουν ένα καινούριο πακέτο με μια νέα κεφαλίδα. Το IPsec βασίζεται σε τρία βασικά πρωτόκολλα [15][51][52].

6. **Authentication Header (AH)**

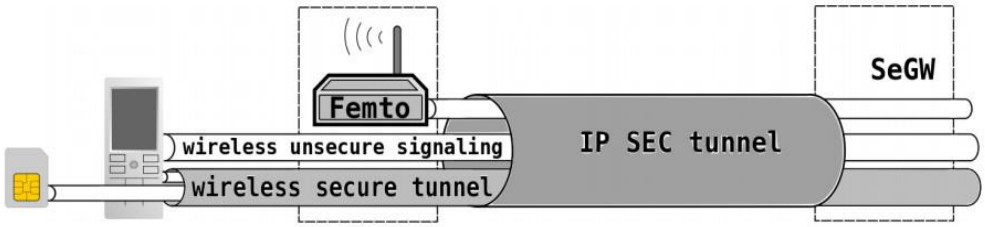
   Προσφέρει αυθεντικοποίηση προέλευσης δεδομένων και υπηρεσίες ακεραιότητας στα πακέτα IP τα οποία όμως δεν τα κρυπτογραφεί. Ο παραλήπτης ενός πακέτου IP έχει τη δυνατότητα να ελέγξει αν το πακέτο που έχει λάβει έχει αλλοιωθεί κατά τη μεταφορά από τον αποστολέα. Είναι ένα πρωτόκολλο που παρέχει έλεγχο ταυτότητας του περιεχομένου του πακέτου, μέσω της προσθήκης μιας κεφαλίδας η οποία υπολογίζεται ανάλογα με τη μέθοδο (Tunnel ή Transport) και το ποια έκδοση του IP πρωτοκόλλου χρησιμοποιείται (v4 ή v6). Βασίζεται σε Checksums που εξαρτώνται από τα κλειδιά που ορίζονται. Εάν τα περιεχόμενα του πακέτου τροποποιήθηκαν στο δίκτυο, η IPsec είναι σε θέση να ανιχνεύει αυτή την αλλαγή και ο δέκτης απορρίπτει το πακέτο και αποφεύγεται με αυτόν τον τρόπο η οποιαδήποτε μη έγκυρη επεξεργασία δεδομένων. Δεν μετασχηματίζει τα δεδομένα ωφέλιμου φορτίου (Payload Data) ενός IP πακέτου, κάτι που αφήνει ανοιχτό το ενδεχόμενο για επιθέσεις τύπου κρυφακούσματος (Eavesdropping).

7. **Encapsulating Security Payload (ESP)**

   Εξασφαλίζει την προστασία της ιδιωτικότητας και εμπιστευτικότητας με την κρυπτογράφηση και ενθυλάκωση είτε του ωφέλιμου φορτίου ενός IP πακέτου δεδομένων (Transport mode), είτε ολόκληρου του IP πακέτου δεδομένων (Tunnel mode). Με αυτόν τον τρόπο εμποδίζεται η παρακολούθηση των πακέτων (Eavesdropping), όταν αυτά αποστέλλονται δια μέσου ενός μη ασφαλούς δικτύου IP και μόνο οι νόμιμοι αποδέκτες ενός IP πακέτου μπορούν να το αναγνώσουν. Για την κρυπτογράφηση χρησιμοποιείται ένα κλειδί με το οποίο γίνονται οι διαδικασίες κρυπτογράφησης αλλά και αποκρυπτογράφησης στην άλλη πλευρά της διόδου (Tunnel) IPsec. Το ESP υποστηρίζει και τις δύο καταστάσεις που εξετάσαμε παραπάνω - Tunnel και Transport mode.

8. **Security Association Protocol (SA)**

Είναι υπεύθυνο για την παραγωγή των μυστικών κλειδιών που μοιράζονται τα δύο άκρα της επικοινωνίας για την διαδικασία την κρυπτογράφησης. Η διαδικασία χρησιμοποιεί πρωτόκολλα όπως το Different Extensible Authentication Protocol (EAP). Στην πλευρά του παραλήπτη όταν λαμβάνεται ένα IP πακέτο αυτό μπορεί να αυθεντικοποιείται και να αποκρυπτογραφείται μόνον εάν ο παραλήπτης μπορεί να το συνδέσει με το περιεχόμενο ενός κατάλληλου SA (Security Association).



Εικόνα 3.10: Χρήση του IPsec σε ένα δίκτυο IP.

Η παράκαμψη του πρωτοκόλλου IPsec από πιθανές απειλές είναι εφικτή διαδικασία, αν και όχι τόσο εύκολη στην πράξη [30].

Extensible Authentication Protocol - EAP

Είναι ένα πλαίσιο ελέγχου ταυτότητας που χρησιμοποιείται συχνά σε ασύρματα δίκτυα με πολλές υλοποιήσεις να έχουν εφαρμοστεί, ανάμεσα τους και αρκετές για τα Femtocells. Παρέχει ασφάλεια και αυθεντικοποίηση που υλοποιείται στο Femto Gateway (FGW). Τέσσερεις εκδοχές του EAP αποτυπώνονται παρακάτω [15][49][51]:

- **Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)**
  Είναι το πιο γνωστό EAP καθώς είναι υλοποιήσιμο από όλες τις ασύρματες συσκευές και βασίζεται στη χρήση της υποδομής δημόσιου κλειδιού Public Key Infrastructure (PKI), που είναι υπεύθυνο για την δημιουργία και διαχείριση των ψηφιακών διαπιστευτηρίων. Η πρώτη του έκδοση είχε την ονομασία EAP-Secure Socket Layer (SSL). Σε αυτό το πρωτόκολλο, μια αρχή πιστοποίησης (Certificate Authority) συνδέει τα δημόσια κλειδιά με τους αντίστοιχους χρήστες τους. Το διαπιστευτήριο μπορεί να δημιουργηθεί αυτόματα από το λογισμικό ή με μηχανικό

τρόπο από τους ίδιους τους χρήστες. Όλες οι παραπάνω εμπλεκόμενες οντότητες διαχειρίζονται από το PKI.

- **Extensible Authentication Protocol - Subscriber Identity Module (EAP-SIM)**
  Χρησιμοποιείται στο πρότυπο GSM για την αυθεντικοποίηση των πληροφοριών στην κάρτα SIM όπως το IMSI (International Mobile Subscriber Identity), το οποίο είναι ένας μοναδικός αριθμός που πιστοποιεί την μοναδική ταυτότητα του κάθε κινητού χρήστη.
- **Extensible Authentication Protocol - Authentication and Key Agreement (EAP-AKA)**
  Χρησιμοποιείται στο πρότυπο UMTS σε συνδυασμό με την Universal Subscriber Identity Module (USIM) κάρτα και τη διαδικασία UMTS Authentication and Key Agreement (AKA). Βασίζεται σε συμμετρικά κλειδιά και περιλαμβάνει προαιρετικά διαδικασίες ανωνυμίας των χρηστών και ελέγχου στοιχείων [49].
- **Extensible Authentication Protocol - Internet Key Exchange version 2 (EAP-IKEv2)**
  Πρόκειται για την δεύτερη έκδοση του EAP-IKE παρέχοντας μεγαλύτερη ασφάλεια με τα εξής χαρακτηριστικά.

    - Το δημόσιο κλειδί είναι ενσωματωμένο σε ένα διαπιστευτήριο, και το αντίστοιχο ιδιωτικό κλειδί είναι γνωστό μόνο σε μία από τις δύο οντότητες που ονομάζονται ασύμμετρα ζεύγη (Asymmetric Pair).
    - Η χρήση κωδικών πρόσβασης που είναι γνωστοί στο FAP και στο FGW.
    - Η χρήση συμμετρικών κλειδιών που είναι επίσης γνωστοί στο FAP και στο FGW.

Τα Femtocells με τη χρήση του EAP μπορούν να αυθεντικοποιούν και να καταχωρούν τους χρήστες που εισέρχονται στην εμβέλεια ενός Femtocell στον ενεργό κατάλογο της.

Η διαδικασία της επιτυχούς αυθεντικοποίησης είναι σημαντική τόσο για τους παρόχους, όσο και για τους χρήστες, απαγορεύοντας σε μη εξουσιοδοτημένους χρήστες και συσκευές την είσοδο και την παραβίαση της ασφάλειας του Femtocell. Δύο τεχνικές που χρησιμοποιούνται για τον σκοπό αυτό, είναι πρώτων η μέθοδος

αυθεντικοποίησης με τη χρήση μίας κάρτας SIM, και δεύτερων, η αυθεντικοποίηση με τη χρήση ενός διαπιστευτηρίου X.509 (X.509 Certificate).

Η πρώτη μέθοδος (SIM Authentication)

Γίνεται εγκατάσταση της SIM ή USIM κάρτας εσωτερικά της φεμτοκυψέλης και τα δεδομένα αυθεντικοποίησης του χρήστη πιστοποιούνται σε σχέση με τα ίδια δεδομένα που υπάρχουν και στον Authentication, Authorization and Accounting (AAA) Server.

Η δεύτερη μέθοδος (X.509 Certificate)

Χρησιμοποιείται συνήθως για την αυθεντικοποίηση σε IP-Based δίκτυα. Τα δεδομένα προς πιστοποίηση αποτυπώνονται σε μια μονάδα υλικού εσωτερικά της φεμτοκυψέλης, Trusted Platform Module (TPM) και τα οποίο δεν μπορούν να τροποποιηθούν. Ο πάροχος με τη σειρά του μαθαίνει τα ευαίσθητα αυτά δεδομένα απευθείας από τον κατασκευαστή και ο χρήστης όταν χρησιμοποιεί τη συσκευή, το δημόσιο κλειδί του μπορεί να χρησιμοποιηθεί μόνο με τα δεδομένα αυτά.

Οι αδυναμίες της πρώτης μεθόδου όταν πρόκειται για κινητά δίκτυα βασισμένα στο IP (στην περίπτωση μας, Femtocell Networks) κάνουν τη χρήση τους ιδιαίτερα προβληματική από την σκοπιά της ασφάλειας, καθώς πολλές είναι οι συσκευές που σήμερα μπορούν να συνδεθούν στο κεντρικό δίκτυο, να αναγνωριστούν από το Femto Gateway (FGW) και να υποδυθούν την FAP (Femtocell Access Point), αλλάζοντας η υποκλέπτοντας ιδιωτικά δεδομένα του χρήστη. Η δεύτερη μέθοδος παρουσιάζεται πιο "δυνατή" και οι όποιες αλλαγές είναι δύσκολες καθώς αποφεύγεται η αναγνώριση του χρήστη στο κεντρικό δίκτυο. Οι διαφορές των δύο μεθόδων παρουσιάζονται συνοπτικά στον Πίνακα 3.4.

USIM Card	X.509
Can be modified	Difficult to hach
Protection of core network required	No interaction with core network
Manufacturing and distribution of cards needed	No cards management
Possibility of using another FAP	Change of FAP made by operator

Πίνακας 3.4: Τρόποι αυθεντικοποίησης χρήστη.

Πρωτόκολλο IKE

Είναι ένα συμμετρικό πρωτόκολλο[14] που χρησιμοποιείται για την ανταλλαγή των ιδιωτικών κλειδιών κατά την διαδικασία εγκαθίδρυσης μιας ασφαλούς σύνδεσης IPsec . Τα (EAP-AKA & EAP-SIM) βασίζοντα στο πρωτόκολλο IKE.

Όπως θα δούμε αναλυτικά στο επόμενο κεφάλαιο, οι επιθέσεις που μπορεί να δεχτεί μια φεμτοκυψέλη είναι ποικίλες και για το λόγο αυτό απαιτείται και μεγαλύτερη προσοχή στα θέματα αυθεντικοποίησης, εμπιστευτικότητας, αλλά και σε θέματα φυσικής προστασίας της συσκευής (καθώς βρίσκεται στο χώρο του συνδρομητή) από την φόρτωση κακόβουλου λογισμικού με σκοπό την αλλαγή ή και υποκλοπή των προσωπικών δεδομένων του ιδιοκτήτη και την παραβίαση του απορρήτου.

[14] Πρωτόκολλο βασισμένο στην ανταλλαγή κλειδιών Diffie-Hellman.

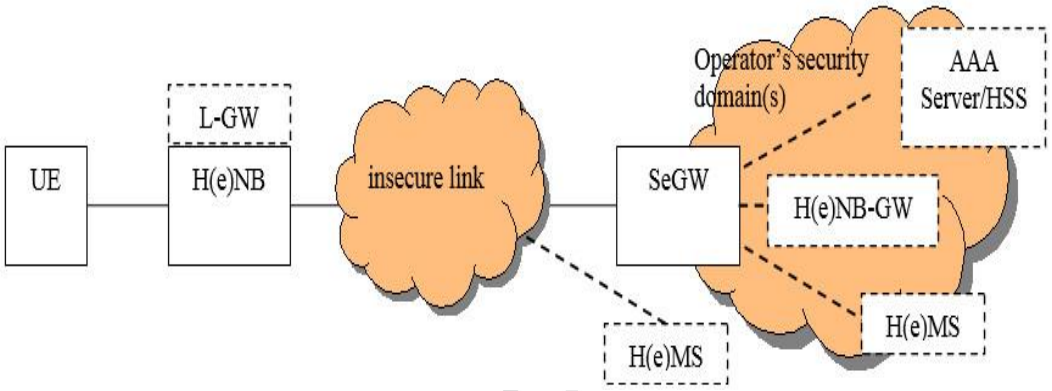
ΚΕΦΑΛΑΙΟ

Αρχιτεκτονική Ασφάλειας H(e)NB (LTE - Femtocell) 4

Ένας σταθμός βάσης Home eNodeB (HeNB), όταν το πρότυπο πρόσβασης που χρησιμοποιείται είναι το LTE, σύμφωνα με το 3GPP είναι ο ορισμός του LTE Femtocell [A1]. Δεδομένου ότι το LTE είναι το σημερινό κυρίαρχο πρότυπο που κερδίζει συνεχώς όλο και περισσότερες εταιρίες κινητής τηλεφωνίας, η ομαλή ένταξη των Femtocells στο LTE είναι ένα ιδιαίτερα σημαντικό ζήτημα για την διεύρυνση των δυνατοτήτων αλλά και της ποιότητας των υπηρεσιών του LTE, αλλά και του LTE/Advanced. Η ασφάλεια ενός σταθμού βάσης HeNB, χωρίζεται σε δύο μέρη σύμφωνα με την αρχιτεκτονική του και κατά πόσο τα μέρη αυτά είναι εκτεθειμένα σε ευπάθειες, αλλά και στην επικινδυνότητα των απειλών αυτών τόσο στη πλευρά του χρήστη όσο και στην πλευρά του παρόχου με τη χρησιμοποίηση της φέμτο-βάσης. Η ιδέα του HeNB σχεδιάστηκε για να παρέχει εσωτερική κάλυψη σε μια οικία ή μια επιχείρηση, βασισμένη στο ίδιο πρότυπο πρόσβασης που χρησιμοποιείται και στις μακροκυψελωτές βάσεις κάτι που σημαίνει ότι επιτρέπει την χρησιμοποίηση του ίδιου εξοπλισμού του χρήστη (UE), είτε πρόκειται για εσωτερικά της οικίας του με τη χρήση φεμτοκυψελών, είτε εξωτερικά χρησιμοποιώντας μακροκυψέλες, με άμεσες μεταπομπές όταν αυτό κρίνεται απαραίτητο. Το HeNB είναι συνδεδεμένο με το κυρίως δίκτυο δια μέσου της ήδη υπάρχουσας Broadband σύνδεσης του χρήστη (DSL).

4.1 Αρχιτεκτονική Ασφάλειας H(e)NB

Παρακάτω αναλύεται η αρχιτεκτονική και τα εκάστοτε στοιχεία δικτύου που αποτελούν την αρχιτεκτονική ασφάλειας της LTE Φεμτοκυψέλης (HeNB) και το ρόλο που έχει το καθένα από αυτά στο δίκτυο (Εικόνα 4.1). Το ενδιαφέρον εστιάζεται στις απαιτήσεις που απαιτούνται ως προς αντιμετώπιση των επιθέσεων που είναι πιθανόν να δεχτεί η φεμτοκυψελωτή βάση όπως θα δούμε αναλυτικά παρακάτω [23].



Εικόνα 4.1: Αρχιτεκτονική HeNB [12].

4.2 Στοιχεία H(e)NB Αρχιτεκτονικής

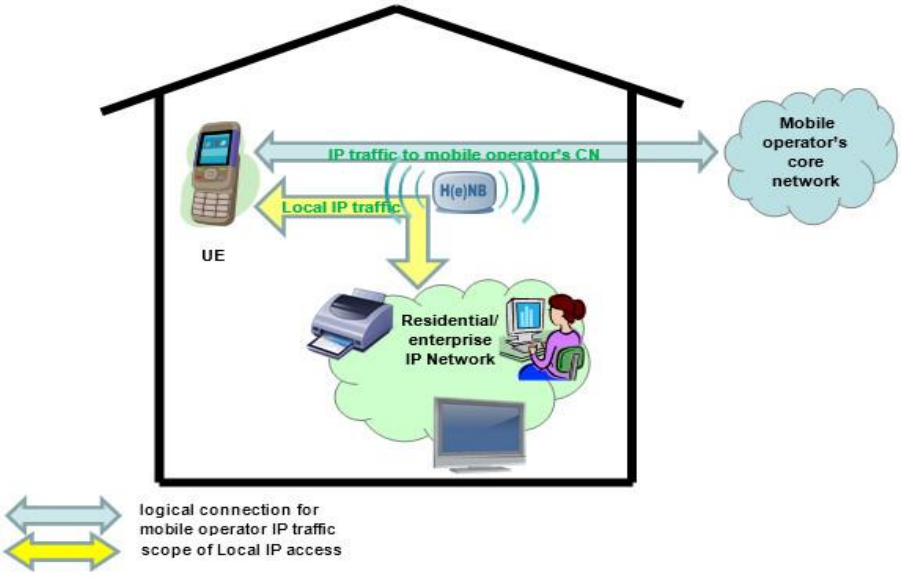
- **Home eNodeB**

Πρόκειται για το σταθμό βάσης που είναι εγκατεστημένο στο χώρο του χρήστη και συνδέει τις διεπαφές του χρήστη (UE) με το κεντρικό δίκτυο (Core Network). Ο πελάτης χρησιμοποιεί τη βάση και το εκπεμπόμενο φάσμα (αδειοδοτημένο φάσμα) σύμφωνα με το συμβόλαιο που του παρέχει ο πάροχος. Ο πελάτης καλείται (HP-Hosting Party) και δεν έχει πλήρη έλεγχο της βάσης για λόγους ασφάλειας, με επακόλουθο κάποιες ρυθμίσεις να είναι διαχειρίσιμες μόνο από τον πάροχο. Η σύνδεση με το κεντρικό δίκτυο γίνεται μέσω του Security Gateway (SeGW) επιτυγχάνοντας αυθεντικοποίηση και διασφάλιση της απαιτούμενης επικοινωνίας για μια ασφαλή σύνδεση.

✦ **Local Gateway (L-GW)**

Το L-GW είναι ενσωματωμένο στο HeNB και από την έκδοση 10 (Release 10) του 3GPP είναι προαιρετικό στοιχείο. Παρέχει τη λειτουργία Local Internet Protocol Access - LIPA (Τοπικό πρωτόκολλο πρόσβασης στο Internet) η οποία επιτρέπει τη σύνδεση άλλων (UEs) μέσω HeNB για να επικοινωνούν με άλλες οντότητες IP στην ίδια κατοικία ή στην ίδια επιχείρηση του δικτύου IP (Εικόνα 4.2). Μια βάση HeNB λοιπόν πρέπει να υποστηρίζει τη λειτουργία LIPA για την παραπάνω επικοινωνία. Από θέμα ασφάλειας εντοπίζονται τα εξής χαρακτηριστικά [5]:

- Μια διεπαφή (UE) πρέπει να έχει έγκυρη συνδρομή με την εταιρεία κινητής τηλεφωνίας, προκειμένου να χρησιμοποιήσει την τοπική IP πρόσβασης.
- Ο διαχειριστής πρέπει να ειδοποιείται όταν η βάση του παρέχει πρόσβαση σε ένα IP δίκτυο και πρέπει να έχει τη δυνατότητα της ενεργοποίησης/ απενεργοποίησης της υπηρεσίας.
- Η επικοινωνία με το HeNB γίνεται με τη μορφή απλού κειμένου (Clear Text) και για αυτό πρέπει να προστατεύεται[15].



Εικόνα 4.2: Λειτουργία (LIPA) - Local Internet Protocol Access.

[15] Συνήθως τοποθετώντας το σε μια ασφαλή περιοχή μαζί με το HeNB, ή κρυπτογραφώντας το σύνδεσμο.

Τα δεδομένα κίνησης του χρήστη στέλνονται κατευθείαν στο τοπικό δίκτυο του χρήστη, όπως ένα LAN. Το L-GW συνδέεται και με το κεντρικό δίκτυο (Core Network) μέσω μιας S5[16] διεπαφής. Ένα σημαντικό κομμάτι ανάμεσα στο HeNB και το L-GW είναι πως η μεταξύ τους επικοινωνία δεν πρέπει να γίνεται κατανοητή από κάποια εξωτερική οντότητα, καθώς τα δεδομένα που ανταλλάσσουν γίνεται στο τοπικό δίκτυο του χρήστη και όχι μέσω ενός Backhaul συνδέσμου.

- **User Equipment (UE)**

Είναι κοινές διεπαφές χρήστη, είτε για το πρότυπο UMTS (HNB) είτε για το πρότυπο LTE (HeNB). Χρησιμοποιούνται ακριβώς όπως και στις μακροκυψέλες στο LTE/EPS.

- **Backhaul-Link**

Ο σύνδεσμος Backhaul έχει σαν σκοπό να εδραιώσει μια ασφαλή σύνδεση μεταξύ του HeNB και του Security Gateway (SeGW) και των άλλων στοιχείων του κεντρικού δικτύου. Μεταφέρει όλη την κίνηση τόσο σε επίπεδο χρήστη (User Plane), όσο και σε επίπεδο ελέγχου (Control Plane), αλλά και την διαχειρίσιμη κυκλοφορία (Management Traffic) όταν δρομολογείται μέσω του (SeGW). Ο σύνδεσμος αυτός και δεδομένου ότι υπάρχει μια σύνδεση καλωδιακή ή DSL, επεκτείνεται προς το δημόσιο Internet και γι' αυτό χαρακτηρίζεται και ως ανασφαλής. Πολλές από τις απειλές που θα δούμε παρακάτω οφείλονται λόγω της συγκεκριμένης σύνδεσης.
Αν η υπηρεσία LIPA είναι ενεργοποιημένη, τότε τη σύνδεση Backhaul τη χρησιμοποιεί και το Local Gateway (L-GW), για να επικοινωνήσει με το κεντρικό δίκτυο κορμού. Η σύνδεση Backhaul μπορεί να μεταφέρει και άλλα δεδομένα μεταξύ του HeNB και τον φορέα ασύρματης πρόσβασης ή το κεντρικό δίκτυο, π.χ. το, Time Protocol Traffic.

- **Security Gateway (SeGW)**

Το Security Gateway (SeGW) είναι η είσοδος στο κεντρικό δίκτυο για όλη την κίνηση από και προς το HeNB. Είναι το μόνο υποχρεωτικό στοιχείο του δικτύου για την ασφάλεια που σκοπό έχει την αμοιβαία αυθεντικοποίηση (Mutual Authentication)

[16] Διεπαφή που διασυνδέει το L-GW με το S-GW στο κεντρικό δίκτυο και χρησιμοποιείται μόνο στην περίπτωση που είναι ενεργοποιημένο το LIPA.

με το HeNB. Η τοποθεσία του είναι εντός του τομέα ασφάλειας του διαχειριστή και συγκεκριμένα στην άκρη, αποτελώντας μια ασφαλή πύλη από την οποία περνάνε όλες οι συνδέσεις για το κεντρικό δίκτυο. Αν χρησιμοποιείται το HeNB-GW, τότε τοποθετείται μπροστά του. Διαφέρει από το SEG (Security Gateway) που χρησιμοποιείται στο Network Domain Security - NDS/IP για τις μακροκυψέλες. Το SEG δουλεύει ανάμεσα σε δύο Security Domains, ενώ αντίθετα το SeGW συνδέει ένα στοιχείο "λογικά" στο ίδιο Security Domain.

- **H(e)NB Management System (HeMS)**

Είναι ένας διακομιστής διαχείρισης (Management Server) που είναι υπεύθυνος για τη διαχείριση του HeNB σύμφωνα με την πολιτική του παρόχου. Μια σημαντική προδιαγραφή του HeMS είναι πως πρέπει να είναι ικανό να διαχειρίζεται HeNBs από διαφορετικούς κατασκευαστές και να υποστηρίζει τη διαλειτουργικότητα. Η προδιαγραφή αυτή βασίζεται στο πρωτόκολλο για τον εξοπλισμό του συνδρομητή (CPE - Customer Premises Equipment) όπως ορίζεται από το Broadband Forum (BBF) [A7]. Μέσω του HeMS μπορούν να γίνουν και ενημερώσεις (Updates) στο λογισμικό του HeNB. Μπορεί να είναι εγκατεστημένο είτε στο τομέα ασφάλειας του διαχειριστή είτε άμεσα διαθέσιμο στο δημόσιο internet.

- **HeNB Gateway (HeNB-GW)**

Είναι προαιρετικό στοιχείο στην αρχιτεκτονική του EPS, αποκλίνοντας από τα 3G δίκτυα όπου το HNB Gateway αποτελεί ένα υποχρεωτικό στοιχείο. Είναι το καθήκον της HeNB-GW να ανακουφίζει το MME - Mobility Management Entity από την παρακολούθηση του τεράστιου αριθμού των HeNBs, καθώς το MME μπορεί να παρακολουθήσει μόνον έναν μικρό αριθμό από HeNBs. Η LTE Φεμτοκυψέλη και το MME δεν γνωρίζουν ότι το HeNB-GW υπάρχει[17], με επακόλουθο το HeNB να το "βλέπει" σαν ένα MME και το MME να "βλέπει" όλα τα HeNBs σαν μια μεγάλη βάση eNB. Από θέμα ασφάλειας δεν έχει σημασία με τον τρόπο που διασυνδέεται ένα HeNB, καθώς η ασφαλής σύνδεση Backhaul τερματίζεται στα σύνορα του τομέα της ασφάλειας του παρόχου στο SeGW [10][23].

[17] Καθώς το HeNB-GW έχει την ίδια διεπαφή διασύνδεσης S1 και στις δύο πλευρές.

✦ **AAA Server**

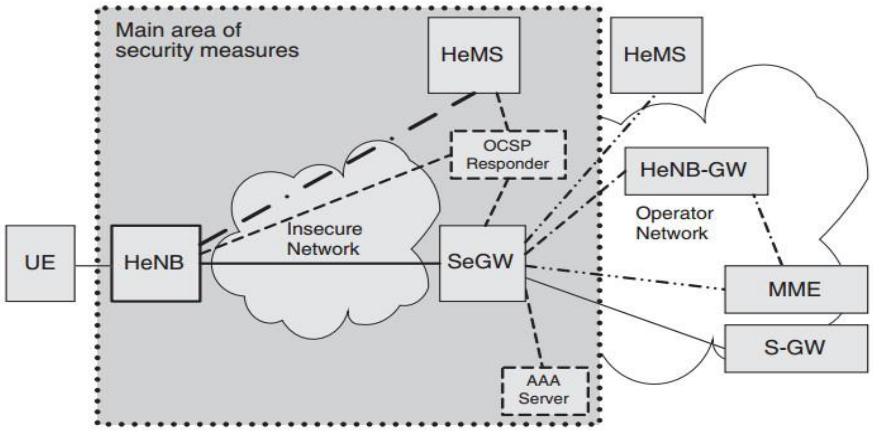
Authentication, Authorization and Accounting - AAA, είναι το πρωτόκολλο που ελέγχει τους χρήστες που έχουν πρόσβαση σε υπηρεσίες και παρακολουθεί τους πόρους που έχουν χρησιμοποιηθεί. Είναι προαιρετικό στοιχείο στην αρχιτεκτονική ασφάλειας και χρησιμοποιείται για δύο λόγους. Πρώτον για επικοινωνία με το Home Location Register/Home Subscriber Server (HLR/HSS) όταν αυθεντικοποιείται το (HP) του χρήστη και δεύτερον, για εξουσιοδότηση πρόσβασης (Access Authorization) όταν ελέγχεται από τον AAA Server.

✦ **X2 interface**

Πρόκειται για την διεπαφή ανάμεσα σε HeNBs που φέρουν την κίνηση τόσο του χρήστη (User Plane Data) όσο και των δεδομένων ελέγχου (Control Plane Data). Χρησιμοποιείται κατά την μεταπομπή μεταξύ δύο σταθμών βάσης HeNB. Οι αντίστοιχη διεπαφή για τις βάσεις HNB είναι η Iurh.

Προαιρετικά στοιχεία είναι επίσης τα MME, S-GW και OCSP Responder, το οποίο παρέχει έγκυρο έλεγχο πληροφοριών για τα διαπιστευτήρια αν ο πάροχος ρυθμίσει τη συσκευή να χρησιμοποιεί την συγκεκριμένη υπηρεσία.

Στην Εικόνα 4.3 αποτυπώνονται όλα τα στοιχεία (υποχρεωτικά και προαιρετικά).



Εικόνα 4.3: Στοιχεία αρχιτεκτονικής ασφάλειας HeNB.

4.3 Ευπάθειες στο H(e)NB

Ο λόγος για τον οποίο χρειάζονται ειδικά μέτρα ασφάλειας για το HeNB, είναι γιατί δεν βρίσκεται εντός του τομέα ασφάλειας του διαχειριστή όπως άλλα στοιχεία δικτύου, αλλά στον χώρο του χρήστη. Κάτι τέτοιο αυτόματα γεννά ανησυχίες και προβληματισμούς, αλλά και ερωτήματα για το πόσο ασφαλές μπορεί να είναι ή όχι ένα περιβάλλον που ο πάροχος δεν ελέγχει άμεσα. Αυτό έχει ως συνέπεια να δημιουργείται έδαφος για κακόβουλες ενέργειες και επιθέσεις. Μερικές σημαντικές ευπάθειες απόρροια του χαρακτηριστικού αυτού είναι οι παρακάτω [23]:

- Η επικοινωνία με το κεντρικό δίκτυο μέσω του Internet και της DSL σύνδεσης δεν είναι άμεσα διαχειρίσιμη από τον πάροχο.
- Το HeNB επιτρέπει αποκρυπτογράφηση στον εξοπλισμό του χρήστη εντός της οικίας του, με συνέπεια τα δεδομένα του χρήστη και τα δεδομένα σηματοδοσίας Radio Resource Control (RRC) να είναι διαθέσιμα σε μορφή απλού κειμένου (Clear Text).
- Τα στοιχεία δικτύου του χρήστη (NE), εφόσον αυθεντικοποιηθούν μέσω από ένα ασφαλές κανάλι, έχουν άμεση πρόσβαση στο κεντρικό δίκτυο (Core Network).
- Υπάρχουν περιπτώσεις για Offline εξέταση από επίδοξους επιτιθέμενους.
- Σε περίπτωση που εντοπιστούν ευπαθή σημεία, τότε μέσω Internet και από την άνεση του χώρου του επιτιθέμενου, ένα ψευδές HP (Hosting Party) μπορεί να εκμεταλλευτεί και να εφαρμόσει τις επιθέσεις του.

Οι επιθέσεις που μπορεί να δεχτεί μια φεμτοκυψέλη αφορούν τον χρήστη αλλά και τον πάροχο.

Από την μεριά του πελάτη χρειάζεται μια μεγάλη εμπορική ανάπτυξη που σημαίνει φτηνότερο κόστος για την απόκτηση και εγκατάστασης μιας φεμτοκυψέλης, κάτι που παράλληλα όμως εμποδίζει και την ανάπτυξη για ακριβότερες μεθόδους για μεγαλύτερη ασφάλεια.

Από τη μεριά του παρόχου γίνονται περισσότερες επισημάνσεις αφού λόγο του αδειοδοτημένου φάσματος τον καθιστά υπεύθυνο για κάθε παραβίαση κανονισμών, (ισχύς, συχνότητα, τοποθεσία). Η υπευθυνότητα όμως δε σταματά εκεί, είναι υπεύθυνος για την ακεραιότητα και την προστασία της ιδιωτικής ζωής καθώς και την

νόμιμη παρακολούθηση των εξοπλισμού του χρήστη (UE) που συνδέεται στο HeNB. Τέλος, μέριμνα του πρέπει να είναι η παρεμπόδιση των όποιων παρεμβολών από ή και σε άλλα δίκτυα και συσκευές.

Σε αυτό το σημείο παραθέτουμε τις ομάδες των επιθέσεων ανάλογα με το ποια στοιχεία του δικτύου παραβιάζουν, ποιές μέθοδοι χρησιμοποιούνται αλλά και σε τι αποσκοπούν οι επιθέσεις αυτές. Η ομαδοποίηση αυτή αποτυπώνεται στον παρακάτω πίνακα (Πίνακας 4.1) [4][11][23]:

1.	Αποκάλυψη ή Υποκλοπή των διαπιστευτηρίων (Credentials) του HeNB
2.	Φυσικές επιθέσεις έναντι του HeNB (Physical Attacks)
3.	Επιθέσεις διαμόρφωσης του HeNB (Configuration Attacks)
4.	Επιθέσεις πρωτοκόλλων (Protocol Attacks)
5.	Επιθέσεις στο κεντρικό δίκτυο & Επιθέσεις τοποθεσίας του HeNB (Core Network & Location-Based Attacks)
6.	Επιθέσεις έναντι ιδιωτικών δεδομένων των χρηστών (Identity Privacy Attacks)

Πίνακας 4.1: Κατηγορίες επιθέσεων (Ομαδοποίηση).

1. **Αποκάλυψη ή Υποκλοπή των διαπιστευτηρίων του HeNB**
   a) Τα διαπιστευτήρια μπορεί να αποκαλυφθούν από τις τοπικές, φυσικές ή απομακρυσμένες αλγοριθμικές επιθέσεις, που επιτρέπουν την κλωνοποίηση των διαπιστευτηρίων για μια πληθώρα συσκευών, ή για την κατάχρηση τους για άλλους σκοπούς.
2. **Φυσικές επιθέσεις έναντι του HeNB**
   a) Η συσκευή μπορεί να παραποιηθεί για να θέσει σε κίνδυνο την ακεραιότητά της, όπως για παράδειγμα να αποκτήσει πρόσβαση σε δεδομένα απλού κειμένου που μεταφέρονται μεταξύ της ασύρματης σύνδεσης και του Backhaul συνδέσμου.
   b) Ψεύτικα ή κλωνοποιημένα διαπιστευτήρια μπορεί να τοποθετηθούν στη συσκευή, επιτρέποντας σε μη εξουσιοδοτημένες συσκευές να αποκτούν πρόσβαση στο κεντρικό δίκτυο.

c) Κακόβουλο λογισμικό ή και λανθασμένα στοιχεία διαμόρφωσης μπορούν να εισαχθούν με φυσικό τρόπο πρόσβασης.

3. Επιθέσεις διαμόρφωσης του HeNB

a) Ακατάλληλο ή παλιότερες και μη ενημερωμένες εκδόσεις λογισμικού μπορεί να φορτωθεί.

b) Λίστες ελέγχου πρόσβασης μπορούν να αλλάξουν εάν εφαρμοστούν στο πλαίσιο του HeNB.

c) Η διαχείριση του ασύρματου μέσου μπορεί να διαμορφωθεί με σκόπιμα λανθασμένο τρόπο.

4. Επιθέσεις πρωτοκόλλων

a) Μια επίθεση "man-in-the-middle" μπορεί να πραγματοποιηθεί στο σύνδεσμο Backhaul με το χειρισμό και εισαγωγή μηνύματα στο HeNB.

b) Denial-of-Service (DoS) επιθέσεις στο HeNB μπορούν να πραγματοποιηθούν με την αποστολή ψεύτικων μηνύματα στο HeNB.

c) Εάν οι ευπάθειες των πρωτοκόλλων που χρησιμοποιούνται για το Backhaul σύνδεσμο ανακαλυφθούν, τότε αυτές μπορούν να χρησιμοποιηθούν για επιθέσεις.

d) Εξωτερικά μηνύματα χρόνου και O&M - Operations and Management μπορούν να διαταραχθούν.

5. Επιθέσεις στο κεντρικό δίκτυο & Επιθέσεις τοποθεσίας του HeNB

a) Μια πλαστή βάση HeNB μπορεί να προσκολληθεί στο κεντρικό δίκτυο και στη συνέχεια με επιθέσεις DoS να επιτεθεί προς άλλες οντότητες του δικτύου.

b) Η κίνηση από άλλα sites μπορεί να οδηγηθεί στο κεντρικό δίκτυο.

c) Μια εσφαλμένη θέση μπορεί να αναφερθεί στο κεντρικό δίκτυο δίνοντας αφορμή στο δίκτυο για την διαμόρφωση του HeNB με λάθος παραμέτρους.

6. Επιθέσεις έναντι ιδιωτικών δεδομένων των χρηστών

a) Καθώς τα δεδομένα σηματοδοσίας RRC (Radio Resource Control) και S1 καταλήγουν στο HeNB, και τα δεδομένα του χρήστη διατίθενται σε μορφή απλού κειμένου, υποκλοπές των δεδομένων των χρηστών είναι εφικτή με τη μέθοδο του κρυφακούσματος (Eavesdropping).

b) Μια ψεύτικη ή παραποιημένη HeNB μπορεί να μεταμφιεστεί (Masquerade) ως μια έγκυρη HeNB και με αυτόν τον τρόπο να προσελκύσει άλλους

χρήστες, όπως τα μέλη διαφορετικών CSGs που δεν χρησιμοποιούν αυτό το HeNB.

Η αναλυτική καταγραφή, καθώς και η περιγραφή των πιο κοινών επιθέσεων έναντι μιας φεμτοκυψέλης καλύπτεται στο επόμενο κεφάλαιο.

4.4 Απαιτήσεις Ασφάλειας

Η τεχνική αναφορά (TR33.820) [4] της 3GPP δίνει μια λίστα από 32 απαιτήσεις ασφάλειας, οι οποίες σχηματίστηκαν παράλληλα σε σχέση με τις ομάδες απειλών της Ενότητας 4.3. Παρακάτω παρουσιάζονται επιγραμματικά και συνολικά κάτω από τα βασικά τους θεματικά πεδία [4][23]:

- **Αυθεντικοποίηση - (Authentication)**
  Αμοιβαία αυθεντικοποίηση ταυτότητας για τη σύνδεση Backhaul και O&M, ισχυροί κρυπτογραφικοί μηχανισμοί, μοναδικά αναγνωριστικά για έλεγχο αυθεντικοποίησης, προστατευόμενη αποθήκευση για αυθεντικοποίηση διαπιστευτηρίων.
- **Backhaul σύνδεσμος και διαχείριση της κυκλοφορίας - (Backhaul Link and Management Traffic)**
  Υποχρεωτική προστασία της ακεραιότητας, υποχρεωτική προστασία της εμπιστευτικότητας για τη διαχείριση και προαιρετική για το Backhaul σύνδεσμο, εξουσιοδότηση που απαιτείται για τη σύνδεση στο κεντρικό δίκτυο.
- **Ακεραιότητα λογισμικού, εμπιστευτικότητα και ακεραιότητα των δεδομένων για το HeNB - (Software Integrity, Data Confidentiality and Integrity for the HeNB)**
  Ασφαλής εκκίνηση (Secure Boot), έγκυρο λογισμικό, hardening της συσκευής, επικύρωση της ακεραιότητας της συσκευής, ασφαλής αποθήκευση δεδομένων και ασφαλής λειτουργίες πάνω σε ευαίσθητα είδους δεδομένα.
- **Ιδιωτικότητα Χρηστών - (User Privacy)**
  Διαφύλαξη του International Mobile Subscriber Identity (IMSI) αναγνωριστικού εσωτερικά της συσκευής αλλά και στο ασύρματο μέσο, εμπιστευτικότητα των δεδομένων σηματοδοσίας και χρήστη.

- **Λειτουργία και διαχείριση της ασφάλειας - (Operation and management security)**

  Διαφορετική αντιμετώπιση για δεδομένα χειριστή και χρήστη με συναφή συστήματα ελέγχου πρόσβασης, απόλυτο έλεγχο από το χειριστή για πολλά δεδομένα.
- **Προστασία του δικτύου από επιθέσεις τύπου DoS - (DoS Protection of Network)**

  Περιορισμός του αριθμού των συνδέσεων ανά HeNB στο δίκτυο, μόνο επικυρωμένα HeNBs στο κεντρικό δίκτυο.
- **Διαχείριση κλειστής ομάδας συνδρομητών - (Closed Subscriber Group Management)**

  Έλεγχος χρήστη από τον πάροχο, επιβολή ελέγχου πρόσβασης στο κεντρικό δίκτυο.
- **Θέση και χρόνος - (Location and Time)**

  Κλείδωμα του HeNB σε συγκεκριμένη θέση, αξιόπιστες πληροφορίες για τη θέση θα πρέπει να συλλέγονται και να μεταφέρονται από το HeNB, πληροφορίες σχετικές με το χρόνο πρέπει να είναι αξιόπιστες.

4.5 Χαρακτηριστικά και Διαδικασίες Ασφάλειας

Παρακάτω παρουσιάζονται τα βασικά χαρακτηριστικά ασφάλειας ενός HeNB. Ακολουθείται μια προσέγγιση αλληλεπίδρασης με τα υπόλοιπα στοιχεία του δικτύου, με επίκεντρο τον τομέα της ασφάλειας, όπως και ποιες μέθοδοι χρησιμοποιούνται και ποια στοιχεία χρίζουν ιδιαίτερης αντιμετώπισης.

4.5.1 Τοπική & Φυσική Ασφάλεια - (Local & Physical Security)

Η τοπική ασφάλεια περιλαμβάνει την ασφαλή αποθήκευση των δεδομένων και την ασφαλή εκτέλεση των λειτουργιών εσωτερικά της συσκευής HeNB, με τη χρήση μιας μονάδας υλικού TrE και UICC. Περιγράφονται οι τρόποι για την αποτροπή υποκλοπών με φυσική παρουσία και πρόσβαση στη φέμτο-βάση.

Trusted Environment (TrE)

Το TrE είναι μια λογική μονάδα εσωτερικά του HeNB, που όμως παρέχει ξεχωριστά ένα αξιόπιστο περιβάλλον για την εκτέλεση ευαίσθητων λειτουργιών (όπως η αποθήκευση των ιδιωτικών κλειδιών και η παροχή κρυπτογραφικών υπολογισμούς χρησιμοποιώντας αυτά τα ιδιωτικά κλειδιά) και την αποθήκευση ευαίσθητων δεδομένων. Όλα τα δεδομένα που παράγονται από τις εσωτερικές λειτουργίες του TrE προστατεύονται και δεν είναι φανερές από μη-εξουσιοδοτημένες οντότητες/χρήστες. Είναι απαραίτητη μονάδα που χρησιμοποιείται στις διαδικασίες της αμοιβαίας αυθεντικοποίησης με το δίκτυο, αλλά και στον έλεγχο της ακεραιότητας της συσκευής. Η πρώτη εργασία που εκτελεί το TrE είναι ένας αυτό-έλεγχος (Secure Boot) για την εγκυρότητα του και μετά η περαιτέρω αναγνώριση λογισμικού που απαιτείται για τις λειτουργίες του (όπως το λειτουργικό σύστημα). Σε περίπτωση που το προαιρετικό στοιχείο L-GW χρησιμοποιείται, τότε πρέπει να επαληθευτεί και όλο το απαιτούμενο λογισμικό για τη λειτουργία του. Το λογισμικό θα πρέπει να έχει τις ίδιες τιμές (Hash Values), με αυτές που είναι αποθηκευμένες στο TrE. Όταν η διαδικασία αυτή ολοκληρωθεί, το δίκτυο και οι οντότητες SeGW και HeMS, ενημερώνονται και θεωρούν πως ο έλεγχος της ακεραιότητας της συσκευής ήταν επιτυχής. Μόνο με τον επιτυχή αυτό έλεγχο μπορούν να εκτελεστούν στη συνέχεια διαδικασίες για την παραγωγή ιδιωτικών κλειδιών για τη διαδικασία της αυθεντικοποίησης [12][30].

Hosting Party Module (HPM)

Η αυθεντικοποίηση του Hosting Party (πελάτης/χρήστης) βασίζεται σε μια μονάδα που ονομάζεται Hosting Party Module - HPM, η οποία είναι μια φυσική μονάδα συνήθως η UICC - Universal IC Card και παρέχει ασφαλή αποθήκευση για το κοινό μυστικό της διαδικασίας EAP-AKA και ένα ασφαλές περιβάλλον για την εκτέλεση των ευαίσθητων λειτουργιών. Το HeNB πρέπει να παρακολουθεί την διαθεσιμότητα του HPM, καθώς μια δεύτερη διαδικασία αυθεντικοποίησης από κάποια άλλη συσκευή μπορεί να εκτελεστεί την στιγμή που το HeNB είναι σε λειτουργία. Αν υπάρξει αίτημα για απομάκρυνση της μονάδας, (Removal HPM) τότε η βάση HeNB αποσυνδέεται από την ασύρματη ζεύξη και τον πάροχο του δικτύου. Η αντίστροφη διαδικασία προϋποθέτει την εγκατάσταση μιας νέας σύνδεσης με το SeGW [12][30].

Η βάση HeNB, πρέπει να είναι σε θέση σε περίπτωση αποσύνδεσης με το κεντρικό δίκτυο, να απενεργοποιεί την εκπομπή προς το δίκτυο μέσα σε ένα χρονικό περιθώριο ικανό να αποτρέψει την μη εξουσιοδοτημένη εκπομπή.

4.5.2 Διαδικασίες Ασφάλειας του HeNB και του SeGW

Αυθεντικοποίηση

Για την αυθεντικοποίηση του HeNB στο δίκτυο, γίνεται χρήση ενός αναγνωριστικού (Identity), το οποίο είναι η ταυτότητα της συσκευής και χρησιμοποιείται σε όλο το EPS με την ονομασία FQDN - Fully Qualified Domain Name[18]. Η αυθεντικοποίηση στο HeNB βασίζεται στην υποδομή δημόσιου κλειδιού (Public Key Infrastructure - PKI), τα πρωτόκολλα IKEv2 για το Backhaul σύνδεσμο και το Transport Layer Security (TLS) για χειραψία (Handshake) με το HeMS. Η αμοιβαία αυθεντικοποίηση βασίζεται στην ανταλλαγή διαπιστευτηρίων (Certificates).

Επειδή το PKI επιλέχθηκε ως η κύρια μέθοδος για τον έλεγχο ταυτότητας της συσκευής, κάθε συσκευή HeNB πρέπει να είναι εφοδιασμένη με ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού, καθώς και ένα διαπιστευτήριο που να φέρει την ταυτότητα και άλλες απαραίτητες πληροφορίες στο δημόσιο κλειδί. Η χρησιμοποίηση αυτού του διαπιστευτηρίου πρέπει να εγκριθεί από τον πάροχο αλλά και τον κατασκευαστή του HeNB, καθώς χρησιμοποιείται για την διαφύλαξη της ακεραιότητας της συσκευής [23].

Η αμοιβαία αυθεντικοποίηση είναι υποχρεωτική διαδικασία και εκτελείται ανάμεσα στα HeNB και SeGW, αλλά και ανάμεσα στα HeNB και HeMS. Δύο είναι οι μηχανισμοί αυθεντικοποίησης που έχουν οριστεί για την αυθεντικοποίηση της συσκευής:

1. IKEv2 – Για την εγκατάσταση μιας ασφαλής IPsec διόδου με το SeGW και
2. TLS χειραψία – Για την εγκατάσταση μιας TLS διόδου με το HeMS.

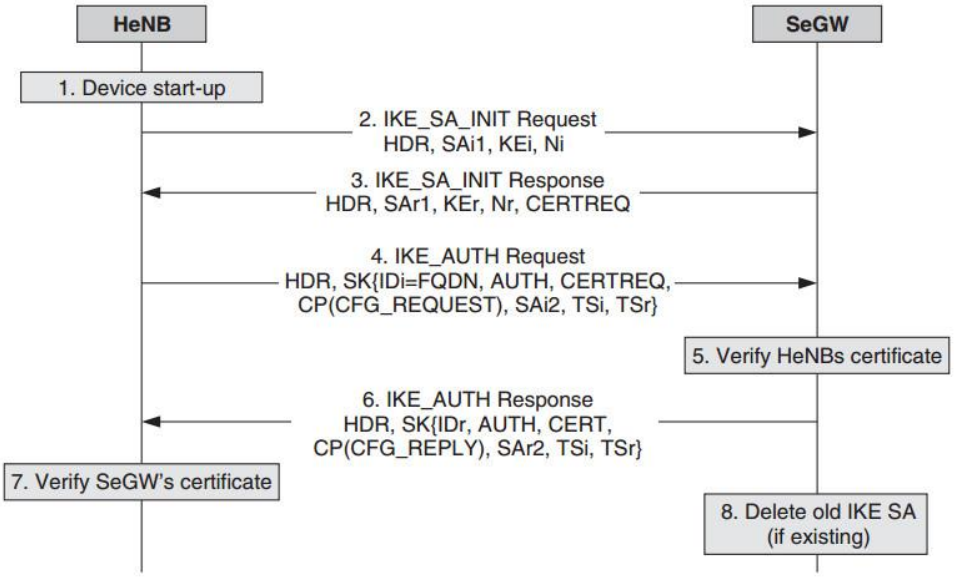
Αμοιβαία αυθεντικοποίηση συσκευής - (Device Mutual Authentication)

Η χρήση διαπιστευτηρίων, αλλά και λειτουργίες ζωτικής σημασίας για την αμοιβαία αυθεντικοποίηση της συσκευής πρέπει να προστατεύονται εσωτερικά ενός ασφαλούς περιβάλλοντος (Trusted Environment - TrE). Το TrE χρησιμοποιείται για τις παρακάτω σημαντικές λειτουργίες [30]:

[18] Πρόκειται για τα X.509 Certificates.

- Η ταυτότητα του HeNB δε θα πρέπει να είναι τροποποιήσιμη για επεξεργασία.
- Τα ιδιωτικά κλειδιά του HeNB δε θα πρέπει να εκτίθενται έξω από την ασφαλή μονάδα TrE.
- Το πιστοποιητικό ρίζας (Root Certificate) αποθηκευμένο στο TrE, που χρησιμοποιείται για να επικυρώσει τα διαπιστευτήρια στο SeGW, θα πρέπει να είναι επεξεργάσιμο μόνο μετά από εξουσιοδοτημένη πρόσβαση.
- Το TrE χρησιμοποιείται για τον υπολογισμό του ωφέλιμου φορτίου AUTH κατά την διαδικασία ανταλλαγής των μηνυμάτων IKE_AUTH Requests.

Απαραίτητη προϋπόθεση για οποιαδήποτε εγκατάσταση σύνδεσης μεταξύ HeNB και του δικτύου κινητής τηλεφωνίας (SeGW), είναι η επιτυχής επικύρωση της ακεραιότητας της συσκευής (Device Integrity Validation) του HeNB από το δίκτυο. Η επικύρωση αυτή βασίζεται στην ασφαλή εκκίνηση (Secure Boot) του HeNB, όπως είδαμε παραπάνω και έλεγχο της ακεραιότητας. Πρόσβαση στο ιδιωτικό κλειδί για τη διαδικασία της αμοιβαίας αυθεντικοποίησης παρέχεται μόνο στην περίπτωση που η συσκευή επικυρωθεί επιτυχώς. Η διαδικασία αυθεντικοποίησης βασίζεται σε ένα ιδιωτικό κλειδί και ένα διαπιστευτήριο τόσο στη μεριά του HeNB όσο και στη μεριά του SeGW. Το διαπιστευτήριο της συσκευής παρέχεται από τον πάροχο, τον κατασκευαστή ή κάποιον διαφορετικό φορέα της εμπιστοσύνης του παρόχου. Αντίθετα το διαπιστευτήριο του SeGW παρέχεται από έναν φορέα CA πάλι με την εμπιστοσύνη του παρόχου. Το HeNB παρακολουθεί την κατάσταση των διαπιστευτηρίων χρησιμοποιώντας το OCSP (Online Certificate Status Protocol), ενώ το HeNB χρησιμοποιεί το CRL (Certificate Revocation List) ή OCSP. Σε περίπτωση που ελεγχθούν τα διαπιστευτήρια και δεν επιστραφεί έγκυρη τιμή OCSP, τότε το HeNB ακυρώνει το πρωτόκολλο IKEv2. Δεδομένου ότι τα ιδιωτικά κλειδιά πρέπει να παραμένουν εμπιστευτικά, πρέπει να διαβιβάζονται με ασφαλή τρόπο αλλά και να προστατεύονται επίσης (Εικόνα 4.4) [12][30].

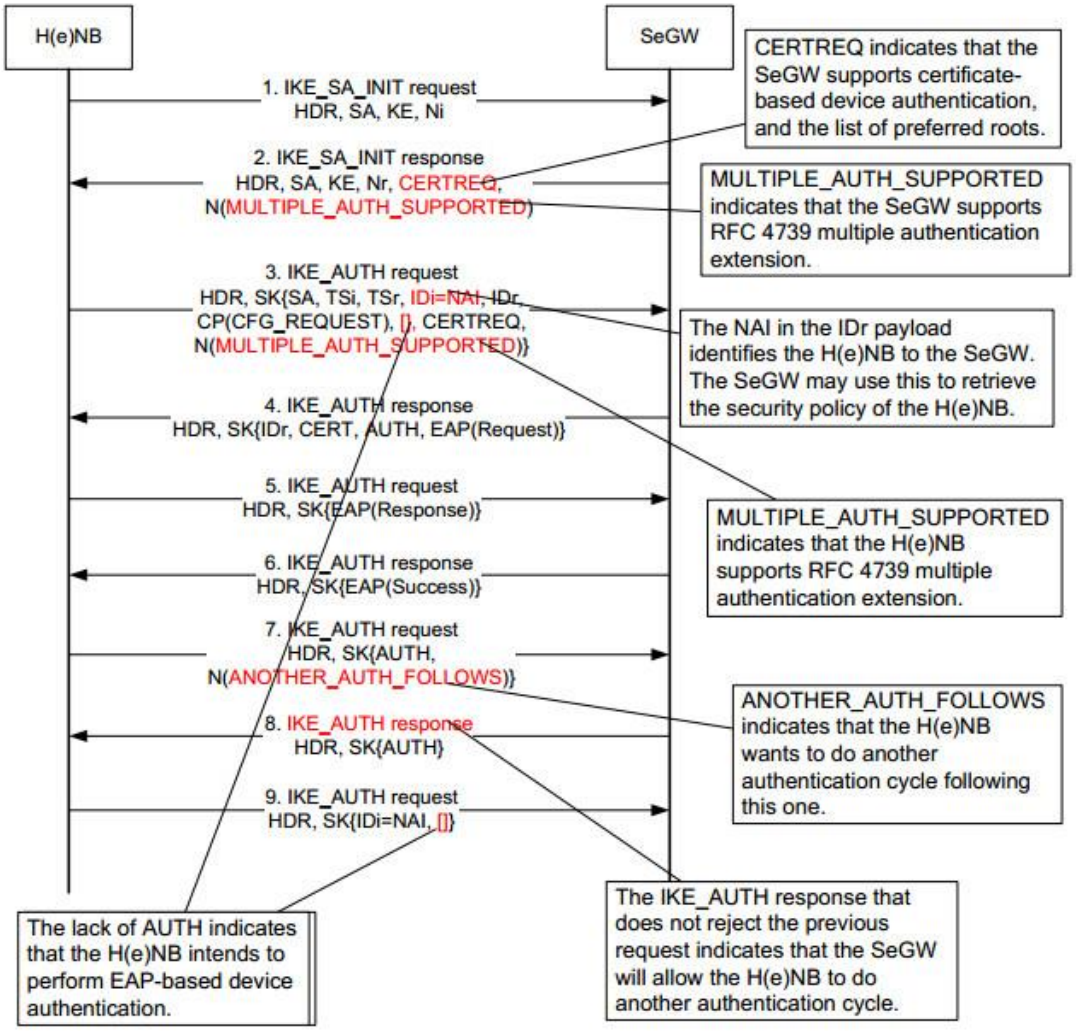


Εικόνα 4.4: Διαδικασία αυθεντικοποίησης με χρήση διαπιστευτηρίων [1].

Αμοιβαία αυθεντικοποίηση HP - (Hosting Party Mutual Authentication)

Η αμοιβαία αυθεντικοποίηση του Hosting Party (Εικόνα 4.5) είναι προαιρετική διαδικασία και εκτελείται μετά την επιτυχή αυθεντικοποίηση της συσκευής, με την χρησιμοποίηση διαπιστευτηρίων τα οποία περιέχονται στη μονάδα HPM του HeNB αλλά και στο MNO (Mobile Network Operator) HLR/HSS. Επιτυγχάνεται ανάμεσα στον διαχειριστή του δικτύου και το HPM. Χρησιμοποιείται η μέθοδος του πρωτοκόλλου Authentication and Key Agreement (AKA), βασισμένη σε ένα μόνιμα κοινό μυστικό αποθηκευμένο στο HPM ή USIM και στο HLR/HSS. Το EAP εκτελείται ανάμεσα στο HeNB και του AAA Server, όπου το SeGW συμπεριφέρεται ως ένας EAP αυθεντικοποιητής και προωθεί τα μηνύματα πρωτοκόλλου EAP στο AAA Server, ώστε να μπορέσει να ανακτήσει ένα διάνυσμα αυθεντικοποίησης από το AuC μέσου του HSS/HLR. Το IKEv2 με τη σειρά του χρησιμοποιείται για την πολλαπλή αυθεντικοποίηση του (EAP-AKA) και αυθεντικοποίηση συσκευής [12][30].

Τόσο η διαδικασία της αυθεντικοποίησης της συσκευής όσο και του Hosting Party, πρέπει να ολοκληρωθούν με επιτυχία πριν την εγκατάσταση μιας ασφαλής διόδου (Secure Tunnel) προς το δίκτυο του παρόχου.



Εικόνα 4.5: EAP-AKA αυθεντικοποίηση συσκευής και EAP-AKA HP.

Συνδυασμός μεθόδων αυθεντικοποίησης

Η αυθεντικοποίηση του HeNB μπορεί να γίνει με δύο μεθόδους (EAP-AKA και Certificates). Αυτό επιτρέπει τους επόμενους συνδυασμούς ανάμεσα στις διαδικασίες αυθεντικοποίησης συσκευής και HP [4]:

1.	Αυθεντικοποίηση συσκευής με τη χρήση Certificates, χωρίς αυθεντικοποίηση HP.
2.	Αυθεντικοποίηση συσκευής με τη χρήση EAP-AKA, χωρίς αυθεντικοποίηση HP.
3.	Αυθεντικοποίηση συσκευής με τη χρήση Certificates, με τη χρήση αυθεντικοποίησης HP και με Certificates.

4.	Αυθεντικοποίηση συσκευής με τη χρήση EAP-AKA, με τη χρήση αυθεντικοποίησης HP και με Certificates.
5.	Αυθεντικοποίηση συσκευής με τη χρήση Certificates, με τη χρήση αυθεντικοποίησης HP και με EAP-AKA.
6.	Αυθεντικοποίηση συσκευής με τη χρήση EAP-AKA, με τη χρήση αυθεντικοποίησης HP και με EAP-AKA.

Πίνακας 4.2: Συνδυασμοί αυθεντικοποίησης.

Εγκατάσταση IPsec Tunnel

Προκειμένου να γίνει αυθεντικοποίηση με τη μέθοδο IKEv2, μια IPsec ασφαλής σύνδεση (IPsec ESP Tunnel) πρέπει να εγκατασταθεί ανάμεσα στο HeNB και το SeGW. Ακολουθεί δέσμευση μιας IP διεύθυνσης από το SeGW. Όλα τα δεδομένα σηματοδοσίας, χρηστών και διαχείρισης της κίνησης στο ασύρματο μέσο μεταξύ των HeNB και SeGW, αποστέλλονται μέσω μιας διόδου IPsec ESP που έχει καθιερωθεί ως αποτέλεσμα της διαδικασίας αυθεντικοποίησης (με τη χρήση NAT-T UDP ενθυλάκωση αν είναι απαραίτητο) [18].

Έλεγχος Πρόσβασης

Για την αποτροπή μη εξουσιοδοτημένης πρόσβασης, μόνο ο εξουσιοδοτημένος χρήστης μπορεί να έχει πρόσβαση σε ένα HeNB. Για έναν τέτοιο έλεγχο πρόσβασης (CSG), ο χρήστης πρέπει να εισάγει πληροφορίες (ταυτότητες, αναγνωριστικά, τηλέφωνα) σε μια λίστα ελέγχου πρόσβασης είτε μέσω τηλεφώνου ή μέσω ενός Web Interface.

Μηχανισμοί Ασφαλείας Συγχρονισμού Ρολογιού/Χρόνου (Time Server)

Η ύπαρξη χρονισμού με κάποιον Time Server για την επικοινωνία του HeNB με το κεντρικό δίκτυο (SeGW), απαιτείται για την εγκατάσταση ασφαλών συνδέσεων (IKEv2 και TLS) και την επικύρωση έγκυρων διαπιστευτηρίων. Κάθε HeNB πρέπει να είναι εφοδιασμένο με ένα ρολόι, το οποίο κατά την σύνδεση του με το κεντρικό δίκτυο πρέπει να συγχρονίζεται με το ασφαλές ρολόι του Time Server. Ο συγχρονισμός αυτός ανανεώνεται κάθε 48 ώρες.

Ένα σημαντικό ζήτημα που προκύπτει σχετικά με το χρονισμό είναι κατά τη διάρκεια μιας ασφαλούς εγκατάστασης μέσω του Backhaul συνδέσμου, όπου δεν υπάρχει άμεσα η δυνατότητα σύνδεσης με κάποιο εξωτερικό Time Server. Στην περίπτωση αυτή είναι αναγκαία η χρήση τοπικού χρονισμού κατά την εκκίνηση. Ο χρόνος αποθηκεύεται στην ασφαλή μονάδα TrE όταν αποσυνδέεται και συνεχίζει τον χρονισμό από το προηγούμενο σημείο κατά την ενεργοποίηση, μέθοδο που αποτρέπει τον λανθασμένο χρονισμό ή και την μη ύπαρξη χρονισμού λόγο αποφόρτισης της μπαταρίας ή κάποιου κακού εξοπλισμού (σφάλμα), παράγοντες που δεν επιτρέπουν την σύνδεση του HeNB στο δίκτυο.

4.5.3 Διαδικασίες Ασφάλειας του HeNB και του HeMS

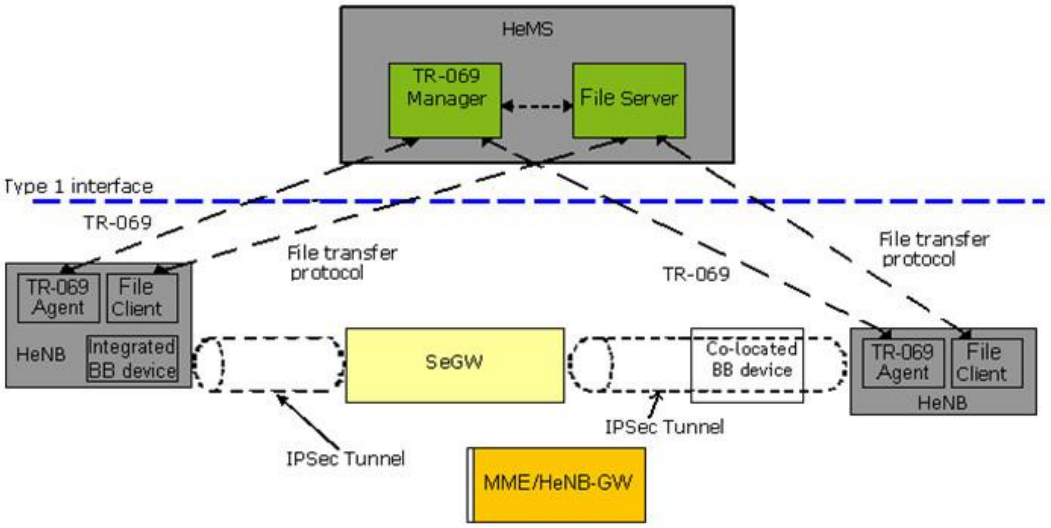
Η ασφάλεια του υπεύθυνου στοιχείο για τη διαχείριση του HeNB (Management System - HeMS), σχετίζεται με τον τρόπο πρόσβασης σε αυτό (Εικόνα 4.6), αν δηλαδή είναι προσβάσιμο,

- ✓ είτε τοπικά στο δίκτυο του διαχειριστή (Intranet του MNO).
- ✓ είτε μέσω του δημόσιου Internet.

Σε περίπτωση που το HeMS είναι προσβάσιμο από το Intranet του MNO, η κίνηση των δεδομένων του HeMS μπορεί να προστατευθεί μέσω της υποστήριξη ενός από τους δύο μηχανισμούς ασφαλείας που καθορίζονται από πολιτικές ασφαλείας του Διαχειριστή του Δικτύου.

- Προστασία με hop-by-hop τρόπο. Η κίνηση του HeMS προστατεύεται με το IPsec πρωτόκολλο εγκατεστημένο ανάμεσα στο HeNB και στο SeGW.
- Προστασία με end-to-end τρόπο ανάμεσα στο HeNB και στο HeMS, με τη χρήση μιας σύνδεσης TLS μέσα στην ήδη υπάρχουσα IPsec σύνδεση. Όταν το TLS χρησιμοποιείται για την επικοινωνία των στοιχείων HeNB και HeMS, η αμοιβαία αυθεντικοποίηση αναμεσά τους βασίζεται στα διαπιστευτήρια συσκευής για το HeNB και στα διαπιστευτήρια δικτύου για το HeNB, ενώ και οι δύο οντότητες ελέγχουν τα διαπιστευτήρια για την εγκυρότητα τους.

Στην άλλη περίπτωση που το HeMS είναι προσβάσιμο από το δημόσιο Internet, είναι εκτεθειμένο μέσω ενός ανασφαλές δικτύου σε απειλές και επιθέσεις. Η εγκατάσταση μιας ασφαλούς TLS σύνδεσης, προστατεύει τα δύο επικοινωνούντα μέρη. Ένα HeNB επαληθεύει την ταυτότητα του HeMS ελέγχοντας το πεδίο subjectAltName στα διαπιστευτήρια του HeMS. Για τη διαχείριση του HeNB από το HeMS αλλά και για το κατέβασμα λογισμικού από το HeMS, το CPE WAN πρωτόκολλο διαχείρισης TR-069 χρησιμοποιείται.



Εικόνα 4.6: Αρχιτεκτονική Διαχείρισης HeMS [46].

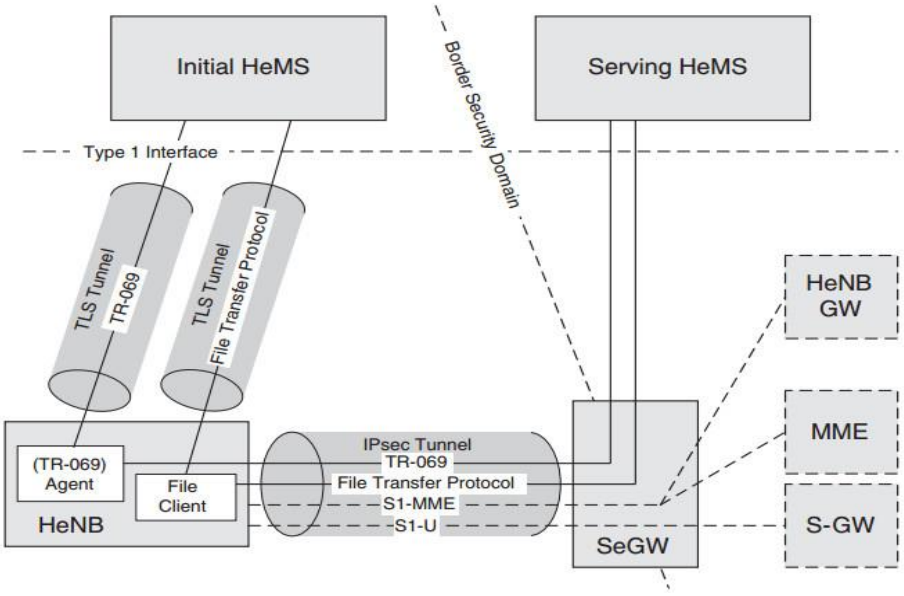
Είναι δυνατόν για λογικό διαχωρισμό ανάμεσα σε δύο συστήματα διαχείρισης HeMS.

1. **Initial HeMS.**
2. **Serving HeMS**.

Το Initial HeMS ορίζεται ως το πρώτο σημείο επαφής για τη διαχείριση του HeNB μετά την πρώτη ενεργοποίηση ή μετά από μια επαναφορά της HeNB στις προεπιλεγμένες εργοστασιακές του τιμές. Οι προδιαγραφές που ορίζονται στο 3GPP δεν προσδιορίζουν αν το Initial HeMS ανήκει στον διαχειριστή του δικτύου, τον κατασκευαστή του HeNB ή του πωλητή, ή από κάποιο τρίτο μέρος (Third Party). Αυτό επιτρέπει μεγαλύτερη ευελιξία της διαδικασίας εγγραφής των HeNBs στο δίκτυο του παρόχου, χωρίς να απαιτείται η τροφοδότηση των παραμέτρων του

παρόχου κατά τη στιγμή της παραγωγής ή της παράδοσης από το εργοστάσιο. Εξαιτίας αυτού, το Initial HeMS χρησιμοποιείται κυρίως για το δημόσιο Internet. Εάν το Initial HeMS βρίσκεται ενός του τομέα ασφάλειας του διαχειριστή πίσω από το SeGW, αυτό ονομάζεται Initial SeGW, και η διεύθυνση αυτού πρέπει να τροφοδοτείται στο HeNB.

Το Serving HeMS είναι το σύστημα διαχείρισης που φροντίζει για τη καθημερινή διαχείριση του HeNB. Είναι πιο πιθανό να βρίσκεται εντός του δικτύου του παρόχου, καθώς τα καθήκοντα διαχείρισης είναι στενά συνδεδεμένα με την πραγματικές λειτουργίες του δικτύου του διαχειριστή σε αντίθεση με το Initial HeMS που περιορίζεται στην τροφοδότηση των παραμέτρων του HeNB. Κατά την πρώτη σύνδεση με το δίκτυο, το HeNB συνδέεται με το Serving HeMS και εκτελεί εργασίες διαχείρισης παραμέτρων και ρυθμίσεων, αλλά και ενημερώσεις λογισμικού. Αν το Serving HeMS βρίσκεται εντός του τομέα ασφάλειας του διαχειριστή, τότε το SeGW χρησιμοποιείται. Αυτό απαιτεί φυσικά διαχωρισμένα SeGW ή μια ξεχωριστή δίοδο IPsec για την διαχείριση της κυκλοφορίας.



Εικόνα 4.7: Initial HeMS και Serving HeMS.

Η διάκριση του Initial HeMS και του Serving HeMS είναι πρωτίστως λογική και δεν υπάρχει ανάγκη για δύο ξεχωριστές οντότητες (Εικόνα 4.7).

Σύμφωνα με την Εικόνα 4.7, κατά την πρώτη ενεργοποίηση του HeNB συνδέεται με το Initial HeMS που έχει ρυθμιστεί με το FQDN του SeGW στην πλευρά του

παρόχου και η εσωτερική FQDN από το Serving HeMS. Τα FQDNs μπορεί να αντικαθίστανται από τις διευθύνσεις IP, αν το DNS δεν είναι διαθέσιμο για την επίλυση Domain Names. Όλα αυτά συμβαίνουν μέσω μιας διόδου TLS. Στη συνέχεια, η HeNB αποσυνδέεται από το Initial HeMS, γίνεται εγκατάσταση μιας ασφαλής σύνδεσης στο Backhaul και στη συνέχεια συνδέεται με το Initial HeMS στο δίκτυο του παρόχου. Η διασύνδεση S1 χρησιμοποιείται για να αποδειχθεί ότι η διαχείριση των δεδομένων του χρήστη αλλά και των δεδομένων σηματοδοσίας αντιμετωπίζονται το ίδιο.

Επαλήθευση Τοποθεσίας

Οι διαχειριστές των δικτύων απαιτούν την γνωστοποίηση της τοποθεσίας των HeNBs, για να μπορούν να παρέχουν υπηρεσίες διαχείρισης και ασφάλειας. Το HeMS διενεργεί την διαδικασία εξακρίβωσης τοποθεσίας. Οι μέθοδοι όπως είδαμε και στο κεφάλαιο 3, είναι τρείς:

- Με τη χρήση της δημόσιας διεύθυνσης IP της συσκευής που παρέχεται από το HeNB ή από τον πάροχο της ευρυζωνικής πρόσβασης.
- Με πληροφορίες για τις κοντινές μακροκυψέλες στο HeNB.
- Με γεωγραφικές συντεταγμένες (Geo-Coordinates) που παρέχονται από ένα δέκτη GNSS ενσωματωμένο στο HeNB.

4.5.4 Διαδικασίες Ασφαλείας Άμεσης Διασύνδεσης μεταξύ HeNBs

Η ασφάλεια για την άμεση σύνδεση των διεπαφών X2, πρέπει να παρέχει εμπιστευτικότητα και ακεραιότητα. Επιλέχτηκαν οι ίδιοι κρυπτογραφικοί μηχανισμοί όπως και για το Backhaul ανάμεσα στα HeNB και στο SeGW, δηλαδή αυθεντικοποίηση με IKEv2, IPsec καθώς και επικύρωση διαπιστευτηρίων.

Απειλές ενάντια στο H(e)NB και η Επικινδυνότητα τους

5

Σύμφωνα με τον πίνακα 4.1 του προηγούμενου κεφαλαίου με την ομαδοποίηση των απειλών σε θεματικές κατηγορίες, ακολουθεί μια λεπτομερής περιγραφή των γνωστών απειλές που έχουν καταγραφεί από το 3GPP και αποτυπώνονται στην τεχνική αναφορά (TR 33.820) [5] και στη συνέχεια χαρακτηρίζονται ως προς τον βαθμό επικινδυνότητας τους, την πιθανότητα εκτέλεσης τους, τα στοιχεία που επηρεάζουν και οι προτεινόμενοι τρόποι αντιμετώπισης τους.

Σύμφωνα με την τεχνική αναφορά η λίστα είναι η παρακάτω:

1.	Έκθεση ενός HeNB Token αυθεντικοποίησης από μία Brute Force απειλή μέσω ενός αδύναμου αλγόριθμου αυθεντικοποίησης.
2.	Έκθεση ενός HeNB Token αυθεντικοποίησης από μια τοπικά φυσική εισβολή.
3.	Εισαγωγή ενός Token αυθεντικοποίησης σε ένα παραποιημένο HeNB.
4.	Κλωνοποίηση του HeNB Token αυθεντικοποίησης από κάποιον χρήστη.
5.	Man-In-The-Middle επιθέσεις στο HeNB κατά την πρώτη πρόσβαση στο δίκτυο.
6.	Εκκίνηση του HeNB με κάποιο κακόβουλο λογισμικό (“Re-Flashing”).
7.	Μη-έγκυρες ενημερώσεις λογισμικού και αλλαγές στις παραμέτρους.
8.	Φυσική παραποίηση του HeNB.
9.	Κρυφάκουσμα των UTRAN ή E-UTRAN δεδομένων ενός χρήστη.
10.	Μεταμφίεση με σκοπό την μίμηση άλλων χρηστών.

11.	Αλλαγή της τοποθεσίας του HeNB χωρίς αναφορά.
12.	Λογισμικό προσομοίωσης του HeNB.
13.	Κίνηση (Traffic Tunneling) μεταξύ HeNBs.
14.	Κακή εγκατάσταση (Misconfiguration) του αναχώματος ασφάλειας (Firewall) στο Modem/Router.
15.	Επιθέσεις άρνησης υπηρεσίας (DoS) ενάντια στο HeNB.
16.	Επιθέσεις άρνησης υπηρεσίας (DoS) ενάντια στο κεντρικό δίκτυο.
17.	Έκθεση του HeNB εκμεταλλεύοντας τις αδυναμίες των ενεργών υπηρεσιών δικτύου.
18.	Αποκάλυψη της ταυτότητας του δικτύου του χρήστη μέσω του HeNB.
19.	Αλλαγές στις ρυθμίσεις του HeNB.
20.	Παραποίηση των ρυθμίσεων της λίστας ελέγχου πρόσβασης (ACL) ή έκθεση της λίστας.
21.	Αλλοίωση πόρων διαχείρισης.
22.	Μεταμφίεση ως ένα έγκυρο HeNB.
23.	Παροχή ασύρματης πρόσβασης μέσω ενός CSG.
24.	Ανακοινώνοντας εσφαλμένη θέση στο δίκτυο.
25.	Χειραγώγηση της εξωτερικής πηγής του χρόνου.
26.	Επιθέσεις περιβάλλοντος/Πλευρικού καναλιού ενάντια του HeNB.
27.	Επίθεση στο OAM και την κίνηση του.
28.	Απειλή του δικτύου πρόσβασης στο HeNB.
29.	Μεταπομπή στο CSG του HeNB.

Πίνακας 5.1: Λίστα απειλών στο HeNB.

5.1 Κατηγοριοποίηση Απειλών

Κατηγοριοποιούνται οι παραπάνω απειλές του Πίνακα 5.1 σε σχέση με τα είδη των απειλών.

Αποκάλυψη ή Υποκλοπή των διαπιστευτηρίων του HeNB

- Έκθεση ενός HeNB Token αυθεντικοποίησης από μία Brute Force απειλή μέσω ενός αδύναμου αλγόριθμου αυθεντικοποίησης.

- Έκθεση ενός HeNB Token αυθεντικοποίησης από μια τοπικά φυσική εισβολή.
- Κλωνοποίηση του HeNB Token αυθεντικοποίησης από κάποιον χρήστη.

Φυσικές επιθέσεις έναντι του HeNB (Physical Attacks)

- Εισαγωγή ενός Token αυθεντικοποίησης σε ένα παραποιημένο HeNB.
- Εκκίνηση του HeNB με κάποιο κακόβουλο λογισμικό ("Re-Flashing").
- Φυσική παραποίηση του HeNB.
- Επιθέσεις περιβάλλοντος/Πλευρικού καναλιού ενάντια του HeNB.

Επιθέσεις διαμόρφωσης του HeNB (Ρύθμιση Attacks)

- Μη-έγκυρες ενημερώσεις λογισμικού και αλλαγές στις παραμέτρους.
- Αλλαγές στις ρυθμίσεις του HeNB.
- Παραποίηση των ρυθμίσεων της λίστας ελέγχου πρόσβασης (ACL), ή έκθεση της λίστας.

Επιθέσεις πρωτοκόλλων (Protocol Attacks)

- Man-In-The-Middle επιθέσεις στο HeNB κατά την πρώτη πρόσβαση στο δίκτυο.
- Επιθέσεις άρνησης υπηρεσίας (DoS) ενάντια στο HeNB.
- Έκθεση του HeNB εκμεταλλεύοντας τις αδυναμίες των ενεργών υπηρεσιών δικτύου.
- Χειραγώγηση της εξωτερικής πηγής του χρόνου.
- Επίθεση στο OAM και την κίνηση του.
- Απειλή του δικτύου πρόσβασης στο HeNB.
- Μεταπομπή στο CSG του HeNB.

Επιθέσεις στο κεντρικό δίκτυο & Επιθέσεις τοποθεσίας του HeNB

- Αλλαγή της τοποθεσίας του HeNB χωρίς αναφορά.
- Λογισμικό προσομοίωσης του HeNB.
- Κίνηση (Traffic Tunneling) μεταξύ HeNBs.
- Κακή εγκατάσταση (Misconfiguration) του αναχώματος ασφάλειας (Firewall) στο Modem/Router.
- Επιθέσεις άρνησης υπηρεσίας (DoS) ενάντια στο κεντρικό δίκτυο.
- Ανακοινώνοντας εσφαλμένη θέση στο δίκτυο.

Επιθέσεις έναντι ιδιωτικών δεδομένων των χρηστών

- Κρυφάκουσμα των UTRAN ή E-UTRAN δεδομένων ενός χρήστη.
- Μεταμφίεση με σκοπό την μίμηση άλλων χρηστών.
- Αποκάλυψη της ταυτότητας του δικτύου του χρήστη μέσω του HeNB.
- Μεταμφίεση ως ένα έγκυρο HeNB.
- Παροχή ασύρματης πρόσβασης μέσω ενός CSG.

Επιθέσεις διαχείρισης και πόρων

- Αλλοίωση πόρων διαχείρισης.

5.2 Περιγραφή και Επικινδυνότητα Απειλών

Παρακάτω ακολουθείται μια περιγραφή των παραπάνω απειλών/επιθέσεων (Πίνακας 5.1), αναφέροντας τις προϋποθέσεις κάτω από τις οποίες η κάθε απειλή χρειάζεται, για να εξαπολύσει την επίθεσή της, την πιθανότητα εκτέλεσης, την έκταση που μπορεί να λάβει και τις οντότητες που μπορεί να βλάψει και τέλος τρόποι για τον περιορισμό της απειλής/επίθεσης [11][48].

1. Έκθεση ενός HeNB Token αυθεντικοποίησης από μία Brute Force απειλή μέσω ενός αδύναμου αλγόριθμου αυθεντικοποίησης

Ένα παράδειγμα Token για έναν αδύναμο αλγόριθμο αυθεντικοποίησης είναι το GSM SIM με COMP128-1, το οποίο είναι γνωστό ότι είναι δυνατόν να "σπάσει" με επίθεση Brute Force. Τέτοιες επιθέσεις σε ένα HeNB μπορούν να ξεκινήσουν από πλαστογραφημένη πρόσβαση στο δίκτυο αν η αρχική επικοινωνία πρόσβασης δεν είναι επαρκώς προστατευμένη.

Πιθανότητα Εκτέλεσης: Πιθανή.
Επικινδυνότητα Επίθεσης/Απειλής: Επιβλαβής, αλλά μόνο σε συνδυασμό με άλλες απειλές.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Τα Token αυθεντικοποίησης με τη χρήση αδύναμων αλγορίθμων δε θα πρέπει να χρησιμοποιούνται για την αυθεντικοποίηση με το HeNB. Επιπλέον, ο

μηχανισμός προστασίας για το Backhaul σύνδεσμο θα πρέπει να είναι αρκετά ισχυρός.

2. Έκθεση ενός HeNB Token αυθεντικοποίησης από μια τοπικά φυσική εισβολή

Ένας εισβολέας εκμεταλλεύεται την τοπική, φυσική πρόσβαση στη συσκευή και μπορεί να διαβάζει τα διαπιστευτήρια αυθεντικοποίησης από τα καλώδια του HeNB. Λαμβάνει ένα αντίγραφο και μετά από αυτό, οποιαδήποτε άλλη συσκευή μπορεί να το χρησιμοποιήσει και να μιμηθεί το HeNB.

Πιθανότητα Εκτέλεσης: Εξαρτάται από την εφαρμογή. Εάν τα δεδομένα αυθεντικοποίησης δεν είναι αποθηκευμένα σε ένα προστατευόμενο τομέα όπως την μονάδα TPM ή UICC, η πιθανότητα μιας τέτοιας απειλής είναι υψηλή. Σε αντίθετη περίπτωση είναι χαμηλή.
Επικινδυνότητα Επίθεσης/Απειλής: Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Τα διαπιστευτήρια αυθεντικοποίησης του HeNB θα πρέπει να αποθηκεύονται μέσα σε μια ασφαλή περιοχή/τομέα, κάνοντας δύσκολη την απόκτησή τους από εξωτερικές οντότητες.

3. Εισαγωγή ενός Token αυθεντικοποίησης σε ένα παραποιημένο HeNB

Ένας χρήστης εισάγει ή κάνει εγκατάσταση έγκυρων Tokens αυθεντικοποίησης σε ένα ψευδές HeNB.

Πιθανότητα Εκτέλεσης: Πιθανή.
Επικινδυνότητα Επίθεσης/Απειλής: Ένα παραποιημένο HeNB με πρόσθετα χαρακτηριστικά (Re-Flashed, ή ένα HeNB ενός διαφορετικού κατασκευαστή μη συμβατού) μπορεί να αυθεντικοποιήσει τον εαυτό του στο δίκτυο κάνοντας χρήση ενός έγκυρου διαπιστευτηρίου, προχωρώντας σε κάθε είδους παραβίαση της ασφάλειας.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.

Αντιμετώπιση: Ένας σταθερό, μη αποσπώμενο Token αυθεντικοποίησης μπορεί να μετριάσει τον κίνδυνο ή η εισαγωγή κρυπτογράφησης ανάμεσα στα δύο μέρη. Επίσης, οι νέοι χρήστες θα μπορούσαν να επιβεβαιώνουν ρητά την αποδοχή τους πριν την σύνδεσή τους με το HeNB. Αυτή η προσέγγιση βασίζεται σε πρόσθετο έλεγχο πρόσβασης στο κεντρικό δίκτυο και όχι μόνο στο HeNB.

4. Κλωνοποίηση του HeNB Token αυθεντικοποίησης από κάποιον χρήστη

Ο επιτιθέμενος κλωνοποιεί διαπιστευτήρια έγκυρων HeNB και τα χρησιμοποιεί εισάγοντας τα σε άλλο HeNB. Το κλωνοποιημένο HeNB ενεργοποιείται κοντά στο νόμιμο HeNB.

Πιθανότητα Εκτέλεσης: Πιθανή.
Επικινδυνότητα Επίθεσης/Απειλής: Πολύ Επιβλαβής
Στοιχεία/Οντότητες που επηρεάζει: Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Τα διαπιστευτήρια αυθεντικοποίησης θα πρέπει να είναι δύσκολο να κλωνοποιηθούν. Πολλαπλές εκδόσεις του ίδιου HeNB στο κεντρικό δίκτυο δε θα πρέπει να επιτρέπονται να αποκτούν πρόσβαση. Ακόμα, ορισμένες μορφές κλειδώματος θέσης (DSL Line) μπορούν να μειώσουν τον κίνδυνο της απειλής.

5. Man-In-The-Middle επιθέσεις στο HeNB κατά την πρώτη πρόσβαση στο δίκτυο

Το HeNB κάνει μια πρώτη επαφή με το δίκτυο του πάροχο και κατά τη διάρκεια αυτής της επαφής τα τερματικά σημεία του διαχειριστή δεν μπορούν να προσδιορίσουν αξιόπιστα τους ομότιμους χρήστες. Ένας εισβολέας στο διαδίκτυο μπορεί να παρακολουθήσει όλη την κυκλοφορία από το HeNB και αργότερα να αποκτήσει πρόσβαση σε όλες τις ιδιωτικές πληροφορίες. Εάν τα δεδομένα αυθεντικοποίησης δεν είναι μοναδικά για το HeNB, μια επανάληψη επίθεσης (Replay Attack) μπορεί να είναι δυνατή.

Πιθανότητα Εκτέλεσης: Πιθανή.
Επικινδυνότητα Επίθεσης/Απειλής: Πολύ Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: Χρήστη, Δίκτυο Παρόχου.

Αντιμετώπιση: Η απειλή είναι πιθανή στην περίπτωση που το HeNB δεν έχει προεγκατεστημένα μοναδικά διαπιστευτήρια αυθεντικοποίησης. Πρέπει να έχει αποκτήσει τα διαπιστευτήρια αυθεντικοποίησης ήδη κατά την πρώτη επαφή με το δίκτυο. Αυτά τα διαπιστευτήρια πρέπει να αναγνωρίζονται στην πλευρά του χειριστή. Μια μη-αυθεντικοποιημένη κυκλοφορία δεν πρέπει να γίνεται αποδεκτή ακόμη και στη πρώτη φάση επικοινωνίας (First-Contact). Μπορούν να χρησιμοποιηθούν τα USIM, UICC ή ακόμα και διαπιστευτήρια του ίδιου του πωλητή για το σκοπό αυτό. Οι υλικοτεχνικές επιπτώσεις θα μπορούσαν να είναι διαφορετικές. Το UICC θα μπορούσε να εισαχθεί στο HeNB από τη στιγμή της πώλησης ή αργότερα από τον ίδιο τον πελάτη. Το διαπιστευτήριο του προμηθευτή πρέπει να είναι εισαχθεί στο HeNB στο στάδιο της κατασκευής. Εάν χρησιμοποιείται κάποιο πρωτόκολλο ανταλλαγής κλειδιών (Key Exchange)[19] τότε η επικοινωνία είναι πιο ασφαλής.

6. Εκκίνηση του HeNB με κάποιο κακόβουλο λογισμικό ("Re-Flashing Software, Firmware")

Το λογισμικό εκκίνησης (Boot Software) στο HeNB τροποποιείται από τον επιτιθέμενο, έχοντας φυσική παρουσία. Οι μέθοδοι επίθεσης που χρησιμοποιεί μετά, είναι και προς το HeNB αλλά και προς τον πάροχο, (κρυφάκουσμα, μίμηση, διακοπή του δικτύου ακόμα και Dos επιθέσεις).

Πιθανότητα Εκτέλεσης:
Επικινδυνότητα Επίθεσης/Απειλής: Καταστροφική σε περίπτωση που ένας κωδικός εκκίνησης χρησιμοποιείται. Για παράδειγμα, Re-Flashing του κινητού τηλεφώνου για να αποφευχθούν διάφοροι περιορισμοί ή να ξεκλειδώσουν προηγμένες λειτουργίες, είναι μια κοινή πρακτική σε ορισμένα μέρη του κόσμου.

Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Η διαδικασία εκκίνησης θα πρέπει να συνδυάζεται με μέσα κρυπτογράφησης όπως μια μονάδα TPM. Σε περίπτωση USIM-Based HeNB στο δίκτυο, περαιτέρω μέτρα ασφάλειας χρειάζονται.

[19] Όπως με την προαιρετική αυθεντικοποίηση κωδικών Diffie-Hellman Key Exchange πρωτόκολλο στο CDMA2000, C.S0016 ή στο IETF RFC 5683.

7. Μη-έγκυρες ενημερώσεις λογισμικού και αλλαγές στις παραμέτρους

Ένα HeNB πρέπει να δέχεται ενημερώσεις από το δίκτυο του παρόχου. Σε περίπτωση που το κέντρο διανομής λογισμικού τεθεί σε κίνδυνο, τότε ένας μεγάλος αριθμός HeNBs μπορεί να λάβει και να εγκαταστήσει κακόβουλο λογισμικό.

Πιθανότητα Εκτέλεσης: Πιθανή. Το κέντρο διανομής βρίσκεται σε έναν ασφαλή τομέα, παρόλα αυτά κάποιος επιτιθέμενος, (πιθανών υπάλληλος) μπορεί να προβεί σε τέτοιες ενέργειες.
Επικινδυνότητα Επίθεσης/Απειλής: Εξαιρετικά Επιβλαβής, (με κίνδυνο επέκτασης σε πληθώρα από HeNBs).
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Όλες οι ενημερώσεις του λογισμικού και των ρυθμίσεων θα πρέπει να συνοδεύονται από μια ψηφιακή κρυπτογραφημένη υπογραφή, που το HeNB θα πρέπει να μπορεί να έχει τα απαιτούμενα μέσα για να επαληθεύσει.

8. Φυσική παραποίηση του HeNB

Στοιχεία του HeNB μπορούν να τροποποιηθούν ή και να αντικατασταθούν.

Πιθανότητα Εκτέλεσης: Πιθανή. Ένας χρήστης ή επιτιθέμενος θα μπορούσε να τροποποιήσει κάποιο στοιχείο του HeNB, για παράδειγμα η αντικατάσταση της κεραίας με κάποια με μεγαλύτερο κέρδος απολαβής, για να επεκτείνει την κάλυψη.
Επικινδυνότητα Επίθεσης/Απειλής: Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: το HeNB θα πρέπει να προστατεύεται τοπικά, αποτρέποντας την εύκολη τροποποίηση. Υπολογιστικές μέθοδοι ασφάλειας μπορούν να χρησιμοποιηθούν για να ανιχνεύονται κρίσιμες τροποποιήσεις του υλικού.

9. Κρυφάκουσμα των UTRAN ή E-UTRAN δεδομένων ενός χρήστη

Ένας εισβολέας με ένα αγορασμένο HeNB το εγκαθιστά και το ρυθμίζει στην λειτουργία ανοικτής πρόσβασης (Open Access). Δεδομένων τα οποία δεν είναι ούτε διαθέσιμα στην ασύρματη ζεύξη χωρίς προστασία, αλλά ούτε με την ασφάλεια IP,

μπορούν να διαβαστούν. Όλα τα στοιχεία που ρέουν μεταξύ του θύματος και του δικτύου θα μπορούσαν να διαβαστούν.

Πιθανότητα Εκτέλεσης: Πιθανή. Η ανάγνωση δεδομένων από τα καλώδια είναι δύσκολη, καθώς και οι κατασκευαστές συνιστούν οι διαδικασίες να εκτελούνται μέσα σε ένα προστατευμένο τσιπ (Chip). Αν ο κατασκευαστής δε μπορεί να το παρέχει αυτό, τότε μπορεί να εκτελείται κρυπτογράφηση στα δεδομένα.

Επικινδυνότητα Επίθεσης/Απειλής: (Πολύ) Επιβλαβής. Εξαρτάται από την ευαισθησία και την αξία των δεδομένων.

Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη.

Αντιμετώπιση: Απροστάτευτα δεδομένα δε θα πρέπει να διακινούνται εκτός ασφαλούς τομέα εσωτερικά του HeNB. Ο χρήστης θα μπορούσε να ενημερώνεται αν πλησιάζει και σε τι τύπου πρόσβασης HeNBs, όπως και αν προστίθεται σε μια λίστα κλειστού τύπου πρόσβασης. Η απειλή εφαρμόζεται και στην περίπτωση του κλειστού τύπου πρόσβασης.

10. Μεταμφίεση με σκοπό την μίμηση άλλων χρηστών

Παρόμοια περιγραφή με την απειλή 9, με τη μόνη διαφορά είναι ότι στο 9 ο εισβολέας ακούει μόνο, ενώ στην απειλή 10 ο εισβολέας διοχετεύει επίσης πλαστογραφημένα δεδομένα κυκλοφορίας.

Πιθανότητα Εκτέλεσης: Πιθανή, αλλά πιο δύσκολη από την απειλή των υποκλοπών.

Επικινδυνότητα Επίθεσης/Απειλής: (Πολύ) Επιβλαβής. Δυνατότητα για την πλαστογράφηση 3G/LTE κλήσεων μπορεί να έχει σοβαρές και εκτεταμένες επιπτώσεις . Αν ένα HeNB λειτουργεί σε ένα ανοικτό τρόπο πρόσβασης, ο αντίκτυπος της επίθεσης είναι χειρότερος δεδομένου ότι ο εισβολέας θα μπορούσε να αφουγκράζομαι κάθε κινητό τερματικό και όχι μόνο εκείνους που έχουν εξουσιοδοτηθεί να χρησιμοποιούν το HeNB.

Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη.

Αντιμετώπιση: Απροστάτευτα δεδομένα του χρήστη δεν πρέπει ποτέ να αφήνουν την ασφαλή περιοχή εσωτερικά του HeNB. Ο χρήστης μπορεί να ειδοποιείται όταν εισέρχεται σε ένα κλειστού ή ανοικτού τύπου πολιτική πρόσβασης.

11. Αλλαγή της τοποθεσίας του HeNB χωρίς αναφορά

Οι πελάτες μπορούν να μεταφέρουν το HeNB και με αυτόν τον τρόπο να κάνουν τα δεδομένα τροφοδότησης τοποθεσίας τους μη διαθέσιμα.

Πιθανότητα Εκτέλεσης: Πολύ Πιθανή.
Επικινδυνότητα Επίθεσης/Απειλής: Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Ο μηχανισμός κλειδώματος θέσης θα πρέπει να σχεδιάζεται και να υλοποιείται. Αν ένα αποσπώμενο Token χρησιμοποιείται για την επικύρωση του HeNB (περίπτωση 3 ή 4), μπορεί να είναι πιο εύκολο για έναν εισβολέα να επωφεληθεί από έναν αδύναμο ή ανύπαρκτο μηχανισμό κλειδώματος τοποθεσίας.

12. Λογισμικό προσομοίωσης του HeNB

Η επικοινωνία του HeNB με το κεντρικό δίκτυο προσομοιώνεται με μια εφαρμογή που τρέχει λογισμικό σε έναν υπολογιστή που είναι συνδεδεμένος στο οικιακό δίκτυο, με ή χωρίς τη συγκατάθεση του χρήστη.

Πιθανότητα Εκτέλεσης: Μάλλον χαμηλή, ανάλογα με τη δύναμη της αυθεντικοποίησης του HeNB με το κεντρικό δίκτυο και σχετικά με τα μέτρα για την απομάκρυνση/κλωνοποίηση του Token αυθεντικοποίησης. Αν το Token είναι αποσπώμενο, ο νόμιμος χρήστης θα μπορούσε να εκτελεί σκόπιμα αυτή την απειλή.

Επικινδυνότητα Επίθεσης/Απειλής: Πολύ Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Επειδή η προσομοίωση λογισμικού δεν μπορεί να προβλεφθεί, είναι απαραίτητο να εφαρμοστεί ισχυρή αυθεντικοποίηση πρόσβασης και να εμποδίζεται η αφαίρεση/κλωνοποίηση Token αυθεντικοποίησης.

13. Κίνηση (Traffic Tunneling) μεταξύ HeNBs

Ένα HeNB χρησιμοποιείται σε μια νόμιμη τοποθεσία αλλά με κίνηση από ένα ή περισσότερα HeNBs με λανθασμένες τοποθεσίες. Η παράνομη επιπρόσθετη κίνηση δρομολογείται δια μέσου του Internet στο HeNB.

Πιθανότητα Εκτέλεσης: Ασαφής.

Επικινδυνότητα Επίθεσης/Απειλής: Πολύ Επιβλαβής.

Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.

Αντιμετώπιση: Το HeNB θα πρέπει να είναι σε θέση να ανιχνεύει την κίνηση που δεν προέρχεται από τις τοπικές συνδεδεμένες συσκευές.

14. Κακή εγκατάσταση (Misconfiguration) του αναχώματος ασφάλειας (Firewall) στο Modem/Router

Τα οικιακά σημεία πρόσβασης (όπως ένα HeNB) είναι συνήθως συνδεδεμένα με το Internet μέσω κάποιας ενσύρματη πρόσβασης (π.χ. DSL, Cable Modem). Σε αυτές τις περιπτώσεις, ένα Modem/Router θα μπορούσε να ενσωματωθεί με το HeNB, ή να είναι σε ξεχωριστό κουτί. Το Firewall στο Modem/Router συνήθως ελέγχεται από το χρήστη μέσω κάποιου Web Interface. Αλλά το HeNB απαιτεί καθορισμένες υπηρεσίες δικτύου (όπως TCP ή UDP πύλες) για να επικοινωνήσει με το GW του κεντρικού δικτύου. Οι υπηρεσίες αυτές αν είναι σε κοντινή απόσταση, εμποδίζουν το HeNB από τη σύνδεση με το κεντρικό δίκτυο. Εάν το μόντεμ δεν είναι ενσωματωμένο με το HeNB, ο χρήστης πρέπει να το ρυθμίσει σωστά, κάτι που οδηγεί σε λάθη.

Πιθανότητα Εκτέλεσης: Πιθανή.

Επικινδυνότητα Επίθεσης/Απειλής: Ενοχλητική. Επηρεάζεται η αξιοπιστία των υπηρεσιών και η υποβάθμιση της χρηστικότητας.

Στοιχεία/Οντότητες που επηρεάζει: Χρήστη.

Αντιμετώπιση: Σε περίπτωση που το Modem/Router είναι ενσωματωμένο με το HeNB, θα πρέπει να έχει προκαθοριστεί και ρυθμιστεί κατάλληλα η διαμόρφωση του καναλιού HeNB πρόσβασης για να μη μπορεί να τροποποιηθεί. Σε περίπτωση που το μόντεμ είναι ένα ξεχωριστό κουτί, πρέπει να εκτελείται σωστή διαμόρφωση. Μία πιθανή προσέγγιση μπορεί να χρησιμοποιεί uPnP μηχανισμό. Επιπλέον, ένα πρόσθετο τείχος προστασίας εντός του HeNB είναι επίσης χρήσιμο.

15. Επιθέσεις άρνησης υπηρεσίας (DoS) ενάντια στο HeNB

Οργάνωση επιθέσεων άρνησης υπηρεσιών από επιτιθέμενους.

Πιθανότητα Εκτέλεσης: Πιθανή.

Επικινδυνότητα Επίθεσης/Απειλής: Ενοχλητική.

Στοιχεία/Οντότητες που επηρεάζει: Χρήστη.

Αντιμετώπιση: Το HeNB απαλλάσσετε από το φόρτο της κίνησης επεξεργασίας με τη χρήση ενός Firewall στο Modem και ρυθμισμένο να δέχεται μόνο τα IKE μηνύματα και την ESP κρυπτογραφημένη κίνηση στο HeNB. Το IKEv2 είναι πιο ισχυρό από το IKEv1 ενάντια σε DoS επιθέσεις.

16. Επιθέσεις άρνησης υπηρεσίας (DoS) ενάντια στο κεντρικό δίκτυο

Εισβολέας οργανώνει επιθέσεις κατά των στοιχείων στο κεντρικό δίκτυο από το HeNB ή τα HeNBs (αν πρόκειται για πολλαπλά) από το σύνδεσμο Backhaul.

Πιθανότητα Εκτέλεσης: Πιθανή.

Επικινδυνότητα Επίθεσης/Απειλής: Από ενοχλητική μέχρι εξαιρετικά επιβλαβής. Οι υπηρεσίες του διαχειριστή μπορούν να διαταραχθούν με ένα μεγάλο αριθμό από HeNBs.

Στοιχεία/Οντότητες που επηρεάζει: HeNB.

Αντιμετώπιση: Βασικά στοιχεία του δικτύου που θα πρέπει να ασφαλίζονται περιλαμβάνουν το Security Gateway, το οποίο θα πρέπει να προστατεύει το Upstream του δικτύου από υπερφόρτωση και υπερχείλιση.

17. Έκθεση του HeNB εκμεταλλεύοντας τις αδυναμίες των ενεργών υπηρεσιών δικτύου

Το HeNB έχει συνήθως πολλές υπηρεσίες δικτύου (χειριστές πρωτοκόλλου) να "ακούνε" στις διεπαφές του δικτύου. Οι υπηρεσίες αυτές μπορεί να απαιτηθούν για κάποια λειτουργία (π.χ. DHCP, IKE, IPsec, PPPoE), ή μπορεί να "ακούνε" μόνο λόγω του σχεδιασμού της συσκευής (π.χ. RPC Portmapper). Ειδικά δημιουργημένη κίνηση που εισάγεται μέσω του Backhaul δικτύου ή τη τοπική σύνδεση μπορεί να προκαλέσει το χειρισμού πρωτοκόλλου να αποτύχει και στη συνέχεια να θέσει σε κίνδυνο το σύνολο του HeNB.

Πιθανότητα Εκτέλεσης: Πιθανή. Αυτό είναι το πιο διαδεδομένο είδος απομακρυσμένων επιθέσεων σε δίκτυα IP.
Επικινδυνότητα Επίθεσης/Απειλής: Εξαιρετικά Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Μειωμένες υπηρεσίες δικτύου (απενεργοποιημένες ή με τείχος προστασίας), δοκιμές για τη λειτουργική ευρωστία χειριστών πρωτοκόλλων, ανίχνευση εισβολών ψάχνουν για μη-φυσιολογική συμπεριφορά HeNB, επαναφορά σε μια ασφαλής επαληθευμένη κατάσταση του συστήματος.

18. Αποκάλυψη της ταυτότητας του δικτύου του χρήστη μέσω του HeNB

Το IMSI μπορεί να αποκαλυφτεί στον ιδιοκτήτη του HeNB κατά τη διάρκεια CSG διαχείρισης.

Πιθανότητα Εκτέλεσης: Υψηλή.
Επικινδυνότητα Επίθεσης/Απειλής: Εκθέτει την ιδιωτικότητα των χρηστών.
Στοιχεία/Οντότητες που επηρεάζει: Χρήστη.
Αντιμετώπιση: Το ID (IMSI) του HeNB προστατεύεται σε έναν ασφαλή τομέα εσωτερικά του HeNB.

19. Αλλαγές στις ρυθμίσεις του HeNB

Έχοντας πρόσβαση στις ρυθμίσεις του HeNB, ο εισβολέας μπορεί είτε να πάρει στα χέρια τους τον πλήρη έλεγχο του HeNB ή να κάνει κάποιες αλλαγές που θα επηρεάσουν την υπηρεσία που του παρέχεται από την HeNB. Εξαρτάται από ποιες δυνατότητες ρυθμίσεων παρέχονται για την εξάπλωση της απειλής.

Πιθανότητα Εκτέλεσης: Ανάλογα με την εφαρμογή και την ανάπτυξη.
Επικινδυνότητα Επίθεσης/Απειλής: Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Ασφαλής πρόσβαση στις ρυθμίσεις του HeNB αν είναι αναγκαίο.

20. Παραποίηση των ρυθμίσεων της λίστας ελέγχου πρόσβασης (ACL) ή έκθεση της λίστας

Ο εισβολέας τροποποιεί το ACL επιτρέποντας έτσι συσκευές που δεν πρέπει να έχουν πρόσβαση στο δίκτυο. Ο εισβολέας θα μπορούσε επίσης να αφαιρέσει συσκευές που πρέπει να έχουν πρόσβαση και ενδεχομένως να αλλάξει το επίπεδο προσβασιμότητας για διαφορετικές συσκευές.

Πιθανότητα Εκτέλεσης: Ανάλογα με την εφαρμογή και την ανάπτυξη.
Επικινδυνότητα Επίθεσης/Απειλής: Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Ασφαλές μέσο για τη δημιουργία, συντήρηση και αποθήκευση του ACL απαιτείται.

21. Αλλοίωση πόρων διαχείρισης

Το HeNB δίνει λανθασμένες πληροφορίες για τους πόρους οδηγώντας έτσι σε θέματα όπως η αύξηση των μεταπομπών, παράδοση όλων των κινητών τηλεφώνων στην περιοχή με της HeNB, ή αναγκαστική παράδοση όλων των συσκευών από την HeNB σε άλλα eNBs. Οι πληροφορίες των πόρων της ζεύξης μπορεί να είναι απλά στη μορφή της στάθμης ισχύος μεταδόσεως. Ο εισβολέας θα μπορούσε να εκτελεί απλή τροποποίηση, όπως την επέκταση διεύρυνσης περιοχής προσθέτοντας Booster σήμα σε κεραίες που οδηγούν σε αυξημένες παρεμβολές, αύξηση στο εύρος κλπ.

Πιθανότητα Εκτέλεσης: Πιθανή.
Επικινδυνότητα Επίθεσης/Απειλής: Δυνητικά Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Δεν θα πρέπει να υπάρχουν μέσα για τον έλεγχο των παραμέτρων των πόρων ασύρματα από ένα χρήστη. Η διεπαφή των ρυθμίσεων του HeNB θα πρέπει να χαρακτηρίζεται από επαρκή προστασία. Θα είναι δύσκολο να παρέχει προστασία έναντι μεγάλου φάσματος επέκτασης.

22. Μεταμφίεση ως ένα έγκυρο HeNB

Ο επιτιθέμενος αγοράζει ένα HeNB και το διαμορφώνει ανάλογα με εκείνο του HeNB που χρησιμοποιεί την κλειστή πολιτική πρόσβασης (CSG). Έχοντας κάνει αυτό ο εισβολέας, πρώτον απενεργοποιεί στο HeNB τις επιλογές κρυπτογράφησης

και ακεραιότητας και δεύτερον ελπίζει να έχει πρόσβαση στα κλειδιά του χρήστη HeNB. Ο εισβολέας μπορεί να το κάνει αυτό με τη σύνδεση του HeNB με την ενσύρματη ραχοκοκαλιά (Backbone) του HeNB της εταιρείας ή με τη χρήση multi-hop για να συνδέσει το HeNB με το έγκυρο HeNB στο ενσύρματο δίκτυο.

Πιθανότητα Εκτέλεσης: Ανάλογα με την εφαρμογή και την ανάπτυξη.
Επικινδυνότητα Επίθεσης/Απειλής: Πολύ Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Ρυθμίσεις για το CSG αλλά και άλλων θα πρέπει να αποκρύπτονται. Πρέπει να είναι δεσμευτικές μεταξύ HeNB και χρηστών που θα πρέπει να είναι γνωστοί στο δίκτυο. Η HeNB θα πρέπει να αυθεντικοποιείται στο δίκτυο. Σε περίπτωση διαρροής κλειδιών, αυτά θα πρέπει να προστατεύονται.

23. Παροχή ασύρματης πρόσβασης μέσω ενός CSG

Υπάρχουν διαφορετικοί τρόποι με τους οποίους ο εισβολέας μπορεί να λειτουργήσει, πρώτος τρόπος, διασυνδέει το HeNB σε μία από τις HeNBs που βρίσκονται στην λίστα του CSG χρησιμοποιώντας ένα καλώδιο Ethernet και δεύτερος τρόπος, ο επιτιθέμενος έχει ένα UE (κινητό ή μια κάρτα δεδομένων) συνδεδεμένο με το HeNB που ανήκει στην CSG και με κάποιο τρόπο είναι συνδεδεμένο με τους επιτιθέμενους HeNBs (ή άλλους τρόπους, όπως (802.11 σημείο πρόσβασης). Αυτό μπορεί να επιτευχθεί εύκολα από τον εισβολέα που συνδέει ένα UE μέσω ενός σημείου πρόσβασης σε ένα φορητό υπολογιστή. Ο εισβολέας μπορεί στη συνέχεια να προβεί σε πολλές επιθέσεις μερικές παρόμοιες με εκείνη που περιεγράφηκε για την απειλή 22 και άλλη είναι η τροφοδότηση δωρεάν υπηρεσιών μέσω από τα HeNBs που ανήκουν σε κάποιο CSG.

Πιθανότητα Εκτέλεσης: Ανάλογα με την εφαρμογή και την ανάπτυξη.
Επικινδυνότητα Επίθεσης/Απειλής: Ανάλογα με την εφαρμογή και την ανάπτυξη.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Η προώθηση στο επίπεδο Radio είναι δύσκολο να μειωθεί. Θα μπορούσαν να απαιτούν τη λήψη δακτυλικών αποτυπωμάτων RF (RF Fingerprinting).

24. Ανακοινώνοντας εσφαλμένη θέση στο δίκτυο

Ο επιτιθέμενος είτε αλλάζει τις πληροφορίες θέσης του HeNB ή είναι σε θέση να ενημερώνει λανθασμένα (Mis-Inform) το HeNB σχετικά με την τοποθεσία του. Έτσι, ένα κλεμμένο HeNB θα μπορούσε να χρησιμοποιηθεί σε μια ανεπιθύμητα θέση.

Πιθανότητα Εκτέλεσης: Πιθανή.
Επικινδυνότητα Επίθεσης/Απειλής: Επιβλαβές, ειδικά για τις υπηρεσίες κλήσης έκτακτης ανάγκης.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Απαιτείται ασφαλής τοποθεσία. Δεν θα πρέπει να είναι δυνατή η χειραγώγηση πληροφοριών τοποθεσίας HeNB. Ευαίσθητες λειτουργίες τοποθεσίας οι οποίες υποστηρίζονται στο HeNB θα μπορούσαν να διατηρούνται ασφαλείς σε ένα ασφαλές περιβάλλον (Trusted Environment).

25. Χειραγώγηση της εξωτερικής πηγής του χρόνου

Ένας εισβολέας μπορεί να παραποιήσει τις διαδικασίες που χρησιμοποιούνται για τον συγχρονισμό του χρόνου στο HeNB, προκειμένου το HeNB να μην εκτελείται σωστά. Ένας εισβολέας μπορεί να εγκαταστήσει μια ψεύτικη μακροκυψέλη κοντά στο επιτιθέμενο HeNB και να το αναγκάσει να εκτελέσει συγχρονισμό του χρόνου με τη μακροκυψέλη. Ο επιτιθέμενος μπορεί επίσης να εκτελέσει μια επίθεση στο σύνδεσμο μεταξύ του HeNB και του διακομιστή του ρολογιού που βρίσκεται στο σταθερό δίκτυο.

Πιθανότητα Εκτέλεσης: Απίθανη.
Επικινδυνότητα Επίθεσης/Απειλής: Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Το HeNB θα πρέπει να ενημερώνεται σχετικά με τις πληροφορίες συγχρονισμού του χρόνου από τις μακροκυψέλες, έτσι ώστε να μπορεί να εκτελεί συγχρονισμό χρόνου με συγκεκριμένες μακροκυψέλες. Ένα αξιόπιστος διακομιστής ρολογιού θα πρέπει να βρίσκεται πίσω από την πύλη ασφαλείας και η επικοινωνία μεταξύ του διακομιστή ρολογιού και το HeNB θα πρέπει να προστατεύεται επαρκώς. Ασφαλής λειτουργίες συγχρονισμού του ρολογιού και συντήρησης που υποστηρίζονται στο HeNB μπορούν να εκτελούνται εντός του προστατευμένου περιβάλλοντος.

26. Επιθέσεις περιβάλλοντος/Πλευρικού καναλιού ενάντια του HeNB

Ο μηχανισμός ασφάλειας μπορεί να παρακαμφτεί.

Πιθανότητα Εκτέλεσης: Πιθανή.
Επικινδυνότητα Επίθεσης/Απειλής: Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Περιβαλλοντικές επιθέσεις με χρήση ισχυρών εφαρμογών παρακολούθησης της παροχής ρεύματος, της θερμοκρασίας και των δεδομένων σύνδεσης.

27. Επίθεση στο OAM και την κίνηση του

Ο φορέας εκμετάλλευσης μπορεί να αποφασίσει να συνδέσει το OAM στο HeNB μέσω του SeGW ή άμεσα. Αν το OAM είναι εντός του δικτύου του παρόχου τότε τα θέματα και τις λύσεις για τη σύνδεση μεταξύ HeNB και SeGW θα είναι η ίδια όπως και για οποιαδήποτε επικοινωνία. Μπορούν να υπάρξουν κι άλλες απειλές όμως όπως, (α) με τη δυνατότητα μιας εσωτερικής επίθεσης από το SeGW έως το OAM, όπου τα πρωτόκολλα διαχείρισης είναι απροστάτευτα και (β) με ένα πρωτόκολλο εφαρμογής σχετικά με τα θέμα, οι OAM διεπαφές συνήθως δεν βασίζονται σε μια ενιαία λειτουργία. Φέρνουν συνήθως 4-10 διαφορετικά πρωτόκολλα μέσα στο κουτί: για διαχείριση σφαλμάτων, γραμμής εντολών, Web GUI, διαχείριση διαμόρφωσης, Firmware Download, ελέγχου αδειών χρήσης λογισμικού, 3rd Party Interfaces. Ακόμη και αν όλα είναι κρυπτογραφικά ασφαλής, θα υπήρχε ακόμα το ζήτημα της εφαρμογής ευρωστίας. Ακόμη και τα κρυπτογραφικά ασφαλή πρωτόκολλα έχουν ελαττώματα που μπορεί να θέσουν σε κίνδυνο το σύστημα. Τα περισσότερα από αυτά είναι προσβάσιμα μέσω του δικτύου Backhaul. Όταν το HeNB είναι άμεσα συνδεδεμένο με το OAM, τότε ο εισβολέας μπορεί να έχει πρόσβαση στο σύνδεση επικοινωνίας μεταξύ του OAM και HeNB έτσι μπορεί να εκτελέσει διάφορες επιθέσεις , όπως Sniffing, Man-In-The-Middle.

Πιθανότητα Εκτέλεσης: Πιθανή.
Επικινδυνότητα Επίθεσης/Απειλής: Πολύ Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: HeNB, Χρήστη, Δίκτυο Παρόχου.

Αντιμετώπιση: Η επικοινωνία ανάμεσα στο HeNB και το OAM θα πρέπει να είναι ασφαλής.

28. Απειλή του δικτύου πρόσβασης στο HeNB

Το κατά πόσον ένα HeNB μπορεί να έχει πρόσβαση στο δίκτυο εξαρτάται από τις πληροφορίες των ιδιοτήτων του που αποκτήθηκαν για να ενεργοποιηθεί ή να απενεργοποιηθεί το HeNB από την οντότητα του δικτύου (π.χ. OAM Server). Αλλά ένα ψεύτικο HeNB μπορεί να επιχειρήσει να συνδεθεί στο δίκτυο ακόμη και εάν οι πληροφορίες κατάστασης της HeNB έχουν οριστεί για να απενεργοποιηθεί. Εάν δεν υπάρχουν τέτοιες πληροφορίες (π.χ. πληροφορίες ελέγχου πρόσβασης του τομέα των υπηρεσιών για την HeNB, ή πληροφορίες του HeNB στο HeNB GW ή άλλη οντότητα του δικτύου να ελεγχθεί το δικαίωμα πρόσβασης του HeNB), το ψεύτικο HeNB μπορεί να κερδίσει την προσβασιμότητα του δικτύου.

Πιθανότητα Εκτέλεσης: Πιθανή.
Επικινδυνότητα Επίθεσης/Απειλής: Επιβλαβής.
Στοιχεία/Οντότητες που επηρεάζει: Χρήστη, Δίκτυο Παρόχου.
Αντιμετώπιση: Το HeNB SeGW ή άλλη οντότητα του δικτύου στο κεντρικό δίκτυο θα πρέπει να έχει ή να μπορεί να αποκτήσει το σχετικό προφίλ πληροφοριών, π.χ. πληροφορίες ελέγχου πρόσβασης για την HeNB, ή πληροφορίες για την κατάσταση του HeNB, για να ελέγξει αν η πρόσβαση ενός HeNB με το δίκτυο μπορεί να επιτευχθεί όταν το επιχειρεί.

29. Μεταπομπή στο CSG του HeNB

Η απόφαση της μεταπομπής λαμβάνεται από το ασύρματο μέσω του δικτύου, ενώ η επιτρεπόμενη λίστα του CSG αποθηκεύεται στο UE και ο έλεγχος πρόσβασης γίνεται στο κεντρικό δίκτυο ή στην πύλη του HeNB. Έτσι, είναι δυνατόν ένα ψεύτικο UE να εκτελέσει την παράδοση στην HeNB με ένα συγκεκριμένο ID CSG, στην οποία δεν ανήκει, με απλή τροποποίηση του καταλόγου CSG . Αυτό μπορεί να είναι ένα ζήτημα ιδίως για την περίπτωση όπου η παράδοση πρέπει να συμβεί για μια εν εξελίξει περιόδου, διότι σε μια τέτοια περίπτωση ο έλεγχος πρόσβασης ενδέχεται να μην εκτελεστεί.

Πιθανότητα Εκτέλεσης: Υψηλή.

Επικινδυνότητα Επίθεσης/Απειλής: Επιβλαβής.

Στοιχεία που επηρεάζει: Χρήστη, Δίκτυο Παρόχου.

Αντιμετώπιση: Ακόμη και στην παράδοση, το δίκτυο θα πρέπει να ελέγχει κατά πόσο η δεδομένη UE επιτρέπεται να έχει πρόσβαση στο HeNB.

Ακολουθούν συγκεντρωτικοί πίνακες που αποτυπώνουν τον βαθμό πιθανότητας και επικινδυνότητας των απειλών/επιθέσεων που αναλύσαμε παραπάνω, καθώς και ποια στοιχεία επηρεάζονται ανά απειλή (HeNB, Χρήστη, Δίκτυο Παρόχου). Το επίπεδο κινδύνου δίνεται, πολλαπλασιάζοντας την πιθανότητα μιας δεδομένης απειλής με την επικινδυνότητα της. Και τα δύο χωρίζονται σε τέσσερα επίπεδα που βαθμολογούνται με τις τιμές 0.25, 0.5, 0.75 και 1.

Threat/Asset correspondence	H(e)NB	User	Operator
Threat-1	X	X	X
Threat-2	X	X	X
Threat-3	X	X	X
Threat-4	--	X	X
Threat-5	--	X	X
Threat-6	X	X	X
Threat-7	X	X	X
Threat-8	X	X	X
Threat-9	X	X	--
Threat-10	X	X	--
Threat-11	X	X	X
Threat-12	X	X	X
Threat-13	--	X	X
Threat-14	--	X	--
Threat-15	--	X	--
Threat-16	--	X	X
Threat-17	X	X	X
Threat-18	--	X	--
Threat-19	X	X	X
Threat-20	X	X	X
Threat-21	X	X	X
Threat-22	--	X	X
Threat-23	--	X	X
Threat-24	X	X	X
Threat-25	X	X	X
Threat-26	X	X	X
Threat-27	X	X	X
Threat-28	--	X	X
Threat-29	--	X	X

Πίνακας 5.2: Στοιχεία που επηρεάζονται ανά απειλή [4].

Threat	Threat Likelihood probability	Impact	Risk-Level	Comments
1	Possible (0.25)	Medium (0.25)	0.0625; Low	
2	Unlikely-Very Likely (0.1 – 1.0)	Medium (0.25)	0.025 – 0.25; Low-Medium	
3	Possible (0.25)	Medium (0.25)	0.0625; Low	
4	Possible (0.25)	High (0.5)	0.125; Medium	
5	Possible (0.25)	High (0.5)	0.125; Medium	
6	Very Likely (1.0)	Very High (1.0)	1.0; High	High
7	Possible (0.25)	Very High (1.0)	0.25; Medium	Medium
8	Possible (0.25)	Medium (0.25)	0.0625; Low	
9	Possible (0.25)	Medium-High (0.25-0.5)	0.0625-0.125; Low-Medium	
10	Possible (0.25)	Medium-High (0.25-0.5)	0.0625-0.125; Low-Medium	
11	Very Likely (1.0)	Medium (0.25)	0.25; Medium	Medium
12	Unlikely (0.1)	High (1.0)	0.1; Low	
13	Unlikely(0.1)	High (1.0)	0.1; Low	
14	Possible (0.25)	Low (0.1)	0.025; Low	
15	Possible (0.25)	Low (0.1)	0.025; Low	
16	Possible (0.25)	Low-Very High (0.1-1.0)	0.025-0.25; Low-Medium	
17	Possible (0.25)	Very High (1.0)	0.25; Medium	Medium
18	Likely (0.5)	Medium (0.25)	0.125; Medium	
19	Possible (0.25)	Low-Medium (0.1-0.25)	0.025-0.0625; Low	
20	Possible (0.25)	Low-Medium (0.1-0.25)	0.025-0.0625; Low	
21	Possible (0.25)	Low-Medium (0.1-0.25)	0.025-0.0625; Low	
22	Possible (0.25)	High (0.5)	0.125; Medium	
23	Possible (0.25)	Medium (0.25)	0.0625; Low	
24	Possible (0.25)	Medium (0.25)	0.0625; Low	
25	Unlikely (0.1)	Medium (0.25)	0.025; Low	
26	Possible (0.25)	Medium (0.25)	0.0625; Low	
27	Likely (0.5)	High (0.5)	0.25; Medium	
28	Likely (0.5)	High (0.5)	0.25; Medium	
29	Likely (0.5)	Medium (0.25)	0.125; Medium	

Πίνακας 5.3: Πιθανότητα & Επικινδυνότητα απειλών [4].

Επίλογος - Συμπεράσματα

Το Femtocell είναι μια αναδυόμενη τεχνολογία, όχι μόνο για τον χρήστη παρέχοντας μεγαλύτερες ταχύτητες δεδομένων, αλλά και για τον χειριστή του δικτύου παρέχοντας βελτίωση της ποιότητας του δικτύου αλλά και των εσόδων του. Ωστόσο, η πρόσβαση στο κεντρικό δίκτυο κινητής τηλεφωνίας μέσω των Femtocell, εγείρει πολλά σημαντικά ζητήματα ασφάλειας, τα οποία και πρέπει να λαμβάνονται υπόψη κατά την σχεδίαση και εγκατάσταση τους σε εσωτερικούς χώρους, όπως οικίες και επιχειρήσεις. Διαδικασίες όπως αμοιβαία αυθεντικοποίηση δικτύου και χρηστών, εμπιστευτικότητα, ιδιωτικότητα, ακεραιότητα, προστασία σηματοδοσίας, διαθεσιμότητα υπηρεσιών, είναι μερικές από τις απαιτήσεις, που αποτελούν σημείο αναφοράς για την ανάπτυξη μεθόδων αντιμετώπισης των απειλών/επιθέσεων προς το Femtocell.

Συμπερασματικά μπορούμε να πούμε πως η φεμτοκυψέλη, πρέπει να αντιμετωπίζεται ως ένα κομμάτι του δικτύου το οποίο είναι ασφαλές από την πλευρά των χρηστών, ενώ ως ένα κομμάτι μη-ασφαλές από τη πλευρά του διαχειριστή του δικτύου. Ο συνδρομητής πρέπει να νοιώθει πως οι επικοινωνίες του (προς το δημόσιο Internet, ή φωνής) προστατεύονται. Από την άλλη μεριά, ο πάροχος πρέπει να αντιμετωπίζει το Femtocell ως ένα ξεχωριστό στοιχείο του δικτύου στο οποίο δεν έχει άμεση πρόσβαση και θα πρέπει να λαμβάνει ιδιαίτερα αντίμετρα για το λόγο αυτό. Θα πρέπει επίσης να είναι σε θέση να αντιλαμβάνεται έγκαιρα την οποιαδήποτε απάτη ενάντια στη φεμτοκυψέλη μέσω δικτύου και να την ενημερώνει με ασφαλές και έγκυρο λογισμικού για την ομαλή λειτουργία και συντήρηση του.

Το μέλλον, με την ανάπτυξη της τέταρτης γενιάς, αλλά και η μετά-4G εποχή δείχνει να ανήκει στην LTE, LTE-Advanced τεχνολογία πρόσβασης, κάτι που όμως παράλληλα χρειάζεται νέες μεθόδους και τρόπους αποσυμφόρησης των μακροκυψελών και τα Femtocells όπως και τα Relay Nodes, αποτελούν την καλύτερη λύση.

Βιβλιογραφία

[1] 3G TR 33.900. 3rd Generation Partnership Project; Technical Specification Group SA WG3; A Guide to 3rd Generation Security. 3G TR 33.900 version 1.2.0. 2000-01.

[2] 3GPP Release 10 and beyond. Whitepaper: 4G Mobile Broadband Evolution: HSPA+, SAE/LTE and LTE-Advanced. 4G Americas. 2011.

[3] 3GPP Release 11 & Release 12 and Beyond. Whitepaper: 4G Mobile Broadband Evolution. 4G Americas. 2014.

[4] 3GPP TR 33.820. 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Security of H(e)NB. Release 8. 2009-12.

[5] 3GPP TS 22.220. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Home Node B (HNB) and Home eNode B (HeNB). (Release 11). 2012-09.

[6] 3GPP TS 32.593 V9.1.0. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Home eNode B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Procedure Flows for Type 1 Interface HeNB to HeNB Management System. Release 9. 2011-06.

[7] 3GPP TS 33.105. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic algorithm requirements. Release 11. 2012-09.

[8] 3GPP TS 33.210. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security. Release 9. 2009-12.

[9] 3GPP TS 35.202., 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification. Release 11.

[10] 3GPP TS 36.300. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2. Release 12. 2014-03.

[11] 3GPP TSG-SA3 (Security). Common threats to H(e)NB. 2009.

[12] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security of Home Node B (HNB) / Home evolved Node B (HeNB). 3GPP TS 33.320 Release 12. 2013-09.

[13] Bilogrevic, I. & Jadliwala, M. & Hubaux, J. P., Security Issues in Next Generation Mobile Networks: LTE and Femtocells. Switzerland.

[14] Blom, R. & Norrman, & Naslund, M. & K. Rommer, S. & Sahlin, B. 2010. Security in the Evolved Packet System. Ericsson Review.

[15] Boccuzzi, J. & Ruggiero, M., 2011. Femtocells Design & Application. United States: McGraw-Hill Companies.

[16] Borgaonkar, R. & Redon, K. & Seifert, J. P., Experimental Analysis of the Femtocell Location Verication Techniques. Berlin, Germany: Technical University Berlin and Deutsche Telekom Laboratories.

[17] Broek, F. & Schreur, R. W., Femtocell Security in Theory and Practice. Digital Security, Radboud University Nijmegen.

[18] Chen, J. & Wong, W. Security Implications and Considerations for Femtocells. 2012. USA: River Publishers.

[19] Cox, C., 2012. An Introduction to LTE, LTE-Advanced, SAE and 4G Mobile Communications. United Kingdom: John Wiley & Sons Ltd.

[20] Dahlman, E. & Parkvall, S. & Skold, J., 2011. 4G LTE/LTE-Advanced for Mobile Broadband. Burlington, MA 01803, USA: Academic Press.

[21] Feldmann, A. & Seifert, J. P. & Niemi, V., 2013. Security Analysis of Femtocell-Enabled Cellular Network Architecture. Berlin: University Berlin.

[22] Femto Forum., 2008. Interference Management in UMTS Femtocells. Published by the Femto Forum.

[23] Forsberg, D. & Horn, G. & Moeller, W.D. & Niemi, V., 2013. LTE Security. Second Edition. United Kingdom: John Wiley and Sons Ltd.

[24] Hamalainen, S. & Sanneck, H. & Sartori, C., 2012. LTE Self-Organising Networks (SON) Network Management Automation for Operational Efficiency. United Kingdom: John Wiley & Sons, Ltd.

[25] Hanchate, S. M. & Borsune, S. & Shahapure, S. 2012. 3GPP LTE FEMTOCELL - PROS & CONS. INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY, Volume-2.

[26] Hillebrand, F. & Trosby, F. & Holley, K. & Harris, I., 2010. Short Message Service, Te Creation of Personal Global Text Messaging. United Kingdom: John Wiley & Sons Ltd.

[27] Holma, H. & Toskala, A., 2009. LTE for UMTS OFDMA and SC-FDMA Based Radio Access. United Kingdom: John Wiley & Sons Ltd.

[28] Holtmanns, S. & Niemi, V. & Ginzboorg, P. & Laitinen, P. & Asokan, N. 2008. Cellular Authentication for Mobile and Internet Services. United Kingdom: John Wiley & Sons Ltd.

[29] Horn, G. 2010. 3GPP Femtocells: Architecture and Protocols. U.S.A.: QUALCOMM Incorporated.

[30] Hughes Systique. H(e)NodeB Security. Rockville. MD 20850. Hughes Systique Corporation.

[31] Knisely, D. N. & Yoshizawa, T. & Favichia, F., 2009. Standardization of Femtocells in 3GPP. IEEE Communications Magazine.

[32] Kreher, R. & Rudebusch, T., 2007. UMTS Signaling, UMTS Interfaces, Protocols, Message Flows and Procedures Analyzed and Explained. Second Edition. Hoboken, NJ: John Wiley & Sons.

[33] Kumar, K. N. S. & Kata, M. & Chaitanya, P. & Mukkollu, D., LTE-Advanced: Future of Mobile Broadband. ΤΑΤΑ CONSULTANCY SERVICES.

[34] Lescuyer, P. & Lucidarme, T., 2008. Evolved Packet System (EPS) The LTE and SAE Evolution of 3G UMTS. England: John Wiley & Sons Ltd.

[35] Lopez-Perez, D. OFDMA Femtocells: A Self-Organizing Approach for Frequency Assignment. PIMRC, Tokyo, Japan, Sept. 2009.

[36] LTE and the Evolution to 4G Wireless Design and Measurement Challenges. Bonus Material: Security in the LTE-SAE Network, www.agilent.com/find/lte/.

[37] Mishra, A.R., 2007. Advanced Cellular Network Planning and Optimisation, 2G/2.5G/3G...Evolution to 4G. England: John Wiley & Sons Ltd.

[38] Niemi, V. & Nyberg, K., 2003. UMTS Security. England: John Wiley and Sons Ltd.

[39] Odadzic, B. & Lukic, N. M. & Jankovic, M., 2012. The Application of Femtocells as a Technical Solution for a Telecomunication Provider - Analysis of Benefit and Utility. Belgrade, Republic of Serbia: TEM Journal-Volume 1.

[40] ORHANOU, G. & HAJJI, S. E. & BENTALEB, Y. & LAASSIRI, J., 2010. EPS Confidentiality and Integrity mechanisms Algorithmic Approach. Universite Mohammed V - Agdal, Faculte des Sciences. Maroc.

[41] Palanigounder, A. 2010. Femtocell Security Framework. 3GPP2 Version 1.0.

[42] Roche, G. & Valcarce, A. & L/opez-P/erez, D. & Zhang, J. JULY 2009. Access Control Mechanisms for Femtocells. IEEE Communications Magazine.

[43] Rumney, M., 2009. LTE and the Evolution to 4G Wireless, Design and Measurement Challenges. Great Britain: Agilent Technologies.

[44] Seidel, E. & Saad, E., 2010. LTE Home Node Bs and its enhancements in Release 9. Germany: Nomor Research GmbH.

[45] Sesia, S. & Toufik, I. & Baker, M., 2009. LTE – The UMTS Long Term Evolution, From Theory to Practice. United Kingdom: John Wiley & Sons Ltd.

[46] SHAH, D. S., 2010. A Tutorial on LTE Evolved UTRAN (EUTRAN) and LTE Self Organizing Networks (SON). University of Texas at Arlington.

[47] Vintila, C. E. & Patriciu, V. V. & Bica, I. 2011. An Analysis of Secure Interoperation of EPC and Mobile Equipments. Romania: Military Technical Academy.

[48] Wong, M. 2013. Femtocells: Secure Communication and Networking. Denmark: River Publishers.

[49] Xenakis, C. & Ntantogian, C., Security Architectures for B3G Mobile Networks. Αθήνα: University of Athens.

[50] Xia, P. & Chandrasekhar, V. Andrews, J.G., 2010. Open vs. Closed Access Femtocells in the Uplink.

[51] Zhang, J. & Roche, G., 2010. Femtocells Technologies and Deployment. United Kingdom: John Wiley & Sons Ltd.

[52] Γκρίτζαλη, Σ. & Κάτσικα, Σ. Κ. & Γκρίτζαλη, Δ., 2003. Ασφάλεια Δικτύων Υπολογιστών, Τεχνολογίες και Υπηρεσίες σε περιβάλλοντα Ηλεκτρονικού Επιχειρείν και Ηλεκτρονικής Διακυβέρνησης. Αθήνα: Εκδόσεις Παπασωτηρίου.

[53] Ηλιάδης, Ν. Χ. & Κακκάβας, Γ. ?., 2012. Συγκριτική ανάλυση αλγορίθμων μεταπομπής σε δίκτυα LTE-Advanced δύο επιπέδων. ΑΘΗΝΑ: Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών.

[54] 3GPP TS 33.401. *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture*. Release 12. 2013-12.

[55] Sauter, M., 2011. *From GSM to LTE an Introduction to Mobile Networks and Mobile Broadband*. United Kingdom: John Wiley & Sons, Ltd.

Αναφορές

[A1] 3GPP, http://www.3gpp.org/. (Διαθέσιμο, 18-05-2014).

[A2] 3GPP2, http://www.3gpp2.org/. (Διαθέσιμο, 18-05-2014).

[A3] 3GPP Specification series, http://www.3gpp.org/DynaReport/33-series.htm/. (Διαθέσιμο, 18-05-2014).

[A4] 4gamericas, http://www.4gamericas.org/index.cfm?fuseaction=page&sectionid=117/. (Διαθέσιμο, 18-05-2014).

[A5] Airvana, http://www.airvana.com/technology/lte-femtocells/. (Διαθέσιμο, 18-05-2014).

[A6] Brighthand, http://www.brighthand.com/default.asp?newsID=19753&news=LTE/.

[A7] Broadband Forum, http://www.broadband-forum.org/. (Διαθέσιμο, 18-05-2014).

[A8] Femtocells - Architecture Network Aspects, http://www.docstoc.com/docs/79695942/Femtocells---Architecture-Network-Aspects-%28PDF%29/. (Διαθέσιμο, 18-05-2014).

[A9] Femto Forum, http://www.femtoforum.com/. (Διαθέσιμο, 18-05-2014).

[A10] Femtocell: Indoor Cellular Communication Redefined, http://www.cse.wustl.edu/~davidh/Pages/femtocell.html/. (Διαθέσιμο, 18-05-2014).

[A11] Internet Key Exchange-Wikipedia, http://en.wikipedia.org/wiki/Internet_Key_Exchange/. (Διαθέσιμο, 18-05-2014).

[A12] IPsec - Wikipedia, http://en.wikipedia.org/wiki/IPsec/. (Διαθέσιμο, 18-05-2014).

[A13] LTE - Wikipedia, http://en.wikipedia.org/wiki/LTE_%28telecommunication%29/. (Διαθέσιμο, 18-05-2014).

[A14] Lte World, http://lteworld.org/wiki/femtocell/. (Διαθέσιμο, 18-05-2014)

(Διαθέσιμο, 18-05-2014).

[A15] Standardization of Femtocells, http://www.airvana.com/technology/standardization-of-femtocells/. (Διαθέσιμο, 18-05-2014).

[A16] Wikipedia, http://en.wikipedia.org/wiki/Home_eNode_B/. (Διαθέσιμο, 18-05-2014).

Παράρτημα - Ακρώνυμα

QAM	Quadrature Amplitude Modulation
1G	First Generation
2G	Second Generation
3G	Third Generation
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
4G	Fourth Generation
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AHR	Access point Home Register
AHR	Home Register of HNB
AKA	Authentication and Key Agreement
AMPS	Advanced Mobile Phone Service
ARIB	Association of Radio Industries and Businesses
ATIS	Alliance for Telecommunications Industry Solutions
AuC	Authentication Centre
AUTN	Authentication Token
AV	Authentication Vector
BBF	Broadband Forum
CCSA	China Communications Standards Association
CDMA	Code Division Multiple Access
CDMA2000	Code Division Multiple Access 2000
CK	Ciphering Key
CN	Core Network
CPE	Customer Premises Equipment
CRL	Certificate Revocation List
CS	Circuit-Switched
CSG	Closed Subscriber Group
D-AMPS	Digital AMPS
DAS	Distributed Antenna Systems
DECT	Digital Enhanced Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol
DLL	Data Link Layer
DoS	Denial of Service
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data Rates for Global Evolution

EPC	Evolved Packet Core
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
ETACS	European Total Access Communication System
ETSI	European Telecommunications Standards Institute
E-UTRA	Evolved UTRA
E-UTRAN	Evolved UTRAN
FAP	Femto Access Point
FAP-MS	Femto Management System
FDMA	Frequency Division Multiple Access
FGW	Femto Gateway
FQDN	Fully Qualified Domain Name
GNSS	Global Navigation Satellite Systems
GPRS	General Packet Radio Services
GPS	Global Positioning System
GSM	Global System for Mobile communications
HE	Home Environment
HeMS	HeNB Management System
HeNB	Home eNodeB
HLR	Home Location Register
HP	Hosting Party
HPM	Hosting Party Module
HSCSD	High-Speed Circuit-Switched Data
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSS	Home Subscription Server
HSUPA	High Speed Uplink Packet Access
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
ISP	Internet Service Provider
LAI	Location Area Identity
LAN	Local Area Network
L-GW	Local Gateway
LIPA	Local Internet Protocol Access
LLC	Logical Link Control
LTE	Long Term Evolution

MAC	Medium Access Control layer
MIMO	Multiple Input Multiple Output
MITM	Man In The Middle
MME	Mobility Management Entity
MNO	Mobile Network Operator
MSC/VLR	Mobile Switching Centre/Visitor Location Register
NAT	Network Address Translation
NB	Node B
NDS	Network Domain Security
NDS/IP	Network Domain Security/IP network
NMT	Nordic Mobile Telephone
NTT	Nippon Telegraph
OAM	Operation, Administration and Management
OCSP	Online Certificate Status Protocol
OFDMA	Orthogonal Frequency Division Multiple Access
PCRF	Policy and Charging Resource Function
PDC	Personal Digital Cellular
P-GW	Packet Data Network Gateway
PKI	Public Key Infrastructure
PLMN ID	Public Land Mobile Network Identity
PPPoE	Point-to-point protocol over Ethernet
PS	Packet-Switched
P-TMSI	Packet Temporary Mobile Subscriber Identity
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RAN	Radio Access Network
RANAP	Radio Access Network Application Protocol
RAND	Random 128-bit string
RAT	Radio Access Technology
RLC	Radio Link Control layer
RNC	Radio Network Controller
RRC	Radio Resource Control
RTMI	Radio Telefono Mobile Intergrato
SA	Security Association
SAE	System Architecture Evolution
SC-FDMA	Single Carrier Frequency Division Multiple Access
SDO	Standards Development Organization
SEG	Security Gateway
SeGW	Security Gateway
SGSN	Serving GPRS Support Node

S-GW	Serving Gateway
SIM	Subscriber Identity Module
SINR	Signal-to-Interference-plus-Noise Ratio
SME	Small to Medium sized Enterprise office
SMS	Short Message Service
SN	Serving Network
SON	Self Organizing Network
SRES	Signed Response
TACS	Total Access Communication System
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access
TLS	Transport Layer Security
TLS/SRTP	Transport Layer Security/The Secure Real-time Transport Protocol
TMSI	Temporary Mobile Subscriber Identity
TPM	Trusted Platform Module
TrE	Trusted Environment
TSG	Technical Specification Group
TTA	Telecommunications Technology Association
TTC	Telecommunication Technology Committee
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal IC Card
UMB	Ulta-Mobile Broadband
UMTS	Universal Mobile Telecommunication System
UP	User Plane
uPnP	Universal Plug and Play
USDC	US Digital Cellular Standard IS-54
USIM	Universal Subscriber Identity Module
UTRA	UMTS - Terrestrial Radio Access
UTRAN	UMTS - Terrestrial Radio Access Network
VoIP	Voice over Internet Protocol
WAP	Wireless Applications Protocol
WCDMA	Wideband Code Division Multiple Access
WG	Working Group
WiMAX	Worldwide Interoperability for Microwave Access
WTLS	Transport Layer Security
XRES	Expected Response