ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

“ Αξιολόγηση παραμέτρων ασφάλειας των δικτύων LTE χρησιμοποιώντας το εργαλείο MobileInsight “

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ονοματεπώνυμο : Τηλέμαχος Τσιώρας

Α.Μ. : MTE1828

Επιβλέπων : Χρήστος Ξενάκης

ΠΕΙΡΑΙΑΣ 2021

1. Πίνακας περιεχομένων

2. Πίνακας Εικόνων

3. Συντομογραφίες

Οι παρακάτω συντομογραφίες θα χρησιμοποιηθούν για τους σκοπούς της εργασίας, έχουν οριστεί από τον 3GPP κατά SAE και χρησιμοποιούνται από το Release 8 που παρουσιάστηκε το LTE μέχρι και το Release 13, στο Release 14 έγινε εισαγωγή νέων όρων για την εκκίνηση προτυποποίησης του 5G οι οποίες δεν αναφέρονται εδώ.

AES	Advanced Encryption Standard
AK	Anonymity Key
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
AN	Access Network
AS	Access Stratum
AUTN	Authentication token
AV	Authentication Vector
ASME	Access Security Management Entity
Cell-ID	Cell Identity
CK	Cipher Key
CKSN	Cipher Key Sequence Number
C-RNTI	Cell RNTI
CRL	Certificate Revocation List
DeNB	Donor eNB
DoS	Denial of Service
DSCP	Differentiated Services Code Point
EARFCN-DL	E-UTRA Absolute Radio Frequency Channel Number-Down Link
ECM	EPS Connection Management
EEA	EPS Encryption Algorithm
EIA	EPS Integrity Algorithm
eKSI	Key Set Identifier in E-UTRAN
EMM	EPS Mobility Management
eNB	Evolved Node-B
EPC	Evolved Packet Core
EPS	Evolved Packet System
EPS-AV	EPS authentication vector
E-UTRAN	Evolved UTRAN
GERAN	GSM EDGE Radio Access Network
GUTI	Globally Unique Temporary Identity
HE	Home Environment
HFN	Hyper Frame Number
HO	Hand Over
HSS	Home Subscriber Server
IK	Integrity Key
IKE	Internet Key Exchange
IMEI	International Mobile Station Equipment Identity
IMEISV	International Mobile Station Equipment Identity and Software Version number
IMSI	International Mobile Subscriber Identity
IOPS	Isolated E-UTRAN Operation for Public Safety
IRAT	Inter-Radio Access Technology
ISR	Idle Mode Signaling Reduction
KDF	Key Derivation Function
KSI	Key Set Identifier
LWIP	LTE WLAN RAN Level Integration using IPSec
LSB	Least Significant Bit

LSM	Limited Service Mode
LWA	LTE-WLAN Aggregation
MAC-I	Message Authentication Code for Integrity
MACT	Message Authentication Code T used in AES CMAC calculation
MeNB	Master eNB
ME	Mobile Equipment
MME	Mobility Management Entity
MME-RN	MME serving the RN
MS	Mobile Station
MSC	Mobile Switching Center
MSIN	Mobile Station Identification Number
NAS	Non Access Stratum
NAS-MAC	Message Authentication Code for NAS for Integrity
NASDVM	Non Access Stratum - Data via MME
NCC	Next hop Chaining Counter
NH	Next Hop
OCSP	Online Certificate Status Protocol
OTA	Over-The-Air
PCI	Physical Cell Identity
PDCP	Packet Data Convergence Protocol
PLMN	Public Land Mobile Network
PRNG	Pseudo Random Number Generator
PSK	Pre-shared Key
P-TMSI	Packet- Temporary Mobile Subscriber Identity
RAND	RANDom number
RAU	Routing Area Update
RN	Relay Node
RRC	Radio Resource Control
SCG	Secondary Cell Group
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SMC	Security Mode Command
SeNB	Secondary eNB
SN	Serving Network
SN id	Serving Network identity
SQN	Sequence Number
SRB	Source Route Bridge
SRVCC	Single Radio Voice Call Continuity
S-TMSI	S-Temporary Mobile Subscriber Identity
TAI	Tracking Area Identity
TAU	Tracking Area Update
UE	User Equipment
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UP	User Plane
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
WT	WLAN Termination
XRES	Expected Response

4. Περίληψη

Η τεχνολογία Long Term Evolution (LTE) / LTE-Advanced (LTE-A) είναι το τελευταίο χρονικά πρότυπο για κινητές συσκευές που εφαρμόζεται και είναι καθιερωμένο παγκοσμίως, αυτό οφείλεται στο ότι παρέχει υψηλές ταχύτητες σε ευρύ φάσμα και χαμηλές τιμές απόκρισης εν αντιθέσει με τα δίκτυα παλαιότερης γενιάς. Χρησιμοποιείται κυρίως για την παροχή συνδεσιμότητας και την πρόσβαση προσωπικών κινητών συσκευών σε προηγμένες υπηρεσίες αλλά και συνδεσιμότητα μεταξύ κρίσιμων υποδομών. Τα δίκτυα LTE θεωρούνται ως ένας από τους κύριους πυλώνες ανάπτυξης συστημάτων επικοινωνίας Machine to machine (M2M) και διάδοσης του Internet of Things (IoT).

Η τεχνολογία αυτή αποτελεί την βάση για την διασύνδεση δισεκατομμυρίων χρηστών σε υπηρεσίες επικοινωνιών αλλά αντιμετωπίζει απειλές λόγω της αρχιτεκτονικής IP του δικτύου, έτσι υπάρχει κρισιμότητα στο να υπάρχει τρόπος να μετρηθεί γρήγορα και με ακρίβεια η ασφάλεια ενός LTE δικτύου. Για να πετύχουμε μια τέτοια μέτρηση πρέπει να γίνει συλλογή δεδομένων που έχουν να κάνουν με την ασφάλεια ως προς της υλοποίησης της τεχνολογίας.

Στην εργασία αυτή γίνεται θεωρητική αλλά και πειραματική μελέτη της τεχνολογίας LTE ως προς την ασφάλεια, θα αναλύσουμε την μέθοδο και τις προτάσεις σύμφωνα με τα ευρήματα, τα προβλήματα που αντιμετωπίστηκαν και προτάσεις για μελλοντική έρευνα. Η έρευνα και η μελέτη των δικτύων αυτών έχει πολύπλευρο ενδιαφέρον τόσο για τεχνο-οικονομικούς λόγους, όσο και για ακαδημαϊκούς σκοπούς.

5. Εισαγωγή

Η ασφάλεια στην υποδομή της τηλεφωνίας ως κρίσιμη υποδομή είναι μεγάλης σημασίας, πρέπει να ικανοποιεί τις αρχές της ασφάλειας: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και παράλληλα να διατηρεί υψηλό επίπεδο ποιότητας υπηρεσιών (QoS). Σε μια τόσο μεγάλη υποδομή είναι αρκετά δύσκολο όμως να εγγυηθεί ο κάθε πάροχος υπηρεσιών διαθεσιμότητα της υπηρεσίας του στο 100% σε 24-ωρη βάση. Μια ευπάθεια όμως που προκαλεί βλάβη σε μια κρίσιμη υποδομή μπορεί και θα επηρεάσει μια άλλη κρίσιμη υποδομή. Έτσι τα σημερινά δίκτυα κυψέλης βρίσκονται υπό παρακολούθηση και συντήρηση από ένα μεγάλο αριθμό διαχειριστών αφού έχουν πια ξεπεράσει τη συμβατική κυκλοφορία φωνής και σύντομης διακίνησης πληροφορίας και είναι πλέον δίκτυα που ενσωματώνουν μετάδοση πληροφορίας υψηλής χωρητικότητας.

Τα συστήματα αυτά τηλεπικοινωνιών ως κρίσιμη υποδομή ακολουθούν τις οδηγίες του 3GPP για απομακρυσμένες συνδέσεις και οφείλουν να ακολουθούν τις νέες εκδόσεις οδηγιών που εκδίδει τακτικά. Η πιο πρόσφατη παγκόσμια καθιερωμένη εξέλιξη των τυποποιήσεων και της ανάπτυξης στον των κινητών τηλεπικοινωνιών είναι η αρχιτεκτονική 4G και τα δίκτυα LTE. Τα δίκτυα LTE προσφέρουν σημαντική αύξηση του εύρους ζώνης, βελτίωση της ασφάλειας σε σχέση με τον προκάτοχό της 3G αλλά και με άλλες λύσεις εκτός 3GPP όπως το WiMAX. Πέρα από τις παραπάνω βελτιώσεις η αρχιτεκτονική του δικτύου είναι αρκετά πιο απλή από τις μέχρι τώρα λύσεις και είναι προσανατολισμένη στην παροχή πολλαπλών υπηρεσιών μέσω IP αρχιτεκτονικής.

Μία από τις σημαντικότερες απλουστεύσεις αφορά την αρχιτεκτονική του σταθμού βάσης - eNodeB ο οποίος αναλαμβάνει πέρα από την σηματοδοσία και τις λειτουργίες ασφάλειας. Λειτουργεί ως διαμεσολαβητής όλης της κίνησης δεδομένων. Αυτός είναι και ο λόγος για τον οποίο το δίκτυο πρόσβασης είναι από τους πιο σημαντικούς τομείς για το σχεδιασμό και τη βελτιστοποίηση του συνόλου του δικτύου και επίσης για την ασφάλεια ελέγχου πρόσβασης και ταυτότητας.

6. Θεωρητικό υπόβαθρο.

6.1 Τί είναι η τεχνολογία LTE

LTE είναι τα αρχικά του Long Term Evolution. Το LTE είναι ένα τηλεπικοινωνιακό πρότυπο 4ης γενιάς (4G) και χρησιμοποιείται για την μεταφορά δεδομένων πάνω από δίκτυα κυψέλης.

Υποστηρίζει ταχύτητες μεταγωγής 100Mbps downstream και 50Mbps upstream. Στην νεότερη έκδοση του προτύπου LTE-Advanced οι ταχύτητες μεταγωγής δεδομένων μπορούν να φτάσουν το 1Gbps downstream και τα 500Mbps upstream, δέκα φορές μεγαλύτερες.

Οι όροι "4G" και "LTE" χρησιμοποιούνται συχνά ως συνώνυμα. Το LTE δεν είναι όμως το μοναδικό πρότυπο τεχνολογίας 4G , το 4G περιέχει επίσης τα πρότυπα Mobile WiMAX (IEEE 802.16e) και WirelessMAN-Advanced (IEEE 802.16m) κ.α. Επειδή όμως το LTE σχεδιάστηκε ως παγκόσμιο τηλεπικοινωνιακό πρότυπο και υιοθετήθηκε από τις Ηνωμένες Πολιτείες Αμερικής , την Ευρωπαϊκή Ένωση και αρκετές χώρες της Ασίας είναι μακράν το πιο διαδεδομένο πρότυπο.

Για να έχει κάποιος πρόσβαση σε ένα δίκτυο LTE πρέπει να έχει συμβατή συσκευή όπως ένα smartphone , tablet , laptop, USB κεραία και άλλα. Το 2009 που έγινε αρχικά διαθέσιμο το πρότυπο οι περισσότερες συσκευές δεν ήταν συμβατές , σήμερα οι περισσότεροι πάροχοι τηλεφωνικών υπηρεσιών προσφέρουν LTE και έτσι οι περισσότερες συσκευές είναι συμβατές.

6.2 Τι είναι ο 3GPP

THIRD GENERATION PARTNERSHIP PROJECT - 3GPP ονομάζεται το πρόγραμμα που έφερε σε επαφή εθνικούς οργανισμούς τυποποίησης, Standards Development Organizations (SDOs), από όλη την υδρόγειο αρχικά για να αναλάβουν την «συντήρηση» των τότε ώριμων δικτύων 2G και με βάση αυτά να αναπτύξουν τον σχεδιασμό των δικτύων 3G UMTS.

Σήμερα αποτελείται από επτά οργανισμούς τυποποίησης στον τομέα των τηλεπικοινωνιών (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC) και παρέχει στα μέλη τους ένα σταθερό περιβάλλον για την ανάπτυξη και δημοσίευση των προδιαγραφών που ορίζουν τις τεχνολογίες 3GPP.

Έτσι με την συνεχή απαίτηση για μεγαλύτερη και ταχύτερη μεταγωγή δεδομένων εξέλιξε τα δίκτυα 4G με το πρότυπο LTE και σήμερα αναπτύσσει τις προδιαγραφές για τα δίκτυα 5G. Άλλα πρότυπα που δημιουργήθηκαν από τον οργανισμό είναι τα : EDGE, HSPA, Carrier Aggregation, NR, EPC και NG-CN.Το πρόγραμμα 3GPP παρέχει ένα ολοκληρωμένο περιβάλλον μελέτης και ανάπτυξης των εκάστοτε

τεχνολογιών, αλλά και τις πλήρεις προδιαγραφές λειτουργίας του κάθε συστήματος. Αξίζει να σημειωθεί πως οι προδιαγραφές παρέχουν επίσης τεχνικές ώστε να υπάρχει πρόσβαση στο δίκτυο κορμού, πέρα από την ραδιοεπικοινωνία, από τρίτα δίκτυα όπως για παράδειγμα για την διασύνδεση με δίκτυα Wi-Fi.

Οι προδιαγραφές και οι μελέτες 3GPP βασίζονται σε συνεισφορές από τους οργανισμούς - μέλη και αναπτύσσονται από πλήθος ομάδων εργασίας που συμπεριλαμβάνουν εξειδικευμένες ομάδες τεχνικών προδιαγραφών.

6.3 Αρχιτεκτονική

Η υποδομή LTE είναι ένας συνδυασμός πολλών οντοτήτων (components) και των διασυνδέσεών τους. Η αρχιτεκτονική του LTE μπορεί να χωριστεί σε τρείς διακριτούς τομείς :

1. Τον εξοπλισμό χρήστη, User Equipment (UE)

UE χαρακτηρίζεται κάθε είδους τερματική συσκευή που χρησιμοποιεί κάποιος χρήστης του δικτύου, όπως ένα smartphone.

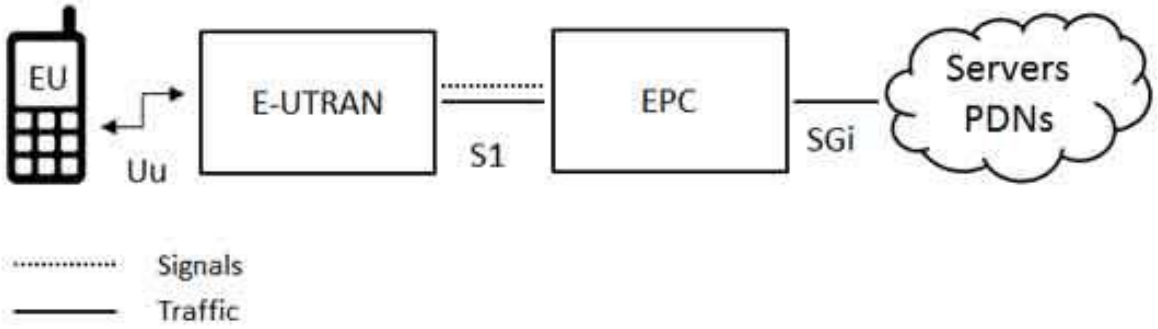
2. Το εξελιγμένο δίκτυο επίγειας ραδιοεπικοινωνίας UMTS, Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)

Είναι ο σταθμός βάσης eNodeB, το πρώτο σημείο σύνδεσης μεταξύ UE και του υπόλοιπου δικτύου.

3. Το εξελιγμένο δίκτυο κορμού, Evolved Packet Core (EPC)

Ο τομέας που δρομολογεί τα πακέτα δεδομένων εντός του δικτύου, αναλαμβάνει την αυθεντικοποίηση των χρηστών, την τιμολόγηση και αρκετές άλλες εργασίες εντός των υποσυστημάτων του. Περιέχει, μεταξύ άλλων στοιχείων τον τοπικό διακομιστής συνδρομητών (Home Subscriber Server - HSS) και την μονάδα διαχείρισης κινητικότητας (Mobility Management Entity - MME).

Το δίκτυο κορμού EPC επικοινωνεί με εξωτερικά δίκτυα μεταγωγής πακέτων – Packet Data Networks (PDN) όπως το internet, ιδιωτικά εταιρικά δίκτυα ή άλλα IP υποσυστήματα. Οι δίαυλοι επικοινωνίας μεταξύ των τομέων του συστήματος συμβολίζονται με Uu, S1, SGi, όπως φαίνεται στην παρακάτω σχηματική αναπαράσταση.



Εικόνα 1. Απλοποιημένη σχηματική αναπαράσταση της αρχιτεκτονικής δικτύου LTE

Οι τομείς E-UTRAN και EPC συνδέονται μέσω της διεπαφής S1. Εκεί υπάρχουν δύο σημαντικές λογικές συνδέσεις μεταξύ τους, η Access Stratum (AS) και η Non Access Stratum (NAS).

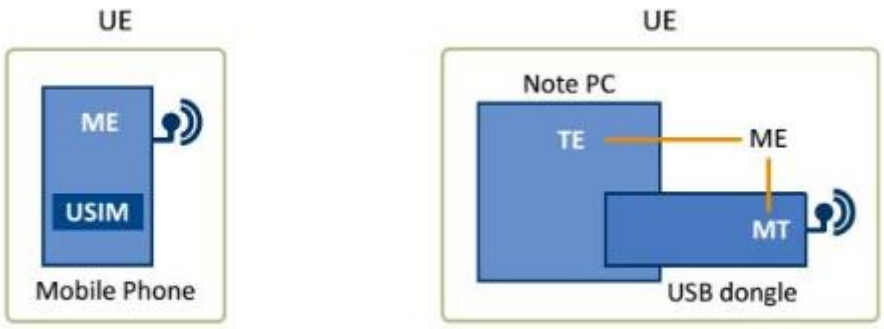
- Η λογική σύνδεση Access Stratum (AS) αντιπροσωπεύει την άμεση σύνδεση μεταξύ UEs και eNodeBs και περιλαμβάνει όλα τα μηνύματα, δηλαδή τα δεδομένα χρηστών που ανταλλάσσονται στο ραδιοφωνικό στρώμα για φυσική πρόσβαση σε δίκτυο LTE.
- Η λογική σύνδεση Non Access Stratum (NAS) αντιπροσωπεύει την σύνδεση μεταξύ του UE και του MME και περιλαμβάνει την εν γένει διαχείριση της επικοινωνίας όπως λχ να ξεκινήσουν συνεδρίες επικοινωνίας, να γίνει διαχείριση της κινητικότητας και της ταυτότητας του χρήστη κλπ.

6.3.1 Συσκευή χρήστη (User Equipment - UE)

Η συσκευή χρήστη είναι αρχικά υπεύθυνη για τη μετάδοση δεδομένων προς και από το δίκτυο. Επιπλέον μέσω της συσκευής, παρέχονται οι διάφορες συμπληρωματικές υπηρεσίες στον χρήστη και φιλοξενούνται οι διάφορες εφαρμογές. Αποτελείται από :

- Mobile Termination (MT) : Χειρίζεται όλες τις λειτουργείες επικοινωνίας
- Terminal Equipment (TE) : Εκεί καταλήγουν όλες οι ροές δεδομένων.
- Universal Integrated Circuit Card (UICC) : Γνωστή και ως κάρτα sim περιλαμβάνει την υλοποίηση USIM – Universal Subscriber Identity Module

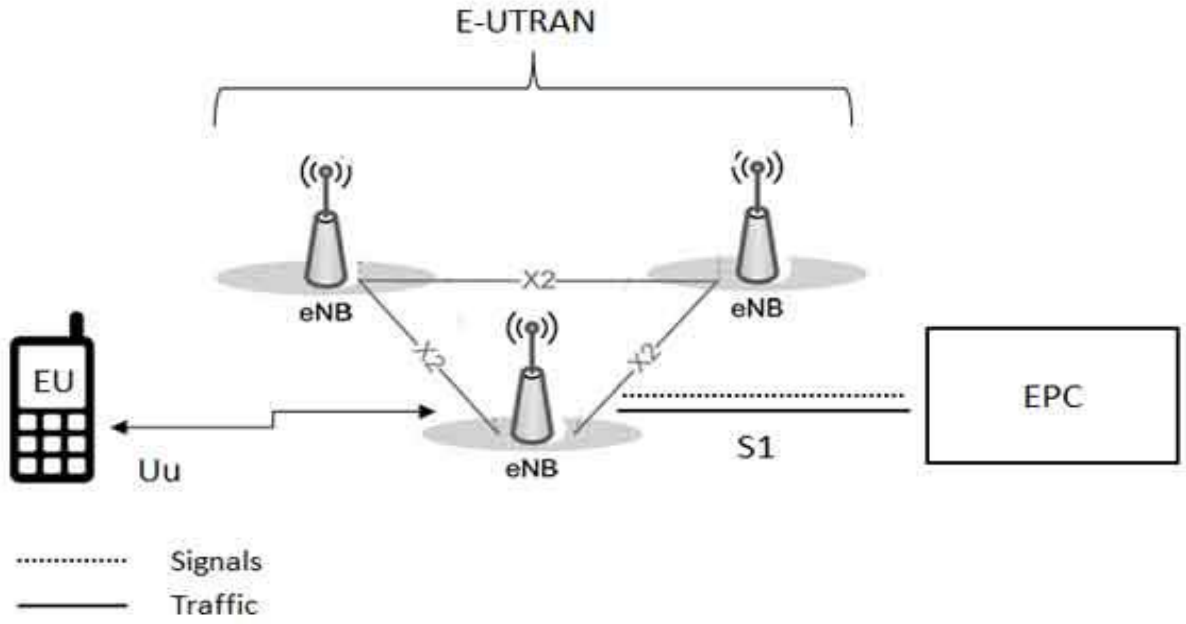
Η USIM αποθηκεύει δεδομένα σχετικά με το χρήστη με τέτοιο τρόπο ώστε να αναγνωρίζεται με μοναδικό τρόπο ο κάθε χρήστης στο δίκτυο. Περιέχει τον τηλεφωνικό αριθμό, τη διεθνή ταυτότητα συνδρομητών κινητής τηλεφωνίας (IMSI), ταυτότητα του δικτύου παρόχου, και το κοινόχρηστο κλειδί ασφαλείας K. Το κλειδί K χρησιμοποιείται στην πρώτη επικοινωνία για να παράγει περαιτέρω κλειδιά που χρησιμοποιούνται κατά τη διαδικασία ελέγχου ταυτότητας.



Εικόνα 2. User Equipment

6.3.2 Ο τομέας E-UTRAN

Ο τομέας E-UTRAN χειρίζεται τις επικοινωνίες μεταξύ User Equipment και Evolvet Packet Core και έχει μόνο ένα στοιχείο, τους σταθμούς βάσης eNodeB ή eNB – evolved base stations. Κάθε eNodeB είναι ένας σταθμός βάσης που χειρίζεται UEs όπως κινητά τηλέφωνα σε μία ή περισσότερες κυψέλες. Ο σταθμός βάσης που επικοινωνεί με το κινητό ονομάζεται serving eNodeB.



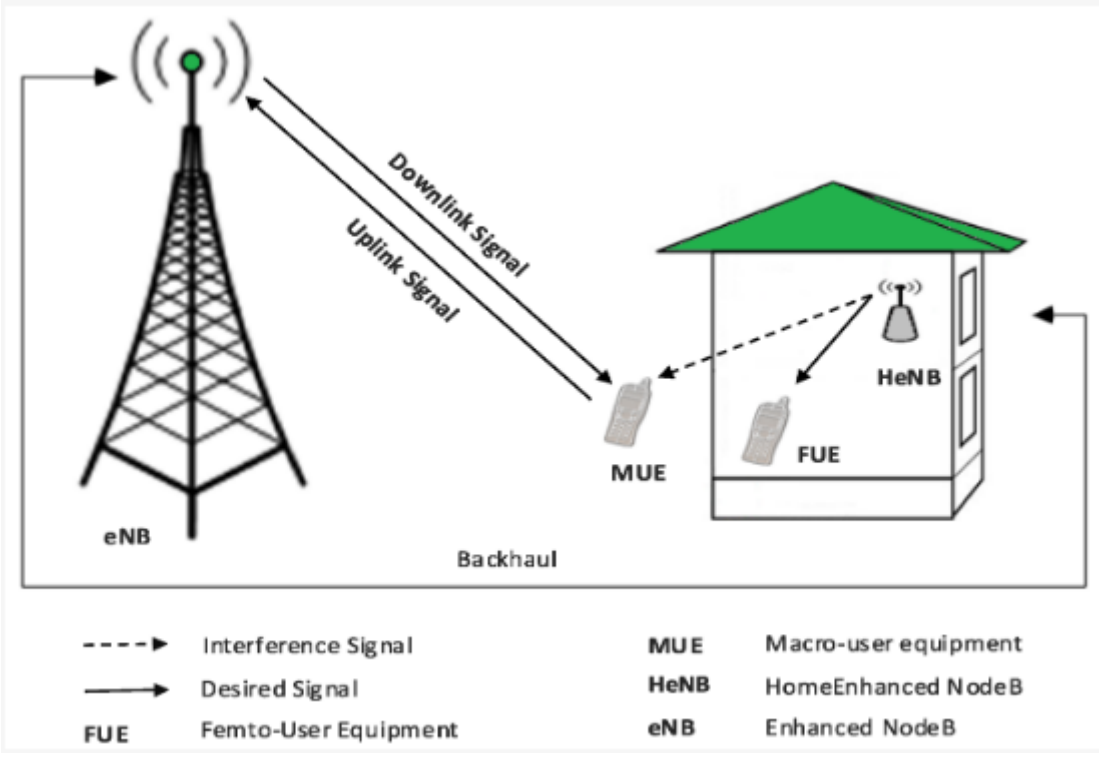
Εικόνα 3. eNBs in E-UTRAN

Μια συσκευή LTE επικοινωνεί μόνο με ένα σταθμό βάσης κάθε φορά και εκτελούνται 2 βασικές διαδικασίες από αυτόν :

- Ο eNodeB ανταλλάσσει εκπομπές με όλες τις συσκευές χρήστη σε αναλογικά και ψηφιακά σήματα και επεξεργάζεται λειτουργίες του LTE
- Ο eNodeB ελέγχει τις low-level λειτουργίες των κινητών που αφορούν τη σηματοδοσία όπως τις εντολές handover αλλαγής κυψέλης.

Κάθε eNodeB συνδέεται με το Evolved Packet Core (EPC) μέσω του S1 μέσω οπτικών ινών, μικροκυματικών κεραιών ή δορυφορικά και συνδέεται και απευθείας όπου είναι εφικτό με γειτονικά eNodeB με το πρωτόκολλο X2. Το πρωτόκολλο X2 χρησιμοποιείται για σηματοδοσία που αφορά κυρίως την προώθηση πακέτων κατά τη διάρκεια του handover ενός User Equipment. Κάθε σταθμός βάσης συμμετέχει στη διαδικασία κρυπτογράφησης δεδομένων ραδιοεπικοινωνίας και προστασίας ακεραιότητας καθώς και στην κρυπτογράφηση των δεδομένων των χρηστών.

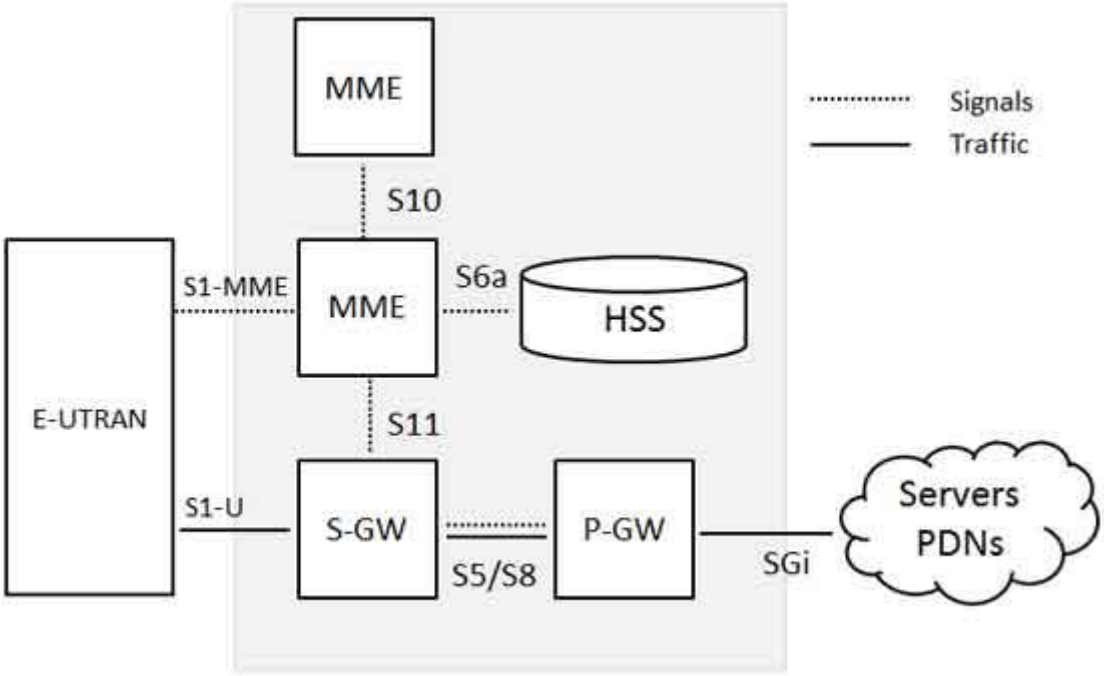
Λύση για περιπτώσεις που δεν υπάρχει κάλυψη εντός σπιτιών είναι τα Home eNodeB (HeNB) που μπορεί να αγοράσει ο χρήστης από τον τηλεφωνικό του πάροχο. Τα HeNB χρησιμοποιώντας την τεχνολογία femtocell έχει κάλυψη σε μια πολύ περιορισμένη περιοχή όπως μια οικία. Μπορεί να εξυπηρετήσει συγκεκριμένες συσκευές με προδηλωμένη USIM, οι κινητές συσκευές αυτές ανήκουν σε κλειστή ομάδα closed subscriber group (CSG) και μόνο αυτή εξυπηρετείτε από το HeNB.



Εικόνα 4.Home eNodeB – FemtoCell

6.3.3 Ο τομέας εξελιγμένου δίκτυο κορμού (Evolved Packet Core - EPC)

Η αρχιτεκτονική Evolved Packet Core (EPC) απεικονίζεται στην παρακάτω εικόνα , σε κάποιες χώρες υπάρχουν επιπλέον υποσυστήματα αλλά δεν συμπεριλαμβάνονται ώστε να απλοποιηθεί η ανάλυση. Κάποια από τα υποσυστήματα αυτά μπορούν να είναι συστήματα προειδοποίησης φυσικών καταστροφών όπως σεισμών και τσουνάμι (Earthquake and Tsunami Warning System - ETWS), υποσυστήματα διαχείρισης συνδρομητών που είναι σε roaming (Equipment Identity Register - EIR) και υποσυστήματα για να παρακολουθούν την ορθή χρήση του δικτύου και την χρέωση (Policy Control and Charging Rules Function -PCRF).



Εικόνα 5. Το δίκτυο κορμού - EPC

6.3.3.1 Μονάδα διαχείριση κινητικότητας (Mobility Management Entity - MME)

Το Mobility Management MME χειρίζεται τη δημιουργία νέων συνδέσεων και τη διαδικασία επαλήθευσης ταυτότητας με τον Home Subscriber Server - HSS. Επιπλέον διαχειρίζεται τα δεδομένα κινητικότητας των συνδεδεμένων συσκευών χρήστη (UE), όπου εφαρμόζει προστασία κρυπτογράφησης και ακεραιότητας.

6.3.3.2 Πύλη υπηρεσιών (Serving Gateway - S-GW)

Η κύρια λειτουργία της πύλης υπηρεσιών Serving Gateway – S-GW είναι η δρομολόγηση και προώθηση πακέτων που προήλθαν από τη συσκευή του συνδρομητή.

Είναι αρμόδια για την εσωτερική κινητικότητα μεταξύ δύο eNodeB των συνδρομητών και παρέχει κινητικότητα μεταξύ δικτύων 2G/3G και P-GW. Για κάθε συσκευή χρήστη UE που σχετίζεται με το EPS, σε δεδομένο χρονικό σημείο, υπάρχει ένα μόνο Serving GW που τον εξυπηρετεί.

Η S-GW παρακολουθεί και συντηρεί πληροφορίες που σχετίζονται με την συσκευή χρήστη UE όσο είναι σε κατάσταση αδράνειας και παράγει αιτήματα τηλε-ειδοποίησης όταν φθάνουν δεδομένα για την συσκευή του χρήστη (π.χ. εισερχόμενη κλήση). Η SGW είναι επίσης υπεύθυνη για την καταγραφή δεδομένων με σκοπό τη νόμιμη παρακολούθηση.

6.3.3.3 Πύλη δικτύου πακέτων δεδομένων (Packet Data Network Gateway – P-GW)

Η πύλη δικτύου πακέτων δεδομένων (P-GW) είναι η πύλη που επικοινωνεί μέσω της διασύνδεση SGi προς τα Packet Data Networks. Η P-GW είναι υπεύθυνη να ενεργεί ως «σταθερό σημείο» κινητικότητας μεταξύ 3GPP και τεχνολογιών που δεν είναι 3GPP. Η PGW παρέχει συνδεσιμότητα από την συσκευή χρήστη UE σε εξωτερικό PDN δίκτυο, αποτελώντας το σημείο εισόδου ή εξόδου της κυκλοφορίας για την συσκευή. Κάθε PDN αναγνωρίζεται από το APN – Access Point Name.

Η PGW διαχειρίζεται την επιβολή πολιτικών, τη διήθηση / φιλτράρισμα πακέτων προς τους χρήστες και τη νόμιμη παρακολούθηση.

6.3.3.4 Τοπικός διακομιστής συνδρομητών (Home Subscriber Server - HSS)

Ο τοπικός διακομιστής συνδρομητών (HSS) αποθηκεύει τις πληροφορίες ελέγχου ταυτότητας των συνδρομητών κινητής τηλεφωνίας. Έτσι, διαδραματίζει κεντρικό ρόλο κατά τη διάρκεια της αρχικής διαδικασίας ελέγχου ταυτότητας ενός μη συνδεδεμένου UE και παρέχει στο Mobility Management Entity (MME) πληροφορίες σχετικές με την ασφάλεια των χρηστών. Περιέχει όλη την βάση δεδομένων των συνδρομητών και είναι ένας διακομιστής που προήλθε από τα δίκτυα UMTS και GSM.

6.4 Πρωτόκολλά δικτύου LTE

Τα παρακάτω πρωτόκολλα χρησιμοποιούνται για την επικοινωνίας στο air interface, την ραδιοεπικοινωνία δηλαδή μεταξύ UE και eNodeB. Το σύνολο των πρωτοκόλλων αυτών είναι γνωστό

ως Air Interface Stack και είναι χωρισμένο σε 3 επίπεδα (layers) τα οποία ορίζουν όλη την ασύρματη TCP/IP επικοινωνία πάνω τους.

Τα πρωτόκολλα είναι :

• **Radio Resource Control (RRC)** - λειτουργεί σε layer 3

Το RRC εκτελεί διεργασίες ελέγχου όπως η εκπομπή πληροφοριών συστήματος, δημιουργία σύνδεσης με eNodeB, paging, αυθεντικοποίηση και μεταφορά μηνυμάτων NAS.

• **Packet Data Convergence Protocol (PDCP)** - λειτουργεί σε layer 2

Το PDCP εκτελεί τις διεργασίες header compression, packet reordering, retransmission και αναλαμβάνει την ασφάλεια του AS περιλαμβανομένης της ακεραιότητας και εμπιστευτικότητας. Πάνω από αυτό το πρωτόκολλο απαιτείται να γίνεται κρυπτογραφική προστασία.

• **Radio Link Control (RLC)** - λειτουργεί σε layer 2

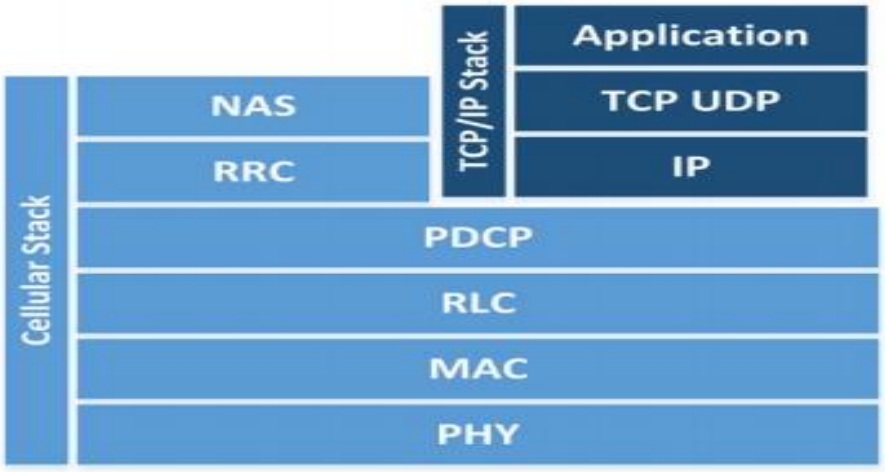
Το RLC προετοιμάζει τα πακέτα ώστε να μεταφερθούν πάνω από το air interface και με μεταφέρει στο MAC επίπεδο, επίσης εκτελεί και αυτό λειτουργείες packet reordering και retransmission.

• **Medium Access Control (MAC)** - λειτουργεί σε layer 2

Το MAC εκτελεί την πολυπλεξία σημάτων αλλά και τον προγραμματισμό μετάδοσης δεδομένων πάνω στο κανάλι επικοινωνίας. Με αυτό τον τρόπο τρέχει κανόνες Quality of Service (QoS) και μεταδίδει δεδομένα στο PHY επίπεδο.

• **Physical Access (PHY)** - λειτουργεί σε layer 1.

Στο επίπεδο PHY γίνεται η διαχείριση σφαλμάτων , επεξεργασία σήματος και η τελική μετάδοση στο air interface.



Εικόνα 6. LTE protocol stack

Κάθε πρωτόκολλο του air interface έχει διαφορετικό ρόλο στις λειτουργείες του και έτσι λειτουργεί στο user plane ή το control plane. Το user plane είναι υπεύθυνο για να μεταφέρει δεδομένα όπως φωνή, sms και δεδομένα εφαρμογών και το control plane είναι υπεύθυνο για την επικοινωνία σηματοδοσίας ώστε να συνδεθεί ένα UE.

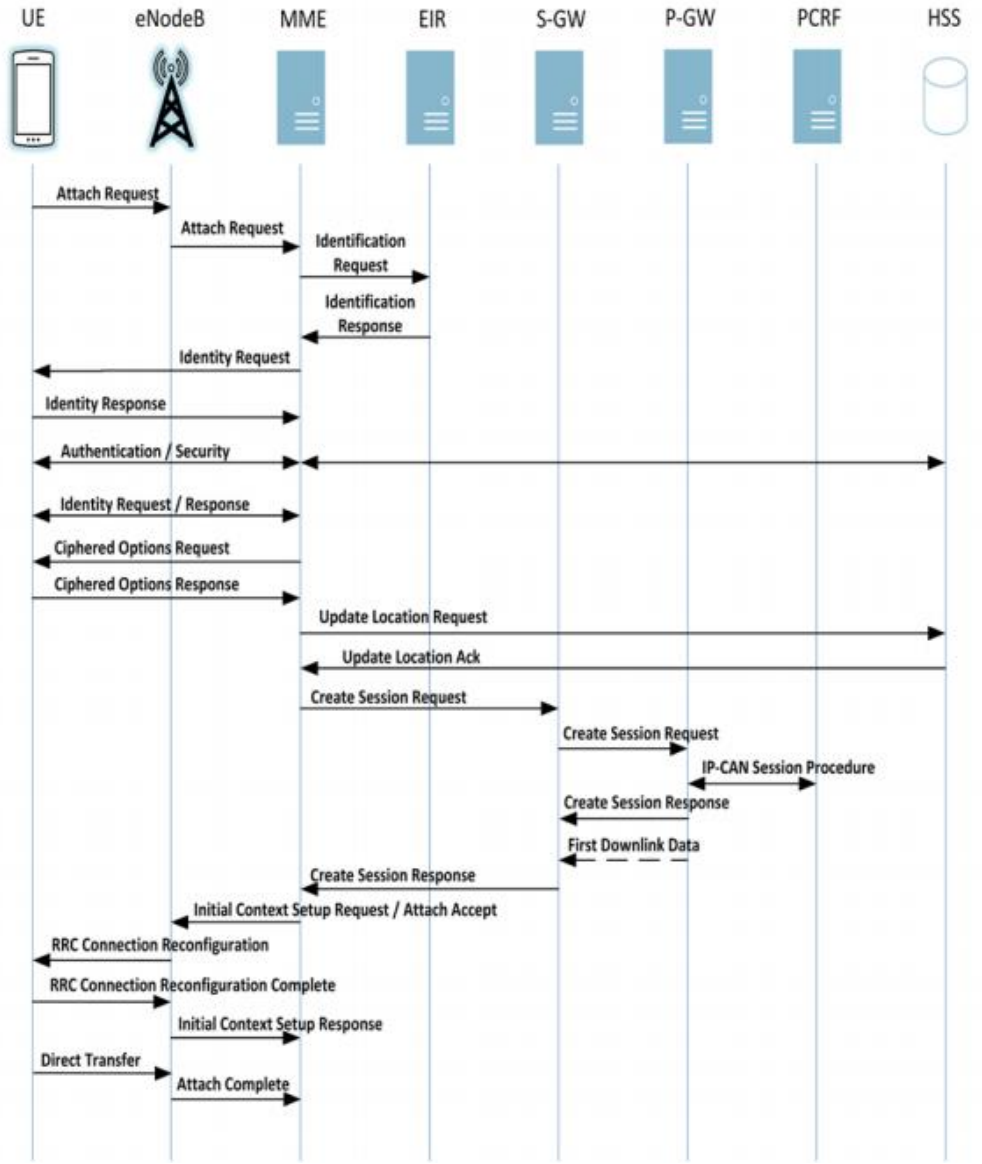
Για να γίνει ξεκάθαρος ο διαχωρισμός ο 3GPP όρισε δύο στρώματα (strata), το Non-Access Stratum (NAS) και το Access Stratum (AS). Το AS είναι όλη η επικοινωνία μεταξύ UE και eNodeB που γίνεται σε κανάλι Radio Frequency (RF). Το NAS περιλαμβάνει όλη την κίνηση μεταξύ UE και MME που δεν έχει να κάνει με την ραδιοεπικοινωνία. Η κίνηση TCP/IP και τα δεδομένα εφαρμογών των χρηστών μεταδίδεται μέσω του user plane. Μέσω του control plane αρχικοποίειται, διατηρείται και διακόπτεται μια σύνδεση μεταξύ UE και MME με το RRC πρωτόκολλο. Τα πρωτόκολλα PDCP, RLC, MAC, και PHY ανήκουν και στο user plane αλλά και στο control plane. Τα πρωτόκολλα μεταξύ των μερών του E-UTRAN και EPC έχουν τα διαφορετικά πρωτόκολλα επικοινωνίας.

6.5 Αρχικοποίηση σύνδεσης User Equipment

Πριν το κάθε UE μπορέσει να συνδεθεί σε ένα δίκτυο LTE και να έχει πρόσβαση σε υπηρεσίες φωνής και δεδομένων πρέπει να ολοκληρώσει μια διαδικασία αυθεντικοποίησης της ταυτότητας του ως προς το δίκτυο. Η διαδικασία είναι γνωστή ως Initial Attach Procedure και χειρίζεται την επικοινωνία μεταξύ UE και EPC ώστε να γίνει έλεγχος αν το UE μπορεί να έχει πρόσβαση στο δίκτυο. Αν είναι επιτυχής η διαδικασία τότε δίνετε πρόσβαση στο δίκτυο με ότι κανόνες χρέωσης επιβάλει το δίκτυο. Η διαδικασία περιγράφεται στην παρακάτω εικόνα συνοπτικά.

Η αρχικοποίηση ξεκινάει με αίτημα του UE στον MME μέσω του eNodeB, το αίτημα περιλαμβάνει το IMSI, πληροφορίες τοποθεσίας και κρυπτογραφικές δυνατότητες και άλλες πληροφορίες του UE. Το αίτημα σύνδεσης είναι ένα NAS μήνυμα και προωθείται από το eNodeB μαζί με τις πληροφορίες της κυψέλης στον MME. Για να συνδεθεί στο PDN το κάθε UE θα γίνει έλεγχος για συγκεκριμένες πολιτικές στον PCRF και στο P-GW και μετά θα του δοθεί διεύθυνση IP.

Ο MME λαμβάνει το IMEI και του UE ώστε να γίνει έλεγχος αποκλεισμού και ύστερα το μεταβιβάζει σε HSS και P-GW. Μόλις ολοκληρωθεί η αρχική σύνδεση τότε το UE λαμβάνει ένα GUTI (Globally Unique Temporary ID) προσωρινά και αποθηκεύεται και στον MME και χρησιμοποιείται αντί για το IMSI, επίσης με την ολοκλήρωση της αρχικοποίησης το UE θα πρέπει να αυθεντικοποιηθεί με το πρωτόκολλο Authentication and Key Agreement (AKA) που θα δούμε παρακάτω.



Εικόνα 7. Initial Attach Procedure

7. Ασφάλεια LTE

7.1 Σύνοψη αρχιτεκτονικής ασφάλειας.

Έχουν καθοριστεί πέντε ομάδες χαρακτηριστικών ασφαλείας. Κάθε μία από αυτές τις ομάδες ανταποκρίνεται σε ορισμένες απειλές και επιτυγχάνει συγκεκριμένους στόχους ασφαλείας:

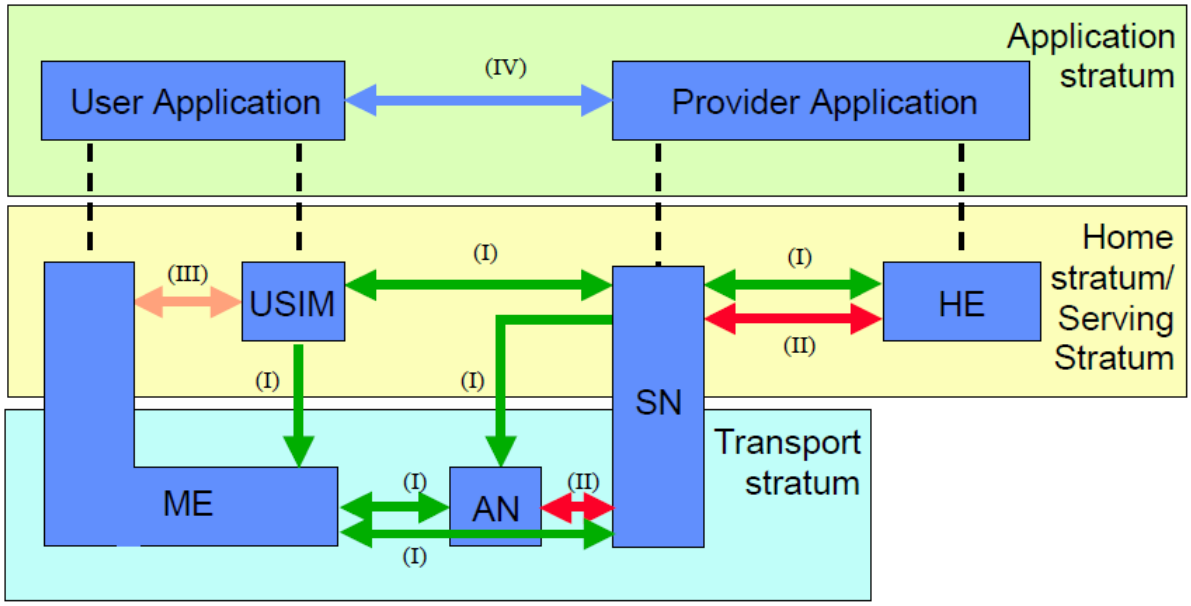
Network access security (I): το σύνολο δυνατοτήτων ασφαλείας που παρέχει στους χρήστες ασφαλή πρόσβαση σε υπηρεσίες, και τα οποία προστατεύουν από επιθέσεις στο radio-access link.

Network domain security (II): το σύνολο δυνατοτήτων ασφαλείας που επιτρέπουν στους κόμβους να ανταλλάσσουν με ασφάλεια δεδομένα σηματοδότησης, δεδομένα χρηστών (μεταξύ AN και SN και εντός AN) και να προστατεύουν από επιθέσεις στο δίκτυο καλωδίων.

User domain security (III): το σύνολο δυνατοτήτων ασφαλείας που εξασφαλίζουν πρόσβαση σε κινητούς σταθμούς.

Application domain security (IV): το σύνολο δυνατοτήτων ασφαλείας που επιτρέπουν στις εφαρμογές του χρήστη και στο domain του παρόχου να ανταλλάσσουν μηνύματα με ασφάλεια.

Visibility and configurability of security (V): το σύνολο των δυνατοτήτων που επιτρέπει στον χρήστη να ενημερώνεται εάν μια λειτουργία ασφαλείας έχει ενεργοποιηθεί ή όχι και εάν η χρήση και η παροχή υπηρεσιών πρέπει να εξαρτώνται από τη λειτουργία της



Εικόνα 8. Security Architecture Overview

7.2 Αλγόριθμοι ασφάλειας

Η προστασία μηνυμάτων στις συνδέσεις AS και NAS μπορεί να επιτευχθεί με μια επιλογή προκαθορισμένων αλγορίθμων ασφαλείας. Για να προσδιοριστεί η κρυπτογράφηση και η προστασία ακεραιότητας των ανταλλασσόμενων μηνυμάτων πρέπει να γίνουν δύο επιλογές από ένα σύνολο αλγορίθμων. Μέχρι τώρα, τέσσερις διαφορετικοί αλγόριθμοι ασφαλείας ορίζονται στις προδιαγραφές, δύο από τους οποίους βασίζονται σε καθιερωμένα κρυπτογραφήματα. Κάθε αλγόριθμος κωδικοποιείται σε έναν διάνυσμα byte όπως φαίνεται στον ακόλουθο πίνακα.

Encoding	Integrity	Ciphering	Algorithm
X000X000	EIA0	EEA0	NULL
X001X001	128-EIA1	128-EEA1	SNOW 3G
X010X010	128-EIA2	128-EEA2	AES
X011X011	128-EIA3	128-EEA3	ZUC

Η κωδικοποίηση είναι: X [#EIA] X [#EEA],

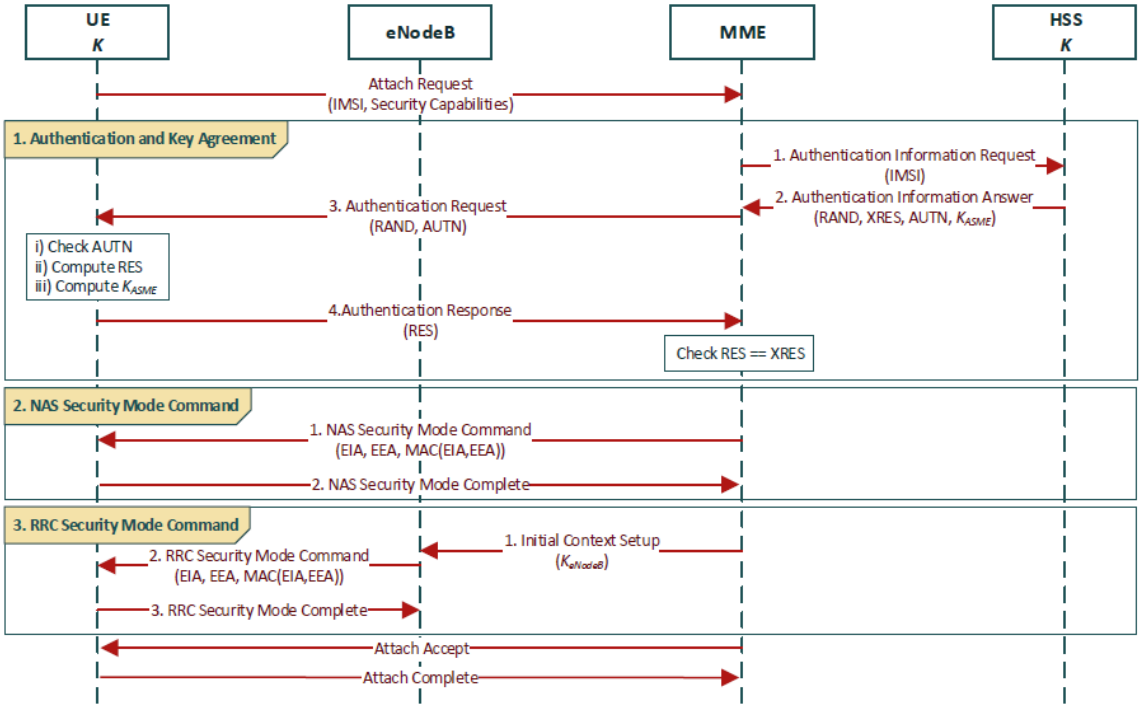
όπου το X είναι μεταβλητή μορφοποίησης.

Εδώ σημειώνουμε ότι, δεν εκχωρούνται όλες οι πιθανές κωδικοποιήσεις σε πραγματικούς αλγόριθμους, αλλά δεσμεύονται για μελλοντική χρήση. Επιπλέον, οι EPS (Evolved Packet System) Αλγόριθμοι Ακεραιότητας (EIAs) και οι EPS Αλγόριθμοι Κρυπτογράφησης (EEAs) μπορούν να συνδυαστούν αυθαίρετα, για παράδειγμα χρησιμοποιώντας 128-EIA1 με 128-EEA2.

Μια ειδική οντότητα και των δύο συνόλων αλγορίθμων είναι η EIA0 και η EEA0. Αυτοί οι αλγόριθμοι είναι άκυρες λειτουργίες που αφήνουν τα δεδομένα κρυπτογραφημένα και / ή δεν παρέχουν προστασία ακεραιότητας. Σύμφωνα με την προδιαγραφή LTE, η EIA0 επιτρέπεται μόνο όταν δημιουργούνται καταστάσεις έκτακτης ανάγκης. Η επιλογή της υλοποίησης της κρυπτογράφησης και του αλγόριθμου προστασίας ακεραιότητας εξαρτάται από τον πάροχο του δικτύου και μπορεί να βασίζεται στον δεσμό με τον επίγειο εξοπλισμό.

7.3 Διαδικασίες ασφάλειας αρχικής σύνδεσης.

Για την εκπλήρωση των στόχων ασφάλειας που συμπεριλαμβάνουν την προστασία της εμπιστευτικότητας και της ακεραιότητας, εφαρμόζονται διαδικασίες ασφαλείας. Αρκετές οντότητες της αρχιτεκτονικής LTE εμπλέκονται στη διαδικασία, π.χ., UE, eNodeB, MME και HSS. Στη συνέχεια, περιγράφουμε την διαδικασία πως μια συσκευή χρήστη UE μεταβαίνει στην κατάσταση επιτυχούς σύνδεσης. Όταν μια συσκευή χρήστη UE ξεκινά μια νέα σύνδεση με ένα δίκτυο LTE, μια φυσική σύνδεση με το eNodeB δημιουργείται αρχικά στο ραδιοφωνικό στρώμα και ύστερα σε γίνεται η αρχικοποίηση της σύνδεσης όπως είδαμε νωρίτερα. Μετά την παραλαβή της ολοκληρωμένη αίτηση επισύναψης, εκτελούνται τρεις φάσεις για τη δημιουργία ασφαλούς σύνδεσης.



Εικόνα 9. Επισκόπηση διαδικασίας ασφαλείας

Οι τρεις φάσεις είναι:

7.3.1 Έλεγχος ταυτότητας και συμφωνία κλειδιού (AKA).

Ο στόχος του AKA είναι η καθιέρωση αμοιβαίας αυθεντικοποίησης μεταξύ του UE και του δικτύου LTE καθώς και η εξαγωγή ενός κοινού κλειδιού συνεδρίας. Η διαδικασία περιλαμβάνει το MME, το οποίο ζητά πληροφορίες αποθηκευμένες στο HSS. Σημειώνεται ότι τόσο το HSS όσο και το UE μοιράζονται το ίδιο μακροπρόθεσμο κλειδί K. Η σειρά των ανταλλασσόμενων μηνυμάτων έχει ως εξής.

I. Το MME στέλνει ένα αίτημα πληροφοριών ταυτότητας στο HSS, το οποίο περιέχει το κοινόχρηστο κλειδί K του αιτούντος χρήστη που προσδιορίζεται από το συμπεριλαμβανόμενο IMSI.

II. Το HSS ξεκινά μια δοκιμή πρόκλησης-απόκρισης μεταξύ του δικτύου και του UE, υπολογίζοντας ένα Authentication Vector (AV) και στέλνοντάς το ξανά στο MME μέσω μιας απάντησης πληροφοριών ελέγχου ταυτότητας. Το AV περιέχει τις ακόλουθες παραμέτρους:

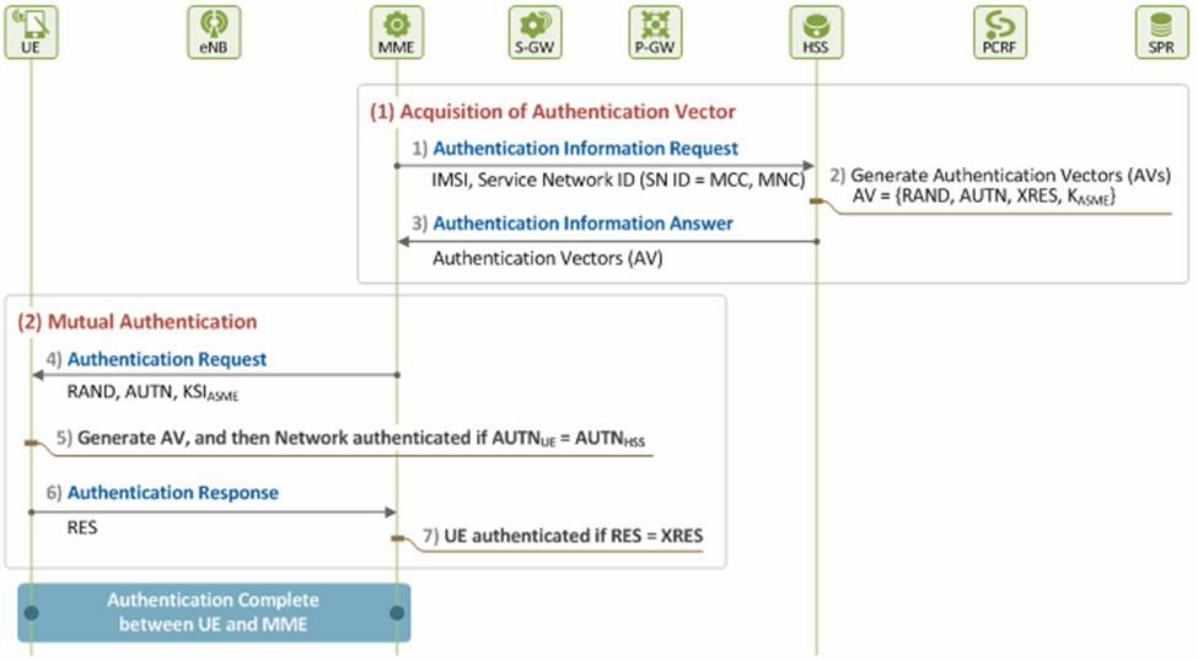
- Τυχαίο αριθμό (RAND)
- Αναμενόμενη απόκριση (XRES)
- Στοιχείο ελέγχου ταυτότητας (AUTN)

- Το ενδιάμεσο κλειδί (KASME), με την Οντότητα Διαχείρισης Ασφάλειας Πρόσβασης KASME που προέρχεται από το μακροπρόθεσμο κλειδί K και το AUTN που περιέχει π.χ. έναν Αύξοντα Αριθμό (SQN), ο οποίος συγχρονίζεται με την τρέχουσα κατάσταση του UE.

III. Το MME αποθηκεύει τα XRES και KASME και διαβιβάζει ένα αίτημα ελέγχου ταυτότητας στον UE με την πρόκληση RAND καθώς και το AUTN.

IV. Το UE
   - επαληθεύει το AUTN ελέγχοντας το εύρος του SQN,
   - υπολογίζει την απόκριση (RES)
   - υπολογίζει και το δικό του ενδιάμεσο κλειδί KASME. Η υπολογιζόμενη ΑΠΕ επιστρέφεται στο MME.

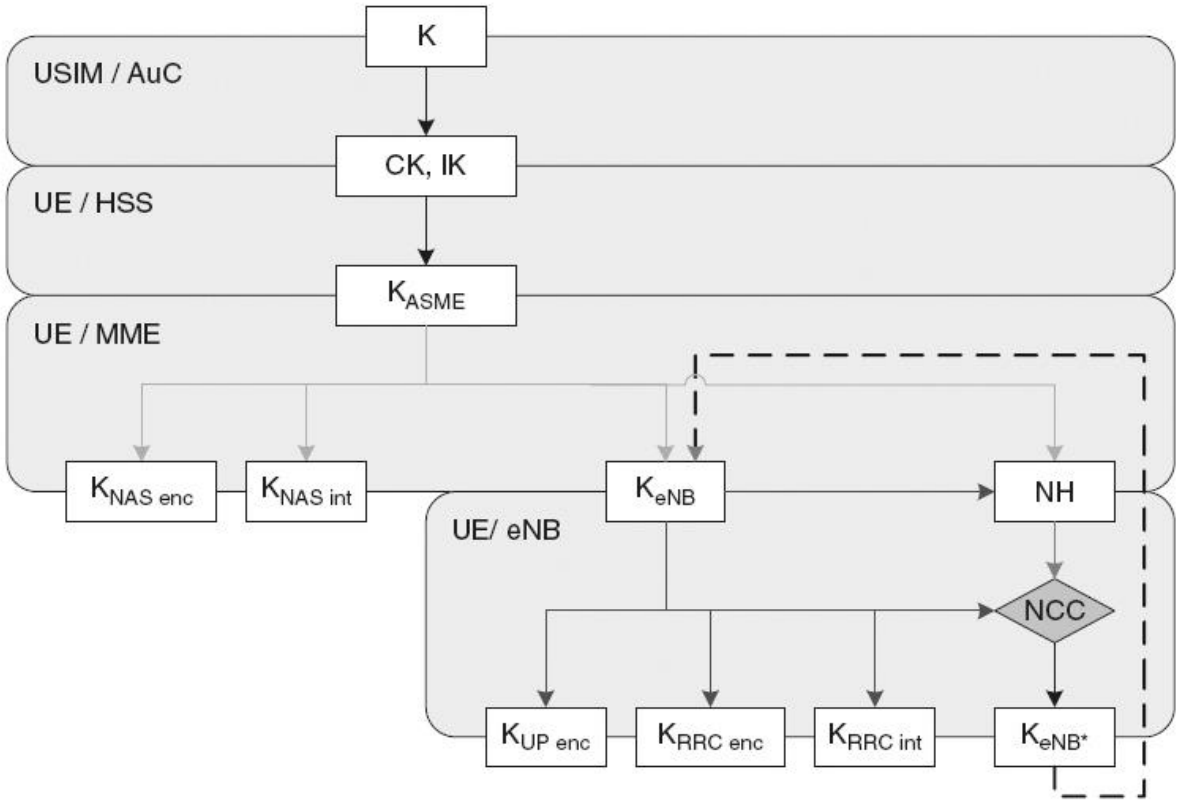
Όταν το XRES και το RES είναι ίσοι, η συσκευή χρήστη UE επιβεβαιώσει ότι διαθέτει το ίδιο μακροπρόθεσμο κλειδί K και έτσι έχει επικυρωθεί έναντι του δικτύου. Διαφορετικά, η διαδικασία AKA διακόπτεται.



Εικόνα 10. UE AKA

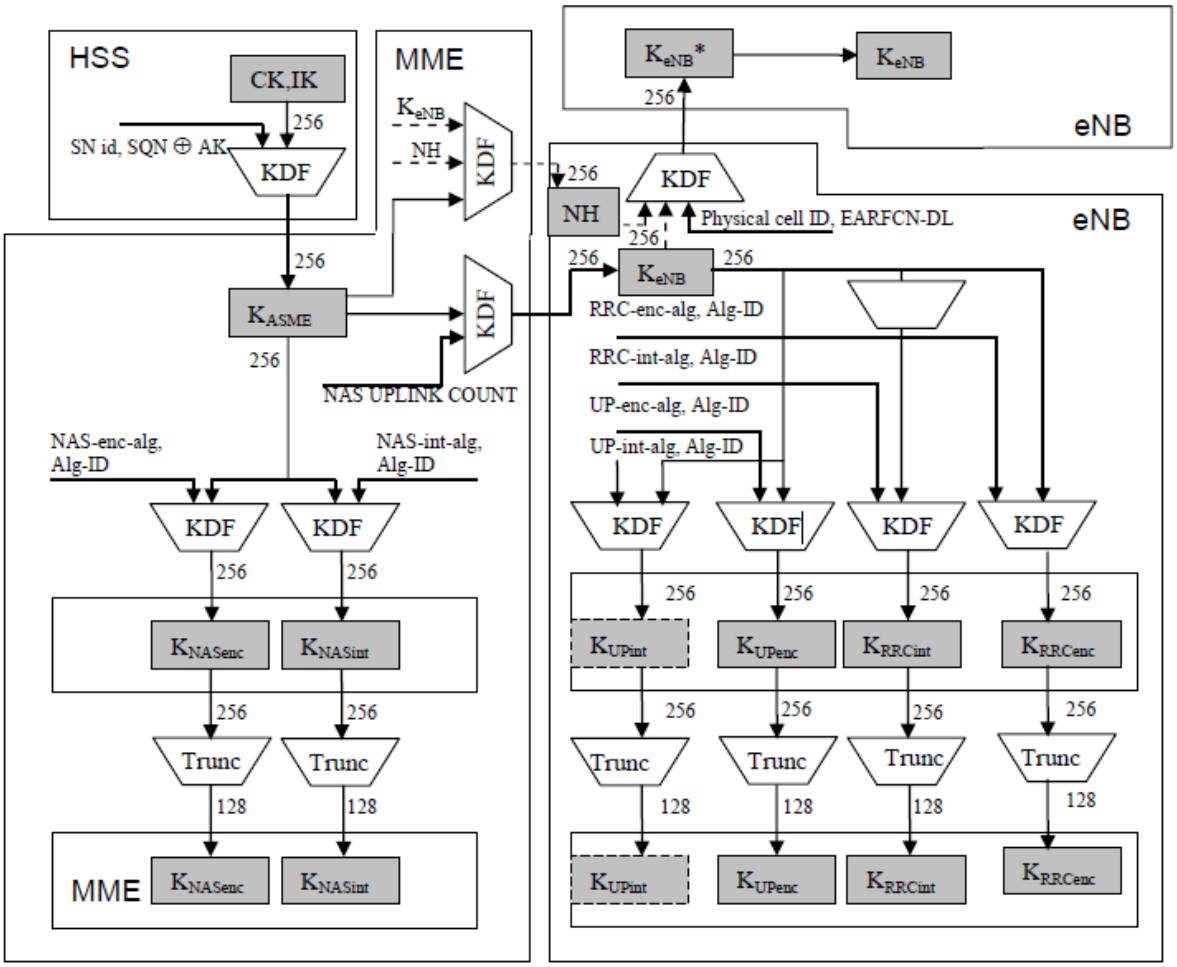
7.3.2 Ιεραρχία και παραγωγή κλειδιών

Με την ολοκλήρωση της AKA διαδικασίας το UE και ο HSS δημιουργούν ένα κοινό προσωρινό κλειδί K_{ASME} το οποίο προωθείται στον MME. Το κλειδί αυτό προκύπτει από τα CK και IK session keys. Από το K_{ASME} παίρνουμε τρία συμπληρωματικά κλειδιά που προωθούνται στο eNB από τον MME και ύστερα ακόμα τρία συμπληρωματικά κλειδιά που χρησιμοποιούνται για κρυπτογράφηση και ακεραιότητα πακέτων μεταξύ UE και eNB. Το KeNB κάθε φορά που το UE αλλάζει eNB αλλάζει.



Εικόνα 11. Ιεραρχία παραγωγής κλειδιών E-UTRAN

Οι απαιτήσεις ασφαλείας σε EPC και E-UTRAN σχετικά με το μήκος κλειδιών στους αλγορίθμους κρυπτογράφησης και ακεραιότητας είναι 128 ή 256 bits. Επίσης τα κλειδιά που χρησιμοποιούνται για προστασία των UP, NAS και AS πρέπει να εξαρτώνται από τον αλγόριθμο που θα χρησιμοποιηθούν.



Εικόνα 12. Διαχείριση κλειδιών στο E-UTRAN

Πιο αναλυτικά η ιεραρχία των κλειδιών περιλαμβάνει τα εξής κλειδιά ασφαλείας: KeNB, KNASint, KNASenc, KUPenc, KRRCint,KRRCenc and KUPint.

- KeNB είναι το κλειδί που δημιουργείται από τον MME και UE από το K_{ASME} ή το UE και το target eNB

Κλειδιά για την κίνηση NAS,

- KNASint , χρησιμοποιείται μόνο για προστασία της κίνησης NAS με συγκεκριμένο αλγόριθμο ακεραιότητας . Το κλειδί συμπληρώνεται από τα UE και MME συνδυάζοντας το K_{ASME} και ένα παράγοντα του αλγορίθμου.
- KNASenc , χρησιμοποιείται μόνο για προστασία της κίνησης NAS με συγκεκριμένο αλγόριθμο κρυπτογράφησης . Το κλειδί συμπληρώνεται από τα UE και MME συνδυάζοντας το K_{ASME} και ένα παράγοντα του αλγορίθμου.

Κλειδιά για την κίνηση στο UP:

- KUPenc χρησιμοποιείται μόνο για την προστασία της κίνησης στο UP με συγκεκριμένο αλγόριθμο κρυπτογράφησης. Το κλειδί συμπληρώνεται από τα UE και eNB συνδυάζοντας το KeNB και ένα παράγοντα του αλγορίθμου.

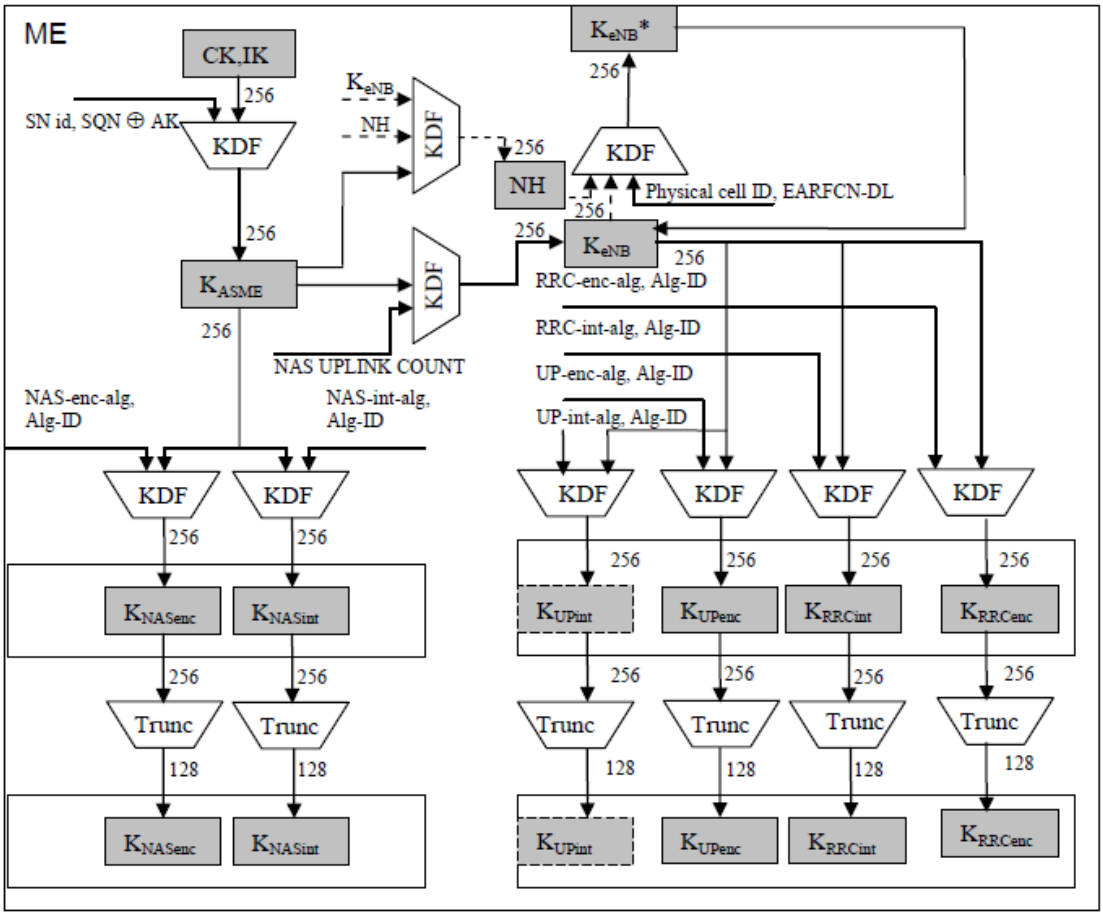
- KUPint χρησιμοποιείται μόνο για την προστασία της κίνησης στο UP μεταξύ των RN και DeNB με συγκεκριμένο αλγόριθμο ακεραιότητας. Το κλειδί συμπληρώνεται συνδυάζοντας το KeNB και ένα παράγοντα του αλγορίθμου.

Κλειδιά για την κίνηση RRC:

- KRRCint , χρησιμοποιείται μόνο για την προστασία της κίνησης στο RRC με συγκεκριμένο αλγόριθμο ακεραιότητας. Το κλειδί συμπληρώνεται από τα UE και eNB συνδυάζοντας το KeNB και ένα παράγοντα του αλγορίθμου.
- KRRCenc , χρησιμοποιείται μόνο για την προστασία της κίνησης στο RRC με συγκεκριμένο αλγόριθμο κρυπτογράφησης. Το κλειδί συμπληρώνεται από τα UE και eNB συνδυάζοντας το KeNB και ένα παράγοντα του αλγορίθμου.

Ενδιάμεσα κλειδιά :

- NH είναι ένα κλειδί που δημιουργείται από UE και MME και παρέχει ασφάλεια μεταγενέστερα στην διαδικασία του handover.
- KeNB είναι το κλειδί που δημιουργείται από το UE και το eNB και λειτουργεί κάθετα αλλά και οριζόντια στην ιεραρχία.



Εικόνα 13. Διαχείριση κλειδιών στο UE

7.3.3 Πρωτόκολλο λειτουργίας ασφάλειας NAS.

Η δεύτερη φάση εκτελεί τη διαπραγμάτευση των αλγορίθμων ασφαλείας, οι οποίοι στη συνέχεια χρησιμοποιούνται για την κρυπτογράφηση δεδομένων διαχείρισης και την προστασία ακεραιότητας στο επίπεδο NAS. Η επικοινωνία περιλαμβάνει το MME και το UE και έχει ως εξής.

I. Το MME αποστέλλει εντολή ασφάλειας λειτουργίας NAS, η οποία περιέχει τους επιλεγμένους αλγόριθμοι ακεραιότητας EIA και τους αλγόριθμους κρυπτογράφησης EEA. Το ίδιο το μήνυμα προστατεύει την ακεραιότητα με έναν κώδικα ελέγχου ταυτότητας μηνυμάτων (MAC) βάσει του επιλεγμένου αλγόριθμου ακεραιότητας EIA και ενός κλειδιού που προέρχεται από το KASME.
II. Κατά τη λήψη, η συσκευή χρήστη UE ελέγχει το MAC και αποκρίνεται με ένα σήμα ολοκλήρωσης της κατάστασης ασφαλείας NAS και επιβεβαιώνοντας ότι οι επιλεγμένοι αλγόριθμοι γίνονται αποδεκτοί.

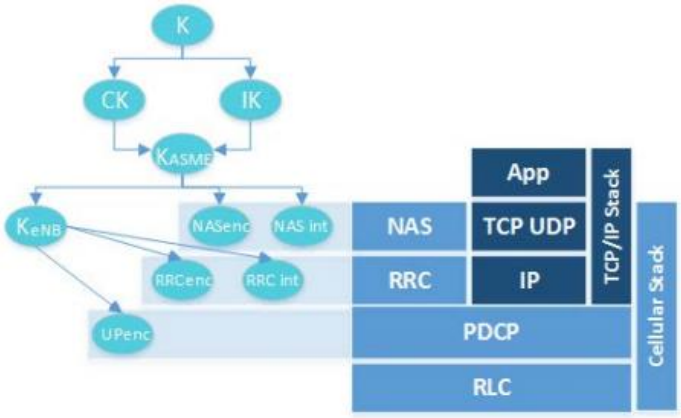
Μετά από επιτυχή διαπραγμάτευση, οι αλγόριθμοι ακεραιότητας EIA και κρυπτογράφησης EEA εφαρμόζονται για την εγκαθίδρυση κρυπτογράφησης των δεδομένων διαχείρισης. Έτσι, το μήνυμα NAS Security Mode Complete και όλα τα μεταγενέστερα μηνύματα που ανταλλάσσονται στο επίπεδο NAS πρέπει να προστατεύονται από τους επιλεγμένους αλγόριθμους ακεραιότητας και κρυπτογράφησης.

7.3.4 Πρωτόκολλο λειτουργίας ασφάλειας ραδιοεπικοινωνίας (RRC).

Η τρίτη φάση διαπραγματεύεται τους αλγόριθμους ασφαλείας στο στρώμα AS. Επιτρέπει την κρυπτογράφηση των δεδομένων χρήστη και προστατεύει όλα τα μηνύματα που ανταλλάσσονται στο στρώμα AS. Οι εμπλεκόμενες οντότητες είναι το MME, το eNodeB και η συσκευή χρήστη UE. Η ροή των μηνυμάτων έχει ως εξής.

I. Η ενεργοποίηση της ασφάλειας AS ξεκινά από το MME χρησιμοποιώντας βασικό υλικό που προέρχεται από το KASME. Το παράγωγο κλειδί KeNodeB αποστέλλεται στο eNodeB μέσω ενός μηνύματος αρχικής ρύθμισης περιβάλλοντος.
II. Το eNodeB επιλέγει τους αλγόριθμους ακεραιότητας EIA και τους αλγόριθμους κρυπτογράφησης EEA ειδικά για την προστασία στρώματος AS. Το μήνυμα εντολής λειτουργίας ασφαλείας της RRC προστατεύει την επιλογή με MAC χρησιμοποιώντας ένα κλειδί που προέρχεται από το KeNodeB.
III. Όταν το UE επαληθεύσει με επιτυχία το MAC, ο UE στέλνει ένα μήνυμα RRC Security Mode Completed πίσω στο eNodeB που επιβεβαιώνει την επιλογή.

Όλα τα επόμενα μηνύματα στρώματος AS είναι κρυπτογραφημένα και προστατεύονται από την ακεραιότητα. Τέλος, το MME στέλνει ένα μήνυμα Attach Accept στην συσκευή χρήστη UE, το οποίο μήνυμα απαντάται από ένα Attach Complete ολοκληρώνοντας έτσι την διαδικασία.



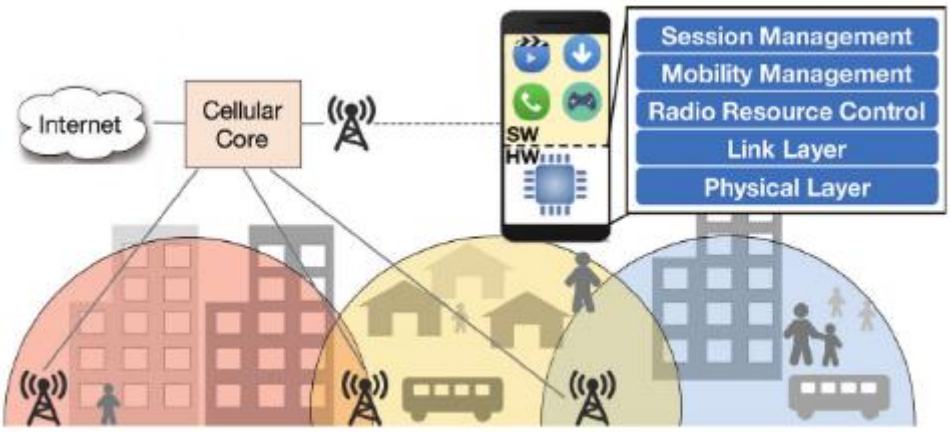
Εικόνα 14. Κλειδιά ανά πρωτόκολλο

Key	Name	Length (bits)	Derived in Part From
K	Master Key	128	N/A: Pre-shared root key
IK	Integrity Key	128	K
CK	Cipher Key	128	K
K_{ASME}	MME Base Key	256	CK, IK
NH	Next Hop	256	K_{ASME}
K_{eNB^*}	eNB Handover Key	256	K_{ASME}, K_{eNB}
K_{eNB}	eNB Base Key	256	K_{ASME}, NH
K_{NASint}	NAS Integrity Key	128	K_{ASME}
K_{NASenc}	NAS Confidentiality Key	128	K_{ASME}
RRC_{enc}	RRC Confidentiality Key	128	K_{eNB}, NH
RRC_{int}	RRC Integrity Key	128	K_{eNB}, NH
UPenc	UP Confidentiality Key	128	K_{eNB}, NH

Εικόνα 15. Πληροφορίες κρυπτογραφικών κλειδιών

8. MobileInsight - Παρουσίαση

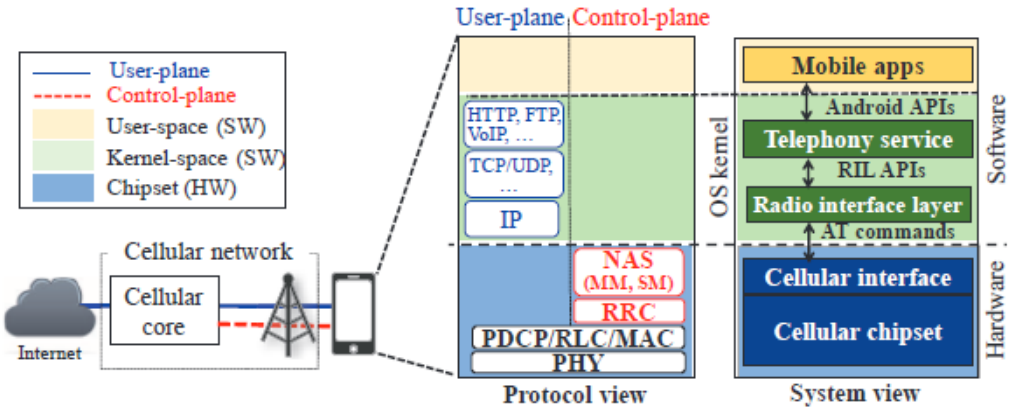
Είναι ένα ανοιχτού κώδικα λογισμικό για κινητές συσκευές Android και υπολογιστές MacOSX ή Linux, η ανάπτυξη του ξεκίνησε αρχικά στα πανεπιστήμια UCLA και Purdue και ο κώδικάς του βρίσκεται στο github. Προσφέρει μια λύση που είναι βασισμένη εντελώς σε λογισμικό και μπορεί να τρέξει εντός μια συσκευής ώστε να γίνει συλλογή και περεταίρω ανάλυση των πρωτοκόλλων κινητής τηλεφωνίας. Τρέχει σαν service στον αποθηκευτικό χώρο της συσκευής που προορίζεται για τον χρήστη αρκεί να του παραχωρηθούν δικαιώματα χρήστη root. Παρεμβαίνει στα μηνύματα που ανταλλάσσει το δίκτυο LTE με την συσκευή UE έχοντας πρόσβαση στο chipset της αυτής με δυνατότητα εξαγωγής των δεδομένων εκτός συσκευής χρησιμοποιώντας την λειτουργία debugging που έχουν οι συσκευές Android. Είναι συμβατό με chipset της Qualcomm και MediaTek.



Εικόνα 16. Protocol stack - UE information access 1

Υποστηρίζει την ανάλυση κάθε μηνύματος από τα προκαθορισμένα πρωτόκολλα κινητής τηλεφωνίας σε επίπεδο control plane και στα κατώτερα layers των πρωτοκόλλων. Δεν μας δίνει πρόσβαση απλά στο τί μεταφέρεται αλλά ξεκαθαρίζει το πώς και γιατί. Υποστηρίζει πληθώρα πληροφοριών κινητής τηλεφωνίας και ο κάθε χρήστης μπορεί να επιλέξει τι θα κάνει καταγραφή ώστε να βγάλει το συμπέρασμα που τον ενδιαφέρει. Καθώς έχουμε δυνατότητα αποθήκευσης των logs στην μνήμη της συσκευής μπορούμε να κάνουμε συλλογή δεδομένων σε πραγματικό χρόνο και να πραγματοποιήσουμε την περεταίρω ανάλυση σε δεύτερο χρόνο.

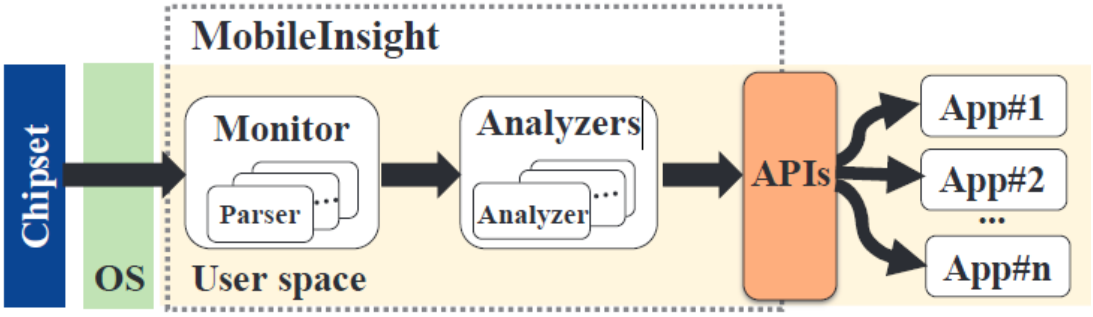
Όπως αναφέραμε παραπάνω είναι ένα λογισμικό ανοιχτού κώδικα έτσι μπορούμε να χρησιμοποιήσουμε τα plug-ins των developers ή να γράψουμε τα δικά μας κατ' ανάγκη.



Εικόνα 17. Protocol stack - UE information access 2

Γενικά το λογισμικό αυτό έχει τρείς βασικούς στόχους

1. Να μπορεί να δουλέψει εντός μιας εμπορικά διαθέσιμης κινητής συσκευής, χωρίς τροποποίησες σε hardware ή λειτουργικό σύστημα.
2. Να παρέχει analytics, για τα πρωτόκολλα σε πραγματικό χρόνο, πέρα από την αρχειοθέτηση τους, σχετικά με την κατάσταση και την λογική λειτουργίας τους με σκοπό την διάγνωση βλαβών και την βελτίωση της υποδομής.
3. Να μας δίνει όλες τις λεπτομέρειες σε μεγάλο εύρος, σε όλα τα πρωτόκολλα και επίπεδα.



Εικόνα 18. Αρχιτεκτονική MobileInsight

Η αρχιτεκτονική λειτουργείας του MobileInsight έχει δύο κύρια στοιχεία

1. **Την παρακολούθηση – Monitor**

Αποκαλύπτει τα raw δεδομένα κινητής τηλεφωνίας που λαμβάνει από το chipset και τα μετατρέπει σε αναγνώσιμα δεδομένα σε πραγματικό χρόνο αφού επεξεργαστούν από parsers ανά πρωτόκολλο ή τα αποθηκεύει στον αποθηκευτικό χώρο της συσκευής. Επίσης προωθεί τα δεδομένα αυτά στους analyzers για περεταίρω επεξεργασία.

2. **Την ανάλυση - Analyzer**

Παραλαμβάνοντας τα μηνύματα που έχουν εξαχθεί από το προηγούμενο στάδιο έχει σκοπό να αναδείξει τις διαδικασίες των πρωτοκόλλων και τον τρόπο λειτουργίας τους. Βασίζεται στα ευρήματα αλλά και στην αναμενόμενη συμπεριφορά για να αναλύσει την κατάσταση των πρωτοκόλλων, τις αλλαγές κατάστασης και τις ενέργειες που γίνονται.

Πέρα από τα δύο κύρια στοιχεία το MobileInsight δίνει δυνατότητα προσθήκης plugin όπως αναφέραμε νωρίτερα πέρα από τα προ εγκατεστημένα. Με τον τρόπο αυτό τα αποτελέσματα που εξάγουμε από τους analyzers έχουμε δυνατότητα να τα φιλτράρουμε για να πάρουμε την πληροφορία που μας ενδιαφέρει ή και που να την ταξινομήσουμε και να αποθηκεύσουμε.

Με το MobileInsight ο κάθε χρήστης μπορεί να κάνει :

- Συλλογή και εξαγωγή over-the-air μηνυμάτων κινητής.
- Επιλέξει ποια μηνύματα θα συλλέξει.
- Επιλέξει ποια μηνύματα θα αναλύσει περεταίρω και ποιες παραμέτρους θα εξετάσει.
- Να τροποποιήσει τους εγκατεστημένους analyzers ή να κατασκευάσει δικούς του.
- Να δημιουργήσει δικά του plugins
- Το χρησιμοποιήσει σε κινητό ή και υπολογιστή.

8.1 Συμβολή στην έρευνα

Το Mobileinsight μπορεί να βοηθήσει ερευνητές και developers στην κατανόηση τω κλειστών αλλά μεγάλων σε μέγεθος δικτύων κινητής τηλεφωνίας. Το αποτέλεσμα θα είναι η ανάπτυξη περεταίρω ερευνών και εφαρμογών Με τις δυνατότητες που έχει να καταγράφει και να αναλύει σε επίπεδο χαμηλότερο του layer 2 μπορεί να χρησιμοποιηθεί για την ανάλυση, διάγνωση αστοχιών, και τη βελτίωση της απόδοσης όπως και τα κενά ασφαλείας ενός δικτύου.

Data analytics – σε layer 2

Η πιο εύχρηστη δυνατότητα του MobileInsight είναι η καταγραφή πληροφοριών κινητής τηλεφωνίας στην ίδια τη συσκευή. Με αυτό πετυχαίνουμε συλλογή δεδομένων από διάφορα σημεία , μοντέλα συσκευών, δίκτυα και παρόχους που σε δεύτερο χρόνο μπορούμε να αναλύσουμε μαζικά. Η ομάδα του MobileInsight έχει δημοσιεύσει πάνω από 250GB δεδομένα σηματοδοσίας με 72 εκατομμύρια μηνύματα στη διεύθυνση http://metro.cs.ucla.edu/mobile_insight/insightshare.html

Διάγνωση προβλημάτων δικτύου.

Εκτός από την ανάλυση συμπεριφοράς κοινής χρήσης, το MobileInsight μπορεί επίσης να βοηθήσει στη διάγνωση προβλημάτων δικτύου χρησιμοποιώντας εμπορικά διαθέσιμες συσκευές. Σε περίπτωση σφαλμάτων, οι χρήστες μπορεί να θέλουν να μάθουν γιατί συμβαίνουν και πώς να τα επιλύσουν (εάν είναι δυνατόν). Παρακολουθώντας τη δυναμική του κάθε πρωτοκόλλου και τη λογική λειτουργίας, το MobileInsight μπορεί να προσφέρει άμεσες συμβουλές και για τα δύο.

Βελτίωση απόδοσης δικτύου.

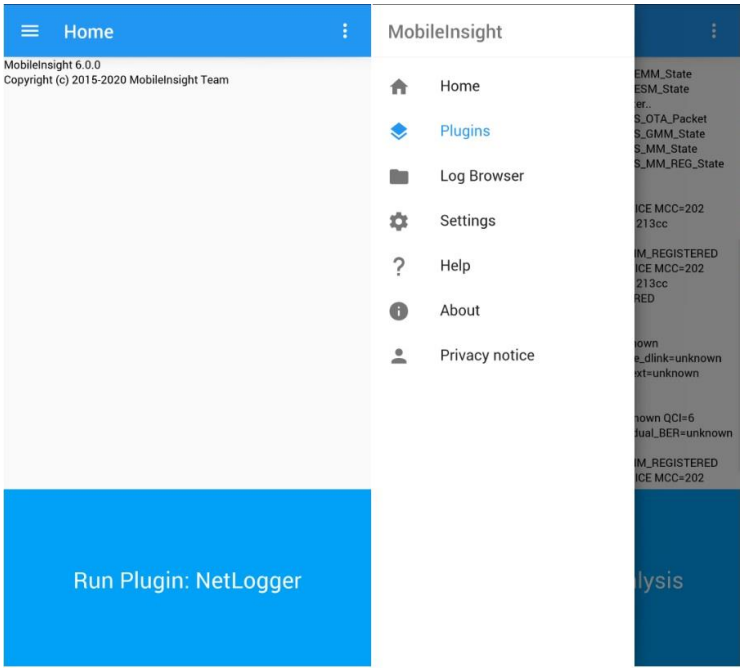
Το MobileInsight μπορεί να παρέχει υποδείξεις για εφαρμογές με στόχο τη βελτίωση της απόδοσης και τη βελτίωση των κρίσιμων υπηρεσιών δικτύου από την πλευρά της συσκευής. Για παράδειγμα, οι εφαρμογές βίντεο streaming μπορούν να αξιοποιήσουν τις πληροφορίες για το διαθέσιμο εύρος ζώνης του φυσικού επιπέδου σε πραγματικό χρόνο ώστε το MobileInsight για να προσαρμόσει την ποιότητα (bitrate) του βίντεο. Ένα άλλο παράδειγμα είναι η περιαγωγή μεταξύ παρόχων εντός μια χώρας. Στις ΗΠΑ οι Google και Apple έχουν ξεκινήσει τα Google Project Fi και Apple SIM αντίστοιχα , οι προσπάθειες αυτές προβλέπουν πρόσβαση σε πολλαπλά δίκτυα με αυτόματη επιλογή της βέλτιστης σύνδεσης για ενίσχυση της ποιότητας πρόσβασης. Οι υπηρεσίες αυτές ελέγχουν τα διαθέσιμα δίκτυα WiFi και LTE και επιλέγουν εκείνο με το ισχυρότερο σήμα και την μεγαλύτερη διαθέσιμη ταχύτητα χωρίς να χρειάζεται επέμβαση από το χρήστη. Η παραπάνω κατεύθυνση είναι πολλά υποσχόμενη και αναμένεται να εξελιχθεί με την έλευση των δικτύων 5G, η μελέτες που έγιναν όμως με το MobileInsight δείχνουν πως στην πραγματικότητα δεν γίνεται πάντα χρήση του βέλτιστου δικτύου ή παρουσιάζονται μεγάλες διακοπές κατά το handover μεταξύ παρόχων. Τα ζητήματα αυτά βασίζονται στην υλοποίηση του roaming μεταξύ παρόχων και στον έλεγχο της κινητικότητας που ελέγχεται από τον serving πάροχο. Η βασική ιδέα είναι να αξιοποιήσουμε τις γνώσεις για τον τομέα των κυψελοειδών δικτύων. Το MobileInsight το καθιστά εφικτό έχοντας πρόσβαση στις πληροφορίες διαχείρισης κινητικότητας σε πραγματικό χρόνο.

Εντοπισμός κενών ασφαλείας.

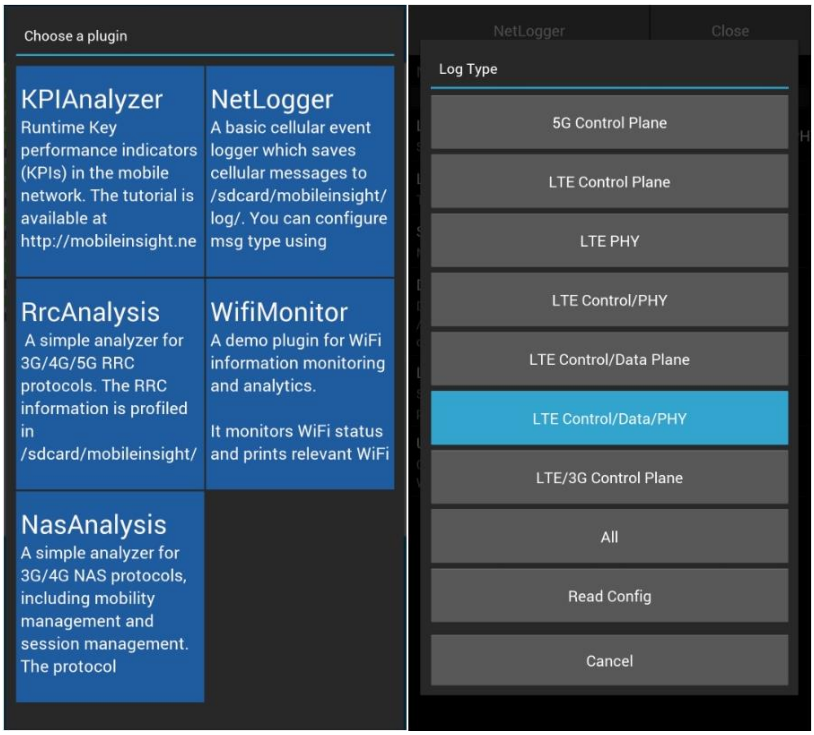
Το MobileInsight καθιστά επίσης δυνατή την ανίχνευση απειλών μεταξύ λειτουργικού συστήματος/εφαρμογών και του δικτύου κινητής. Παράδειγμα οι υπηρεσίες φωνής και σύντομων μηνυμάτων (SMS), οι οποίες δεν είναι μόνο οι βασικές λειτουργίες μιας συσκευής, αλλά και δομικά στοιχεία για άλλες εφαρμογές (ανταλλαγή άμεσων μηνυμάτων, τραπεζική τηλεφωνία, κοινωνική δικτύωση κ.λπ.). Ωστόσο, έχει αποδειχθεί ότι και τα δύο υπηρεσίες μπορούν να γίνουν exploit καθώς οι υπηρεσίες φωνής και SMS πλέων υλοποιούνται από IP δίκτυα. Έτσι μπορεί να ξεκινήσει μια νέα επίθεση όπως δωρεάν μεταφορά δεδομένων μέσω φωνής, SMS spoofing, ή υποκλοπή social λογαριασμών και πρόσβαση σε εφαρμογές e-banking. Η μετατροπή σε δίκτυα all-IP παρακάμπτει δικλείδες ασφαλείας του λειτουργικού συστήματος όπως την απομόνωση μεταξύ φωνής και δεδομένων, άδειες πρόσβασης εφαρμογών κ.α. Το MobileInsight μπορεί να διευκολύνει τον εντοπισμό αυτών των απειλών, αφού μας δίνει παραμέτρους του δικτύου κινητής (κρυπτογραφικά κλειδιά, λειτουργίες ασφαλείας, συνεδρίες δεδομένων κ.λπ.) στο χώρο του χρήστη με σκοπό να πραγματοποιήσουμε έλεγχο ασφαλείας στα δεδομένα που λαμβάνει το λειτουργικού συστήματος.

8.2 Mobile interface

Για την χρήση της mobile έκδοσης απαιτείται το chipset της συσκευή να είναι Qualcomm ή MediaTek και η συσκευή να είναι rooted. Δεν έχει σχεδιαστεί να τρέχει σε chipset άλλου κατασκευαστή όμως υπάρχουν αναφορές ότι έχει δουλέψει και σε άλλες συσκευές ακόμα και σε iPhone. Κατεβάζοντας και εγκαθιστώντας την εφαρμογή μέσω του .apk αρχείου το μόνο που πρέπει να κάνουμε πέρα από την παραχώρηση δικαιωμάτων root είναι να κλείσουμε την εξοικονόμηση ενέργειας και να παραχωρήσουμε κάποιες άδειες. Η εγκατάσταση της beta 6.0 έκδοσης λειτούργησε χωρίς κανένα σφάλμα σε συσκευή Xiaomi με Android 8.1 Oreo.

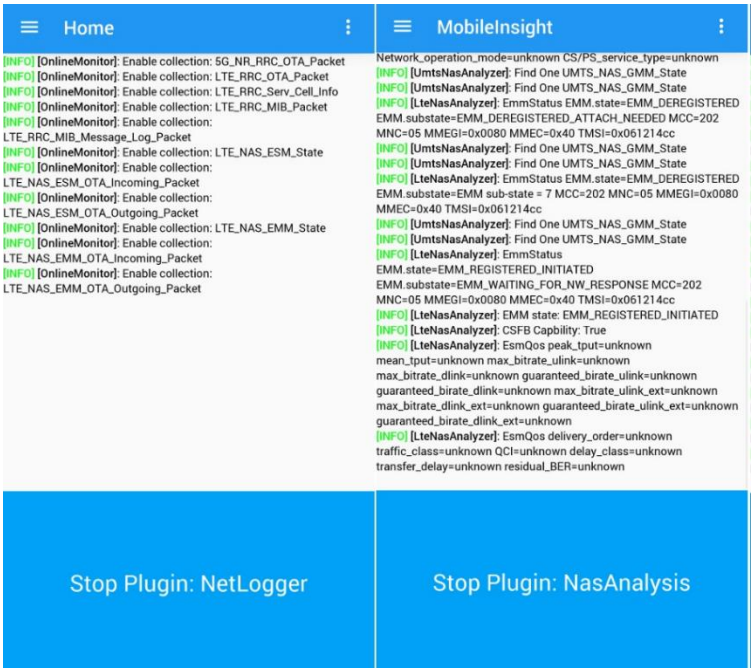


Εικόνα 19. MobileInsight – κεντρικό μενού



Εικόνα 20. Επιλογές Plugin

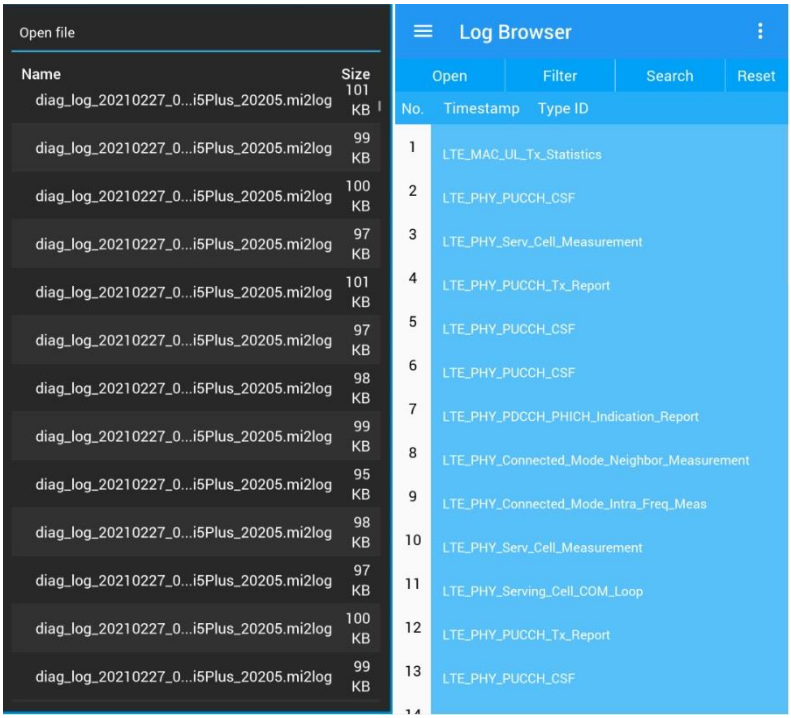
Το περιβάλλον της εφαρμογής είναι αρκετά εύχρηστο και δίνει αρκετές επιλογές. Μπορούμε να επιλέξουμε ποιο plugin θα ενεργοποιήσουμε κατά περίπτωση αλλά και τον τύπο του log που θα κρατήσουμε.



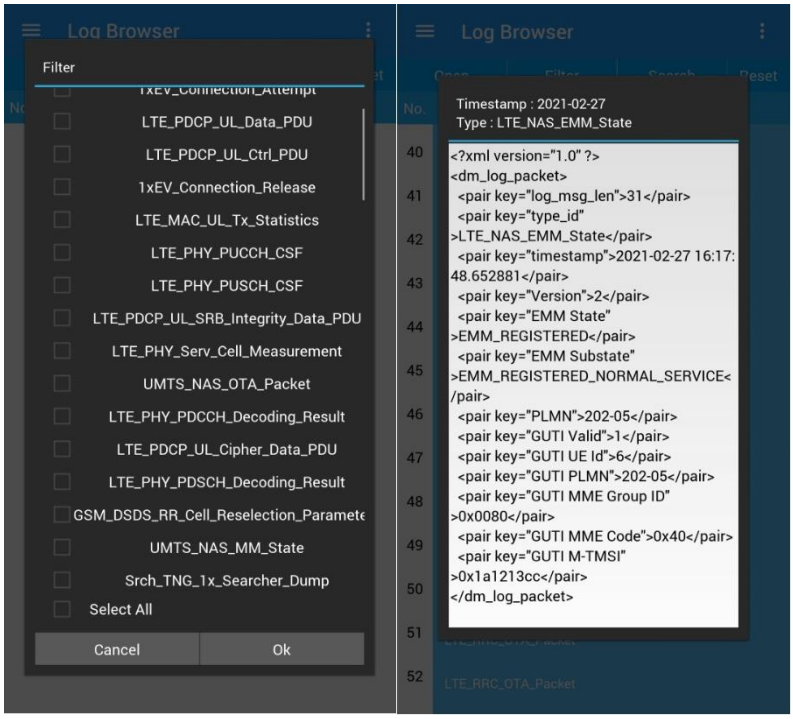
Εικόνα 21. Plugins σε λειτουργεία καταγραφής

Εικόνα 22. Plugins σε λειτουργεία καταγραφής

Αφού γίνει επιλογή του plugin, στο κάτω μέρος της οθόνης υπάρχει πλήκτρο που ξεκινάει και σταματάει την καταγραφή. Κατά την διάρκεια της καταγραφής και ανάλυσης η εφαρμογή εμφανίζει επεξεργασμένα δεδομένα σε πραγματικό χρόνο που περιέχουν πληροφορίες για παραμέτρους και τις τιμές τους ανάλογα τον analyzer που θα χρησιμοποιήσουμε.



Εικόνα 23. Log browser



Εικόνα 24. Log Filtering

Ταυτόχρονα αποθηκεύει logs κάθε κάποια KB ανάλογα με τις επιλογές στις ρυθμίσεις. Τα logs αποθηκεύονται σε αρχεία με κατάληξη .mi2log αλλά η μορφή τους είναι xml. Τα αρχεία αυτά μπορούμε να τα εισάγουμε στην desktop έκδοση για περεταίρω ανάλυση.

8.3 Desktop Interface

Από τον ίδιο κώδικα που γίνεται compile η mobile εφαρμογή υλοποιείται και η desktop έκδοση. Η desktop έκδοση προσφέρει καλύτερη εμπειρία στην εξαγωγή συμπεράσματος με τον log viewer που διαθέτει διότι είναι πιο εύχρηστος και αποδοτικός. Για την εγκατάσταση σε ένα σύστημα Ubuntu απαιτούνται κάποια επιπλέον packages και dependencies ώστε να μπορέσει να εγκατασταθεί. Σε παλιότερες εκδόσεις του mobile insight χρειαζόταν να εγκατασταθούν αρκετές βιβλιοθήκες αλλά από την έκδοση 5.0 και μετά ο κώδικας είναι εξολοκλήρου σε Python 3 και αυτό απλοποιεί την διαδικασία εγκατάστασης. Στην υλοποίηση που πραγματοποιήθηκε έγινε εγκατάσταση της έκδοσης beta 6.0 σε Ubuntu 20.04 LTS x64.

Τα προαπαιτούμενα εγκαταστάθηκαν με τις εντολές :

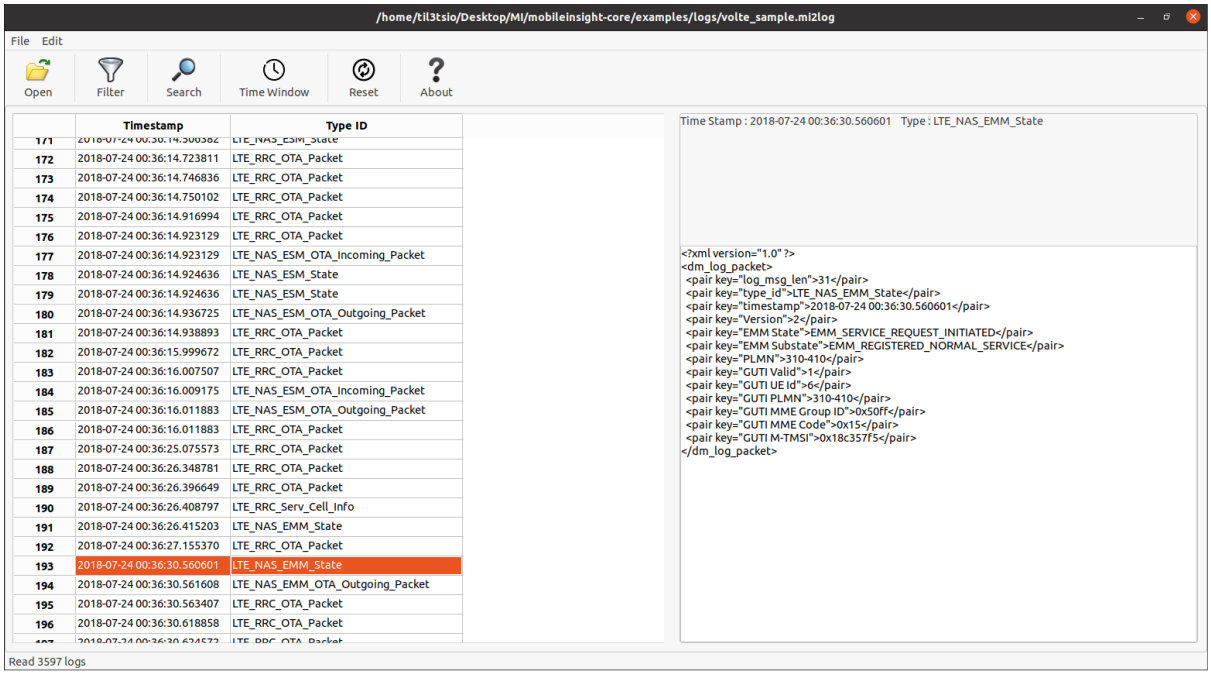
apt-get -y install python3-pip python3-crcmod python3-serial

apt-get -y install python3-matplotlib python3-wxgtk4.0

και η εγκατάσταση ξεκινάει με την εντολή :

./install-ubuntu.sh

Μετά την εγκατάσταση τρέχουμε την εντολή ***mi-gui*** και έχουμε την παρακάτω εικόνα του interface. Είναι φιλική προς το χρήστη πλατφόρμα και μπορεί να επεξεργαστεί *.mi2logs ή *.qmdl αρχεία.



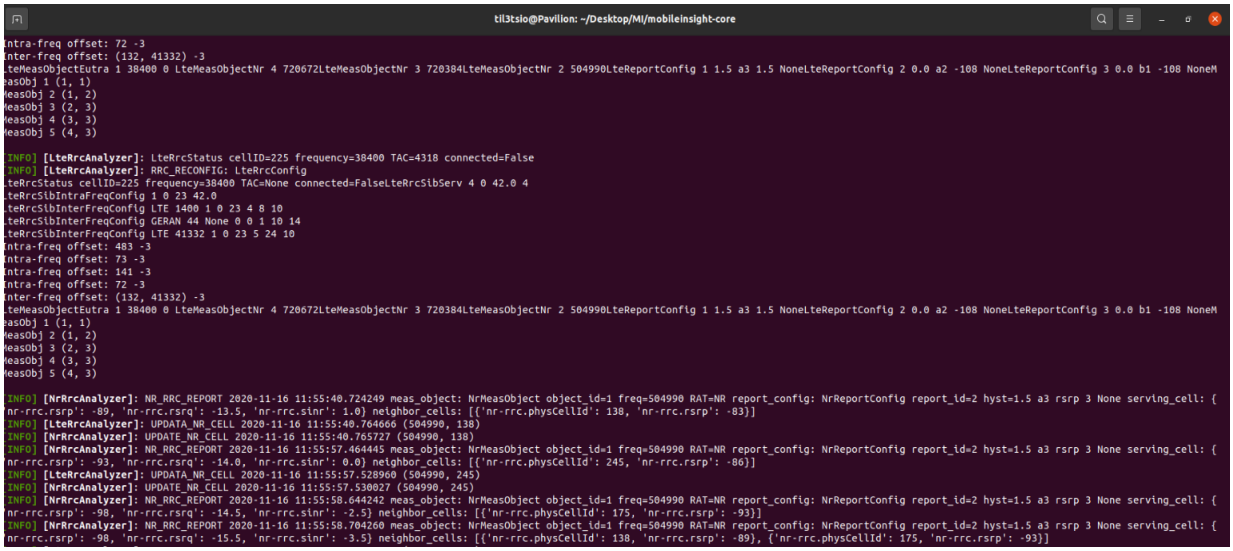
Εικόνα 25 .MobileIsight GUI

Στην desktop έκδοση μπορούμε να συλλέξουμε απευθείας δεδομένα από ένα UE. Για να γίνει αυτό θα πρέπει να ενεργοποιήσουμε στις λειτουργείες προγραμματιστή την λειτουργεία USB debugging και την λειτουργεία διάγνωσης του chipset.
Ανάλογα την συσκευή υπάρχει συγκεκριμένη αριθμοσειρά για να γίνει αυτό, στην Xiaomi συσκευή που έχει chipset Qualcomm πληκτρολογήσαμε ***#*#717717#*#*** στον dialer. Πριν προχωρήσουμε όμως στην σύνδεση πρέπει να εγκαταστήσουμε το πακέτο android adb με την εντολή:
apt-get -y install android-tools-fastboot android-tools-abd
και να τρέξουμε από terminal στο κινητό τηλέφωνο την εντολή:
setprop sys.usb.config diag,adb αφού το έχουμε συνδέσει στον υπολογιστή μας.

Πριν ξεκινήσει η καταγραφή όμως μέσω του UE στον υπολογιστή θα πρέπει να αντιστοιχίσουμε μια εικονική σειριακή θύρα στην υποδοχή usb που έχουμε συνδέσει τη συσκευή μας. Δίνοντας την εντολή ***lsusb*** βλέπουμε όλες τις συνδεδεμένες συσκευές και αφού εντοπίσουμε την συσκευή που μας ενδιαφέρει δίνουμε την παρακάτω εντολή για να κάνουμε την αντιστοιχία.
modprobe usbserial vendor=0x05c6 product=0x901d

Εικόνα 26. USB to serial

Για να ξεκινήσει η καταγραφή δίνουμε την εντολή :
python3 monitor-example.py /dev/ttyUSB0 115200
στο αρχείο monitor-example.py υπάρχουν οι οδηγίες για το ποια plugins θα φορτωθούν και που θα αποθηκεύει το .mi2log αρχείο , ttyUSB0 είναι το serial interface που έχουμε ορίσει να έχει το κινητό τηλέφωνο και 115200 είναι το baud rate που δούλεψε η εξαγωγή δεδομένων στη συγκεκριμένη συσκευή. Αν ξεκινήσει με επιτυχία η λήψη δειγμάτων έχουμε την παρακάτω εικόνα στην οθόνη μας με πλήθος δεδομένων.



Εικόνα 27. Datalogging through diag port

Αφού έχουμε λάβει ικανοποιητικό αριθμό δειγμάτων διακόπτουμε την καταγραφή με Ctrl-C. Τα log έχουν καταγραφεί σε αρχείο κατάληξης .mi2log στον ίδιο φάκελο σύμφωνα με τις οδηγίες που περιέχονται στο monitor-example.py που αναφέραμε νωρίτερα.

```
1435219131.01 [INFO] WCDMA_RRC_Serv_Cell_Info
<dm_log_packet>
        <pair key="type_id">WCDMA_RRC_Serv_Cell_Info</pair>
        <pair key="timestamp">2020-06-28 23:37:59.130003</pair>
        <pair key="Uplink RF channel number">9763</pair>
        <pair key="Download RF channel number">10713</pair>
        <pair key="Cell ID">42602391</pair>
        <pair key="UTRA registration area (overlapping URAs)">11</pair>
        <pair key="Allowed Call Access">0</pair>
        <pair key="PSC">3504</pair>
        <pair key="PLMN">460-0115</pair>
        <pair key="LAC">46345</pair>
        <pair key="RAC">1</pair>
</dm_log_packet>
1435219131.76 [INFO] WCDMA_RRC_OTA_Packet
...
1435219135.51 [INFO] LTE_RRC_OTA_Packet
...
```

Εικόνα 28. dump messages format

Το log είναι της παραπάνω μορφής και μπορούμε να δούμε λεπτομέρειες και να χρησιμοποιήσουμε φίλτρα ανοίγοντας το από το GUI του MobileInsight. Για να πάρουμε στοχευμένα αποτελέσματα

σχετικά με τις παραμέτρους που θέλουμε να ερευνήσουμε μπορούμε να ορίσουμε δικά μας script όπως έχουμε αναφέρει και παραπάνω.

8.4 Analytics δικτύου.

Όπως έχουμε αναφέρει παραπάνω το Mobile Insight έχει δύο κύρια modules, monitors και analyzers. Τα monitors κάνουν συλλογή raw δεδομένων και τα μετατρέπουν σε μηνύματα πρωτοκόλλων, τα μηνύματα αυτά χρησιμοποιούνται για περεταίρω έρευνα του δικτύου. Οι analyzers λειτουργούν βάση γεγονότων και μπορούν να χρησιμοποιηθούν για online ή και offline ανάλυση.

Το framework της εφαρμογής είναι αρκετά αρθρωτό και επεκτάσιμο στο σχεδιασμό. Για να κάνει ο χρήστης μια ανάλυση πρέπει να δηλώσει ένα monitor και οποιανδήποτε αριθμό analyzer. Είναι εφικτό ο χρήστης να γράψει τους δικούς του analyzers για να πετύχει συγκεκριμένο σκοπό.

8.4.1 Monitor logs

Τα logs που συλλέξαμε και αποθηκεύσαμε στο προηγούμενο κεφάλαιο βασίστηκαν στον παρακάτω κώδικα. Ο παρακάτω κώδικας εκτελεί την πιο απλή εργασία του να συλλέξει μόνο logs που αφορούν τις κυψέλες του δικτύου.

Με τον κώδικα αυτό ζητάμε να γίνεται καταγραφή των μηνυμάτων για 3G, 4G και 5G μηνύματα κυψέλης. Με την εντολή enable_log( ) ζητάμε συγκεκριμένους τύπους logs. Δεν περιέχει ο κώδικας αυτός κάποιον analyzer άρα δεν πραγματοποιείται κάποια ανάλυση. Όταν ο κώδικας θα εκτελεστεί θα αποθηκεύσει τις καταγραφές στο monitor-example.mi2log που μπορεί να χρησιμοποιηθεί για ανάλυση offline ή να ανοιχτεί από το GUI.

```
import os
import sys

# Import MobileInsight modules
from mobile_insight.monitor import OnlineMonitor
from mobile_insight.analyzer import MsgLogger

if len(sys.argv) < 3:
        opt.error("please specify physical port name and baudrate.")
        sys.exit(1)

# Initialize a 3G/4G monitor
src = OnlineMonitor()
src.set_serial_port(sys.argv[1]) #the serial port to collect the traces
src.set_baudrate(int(sys.argv[2])) #the baudrate of the port
```

```
# Specify logs to be collected: RRC (radio resource control) in this example
src.enable_log("5G_NR_RRC_OTA_Packet") # 5G RRC
src.enable_log("LTE_RRC_OTA_Packet") # 4G LTE RRC
src.enable_log("WCDMA_RRC_OTA_Packet") # 3G WCDMA RRC

# Save the monitoring results as an offline log
src.save_log_as("./monitor-example.mi2log")

#Print messages.
dumper = MsgLogger()  #Declare an analyzer
dumper.set_source(src) #Bind the analyzer to the monitor
dumper.set_decoding(MsgLogger.XML)  #decode the message as xml

# Start the monitoring
src.run()
```

Εικόνα 29 .Κώδικας συλλογής cellular logs

8.4.2 Απλή ανάλυση – Εμφάνιση μηνυμάτων κυψέλης.

Το επόμενο βήμα είναι να δημιουργηθεί ένα task χρησιμοποιώντας ένα analyzer. Αφού συμπληρωθεί ο κώδικας με κατάλληλες οδηγίες, καλείται ο MsgLogger analyzer που έχει δυνατότητα να αποκωδικοποιήσει κάθε μήνυμα σε xml ή και json format. Το αποτέλεσμα της σύνδεση του στον monitor είναι ότι θα λαμβάνουμε τα μηνύματα αυτά σε πραγματικό χρόνο για περαιτέρω ανάλυση.

```
import os
import sys

# Import MobileInsight modules
from mobile_insight.monitor import OnlineMonitor
from mobile_insight.analyzer import MsgLogger

if len(sys.argv) < 3:
        opt.error("please specify physical port name and baudrate.")
        sys.exit(1)

# Initialize a 3G/4G monitor
src = OnlineMonitor()
src.set_serial_port(sys.argv[1]) #the serial port to collect the traces
src.set_baudrate(int(sys.argv[2])) #the baudrate of the port

# Specify logs to be collected: RRC (radio resource control) in this example
src.enable_log("5G_NR_RRC_OTA_Packet") # 5G RRC
src.enable_log("LTE_RRC_OTA_Packet") # 4G LTE RRC
src.enable_log("WCDMA_RRC_OTA_Packet") # 3G WCDMA RRC

# Save the monitoring results as an offline log
src.save_log_as("./monitor-example.mi2log")
```

```
#Print messages.
dumper = MsgLogger()  #Declare an analyzer
dumper.set_source(src) #Bind the analyzer to the monitor
dumper.set_decoding(MsgLogger.XML)  #decode the message as xml

# Start the monitoring
src.run()
```

Εικόνα 30. Κώδικας απλής ανάλυσης

8.4.3 Σύνθετη ανάλυση.

Το MobileInsight υποστηρίζει αρθρωτή ανάλυση, πολλοί analyzers να μπορούν να συνδεθούν σε ένα μοναδικό monitor. Αυτό βοηθά στην δημιουργία μιας πιο σύνθετης εργασίας ανάλυσης. Στον παρακάτω κώδικα το monitor λαμβάνει τα μηνύματα κυψέλης RRC και τα μεταφέρει στους WcdmaRrcAnalyzer και LteRrcAnalyzer.

```
import os
import sys

from mobile_insight.monitor import OnlineMonitor
from mobile_insight.analyzer import LteRrcAnalyzer,WcdmaRrcAnalyzer

if len(sys.argv) < 3:
        opt.error("please specify physical port name and baudrate.")
        sys.exit(1)

# Initialize a monitor
src = OnlineMonitor()
src.set_serial_port(sys.argv[1]) #the serial port to collect the traces
src.set_baudrate(int(sys.argv[2])) #the baudrate of the port

# 5G RRC analyzer
nr_rrc_analyzer = NrRrcAnalyzer()
nr_rrc_analyzer.set_source(src)  # bind with the monitor

# 4G RRC analyzer
lte_rrc_analyzer = LteRrcAnalyzer()
lte_rrc_analyzer.set_source(src) #bind with the monitor

# 3G RRC analyzer
wcdma_rrc_analyzer = WcdmaRrcAnalyzer()
wcdma_rrc_analyzer.set_source(src) #bind with the monitor

src.run()
```

Εικόνα 31 .Κώδικας σύνθετης ανάλυσης

Όλα τα παραπάνω παραδείγματα είναι online αναλύσεις, συλλέγουν logs από τις κυψέλες και πραγματοποιούν ανάλυση σε πραγματικό χρόνο. Υπάρχει δυνατότητα να κάνουμε και offline ανάλυση με το MobileInsight, αφού φορτωθεί κάποιο *.mi2log αρχείο που έχει δημιουργηθεί από κάποιο monitor. Αυτό είναι αρκετά χρήσιμο σε κάποιες περιπτώσεις όπως το να κάνουμε μια πολύπλοκη ανάλυση που προτιμάται να γίνει offline ή στην διαδικασία ανάπτυξης κάποιου δικού μας analyzer.

```
import os
import sys

from mobile_insight.monitor import OfflineReplayer
from mobile_insight.analyzer import LteRrcAnalyzer,WcdmaRrcAnalyzer


src = OfflineReplayer()
# Load offline logs
src.set_input_path("./offline_log_examples/")

# RRC analyzer

nr_rrc_analyzer = NrRrcAnalyzer() # 5G NR
nr_rrc_analyzer.set_source(src)  # bind with the monitor

lte_rrc_analyzer = LteRrcAnalyzer() # 4G LTE
lte_rrc_analyzer.set_source(src) #bind with the monitor

wcdma_rrc_analyzer = WcdmaRrcAnalyzer() # 3G WCDMA
wcdma_rrc_analyzer.set_source(src) #bind with the monitor

src.run()
```

Εικόνα 32 . Κώδικας offline ανάλυσης

```
[INFO] [LteRrcAnalyzer]: MEAS_PCELL: {'timestamp': '2020-11-16 04:33:58.484149', 'rsrp': 39, 'rssi': -102, 'rsrq': 17}
[INFO] [LteRrcAnalyzer]: NR_RRC_REPORT 2020-11-16 04:33:58.484149 meas_object: LteMeasObjectNr 3 720672 config: LteReportC
onfig 5 0.0 a5 -108 -105 NR cells: [{'lte-rrc.pci_r15': 283, 'lte-rrc.rsrpResult_r15': None}, {'lte-rrc.pci_r15': 138, 'lt
e-rrc.rsrpResult_r15': None}, {'lte-rrc.pci_r15': 349, 'lte-rrc.rsrpResult_r15': None}, {'lte-rrc.pci_r15': 432, 'lte-rrc.
rsrpResult_r15': None}]
[INFO] [LteRrcAnalyzer]: UPDATA_NR_CELL 2020-11-16 04:33:58.531553 (504990, 283)
[INFO] [NrRrcAnalyzer]: UPDATE_NR_CELL 2020-11-16 04:33:58.532642 (504990, 283)
[INFO] [NrRrcAnalyzer]: NR_RRC_REPORT 2020-11-16 04:34:00.360805 meas_object: NrMeasObject object_id=1 freq=504990 RAT=NR
report_config: NrReportConfig report_id=2 hyst=1.5 a3 rsrp 3 None serving_cell: {'nr-rrc.rsrp': -99, 'nr-rrc.rsrq': -12.5,
 'nr-rrc.sinr': 1.5} neighbor_cells: [{'nr-rrc.physCellId': 138, 'nr-rrc.rsrp': -95}]
[INFO] [LteRrcAnalyzer]: UPDATA_NR_CELL 2020-11-16 04:34:00.450631 (504990, 138)
[INFO] [NrRrcAnalyzer]: UPDATE_NR_CELL 2020-11-16 04:34:00.452142 (504990, 138)
[INFO] [NrRrcAnalyzer]: NR_RRC_REPORT 2020-11-16 04:34:04.420457 meas_object: NrMeasObject object_id=1 freq=504990 RAT=NR
report_config: NrReportConfig report_id=2 hyst=1.5 a3 rsrp 3 None serving_cell: {'nr-rrc.rsrp': -104, 'nr-rrc.rsrq': -14.5
, 'nr-rrc.sinr': -2.0} neighbor_cells: [{'nr-rrc.physCellId': 283, 'nr-rrc.rsrp': -98}]
[INFO] [LteRrcAnalyzer]: UPDATA_NR_CELL 2020-11-16 04:34:04.490328 (504990, 283)
[INFO] [NrRrcAnalyzer]: UPDATE_NR_CELL 2020-11-16 04:34:04.491318 (504990, 283)
[INFO] [LteRrcAnalyzer]: RRC_RECONFIG: LteRrcConfig
```

Εικόνα 33 .Αποτελέσματα ανάλυσης

8.5 KPI analyzers.

Οι Βασικοί Δείκτες Απόδοσης- KPIs είναι σχεδιασμένοι ώστε να αντικατοπτρίζουν την απόδοση του δικτύου. Οι πάροχοι χρησιμοποιούν τους δείκτες αυτούς για να αξιολογούν ποιότητα που παρέχεται σε κάθε υπηρεσία όπως για παράδειγμα η προσβασιμότητα , η κινητικότητα , η διατηρησιμότητα και η ακεραιότητα. Ο 3GPP έχει ορίσει βασικές μετρήσεις KPI με οδηγίες στο πως να υπολογιστούν [TS32.450 και TS32.355]. Τα KPI αυτά υπολογίζονται μέχρι τώρα από την μεριά του δικτύου αλλά το MobileInsight.

8.5.1 Διαθέσιμα KPIs.

Το MobileInsight παρέχει KPI analyzers για online monitors αλλά και offline logs. Οι προτυποποιημένοι KPIs που περιέχει είναι οι παρακάτω :

- Accessibility:

RRC connection establishment success rate (KPI.Accessibility.RRC_SR)
Attach success rate (KPI.Accessibility.ATTACH_SR)
Dedicated EPS bearer setup success rate (KPI.Accessibility.DEDICATED_BEARER_SR_QCIx_SR)
Service request success rate (KPI.Accessibility.SR_SR)

- Mobility:

Tracking area update success rate (KPI.Mobility.TAU_SR)
Intra RAT handover success rate (KPI.Mobility.HO_SR)

- Retainability:

Abnormal RRC connection release rate (KPI.Retainability.RRC_AB_REL)

- Integrity:

IP throughput (KPI.Integrity.DL_TPUT)

Εκτός των προτυποποιημένων KPIs παρέχει και πειραματικούς δείκτες απόδοσης κινητικότητας και μεταφοράς δεδομένων στο data plane. Οι δείκτες αυτοί δεν έχουν προτυποποιηθεί αλλά βοηθούν στην εκτίμηση και κατανόηση του δικτύου πρόσβασης.

- Mobility:

Handover disruption time (KPI.Mobility.HANDOVER_LATENCY)
Handover prediction (KPI.Mobility.HANDOVER_PREDICTION)

Handover head of line blocking (KPI.Mobility.HANDOVER_HOL)

- Data plane (L1/L2):

Downlink PDCP packet loss (KPI.Wireless.UL_PDCP_LOSS)

Uplink PDCP packet loss (KPI.Wireless.UL_PDCP_LOSS)

Block Error Ratio (KPI.Wireless.BLER)

8.5.2 Χρήση των KPIs.

Ένα παράδειγμα online monitoring και μιας offline ανάλυσης δίνεται παρακάτω. Για να χρησιμοποιήσουμε τον KPI manager πρέπει να τον δηλώσουμε στον κώδικα, χρησιμοποιείται η εντολή list_kpis για να εμφανίσει όλα τα υποστηριζόμενα KPIs και καλούμε enable_kpi για να ενεργοποιήσουμε το KPI με το όνομα του. Μόλις καλέσουμε τη συνάρτηση θα δηλωθεί και ο KPI manager που θα χρησιμοποιηθεί και θα ξεκινήσει τη διαδικασία monitoring.

```
from mobile_insight.monitor import OfflineReplayer
from mobile_insight.analyzer.kpi import KPIManager

# Initialize a replayer and set input log
src = OfflineReplayer()
path = "./logs/attach_sample.mi2log"
src.set_input_path(path)

# Initialize the KPI manager
kpi_manager = KPIManager()

# Test Accessibility KPIs
kpi_manager.enable_kpi("KPI.Accessibility.RRC_SR")
kpi_manager.enable_kpi("KPI.Accessibility.SR_SR")
kpi_manager.enable_kpi("KPI.Accessibility.ATTACH_SR")
kpi_manager.enable_kpi("KPI.Accessibility.DEDICATED_BEARER_SR_QCI1_SR")

# Test Mobility KPIs
kpi_manager.enable_kpi("KPI.Mobility.HO_SR")
kpi_manager.enable_kpi("KPI.Mobility.TAU_SR")

# Test Retainability KPIs
kpi_manager.enable_kpi("KPI.Retainability.RRC_AB_REL")

# Test Integrity KPIs
kpi_manager.enable_kpi("KPI.Integrity.DL_TPUT")

kpi_manager.set_source(src)

# Start analysis
src.run()
```

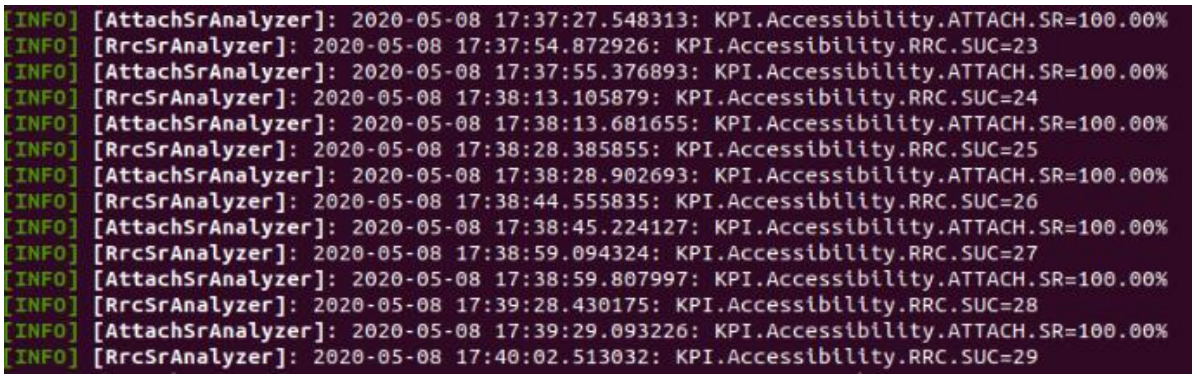
Εικόνα 34 .Κώδικας για χρήση KPIs

Με την εκτέλεση του κώδικα βλέπουμε την χρήση του KPI στο log που έχει αναλυθεί. Υπάρχει δυνατότητα να επιλέξουμε συγκεκριμένη κυψέλη για ανάλυση δηλώνοντας την με τον μοναδικό της αριθμό :

```
kpi_manager.enable_kpi("KPI.Accessibility.RRC_SR", cell='22205186')
```

Επίσης μπορούμε να θέσουμε και την περιοδικότητα

```
kpi_manager.enable_kpi("KPI.Accessibility.RRC_SR", periodicity='1h')
```



Εικόνα 35 .KPI analyzer

9. Εξέταση Δεδομένων

Στο κεφάλαιο αυτό θα παρουσιαστούν τα ευρήματα των αναλύσεων καθώς και ο τρόπος που χρησιμοποιήθηκε το MobileInsight για να μετρηθούν παράγοντες ασφάλειας και να εξάγουμε συμπεράσματα σχετικά με τις διαφοροποιήσεις σε αυτούς ανάμεσα στους τρείς παρόχους κινητής τηλεφωνίας. Θα εστιάσουμε σε συγκεκριμένους παράγοντες που είναι κρίσιμοι για την ασφάλεια των δικτύων.

9.1 Ζητούμενα.

- **Συχνότητα AKA**

Η διαδικασία AKA είναι σημαντικό να εκτελείται με μεγάλη συχνότητα. Η μη συχνή εκτέλεση της εκθέτει τον συνδρομητή σε επιθέσεις κακόβουλων για μεγάλη διάρκεια. Η διαδικασία όπως

αναφέρθηκε σε προηγούμενο κεφάλαιο αυθεντικοποιεί το UE στον MME και το αντίστροφο δημιουργώντας προσωρινά κλειδιά Integrity Key – IK , Cyphering Key – CK από την τιμή RAND.

- **RAND**

Όπως αναφέραμε σε προηγούμενο κεφάλαιο στην τεχνολογία του LTE η τιμή RAND μαζί με άλλες συναρτήσεις έχουν κύριο ρόλο στον υπολογισμό κρίσιμων παραμέτρων που αφορούν τα IK και CK σε συνάρτηση με το κλειδί K. Κάθε φορά που το RAND αλλάζει αλλάζουν και τα IK και CK ως συνέπεια. Με τον τρόπο αυτό η ασφάλεια του δικτύου ενισχύεται και ο χρήστης προστατεύεται περισσότερο. ;Οσο πιο συχνή η αλλαγή των IK και CK τόσο πιο δύσκολο για κάποιον κακόβουλο, που έχει καταφέρει να βρει τα προσωρινά αυτά κλειδιά, να αποκτήσει πρόσβαση στα δεδομένα που μετακινούνται μεταξύ UE και eNB. Εξετάζοντας την τιμή RAND, μπορούμε να συμπεράνουμε εάν αλλάζουν ή όχι τα κλειδιά.

- **T-IMSI (TMSI)**

Κατά την διαδικασία AKA τα κλειδιά που δημιουργούνται χρησιμοποιούνται για να κρυπτογραφήσουν το TMSI**.** Το TMSI χρησιμοποιείται ως προσωρινή ταυτότητα αντί για το IMSI και αυξάνει την ανωνυμία. Ορίζεται από το δίκτυο και πρέπει να αλλάζει συχνά ώστε να αποφευχθούν επιθέσεις τύπου replay. Είναι σημαντικό να εκτελείται η διαδικασία AKA συχνά ώστε να αλλάζουν τα κλειδιά για αποφυγή επιθέσεων. Μετρώντας την συχνότητα των authentication requests μπορούμε να καταλάβουμε πόσο συχνά εκτελείται η διαδικασία. Το IMSI δεν πρέπει να μεταδίδεται και το TMSI δεν πρέπει να παραμένει ίδιο. Με τα IMSI και TMSI μπορεί να γίνει παρακολουθηθεί η τοποθεσία της συσκευής.

- **TAI - TAC**

TAI – Tracking Area Identity είναι ένας κωδικός που δίνεται σε κάθε eNB και καθορίζει την περιοχή που καλύπτει. Με την καταγραφή των αλλαγών του μπορούμε να καταλάβουμε πότε γίνεται handover.

- **Αλγόριθμοι κρυπτογράφησης**

Σύμφωνα με τα πρότυπα που έχει ορίσει ο 3GPP πρέπει να γίνεται χρήση αλγορίθμων στην μετάδοση φωνής, δεδομένων αλλά και στα μηνύματα σηματοδοσίας.

9.2 Μέθοδος.

Η δειγματοληψία έγινε κυρίως χρησιμοποιώντας το κινητό συνδεδεμένο στον υπολογιστή. Αρχικά για λόγους ευκολίας είχε χρησιμοποιηθεί αυτόνομα αλλά η εφαρμογή μετά από κάποια ώρα έκλεινε με σφάλμα και σταματούσε την καταγραφή. Τα logs που έγιναν εξαγωγή έδειχναν να μην παρουσιάζουν κάποιο επαναλαμβανόμενο μοτίβο και έτσι απορρίφθηκαν. Η έκδοση του MobileInsight που χρησιμοποιήθηκε ήταν η Beta 6.0 σε κινητό τηλέφωνο και υπολογιστή.

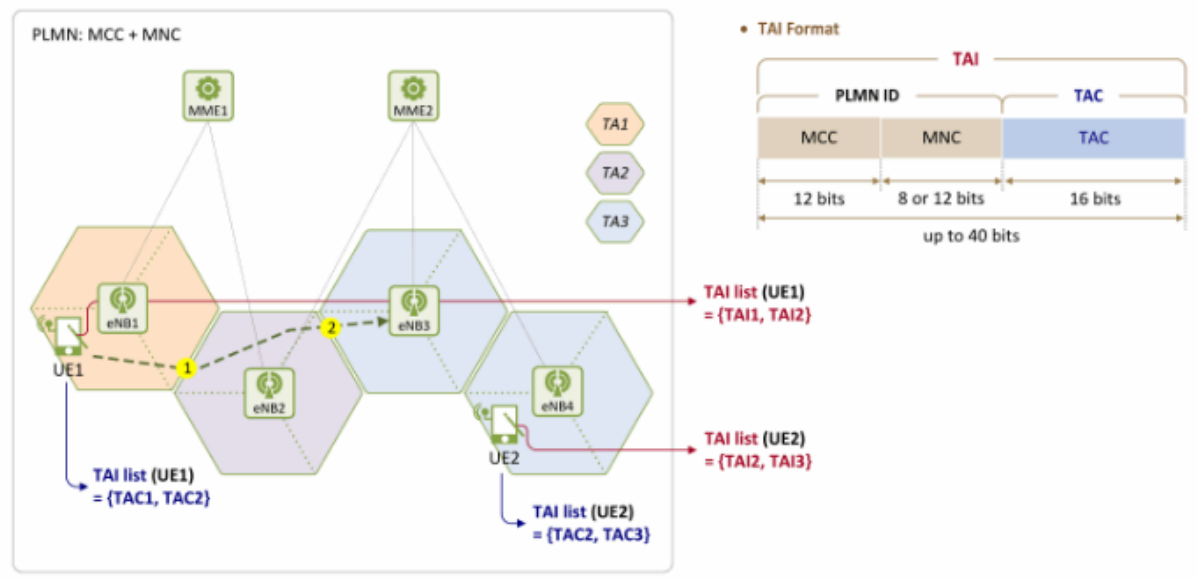
Στόχος είναι να εξεταστούν οι παραπάνω παράμετροι ως προς την συχνότητα αλλαγής και όχι σαν αριθμητική τιμή σε δίκτυα LTE. Η καταγραφή των δεδομένων έχει γίνει με δύο τρόπους. Με τη συσκευή στατική σε ένα σημείο για αρκετές ώρες αλλά και την συσκευή σε διαρκή μετακίνηση. Κατά τη μελέτη με την συσκευή στατική επιλέχθηκε μία τοποθεσία για τις καταγραφές και στα τρία δίκτυα κινητής τηλεφωνίας για να αποκλειστούν παράγοντες που δεν μπορούμε να καθορίσουμε και να έχουμε όσο είναι δυνατόν ίδια δεδομένα. Το ίδιο έγινε και με τις μετρήσεις εν κινήσει, επιλέχθηκε συγκεκριμένη διαδρομή που ακολουθήθηκε όσο είναι δυνατόν με τον ίδιο τρόπο μέχρι να ολοκληρωθούν οι καταγραφές και στους τρείς παρόχους.

Οι δοκιμές – καταγραφές έγιναν πολλαπλές φορές ώστε να κατανοήσω αυξομειώσεις που παρατηρούνταν κατά την ανάλυση στην συχνότητα αλλαγής των παραμέτρων. Μετρώντας πόσο συχνά αλλάζουν τα TMSI, RAND και TAI αλλά και παρατηρώντας τους αλγόριθμους κρυπτογράφησης όπως και τα πρωτόκολλά αυθεντικοποίησης μπορούμε να καταλήξουμε στο συμπέρασμα της αλλαγής των Session Keys.

Κατά την διάρκεια της AKA διαδικασίας όπως είναι γνωστό πως τα UE και eNB ανταλλάσσουν μηνύματα για κοινή αυθεντικοποίηση. Με την ολοκλήρωση της αυθεντικοποίησης τα προσωρινά κλειδιά CK,IK αποθηκεύονται στον HSS. Τα κλειδιά υπολογίζονται συναρτήσει του master key K και της τιμής RAND, άρα όποτε αλλάζει η τιμή RAND τα CK, IK υπολογίζονται ξανά. Τα κλειδιά έπειτα θα χρησιμοποιηθούν για την προστασία της RRC και NAS σηματοδοσίας όπως και στα δεδομένα του user plane. Όλα τα κλειδιά παράγονται από την διαδικασία AKA όπως έχει περιγραφεί σε προηγούμενο κεφάλαιο άρα όσο πιο συχνά γίνεται διαδικασία AKA τόσο πιο συχνά θα ανανεώνονται τα κλειδιά.

Στη συλλογή δεδομένων κατά την μετακίνηση στην ορισμένη διαδρομή στόχος είναι να καταγράψουμε και τα μηνύματα tracking area update - TAU και tracking area identify – TAI που λαμβάνουμε όσο μετακινείται το UE και περνάει από την περιοχή ενός eNB στην περιοχή ενός άλλου. Το UE λαμβάνει μια λίστα με tracking area codes – TAC από τον MME που περιλαμβάνει τις τοποθεσίες που προβλέπει να μετακινηθεί χωρίς να λάβει TAU. Αν μετακινηθεί εκτός της περιοχής που έχει λάβει TAC τότε ο MME θα στείλει TAU. Επίσης κατά την διάρκεια της μετακίνησης θα αλλάξει το KeNB και τα K-RRCint, K-RRCenc , K-UPenc ως αποτέλεσμα.

Με τις μετρήσεις αυτές θα ελέγξουμε αν ακολουθούνται οι οδηγίες του 3GPP από του τρείς παρόχους κινητής τηλεφωνίας και πως υλοποιούν τους μηχανισμούς της ασφάλειας.



Εικόνα 36 .Tracking Area Codes

Χρησιμοποιήθηκε κυρίως ο LTE NAS Analyzer αλλά και ο LTE RRC Analyzer για την online ανάλυση των δεδομένων. Τους δύο analyzers επέλεξα με τον παρακάτω τρόπο γράφοντας το παρακάτω script :

```
#!/usr/bin/python
# Filename: lte-measurement
import os
import sys

# Import MobileInsight modules
from mobile_insight.analyzer import *
from mobile_insight.monitor import OnlineMonitor

if __name__ == "__main__":

    if len(sys.argv) < 3:
        print("Error: please specify physical port name and baudrate.")
        print((__file__, "SERIAL_PORT_NAME BAUNRATE"))
        sys.exit(1)

    # Initialize a DM monitor
    src = OnlineMonitor()
    src.set_serial_port(sys.argv[1])  # the serial port to collect the traces
    src.set_baudrate(int(sys.argv[2]))  # the baudrate of the port
```

```
    # Save the monitoring results as an offline log
    src.save_log_as("./mytest1.mi2log")

    dumper = MsgLogger()
    dumper.set_source(src)
    dumper.set_decoding(MsgLogger.XML)  # decode the message as xml

    nas_analyzer = LteNasAnalyzer()
    nas_analyzer.set_source(src)

    # save the analysis result. All analyzers share the same output file.
    dumper.set_log("./nas-analyzer-test1.txt")
    nas_analyzer.set_log("./nas-analyzer-test1.txt")

    # Start the monitoring
    src.run()
```

Εικόνα 377. Script για χρήση του LTE NAS Analyzer

```
#!/usr/bin/python
# Filename: online-analysis-1.py
import os
import sys

# Import MobileInsight modules
from mobile_insight.analyzer import *
from mobile_insight.monitor import OnlineMonitor

if __name__ == "__main__":

    if len(sys.argv) < 3:
        print("Error: please specify physical port name and baudrate.")
        print((__file__, "SERIAL_PORT_NAME BAUNRATE"))
        sys.exit(1)

    # Initialize a 4G monitor
    src = OnlineMonitor()
    src.set_serial_port(sys.argv[1])  # the serial port to collect the traces
    src.set_baudrate(int(sys.argv[2]))  # the baudrate of the port

    # Save the monitoring results as an offline log
    src.save_log_as("./my-test.mi2log")

    # Enable 4G RRC (radio resource control) monitoring
    src.enable_log("LTE_RRC_OTA_Packet")


    # 4G RRC analyzer
    lte_rrc_analyzer = LteRrcAnalyzer()
    lte_rrc_analyzer.set_source(src)  # bind with the monitor

    # Start the monitoring
    src.run()
```

Εικόνα 388. Script επιλογής LTE RRC Analyzer

Η ανάλυση γινόταν με παρακολούθηση του output στο terminal κάνοντας αναζήτηση των παραμέτρων που μας ενδιαφέρουν και συγκρίνοντας τα timestamps που έχει το κάθε μήνυμα. Μετά την ολοκλήρωση της καταγραφής κάνοντας χρήση των φίλτρων στο GUI του MobileInsight μπορούμε να εξάγουμε πλήρες συμπέρασμα γιατί το mi2log που αποθηκεύεται περιέχει περισσότερη πληροφορία και πιο εύκολα αντιληπτή από το output στο terminal .

Στην python του κάθε analyzer μπορούμε να δούμε επίσης τι πληροφορία θα μας εμφανίσει συνολικά η καταγραφή ώστε να έχουμε μια καθοδήγηση στον τρόπο που μεταφράζονται τα δεδομένα που λαμβάνουμε από την διάγνωση του chipset στο log.

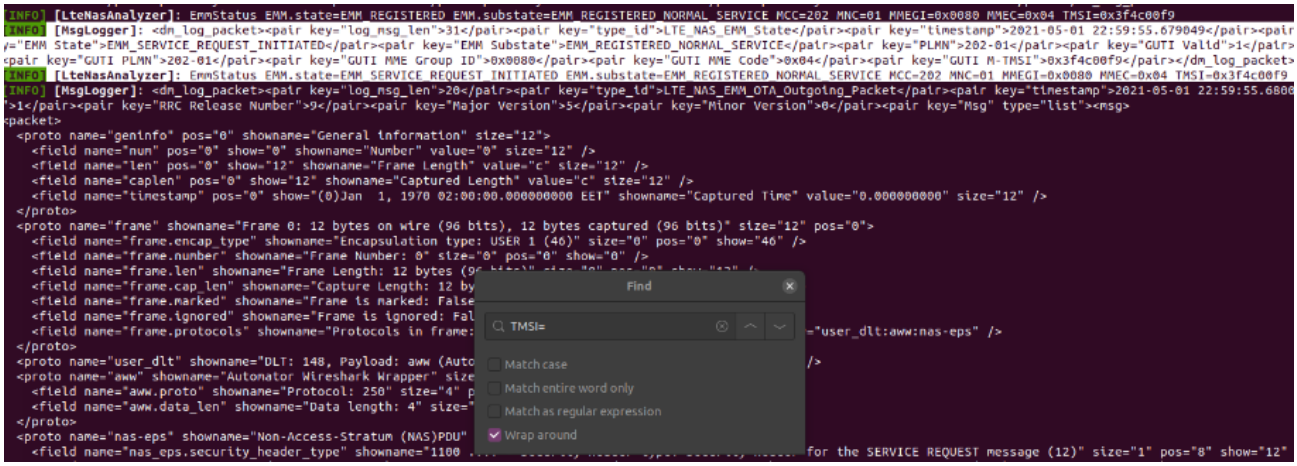
```
return (self.__class__.__name__

    + ' RAND COUNTER='+ xstr(rand_counter)
    + ' TMSI Reallocations='+ xstr(tmsi_re)
    + ' AKA EXECUTIONS='+ xstr(autreq_counter)

    + ' eea0 ='+ xstr(eea0)
    + ' 128-eea1 ='+ xstr(eea1)
    + ' 128-eea2 ='+ xstr(eea2)
    + ' eea3 ='+ xstr(eea3)
    + ' eea4 ='+ xstr(eea4)
    + ' eea5 ='+ xstr(eea5)
    + ' eia0 ='+ xstr(eia0)
    + ' 128-eia1 ='+ xstr(eia1)
    + ' 128-eia2 ='+ xstr(eia2)
    + ' eia3 ='+ xstr(eia3)
    + ' eia4 ='+ xstr(eia4)
    + ' eia5 ='+ xstr(eia5)
    + ' uea1 ='+ xstr(uea1)
    + ' uea2 ='+ xstr(uea2)
    + ' uea3 ='+ xstr(uea3)
    + ' uea4 ='+ xstr(uea4)
    + ' uea5 ='+ xstr(uea5)
    + ' uia1 ='+ xstr(uia1)
    + ' uia2 ='+ xstr(uia2)
    + ' aui3 ='+ xstr(uia3)
    + ' aui4 ='+ xstr(uia4)
    + ' uia5 ='+ xstr(uia5)
    + ' gea1 ='+ xstr(gea1)
    + ' gea2 ='+ xstr(gea2)
    + ' gea3 ='+ xstr(gea3)
    + ' gea4 ='+ xstr(gea4)
    + ' gea5 ='+ xstr(gea5)


   # + ' TMSI=' + xstr(self.guti.m_tmsi)
    )
```

Εικόνα 39. Κομμάτι κώδικα python του LteNasAnalyzer



Εικόνα 40. αναζήτηση TMSI καταγραφών σε terminal κατά την online ανάλυση

```
GI=0x0080 MMEC=0x40 TMSI=0xb01252c3
=202 MNC=05 MMEGI=0x0080 MMEC=0x40 TMSI=0xb01252c3
uaranteed_birate_ulink=unknown guaranteed_birate_dlink=u
nown residual_BER=unknown
uaranteed_birate_ulink=unknown guaranteed_birate_dlink=u
nown residual_BER=unknown
uaranteed_birate_ulink=unknown guaranteed_birate_dlink=u
nown residual_BER=unknown
GI=0x0080 MMEC=0x40 TMSI=0x371258c3

link=unknown max_bitrate_ulink_ext=unknown max_bitrate_d


link=unknown max_bitrate_ulink_ext=unknown max_bitrate_d

GI=0x0080 MMEC=0x40 TMSI=0x371258c3
=202 MNC=05 MMEGI=0x0080 MMEC=0x40 TMSI=0x371258c3
uaranteed_birate_ulink=unknown guaranteed_birate_dlink=u
nown residual_BER=unknown
GI=0x0080 MMEC=0x40 TMSI=0x371258c3

link=unknown max_bitrate_ulink_ext=unknown max_bitrate_d
```

Εικόνα 41. Φιλτράρισμα txt log για εύρεση της αλλαγής TMSI

9.3 Αποτελέσματα.

Στις δοκιμές και τις καταγραφές που γίνανε κατά τη διάρκεια της έρευνας εντοπίστηκαν πληθώρα πληροφοριών που μεταφέρεται μεταξύ UE και δικτυού. Κάποιες από αυτές είναι ζώνη ώρας, επιλογή θερινής ώρας, τοποθεσία eNB, text string που θα εμφανίζει η συσκευή αντί για όνομα δικτύου, APN , μέγιστο bitrate κα.

- **Αλγόριθμοι κρυπτογράφησης**

Σχετικά με τα ζητούμενα που θέλαμε να εξεταστούν βρέθηκε πως και οι τρεις πάροχοι υποστηρίζουν και χρησιμοποιούν τους ίδιους αλγόριθμους κρυπτογράφησης και ακεραιότητας. Οι αλγόριθμοι που εντοπίστηκαν είναι οι εξής:

EEA0, 128-EEA1, 128-EEA2, EEA3,

128-EIA1, 128-EIA2, 128-EIA3,

UEA0, UEA1,

UIA1,

GEA1, GEA2, GEA3

Κάθε φορά που ενα UE θα ξεκινήσει επικοινωνία με κάποιο eNB , θα λάβει λίστα με τους υποστηριζόμενους αλγορίθμους όπως φένεται παρακάτω. Αυτό συμβαίνει για να μπορέσουν να έχουν κοινή σημφωνία αλγορίθμων ανάλογα και με την τεχνολογία του UE

```
<field name="" show="UE security capability - Replayed UE security capabilities" size="6" pos="12" val
  <field name="gsm_a.len" showname="Length: 5" size="1" pos="12" show="5" value="05" />
  <field name="nas_eps.emm.eea0" showname="1... .... = EEA0: Supported" size="1" pos="13" show="1" val
  <field name="nas_eps.emm.128eea1" showname=".1.. .... = 128-EEA1: Supported" size="1" pos="13" show=
  <field name="nas_eps.emm.128eea2" showname="..1. .... = 128-EEA2: Supported" size="1" pos="13" show=
  <field name="nas_eps.emm.eea3" showname="...1 .... = 128-EEA3: Supported" size="1" pos="13" show="1
  <field name="nas_eps.emm.eea4" showname="... 0... = EEA4: Not supported" size="1" pos="13" show="0
  <field name="nas_eps.emm.eea5" showname="... .0.. = EEA5: Not supported" size="1" pos="13" show="0
  <field name="nas_eps.emm.eea6" showname="... ..0. = EEA6: Not supported" size="1" pos="13" show="0
  <field name="nas_eps.emm.eea7" showname="... ...0 = EEA7: Not supported" size="1" pos="13" show="0
  <field name="nas_eps.emm.eia0" showname="0... .... = EIA0: Not supported" size="1" pos="14" show="0
  <field name="nas_eps.emm.128eia1" showname=".1.. .... = 128-EIA1: Supported" size="1" pos="14" show=
  <field name="nas_eps.emm.128eia2" showname="..1. .... = 128-EIA2: Supported" size="1" pos="14" show=
  <field name="nas_eps.emm.eia3" showname="...1 .... = 128-EIA3: Supported" size="1" pos="14" show="1
  <field name="nas_eps.emm.eia4" showname="... 0... = EIA4: Not supported" size="1" pos="14" show="0
  <field name="nas_eps.emm.eia5" showname="... .0.. = EIA5: Not supported" size="1" pos="14" show="0
  <field name="nas_eps.emm.eia6" showname="... ..0. = EIA6: Not supported" size="1" pos="14" show="0
  <field name="nas_eps.emm.eia7" showname="... ...0 = EIA7: Not supported" size="1" pos="14" show="0
  <field name="nas_eps.emm.uea0" showname="1... .... = UEA0: Supported" size="1" pos="15" show="1" val
  <field name="nas_eps.emm.uea1" showname=".1.. .... = UEA1: Supported" size="1" pos="15" show="1" val
  <field name="nas_eps.emm.uea2" showname="..0. .... = UEA2: Not supported" size="1" pos="15" show="0
  <field name="nas_eps.emm.uea3" showname="...0 .... = UEA3: Not supported" size="1" pos="15" show="0
  <field name="nas_eps.emm.uea4" showname="... 0... = UEA4: Not supported" size="1" pos="15" show="0
  <field name="nas_eps.emm.uea5" showname="... .0.. = UEA5: Not supported" size="1" pos="15" show="0
  <field name="nas_eps.emm.uea6" showname="... ..0. = UEA6: Not supported" size="1" pos="15" show="0
  <field name="nas_eps.emm.uea7" showname="... ...0 = UEA7: Not supported" size="1" pos="15" show="0
  <field name="nas_eps.spare_bits" showname="0... .... = Spare bit(s): 0x0" size="1" pos="16" show="0x
  <field name="nas_eps.emm.uia1" showname=".1.. .... = UMTS integrity algorithm UIA1: Supported" size=
  <field name="nas_eps.emm.uia2" showname="..0. .... = UMTS integrity algorithm UIA2: Not supported"
  <field name="nas_eps.emm.uia3" showname="...0 .... = UMTS integrity algorithm UIA3: Not supported"
  <field name="nas_eps.emm.uia4" showname="... 0... = UMTS integrity algorithm UIA4: Not supported"
  <field name="nas_eps.emm.uia5" showname="... .0.. = UMTS integrity algorithm UIA5: Not supported"
  <field name="nas_eps.emm.uia6" showname="... ..0. = UMTS integrity algorithm UIA6: Not supported"
  <field name="nas_eps.emm.uia7" showname="... ...0 = UMTS integrity algorithm UIA7: Not supported"
  <field name="nas_eps.spare_bits" showname="0... .... = Spare bit(s): 0x0" size="1" pos="17" show="0x
  <field name="nas_eps.emm.gea1" showname=".1.. .... = GPRS encryption algorithm GEA1: Supported" size
  <field name="nas_eps.emm.gea2" showname="..1. .... = GPRS encryption algorithm GEA2: Supported" size
  <field name="nas_eps.emm.gea3" showname="...1 .... = GPRS encryption algorithm GEA3: Supported" size
  <field name="nas_eps.emm.gea4" showname="... 0... = GPRS encryption algorithm GEA4: Not supported"
  <field name="nas_eps.emm.gea5" showname="... .0.. = GPRS encryption algorithm GEA5: Not supported"
  <field name="nas_eps.emm.gea6" showname="... ..0. = GPRS encryption algorithm GEA6: Not supported"
  <field name="nas_eps.emm.gea7" showname="... ...0 = GPRS encryption algorithm GEA7: Not supported"
</field>
```

Εικόνα 42 .Αλγόριθμοι UE

Εικόνα 43 .eNB αλγόριθμοι

9.3.1 Με στάσιμο UE

- **Συχνότητα AKA**

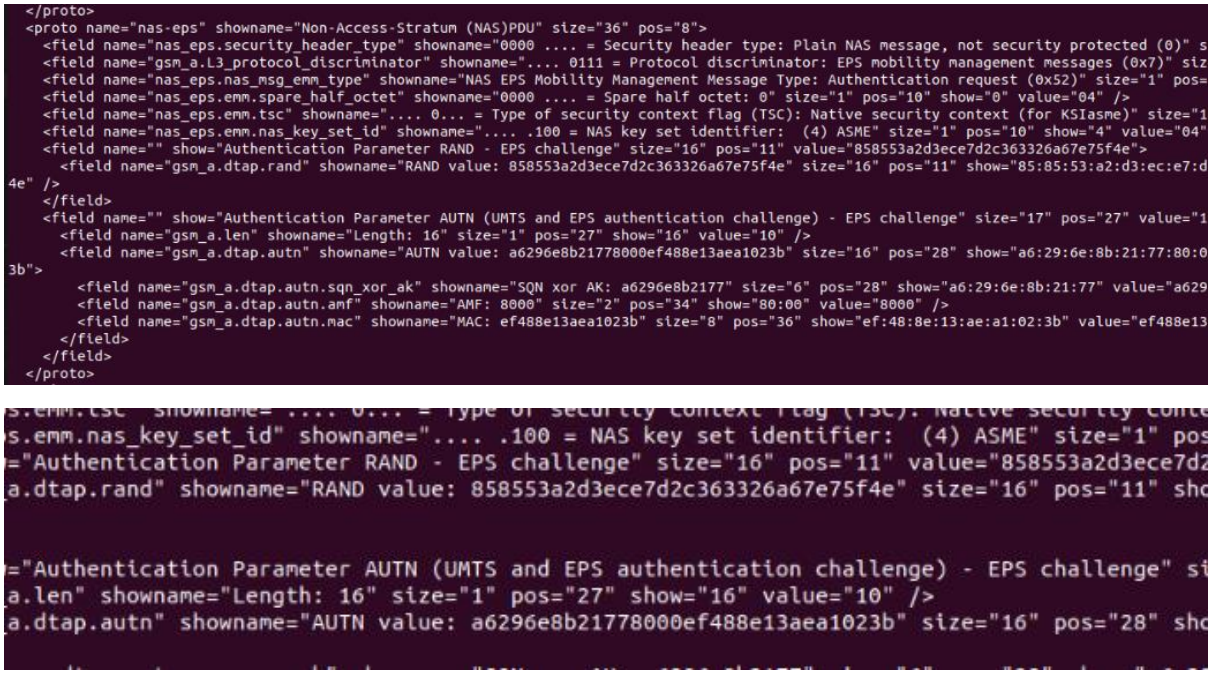
Κατά την ανάλυση παρατηρήθηκε η συχνότητα που γινόταν αποστολή της τιμής RAND. Δεν υπάρχει τρόπος να ελέγξουμε με το MobileInsight τις αλλαγές κλειδιών CK και IK διότι τα κλειδιά αυτά δεν μεταδίδονται αλλά υπολογίζονται τοπικά με βάση την τιμή RAND. Η τιμή RAND όπως είδαμε σε προηγούμενο κεφάλαιο μεταδίδεται ως μέρος ενός challenge που λαμβάνει χώρα στην διαδικασία AKA και έτσι όταν εμφανιστεί γνωρίζουμε πως έγινε η διαδικασία αυτή.

Συχνότητα AKA :

Cosmote : 9 λεπτά

Vodafone : 7 λεπτά

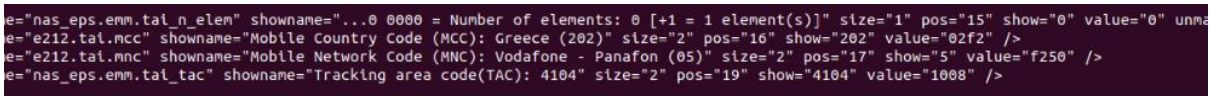
Wind : 6 λεπτά



Εικόνα 44 . Αποστολή RAND - Λήψη AUTN token

- **TAI - TAC**

Κατά την διάρκεια της στατικής μελέτης δεν παρατηρήθηκε κάποιο handover σε κανένα από τους τρείς παρόχους ώστε να αλλάξει το eNB, αυτό μπορεί να φανεί από τα μηνύματα Tracking Area Identity που περιέχουν τον ίδιο Tracking Area Code. Συμπερασματικά αυτό σημαίνει ότι και με τους τρείς παρόχους είμασταν εντός κάλυψης μιας κυψέλης και όχι σε σημείο ενδιάμεσο δυο κυψελών.



Εικόνα 45. Tracking Area Identity - Code

- **T-IMSI (TMSI)**

Κατά την διάρκεια της στατικής μελέτης παρατηρήθηκαν μεγάλες διαφορές μεταξύ των παρόχων όσο αφορά τον χρόνο αλλαγής TMSI. Στις δοκιμές φάνηκε το TMSI να μην αλλάζει ακόμη και μετά από αποσύνδεση και επανασύνδεση στο δίκτυο βάζοντας τη συσκευή σε λειτουργία πτήσεις ή μετά από επανεκκίνηση της. Η συσκευή κατά την διάρκεια της μέτρησης δεν πραγματοποίησε κλήσεις και είχε ανοιχτή την πρόσβαση δεδομένων. Η συχνότητα αλλαγών που καταγράφηκε είναι.

Συχνότητα αλλαγής TMSI:

Cosmote : 6 - 12 ώρες

Vodafone : 2 ώρες

Wind : 3 ώρες

Εικόνα 46. EMM service request - TMSI

9.3.2 Με UE σε κίνηση

- **Συχνότητα AKA**

Κατά την ανάλυση παρατηρήθηκε η συχνότητα που γινόταν αποστολή της τιμής RAND. Δεν υπάρχει τρόπος να ελέγξουμε με το MobileInsight τις αλλαγές κλειδιών CK και IK διότι τα κλειδιά αυτά δεν μεταδίδονται αλλά υπολογίζονται τοπικά με βάση την τιμή RAND. Η τιμή RAND όπως είδαμε σε προηγούμενο κεφάλαιο μεταδίδεται ως μέρος ενός challenge που λαμβάνει χώρα στην διαδικασία AKA και έτσι όταν εμφανιστεί γνωρίζουμε πως έγινε η διαδικασία αυτή.

Συχνότητα AKA :

Cosmote : 10 λεπτά

Vodafone : 8 λεπτά

Wind : 6 λεπτά

Συγκριτικά με τη στατική μελέτη οι Cosmote και Vodafone είχαν αύξηση του χρόνου εκτέλεσης AKA κατά ένα λεπτό ενώ η Wind συνέχισε με τον ίδιο ρυθμό.

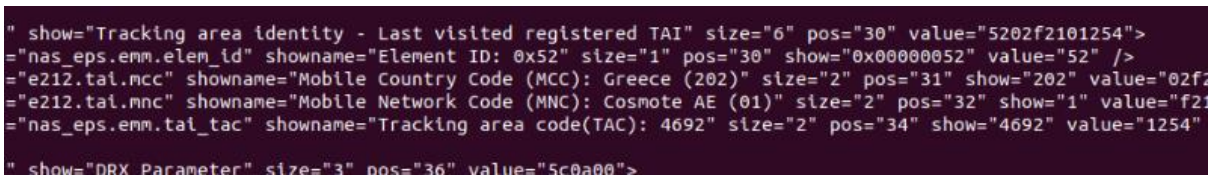
- **TAI - TAC**

Κατά την μετακίνηση παρατηρήθηκαν αλλαγές στα TAI και TAC που αντιπροσωπεύουν πόσα handover ανάμεσα σε eNB έγιναν άρα και πόσες φορές άλλαξε το KeNB.

Cosmote : TAI : 13 φορές

Vodafone : TAI : 7 φορές

Wind : TAI : 6 φορές



Εικόνα 47 .TAC update

- **T-IMSI (TMSI)**

Η διαδρομή που γινόταν οι μετρήσει διαρκούσε 20 λεπτά και μέσα στην διάρκεια αυτή το TMSI έκανε μόνο μια αλλαγή και στους τρείς παρόχους. Πάντα η διαδρομή ξεκίναγε από μια μεγάλη διάρκεια στάσης και παρατηρήθηκε το εξής , κάθε φορά που θα ξεκίναγε η μετακίνηση της συσκευής μέσα σε χρονικό διάστημα ενός λεπτού άλλαζε TMSI ανεξάρτητα από το χρόνο που είχε το αμέσως προηγούμενο.

9.4 Συμπεράσματα

- **Στατική μελέτη**

Όλες οι μετρήσεις πραγματοποιήθηκαν με τη συσκευή σε αδράνεια αλλά με ενεργή σύνδεση δεδομένων. Οι μετρήσεις έγιναν ξανά χρησιμοποιώντας το τηλέφωνο για κλήσεις και browsing , δεν εμφανίστηκε κάποια διαφοροποίηση ή downgrade από LTE σε 3G καθώς και οι τρεις πάροχοι σήμερα υποστηρίζουν VoLTE. Το TMSI παρατηρήθηκε να αλλάζει με πολύ μικρή συχνότητα και στους τρείς παρόχους αλλά ειδικά στο δίκτυο της Cosmote το ίδιο TMSI διατηρήθηκε μέχρι και 12 ώρες, οι Wind και Vodafone αλλάζουν το TMSI αρκετά συχνότερα από την Cosmote αλλά οι χρόνοι διατήρησης του είναι μεγάλοι με 3 ώρες και 2 ώρες αντίστοιχα, κάτι που μπορεί να διευκολύνει τον εντοπισμό του χρήστη από κάποιον κακόβουλο ή κάποιον που θέλει να εκμεταλλευτεί για παράδειγμα την τοποθεσία

της συσκευής έστω και για λόγους ερευνάς αγοράς . Σχετικά με την συχνότητα εκτέλεσης AKA και οι τρείς πάροχοι ήταν αρκετά κοντά σε όλες τις μετρήσεις, οι οποίες κρίνονται ικανοποιητικές με την Wind να κάνει τις αλλαγές κλειδιών συχνότερα.

- **Μελέτη σε κίνηση**

Παρατηρήθηκε ότι κατά την διάρκεια της κίνησης η διαδικασία AKA εκτελούνταν ελάχιστα πιο αργά στους δυο παρόχους αντίθετα με την Wind που διατήρησε τις τιμές της στατικής μελέτης. Το TMSI συνεχίζει να αλλάζει με πολύ αργούς ρυθμούς καθώς μετρήθηκε να αλλάζει μόνο μια φορά σε διάστημα 20 λεπτών κίνησης με συνεχόμενα handover. Αξιοσημείωτο είναι ότι κατά την έναρξη της κίνησης στο πρώτο λεπτό άλλαζε το TMSI χωρίς να έχει σημασία πόση ώρα είχε το αμέσως προηγούμενο που είχε όσο βρισκόταν στατική η συσκευή.

- **Γενικά**

Η εργασία αυτή είχε σκοπό να παρουσιάσει τον τρόπο με τον οποίο μπορεί να γίνει καταγραφή και αποκωδικοποίηση των μηνυμάτων που αποστέλλονται σε ένα κυψελωτό δίκτυο κινητής τηλεφωνίας χρησιμοποιώντας την υλοποίηση του MobileInsight. Χρησιμοποιώντας το MobileInsight έγινε καταγραφή over the air μηνυμάτων και έγινε αξιολόγηση αυτών ως προς την ορθή χρήση κρυπτογραφικών κλειδιών και αλγορίθμων. Δυστυχώς το συμπέρασμα είναι πως η ασφάλεια έχει μεγάλο περιθώριο βελτίωσης από τη μεριά των παρόχων και αντιμετωπίζει ελλείψεις. Αυτό οφείλεται στις όχι και τόσο αυστηρά ορισμένες οδηγίες του 3GPP και στην επιλογή των παρόχων να προσφέρουν πιο ποιητικές υπηρεσίες όσον αφορά την κάλυψη και ταχύτητα σύνδεσης χωρίς όμως να δίνουν την ανάλογη σημασία σε θέματα ασφάλειας.

Το αποτέλεσμα των πολιτικών ασφαλείας που έχουν υιοθετηθεί από τους τρείς παρόχους μπορεί να έχει διάφορα ανεπιθύμητα αποτέλεσμα. Τον εντοπισμό του συνδρομητή, όπως είδαμε ο ίδιος TMSI μπορεί να διατηρηθεί μέχρι και δώδεκα ώρες. Οι χρόνοι αλλαγής κρυπτογραφικών κλειδιών δεν είναι αρκετά συχνοί αν αναλογιστεί κανείς τον όγκο πληροφορίας που μπορούμε να μετακινήσουμε από το κινητό μας , και αυτό παρουσιάζει τον κίνδυνο της υποκλοπής τους και άρα πρόσβαση σε κλήσης και μηνύματα συνδρομητών.

Θεμιτό λοιπόν είναι οι υλοποιήσεις που αφορούν την ασφάλεια να ξανασχεδιαστούν ώστε τα δίκτυα να είναι ασφαλέστερα και όχι μόνο πιο γρήγορα με την πάροδο του χρόνου.

10. Επίλογος – Μελλοντική έρευνα

Το MobileInsight είναι η πρώτη προσπάθεια που δίνει στον απλό ερευνητή την δυνατότητα να κάνει βήματα προς την μελέτη των δικτύων κυψέλης επί του πρακτέου. Τα δίκτυα κινητής τηλεφωνίας πριν την εμφάνιση του MobileInsight αντιμετωπιζόντουσαν ως “black box” και προσεγγιζόταν μόνο θεωρητικά αν κάποιος δεν είχε πρόσβαση σε μηχανισμούς και εξοπλισμό επιπέδου παρόχου. Με το MobileInsight μπορούμε να ξεκινήσουμε την έρευνα και να κατανοήσουμε πρωτόκολλα λειτουργίας, να μελετήσουμε την ασφάλεια των δικτύων και να σχεδιάσουμε την ανάπτυξη και βελτίωση τους παίρνοντας πλήρη εικόνα από την μεριά της συσκευής. Η χρήση του δεν απαιτεί ειδικό εξοπλισμό παρά μόνο ένα κινητό τηλέφωνο που να έχει κάποιες βασικές προϋποθέσεις.

Κάνει εξαγωγή μηνυμάτων σηματοδοσίας για 3G, 4G και σύντομα 5G δίκτυα. Αποκρυπτογραφεί μηνύματα πρωτοκόλλων και παρουσιάζει τη δυναμική λειτουργείας μέσω analyzers. Αποκτώντας πρόσβαση στο low-level domain θα αποκομίσουμε γνώση μέσω APIs και σε περίπτωση βλάβης, υποβιβασμό απόδοσης ή και κενά ασφαλείας μπορούμε να εντοπίσουμε την πηγή του προβλήματος και να προτείνουμε λύσεις .

Σχεδιασμένο ως λογισμικό που απευθύνεται στην κοινότητα αλλά και από την κοινότητα μπορούμε να εξετάσουμε τα δίκτυα κινητής σε μεγάλη κλίμακα με την μέθοδο του crowdsourcing. Φυσικά απαιτείται συνεχής προσπάθεια από τη μεριά της κοινότητας ώστε οι analyzers που διαθέτει να μπορέσουν να καλύψουν τις αυξανόμενες παραμέτρους των δικτύων και να ενημερώνονται σύμφωνα με τα νέα 3GPP releases.

Με την εργαλειοθήκη του MobileInsight λοιπόν όπως αναλύσαμε τις βασικές παραμέτρους ασφάλειας στα τρία ελληνικά δίκτυα LTE, μπορούμε να προχωρήσουμε την έρευνα μελλοντικά σε πιο ειδική κλίμακα και να την επεκτείνουμε στα αναπτυσσόμενα δίκτυα 5G. Τα αποτελέσματα της συλλογής δεδομένων μπορούν πάντα να μοιραστούν με την κοινότητα και η μέχρι τώρα εικόνα επιβεβαιώνει ότι η προσπάθεια δημιουργίας εργαλείων είναι αξιόλογη όταν η προσπάθεια είναι συλλογική.

11. Βιβλιογραφία.

1. MobileInsight (http://www.mobileinsight.net)
2. MobileInsight: Extracting and Analyzing Cellular Network Information on Smartphones (University of California,The Ohio State University,Peking University)
3. Mr. Professor Christos Xenakis' παρουσιάσεις 'Lte security'
4. Review of The LTE and LTE-A Security In Handover Technology (Murtadha Ali Nsaif Shukur, Dr. H. P. Sinha, Dr. Kuldip Pahwa and Er. Ankur Singhal4)
5. Research on 3GPP LTE Security Architecture (Li Zhu1, Hang Qin, Huaqing Mao, Zhiwen Hu)
6. Guide to LTE Security (NIST Special Publication 800-187)
7. 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3GPP System Architecture Evolution (SAE) ,Security architecture (3GPP)
8. AUTHENTICATION AND KEYAGREEMENT IN 3GPP NETWORKS (Krishna Prakash and Balachandra)
9. Analysis of authentication and key establishment in inter-generational mobile telephony (Chunyu Tang, David A. Naumann, and Susanne Wetzel)
10. Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-preserving Schemes (Mohamed Amine Ferrag, Leandros Maglaras, Dimitrios Kosmanos)
11. Control-Plane Protocol Interactions in Cellular Networks (Guan-Hua Tu, Yuanjie Li, Chunyi Peng, Chi-Yu Li, Hongyi Wang, Songwu Lu)
12. 4G LTE Security for Mobile Network Operators (Daksha Bhasker)
13. Long Term Evolution Protocol Overview (Freescale Semiconductors)
14. Learn LTE (https://www.tutorialspoint.com/lte/index.htm)
15. Security Analysis of Handover Key Management in 4G LTE/SAE Networks (Chan-Kyu Han, Hyoung-Kee Choi)
16. LTE, LTE-Advanced and WiMAX: Towards IMT-Advanced Networks (O'Reilly)