2014

Ασφάλεια στα δίκτυα κινητής τηλεφωνίας – Αυθεντικοποίηση κινητής συσκευής

Παπαντωνίου Χρήστος
Πανεπιστήμιο Πειραιά
Τμήμα Ασφάλειας Ψηφιακών Συστημάτων
Επιβλέπων Καθηγητής:
Ξενάκης Χρήστος

Πίνακας Περιεχομένων

Πανεπιστήμιο Πειραιώς

Πανεπιστήμιο Πειραιώς

Λίστα Διαγραμμάτων

Πανεπιστήμιο Πειραιώς

Λίστα Πινάκων

Λίστα Εικόνων

Πανεπιστήμιο Πειραιώς

Πανεπιστήμιο Πειραιώς

Λίστα Ακρωνυμίων

Ακρωνύμιο	*Περιγραφή*
3GPP	3rd Generation Partnership Project
AKA	Authentication and Key Agreement
AM	Amplitude Modulation
AMF	Authentication Management Field
AMPS	Advanced Mobile Phone System
ARIB	Association of Radio Industries and Businesses
AS	Access Stratum
ASME	Access Security Management Entity
AUC	Authentication Center
AUTN	Authentication Token
AV	Authentication Vectors
BSC	Base Station Controller
BSS	Base Station Subsystem
BST	Base Station Transceiver
CDMA	Code Division Multiple Access
CFN	Correction Frame Number
CK	Cipher Key
CT	Cordless Telephone
DECT	Digital Enhanced Cordless Telecommunications
DoS	Denial-of-service attack
DRBs	Data Radio Bearers
EAP-AKA	Extensible Authentication Protocol – AKA
ECC	Ellipse Curve Cipher
EDGE	Enhanced Data Rates for Global Evolution
EIR	Equipment Identity Register
EIR	Equipment Identity Register

Πανεπιστήμιο Πειραιώς

eKSI	evolved Key Set Identifier
eNB	Evolved Node B
EPA	Extended Pedestrian AKA
EPC	Evolved packet core
EPS	Encapsulating Security Payload
EPS	Evolved packet system
ETSI	European Telecommunications Standard Institute
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FDM	Frequency Division Multiple
FM	Frequency Modulation
FN	Foreign Network
GMSC	Gateway Mobile Switching Center
GPRS	General Packet Radio System
GSM	Groupe Spèciale Mobile - Global System for Mobile communications
GTP	GPRS Tunneling Protocol
GUMMEI	Globally Unique MME Identity
GUTI	Globally Unique Temporary Identity
HFN	Hyper Frame Number
HLR	Home Location Register
HN	Home Network
HN	Home Network
HSCSD	High Speed Circuit Switched Data
HSS	Home Subscription Server
I-AKA	Improved AKA
I-CSCF	Interrogating Call Session Control Function
IKE	Internet Key Exchange
IM CN SS	IMS Core Network Subsystem
IMEI	International Mobile Equipment Identity
IMPI	IM Private Identity

Πανεπιστήμιο Πειραιώς

IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IMT	International Mobile Telephony
IS	Interface Modules
ISIM	IM Services Identity Module
ITU	International Telecommunication Union
J-PAKE	Password Authentication Key Exchange by Juggling
KAC	Key Administration Centre
KASME	Key Access Security Management Entity
LAI	Local Area Identity
LTE	Long-Term Evolution
MAC	Medium Access Control / Message Authentication Code
MAP	Mobile Application Protocol, Mobile Application Part
MitM	Man-in-the-Middle
MME	Mobility Management Entity
MMEI	MME Identifier
MS	Mobile Station
MSC	Mobile Switching Center
MTC	Machine to Machine (M2M) communication
NAS	Non- Access Stratum
NCC	NH Chaining Count
NDS	Network Domain Security
NDS/IP	Network Domain IP-based interfaces
NH	Next Hop
NMTS	Nordic Mobile Telecommunication System
OFDMA	Orthogonal Freguency Division Multiple Access
OMC	Operation and Maintenance Center
P-CSCF	Proxy Call Session Control Function
PDCP	Packet Data Control Plane
PDUs	Packet Data Units

Πανεπιστήμιο Πειραιώς

PHY	Physical Layer
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
QPSK	Quadrature-Phase Shift Keying
RAI	Routing Area Identity
RANAP	Radio Access Network Application Protocol
RAND	Random Number
RES	RESult
RLC	Radio Link Control
RLC-SN	RLC sequence number
RNC	Radio Network Subsystems
RRC	Radio Resource Control
SA	Security Association
SAE	System Architecture Evolution
S-CSCF	Serving Call Session Control Function
SE-EPS AKA	Security Enhanced Authentication and Key Agreement
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SIP	Session Internet Protocol
SN	Service Network
SPAKA	Self-Certified Public Key
SQN	Sequence Number
SRB1	Signalling Radio Bearer 1
SRES	Signed Response
TAU	Tracking Area Update
TDMA	Time Division Multiple Access
TMP	Trust Model Platform
TMSI	Temporary Mobile Subscriber Identity
TTP	Trusted Third Party
UE	User Equipment

Πανεπιστήμιο Πειραιώς

UICC	Universal Integrated Circuit Chip
UMTS	Universal Mobile Telecommunication System
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
VN	Visited Network
WiMax	Worldwide Interoperability for Microwave Access
XRES	Expected Response
IK	Integrity Key
NE	Network Elements
XMAC	Expected MAC

Πανεπιστήμιο Πειραιώς

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Πρόλογος

Είναι καθολικά αποδεκτό το γεγονός πως η κινητή τηλεφωνία και η κινητή επικοινωνία γενικότερα, στις μέρες μας αποτελεί αναπόσπαστο κομμάτι της καθημερινής ζωής. Η εξέλιξη της μάλιστα λαμβάνει χώρα με ραγδαίους ρυθμούς, ιδιαίτερα την τελευταία περίοδο όπου το φαινόμενο ακολουθεί πρόοδο που θα μπορούσε δόκιμα να χαρακτηριστεί γεωμετρική. Αποτέλεσμα αυτής της εξέλιξης είναι η αρχική μορφή της κυψελοειδούς κινητής τηλεφωνίας να δώσει τη θέση της στα κινητά ανώτερης γενιάς (3ης και 4ης), τα οποία συνδυάζουν πολυμεσικές εφαρμογές (εικόνα, video) με εφαρμογές διαδικτύου, επιτρέποντας έτσι την εκμετάλλευση στο έπακρο των τεράστιων δυνατοτήτων που προσφέρει το διαδίκτυο και μετατρέποντας το κινητό σε έναν εύχρηστο και «ευέλικτο» φορητό υπολογιστή.

Μια τέτοια όμως διαδικασία δε μπορεί παρά να «κρύβει» ένα σύνολο τεχνολογιών που αποτελεί για το ευρύ κοινό ένα άγνωστο πεδίο για τους περισσότερους όσον αφορά στον τρόπο δόμησης και λειτουργίας τους. Αυτό ακριβώς το σύνολο θα επιχειρηθεί να προσεγγιστεί στην παρούσα εργασία με ιδιαίτερη έμφαση στον τομέα της ασφάλειας στα δίκτυα κινητής τηλεφωνίας. Πρόκειται αναμφίβολα για μια παράμετρο κομβικής σημασίας αφού τα ανταλλασσόμενα δεδομένα (προσωπικά, εταιρικά κτλ.) θα πρέπει να προστατευτούν έτσι ώστε να μη γίνουν «βορά» ανεπιθύμητων κατόχων.

Αντικείμενο λοιπόν της παρούσας εργασίας είναι να αναλυθεί εκείνη η διαδικασία με την οποία επιτυγχάνεται η ασφάλεια των δεδομένων στα δίκτυα κινητής τηλεφωνίας, λαμβάνοντας υπόψη τις ιδιαιτερότητες που την χαρακτηρίζουν εξαιτίας της ποικιλίας των συνδεόμενων συσκευών αλλά και της κινητικότητάς τους. Στόχος της εργασίας είναι μετά το πέρας της να γίνει κατανοητός ο τρόπος λειτουργίας ενός δικτύου κινητής τηλεφωνίας όσον αφορά στο ζήτημα της ασφάλειας των ανταλλασσόμενων δεδομένων και στο πως πραγματοποιήθηκε η σχετική εξέλιξη στο πέρασμα του χρόνου για να οδηγηθούμε στην

Πανεπιστήμιο Πειραιώς

κατάσταση που επικρατεί σήμερα. Ζητούμενο επίσης αποτελεί ο προσδιορισμός τυχόν αδυναμιών, έτσι ώστε να προταθούν κατευθύνσεις βελτίωσης του συγκεκριμένου τομέα.

Η διάρθρωση της παρούσας εργασίας συνοψίζεται στις εξής ενότητες: Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή σχετικά με το σκοπό, το αντικείμενο και τη δομή της, επισημαίνοντας ταυτόχρονα τους λόγους που υποδεικνύουν την ενασχόληση με το συγκεκριμένο ζήτημα.

Στο δεύτερο κεφάλαιο παρουσιάζονται οι διάφορες τεχνολογίες κινητής τηλεφωνίας, καταγράφοντας την ιστορική τους εξέλιξη από «γενιά σε γενιά» (2G to 4G), όσον αφορά στα τεχνικά χαρακτηριστικά και στον τρόπο υλοποίησης της επικοινωνίας ανά περίοδο. Συγκεκριμένα, παρουσιάζονται τα συστήματα GSM, UMTS και LTE, τα σχετικά πρότυπα και πρωτόκολλα που χρησιμοποιούν καθώς και τα πλεονεκτήματα – μειονεκτήματα που τα χαρακτηρίζουν.

Στο τρίτο κεφάλαιο αναλύονται οι υφιστάμενοι μηχανισμοί ασφαλείας για περιβάλλοντα κινητών επικοινωνιών και ποιες υπηρεσίες ασφαλείας είναι διαθέσιμοι εξαιτίας αυτών ακριβώς των μηχανισμών, εμμένοντας στη διαδικασία της πιστοποίησης αυθεντικότητας, αναλύοντάς την διεξοδικά στο τέταρτο κεφάλαιο, όσον αφορά στις καταστάσεις, πιστοποιητικά και πρωτόκολλα που τη χαρακτηρίζουν.

Στο πέμπτο κεφάλαιο, αναλύονται οι μηχανισμοί ασφαλείας που έχουν χρησιμοποιηθεί ή χρησιμοποιούνται ανά σύστημα κινητής τηλεφωνίας, κάνοντας έτσι μια επισκόπηση των εξελίξεων στον τομέα της ασφάλειας από μια γενιά στην επόμενη.

Στο έκτο κεφάλαιο παρουσιάζεται πως τα προαναφερόμενα θεωρητικά σχήματα βρίσκουν πρακτική εφαρμογή σε μια εταιρία κινητής τηλεφωνίας, η οποία καλείται να φροντίσει τόσο για θέματα εξασφάλισης της απρόσκοπτης επικοινωνίας των συνδρομητών της όσο και για ζητήματα ασφαλείας των ανταλλασσόμενων πληροφοριών και των δεδομένων της πελατειακής βάσης.

Στο έβδομο κεφάλαιο αναγνωρίζονται οι προβληματισμοί σχετικά με το συγκεκριμένο ζήτημα και ταυτόχρονα καταγράφονται συγκεκριμένα συμπεράσματα και προτάσεις με βάση όλα όσα έχουν παρατεθεί στις προηγούμενες ενότητες της εργασίας, ανιχνεύοντας παράλληλα μελλοντικές προεκτάσεις του ζητήματος και παραμέτρους που απαιτούν περαιτέρω έρευνα.

Πανεπιστήμιο Πειραιώς

1.2 Η αναγκαιότητα επίλυσης του συγκεκριμένου θέματος

Η εξασφάλιση της απρόσκοπτης λειτουργίας ενός δικτύου κινητής τηλεφωνίας όσον αφορά στο ζήτημα της ασφάλειας της ανταλλασσόμενης πληροφορίας και κατ΄ επέκταση των χρηστών του δικτύου, αποτελεί ζητούμενο τόσο των εταιριών κινητής τηλεφωνίας όσο και των πελατών τους. Η συγκεκριμένη αναγκαιότητα ενισχύεται κατά πολύ από τα μεγέθη των μεταβλητών που συνιστούν την αγορά της κινητής τηλεφωνίας στο σύνολό της (πληροφορία, εταιρίες, πελάτες – χρήστες του δικτύου). Στοιχεία που καταδεικνύουν αυτό το μέγεθος παρατίθενται στην ενότητα που ακολουθεί.

1.2.1 Η ανάπτυξη του κλάδου της κινητής τηλεφωνίας

Ο κλάδος της κινητής τηλεφωνίας χαρακτηρίζεται από ανοδική τάση, «σε πείσμα» των καιρών που θέλουν την ύφεση να υπεισέρχεται σε κάθε τομέα επιχειρηματικής δράσης. Χαρακτηριστικά είναι τα στοιχεία του παρακάτω πίνακα (International Telecommunication Union, Φεβρουάριος 2013).

Πανεπιστήμιο Πειραιώς

Δείκτες Χρήσης Υπηρεσιών Κινητής Τηλεφωνίας σε παγκόσμια κλίμακα (2012)								
	Παγκοσμίως (m)	*Αναπτυγμένα Κράτη*	*Αναπτυσσόμενα Κράτη*	*Αφρική*	*Αραβικά Κράτη*	*Ασία*	*Ευρώπη*	*Αμερική*
Συμβόλαια (εκατ.)	6,835	1,600	5,235	545	396	3,547	790	1,048
Ποσοστό συμβολαίων	96.2%	128.2%	89.4%	63.5%	105.1%	89.7%	126.5%	109.4%
Τηλεφωνικές γραμμές (εκατ.)	1,171m	520m	652m	12m	35m	515m	243m	272m
Ποσοστό τηλ. γραμμών	16.5	41.6%	11.1%	1.4%	9.3%	12.9%	39.0%	28.4%
Ενεργές ευρυζωνικές κινητές συνδέσεις (εκατ.)	2,096m	934m	1,162m	93m	71m	895m	422m	460m
Ποσοστό ενεργών ευρυζωνικών κινητών συνδέσεων	29.5%	74.8%	19.8%	10.9%	18.9%	22.4%	67.5%	48.0%
Αύξηση ενεργών ευρυζωνικών κινητών συνδέσεων (περίοδος 2010-2013 (εκατ.)	40%	N/A	N/A	82%	55%	22%	33%	28%

Πίνακας 1: Δείκτες Χρήσης Υπηρεσιών Κινητής Τηλεφωνίας σε παγκόσμια κλίμακα

Σε εγχώριο επίπεδο, τα τεκταινόμενα στον τομέα της κινητής τηλεφωνίας είναι επίσης ενθαρρυντικά όσον αφορά στην ανάπτυξή του και στο σημαίνοντα ρόλο που διαδραματίζει στα σύγχρονα οικονομικά δρώμενα. Συγκεκριμένα. ο κλάδος κινητής τηλεφωνίας στην Ελλάδα έρχεται τρίτος σε επενδύσεις στην Ευρώπη, παρά την κρίση, με τη συνεισφορά του κλάδου να ανέρχεται στο 3,4% του συνολικού ΑΕΠ της χώρας το 2011 (σύμφωνα με σχετική μελέτη του Οικονομικού Πανεπιστημίου Αθηνών και της ICAP για τη χρονική περίοδο 2011-2012). Η συγκεκριμένη συνεισφορά δε σχετίζεται μόνο με τον τομέα των επενδύσεων αλλά και με τη διατήρηση 59 χιλ. θέσεων εργασίας και με τη δημιουργία ενός συνόλου εσόδων της τάξης του 1,99 δισ. ευρώ. Επιπρόσθετα, η υλοποίηση ενός πλαισίου προτάσεων στην κατεύθυνση ανάπτυξης του κλάδου μπορεί να επιφέρει σε διάστημα μιας τριετίας (2015), άμεση επιπλέον συνεισφορά στο ΑΕΠ κατά €420 εκ. και αύξηση δημοσίων εσόδων κατά €170 εκ. (http://portal.kathimerini.gr).

Πανεπιστήμιο Πειραιώς

ΚΕΦΑΛΑΙΟ 2: Τεχνολογίες Κινητής Τηλεφωνίας

2.1 Ιστορική εξέλιξη της Κινητής Τηλεφωνίας

Η ύπαρξη της κινητής τηλεφωνίας βρίσκει την απαρχή της στην ανακάλυψη της ασύρματης επικοινωνίας, η οποία σύμφωνα με το Patrice Flichy αποδίδεται στον Άγγλο James Clerk Maxwell που ενοποίησε σε μια θεωρία τις υπάρχουσες γνώσεις της εποχής περί διάδοσης φωτός, μαγνητισμού και ηλεκτρισμού και το Γερμανό Heinrich Hertz που επαλήθευσε το συγκεκριμένο θεωρητικό πλαίσιο πειραματικά (Flichy, 2004).

Ως μια πρώτη οργανωμένη δομή ασύρματης επικοινωνίας συναντά κανείς ένα σύστημα ασύρματης επικοινωνίας το οποίο εγκαταστάθηκε από τον Marconi το έτος 1898 στο νησί Wight της Αγγλίας, για λογαριασμό της Βασίλισσας Βικτορίας. Το εγκατεστημένο «κανάλι» επικοινωνίας ένωνε το Παλάτι της βασίλισσας με το βασιλικό γιοτ (κινητή μονάδα).

Οι βρετανικές αστυνομικές υπηρεσίες χρησιμοποίησαν εκτενώς την ασύρματη επικοινωνία πριν από τον Δεύτερο Παγκόσμιο Πόλεμο και συγκεκριμένα στη ζώνη συχνοτήτων 2-3 MHZ. Κατά τη διάρκεια του Δεύτερου Παγκόσμιου Πολέμου, η χρήση των συστημάτων αυτού του είδους επεκτάθηκε στις ένοπλες δυνάμεις και στις υπηρεσίες αμέσου επεμβάσεως. Το χρησιμοποιούμενο μοτίβο διαμόρφωσης ήταν μέχρι τη δεδομένη στιγμή η Διαμόρφωση Εύρους (AM - Amplitude Modulation). Λόγοι όμως βελτίωσης της ποιότητας οδήγησαν στη δοκιμή της Διαμόρφωσης Συχνότητας (FM - Frequency Modulation).

Ο βαθμός επέκτασης των συγκεκριμένων συστημάτων (τα οποία και αποτέλεσαν την 1η γενιά κινητής επικοινωνίας) καταδεικνύεται από το γεγονός ότι το έτος 1945 στο Ηνωμένο Βασίλειο υπήρχαν περίπου 1000 χρήστες των συστημάτων κινητής τηλεφωνίας, με τον αριθμό να ακολουθεί αυξητική δυναμική.

Πανεπιστήμιο Πειραιώς

Σημαντικό σταθμό στην εξέλιξη των κινητών επικοινωνιών αποτέλεσε η κατανομή του ραδιοφάσματος για τους χρήστες των κινητών επικοινωνιών η οποία πραγματοποιήθηκε το 1947 στα πλαίσια των εργασιών του Διεθνούς Συνεδρίου Ραδιοεπικοινωνιών International Radio Communication Conference η οποία έλαβε χώρα στο Atlantic City των ΗΠΑ (Κωτσόπουλος, Καραγιαννίδης, 1977).

Προκειμένου να επιτευχθεί η χρήση κοινών προτύπων μετά το πέρας του Β΄ Παγκοσμίου Πολέμου, οι βόρειες Ευρωπαϊκές χώρες προχώρησαν στην κοινή υιοθέτηση του συστήματος NMTS (Nordic Mobile Telecommunication System). Στα ίδια πλαίσια, το 1982 αναπτύσσεται από το σύνολο της Ευρωπαϊκής Ένωσης το πανευρωπαϊκό δίκτυο GSM (Groupe Spèciale Mobile), με το αντίπαλο δέος από την πλευρά των ΗΠΑ να είναι το αναλογικό AMPS (Advanced Mobile Phone System), ενώ για τη μετατροπή του αναλογικού σήματος σε ψηφιακό χρησιμοποιείται το πρότυπο CT1 (Cordless Telephone) (1984).

Το συγκεκριμένο πρότυπο αντικαθίσταται το 1991 από το αντίστοιχο DECT (Digital European Cordless Telephone, γνωστό σήμερα σαν Digital Enhanced Cordless Telecommunications), σύμφωνα με οδηγίες του Ευρωπαϊκού Ιδρύματος Τηλεπικοινωνιακών Προτύπων ETSI (European Telecommunications Standard Institute). Το νέο πρότυπο λειτουργούσε σε φάσμα συχνοτήτων 1880 – 1900 MHz ενώ η εμβέλειά του έφτανε την ακτίνα των 100 – 150 μέτρων.

Στη συγκεκριμένη χρονική περίοδο προτυποποιείται το δίκτυο GSM το οποίο μετονομάζεται σε Global System for Mobile communications, λειτουργεί στα 900 MHz και χρησιμοποιεί 124 full-duplex κανάλια, εγκαινιάζοντας ουσιαστικά τα δίκτυα δεύτερης γενιάς (2G). Το πρώτο δίκτυο GSM εγκαταστάθηκε το 1991 στη Φινλανδία, ενώ η αποδοχή τους καταδεικνύεται από το γεγονός ότι το Σεπτέμβριο του 2002 υπήρχαν 460 δίκτυα GSM στον αέρα παγκοσμίως, εξυπηρετώντας στο σύνολό τους 747,5 εκατομμύρια συνδρομητές.

Εντούτοις, οι ανάγκες των χρηστών αυξάνονταν συνεχώς με αποτέλεσμα το έδαφος να προετοιμάζεται για τα κινητά δίκτυα της επόμενης γενιάς μέσω σχετικών εργασιών προτυποποίησης. Το νέο σύστημα που δημιουργήθηκε ονομάστηκε UMTS, με βασική πλατφόρμα ανάπτυξης της πλατφόρμας 3ης γενιάς (3G) την τεχνική WCDMA με βάση τις επιλογές των Association of Radio Industries and Businesses (ARIB) και ETSI.

Πανεπιστήμιο Πειραιώς

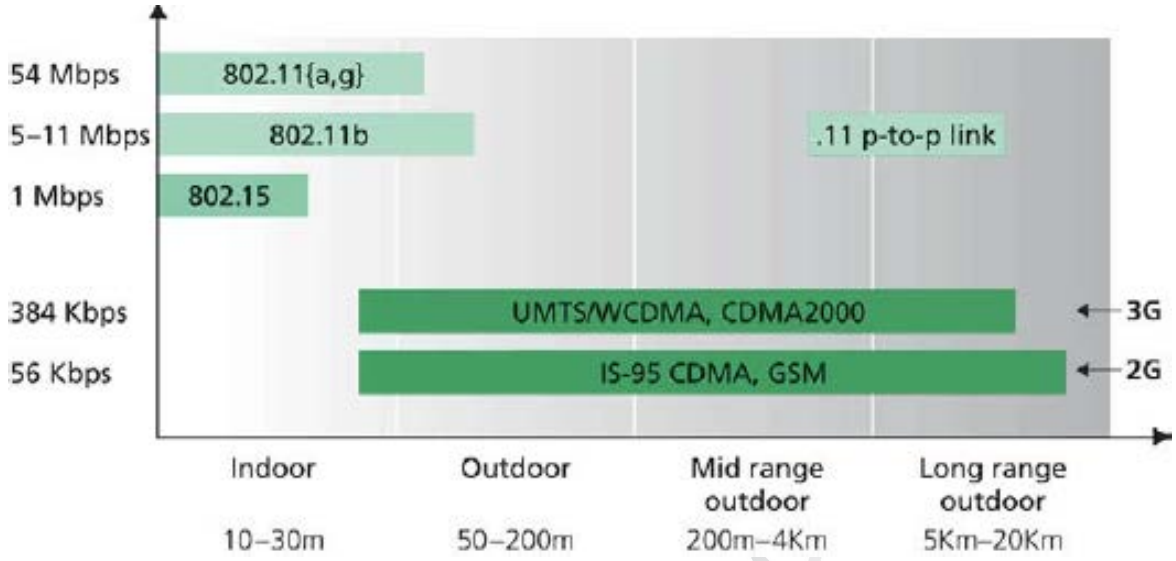
Το πρώτο μεγάλης κλίμακας εμπορικό UMTS δίκτυο ξεκίνησε τη λειτουργία του στην Ιαπωνία το 2001 από την εταιρεία NTT DoCoMo, ενώ ακολούθησε δύο χρόνια αργότερα το πρώτο ευρωπαϊκό UMTS σύστημα στην Αυστρία από την T-Mobile (Πανεπιστήμιο Αιγαίου, 2007).

Η τέταρτη γενιά της ασύρματης δικτύωσης κάνει την εμφάνισή της το 2001 μέσω του WiMAX Forum (Worldwide Interoperability for Microwave Access), που βασίζεται στο πρότυπο 802.16. Το WiMAX αποτελεί ουσιαστικά τη μεγάλη επέκταση του Wi-Fi (μιας τεχνολογίας συμβατής με το πρότυπο IEEE 802.11, εμβέλειας μέχρι 100 μέτρα και καθορισμένο εύρος ζώνης καναλιού στα 20 MHz), προσφέροντας εμβέλεια σημείο-σε-σημείο (point-to-point) 50 χιλιομέτρων με διεκπαιρεωτική ικανότητα 72 Mbit/sec, ενώ σε περιπτώσεις μη οπτικής επαφής η εμβέλεια γίνεται 6 χλμ (Parekh, 2006, Rao and Radhamani, 2008).

Η τεχνολογία LTE (Long-Term Evolution) ήρθε στο προσκήνιο προκειμένου να εξυπηρετήσει την αυξημένη ανάγκη σε πολυμεσικές εφαρμογές, η οποία έχει μεγιστοποιηθεί με την καθολική συμμετοχή σε διάφορα κοινωνικά δίκτυα και την απαίτηση για υψηλή ποιότητα μετάδοσης (για παράδειγμα σε εφαρμογές on line gaming). Για το λόγο αυτό σχεδιαστήκαν τα συστήματα LTE με μεταβλητά πλαίσια (frameworks), εύκολα προσαρμόσιμα στις ανάγκες του χρήστη των ευρυζωνικών ασύρματων τεχνολογιών 4ης γενιάς,

Το παρακάτω διάγραμμα δείχνει τις διάφορες τεχνολογίες ασύρματης επικοινωνίας, με βάση κριτήρια όπως η ταχύτητα μετάδοσης, η εμβέλεια και τα χρησιμοποιούμενα πρωτόκολλα.

Πανεπιστήμιο Πειραιώς



Διάγραμμα 1: Τεχνολογίες ασύρματης επικοινωνίας των τριών πρώτων γενεών σε σχέση με χρησιμοποιούμενα πρωτόκολλα, εμβέλεια και ταχύτητα μετάδοσης (Μάγκος, 2008)

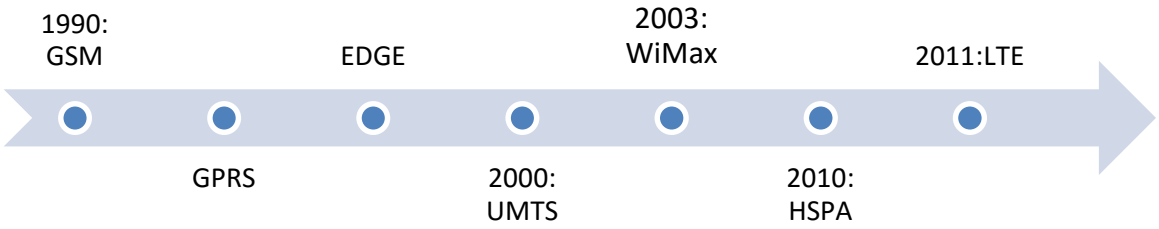
Εξετάζοντας την εξέλιξη της κινητής επικοινωνίας μέσω απλών πρακτικών κριτηρίων, θα μπορούσε να καταρτιστεί ο ακόλουθος πίνακας. Αντίστοιχα, η χρονική τους εξέλιξη σε σχέση με τις τεχνολογίες ανά χρονική περίοδο παρατίθενται στο αμέσως επόμενο διάγραμμα.

Γενιά	*Τεχνολογία*	*Χρονική Περίοδος*	*Ταχύτητα Μεταφοράς*	*Πλεονεκτήματα - Χαρακτηριστικά*
1G	Αναλογικό Σύστημα (Πολυπλεξία Frequency Division Multiple - FDM για κατανομή χωρητικότητας)	Δεκαετία 80	Έως 2,4 kbps	Μετάδοση φωνής
2G	GSM, IS-136 (πολυπλεξία TDMA - Time Division Multiple Access – ανάθεση	Δεκαετία 90	Έως 64 kbps	Κρυπτογράφηση, Προσθήκη sms, e-mails, κατανάλωση λιγότερης ισχύος

	χρηστών σε χρονοθυρίδες), IS-95 (πολυπλεξία CDMA - Code Division Multiple Access)			
"2,5G"	GPRS (General Packet Radio System) HSCSD - High Speed Circuit Switched Data, EDGE – Enhanced Data Rates for Global Evolution (συχνά αναφέρονται και ως γενιά 2.7G)		56-115 kbps, EDGE έως 384 kbps	WAP, MMS, email
3G	UMTS (W-CDMA) – (Ευρώπη) CDMA 2000 – (ΗΠΑ)	Τέλη δεκαετίας 90	125 kbps έως 2 Mbps (κατά ITU 2 Mbps για σταθερές συσκευές, 384 kbps εν κινήσει (βάδισμα), 144 kbps εν κινήσει (αυτοκίνητο))	Παγκόσμια περιαγωγή, mobile TV, video on demand, video conferencing, μεγαλύτερη ασφάλεια
4G	LTE- Long Term Evolution		1 Gbps	IPv6 support. wwww(world wide wireless web)

Πίνακας 2: Εξέλιξη των τεχνολογιών ασύρματης επικοινωνίας με βάση τα χαρακτηριστικά τους (Pashtan, 2006 και Μάγκος, 2008)

Πανεπιστήμιο Πειραιώς



Διάγραμμα 2: Χρονική εξέλιξη των ασύρματων δικτύων

2.2 GSM

Η συγκεκριμένη τεχνολογία βασίζεται στην κυτταρική δομή γεωγραφικής κάλυψης μιας περιοχής. Σε αντίθεση με τα συμβατικά συστήματα που για την ηλεκτρομαγνητική κάλυψη μιας περιοχής χρησιμοποιείτο ένας πομποδέκτης υψηλής ισχύος σε κατάλληλη θέση (σε ψηλό συνήθως σημείο), το κυψελωτό σύστημα περιελάμβανε ένα δίκτυο σταθμών πομποδεκτών με μικρότερη ισχύ εκπομπής και σε συγκεκριμένες θέσεις. Κάθε γεωγραφικός τομέας αποτελεί ένα «κύτταρο», με υπεύθυνο έναν σταθερό πομποδέκτη για την εξυπηρέτηση των κινητών χρηστών εντός του κυττάρου. Για να αποφεύγονται προβλήματα παρεμβολών κάθε κύτταρο χρησιμοποιεί ένα συγκεκριμένο σύνολο συχνοτήτων. Προκειμένου να αντιμετωπιστούν προβλήματα υψηλού φόρτου του δικτύου χρησιμοποιείται η τεχνική της κυτταρικής διάσπασης.

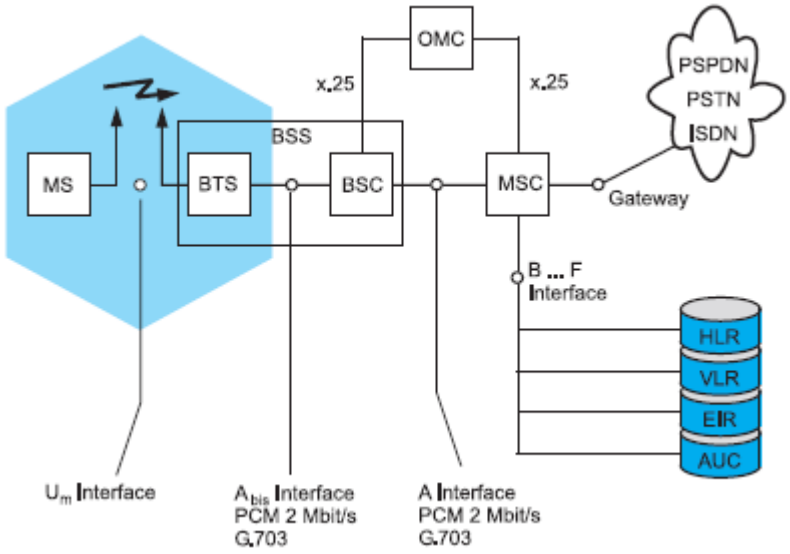
Ένα δίκτυο GSM κινητής τηλεφωνίας περιλαμβάνει τρεις βασικές δομικές μονάδες: τον κινητό σταθμό (Mobile Station MS), το υποσύστημα σταθμού βάσης (Base Station Subsystem BSS) και το υποσύστημα δικτύου. Ο κινητός σταθμός είναι οποιαδήποτε κινητή συσκευή που συνδέεται στο δίκτυο. Το υποσύστημα σταθμού βάσης αποτελείται από τον ελεγκτή σταθμού βάσης (Base Station Controller BSC) και το πομποδέκτη σταθμού βάσης (Base Station Transceiver BTS). Ο πομποδέκτης σταθμού βάσης είναι τοποθετημένος στο κέντρο του κυττάρου και αποτελείται από μια σειρά 1-16 πομποδεκτών, ενώ ο ελεγκτής είναι υπεύθυνος για τον έλεγχο μιας ομάδας BTS, με τον έλεγχο να αφορά στη διαχείριση των συχνοτήτων και στη συντήρηση των κλήσεων, ενώ βασικό στοιχείο για τη λειτουργία του είναι η λήψη μιας αναφοράς με την ισχύ του λαμβανόμενου σήματος κάθε 480 ms από

Πανεπιστήμιο Πειραιώς

τους κινητούς σταθμούς. Το υποσύστημα δικτύου περιλαμβάνει μια σειρά κόμβων και συγκεκριμένα:

- το Κέντρο Μεταγωγής Κινητής Τηλεφωνίας (Mobile Switching Center MSC) το οποίο είναι υπεύθυνο για την εγγραφή (registration), τον έλεγχο της αυθεντικότητας του κινητού σταθμού (authentication), την ενημέρωση της τρέχουσας θέσης του κινητού σταθμού (location update), τις μεταγωγές (handovers), τη δρομολόγηση των κλήσεων κ.τ.λ.,
- τον κόμβο Home Location Register (HLR) ο οποίος είναι υπεύθυνος για την αποθήκευση όλων εκείνων των πληροφοριών που αφορούν τους συνδρομητές του δικτύου,
- τον κόμβο Visitor Location Register (VLR) ο οποίος κόμβος αποθηκεύει επίσης πληροφορίες, αλλά μόνο για την περίπτωση των συνδρομητών που συνδέονται την τρέχουσα στιγμή στον MSC κόμβο,
- το κέντρο αυθεντικότητας (Authentication Center AUC) το οποίο περιέχει αντίγραφα των καρτών SIM των συνδρομητών προκειμένου να υλοποιηθεί η διαδικασία αυθεντικότητας,
- τον κόμβο Equipment Identity Register (EIR) ο οποίος είναι υπεύθυνος για την καταγραφή των συσκευών των συνδρομητών σύμφωνα με τον αποκλειστικό αριθμό IMEI (International Mobile Equipment Identity),
- το Κέντρο λειτουργίας και συντήρησης (Operation and Maintenance Center - OMC), που ουσιαστικά συντονίζει τους επιμέρους κόμβους του δικτύου GSM (Redl 1995, Kahabka 1998).

Πανεπιστήμιο Πειραιώς

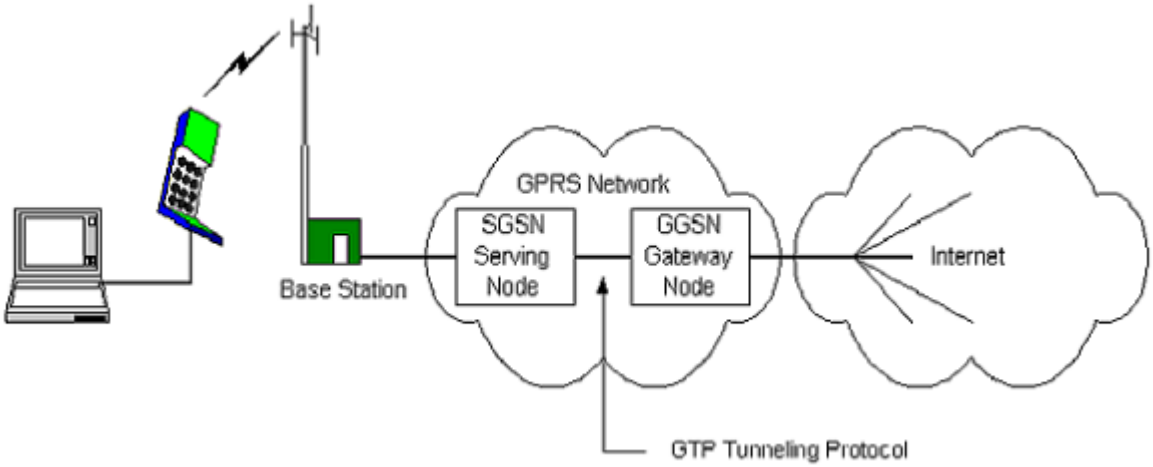


Διάγραμμα 3: Αρχιτεκτονική συστήματος GSM (Kahabka, 1998)

2.2.1 GPRS

Το πρωτόκολλο GPRS αποτελεί ουσιαστικά μια εξέλιξη του GSM όσον αφορά στη χρήση υπηρεσιών Internet στην κινητή τηλεφωνία. Ο βασικός του μηχανισμός έγκειται στο ότι ο χρήστης δεν συνδέεται στο Internet κάθε φορά που χρειάζεται να το χρησιμοποιήσει, αλλά διατηρώντας μόνιμη σύνδεση με αυτό, μπορεί να «κατεβάσει» την πληροφορία που θέλει με τη μορφή πακέτου (Switched Packet System), ενώ το πλεονέκτημα για το χρήστη είναι ότι χρεώνεται μόνο για το πακέτο πληροφορίας που «κατεβαίνει» κάθε φορά και όχι για το χρόνο που είναι συνδεδεμένο το κινητό τερματικό.

Βασικές δομικές μονάδες του πρωτοκόλλου είναι ο κόμβος υποστήριξης και παροχής υπηρεσιών (Serving GPRS Support Node, SGSN), η βασική λειτουργία του οποίου είναι η διαχείριση κινητικότητας (επιτυγχάνεται με τη συνεχή γνώση της τοποθεσίας κάθε συνδρομητή και την υλοποίηση μηχανισμών ασφαλείας για την προστασία της σύνδεσης) και ο διαβιβαστικός κόμβος υποστήριξης (GGSN), ο οποίος παρέχει τη σύνδεση με το εξωτερικό δίκτυο δεδομένων. Η επικοινωνία μεταξύ των κόμβων γίνεται μέσω του πρωτοκόλλου GTP (GPRS tunneling protocol). Οι παραπάνω δομικές μονάδες και η διασύνδεσή τους παρουσιάζονται στο ακόλουθο διάγραμμα.



Διάγραμμα 4: Αρχιτεκτονική δικτύου GPRS (http://misnt.indstate.edu)

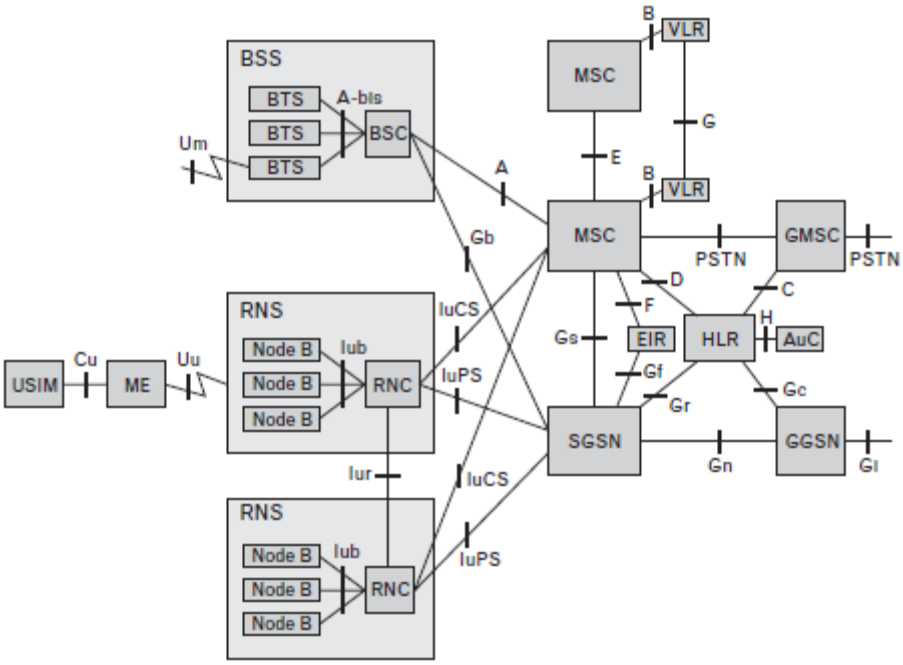
2.3 UMTS

Η μετάβαση από τα δεύτερης στα τρίτης γενιάς συστήματα εντάχθηκε στο σχέδιο IMT 2000 (International Mobile Telephony 2000) που είχε αναπτυχθεί από την ITU προκειμένου να καλυφθεί από πλευράς τυποποίησης και αναγκών η παγκόσμια παροχή υπηρεσιών κινητής τηλεφωνίας. Τα πλεονεκτήματα του συστήματος UMTS (Universal Mobile Telecommunication System – Παγκόσμιο Σύστημα Κινητών Επικοινωνιών) σχετίζονται με τη χρήση νέων τεχνικών ασύρματης πρόσβασης (CDMA), ευφυών δικτύων IN, μικτής αρχιτεκτονικής κυψελών, συγκεκριμένης ποιότητας υπηρεσίας (Quality of Service), παγκόσμιας κινητικότητας (global roaming) κ.τ.λ.

Οι εκδόσεις του συστήματος είναι κατά χρονική σειρά η Έκδοση 99 (Release 99) και η Έκδοση 00 (Release 00), η οποία μετέπειτα διαιρέθηκε στην Έκδοση 4 (Release 4) και στην Έκδοση 5 (Release 5). Η ALL – IP αρχιτεκτονική βασίζεται στην ενσωμάτωση τεχνολογίας IP στο σύνολο των σχετικών υπηρεσιών.

Η αρχιτεκτονική της βασικής έκδοσης του συστήματος (Έκδοση 99) παρουσιάζεται στο ακόλουθο διάγραμμα.

Πανεπιστήμιο Πειρ



Διάγραμμα 5: Αρχιτεκτονική συστήματος UMTS (Έκδοση 9) (Korhonen, 2003)

Αναλυτικότερα, οι μονάδες οι οποίες έχουν ουσιαστικά προστεθεί σε σχέση με τα πρόδρομα δίκτυα και εντοπίζονται στο παραπάνω διάγραμμα έχουν ως εξής:

- Κόμβος B (node B): Παρέχει το φυσικό «δρόμο» μεταξύ του κινητού κόμβου και του δικτύου μέσω κατάλληλων μηχανισμών κωδικοποίησης (τεχνική CDMA).
- Ελεγκτής Radio Network Subsystems (RNC): ελέγχει τη συνολική διακίνηση της πληροφορίας και τη λειτουργία του δικτύου.
- Δομοστοιχεία διεπαφών (interface modules - IS): χρησιμοποιούνται από τους κινητούς κόμβους προκειμένου να λειτουργήσουν εντός του δικτύου.
- Gateway MSC (GMSC): Πρόκειται για ένα Κέντρο Μεταγωγής Κινητής Τηλεφωνίας (Gateway Mobile Switching Center) που λειτουργεί ως πύλη ένωσης με ένα άλλο δίκτυο.

Ασφαλώς, προκειμένου να καλυφθεί το σύνολο των νέων υπηρεσιών, οι προϋπάρχουσες υποδομές αναβαθμίστηκαν σε διάφορα επίπεδα, με την αναβάθμιση στον τομέα της ασφάλειας να αναλύεται διεξοδικά στη συνέχεια.

Πανεπιστήμιο Π

2.4 LTE

Τα LTE δίκτυα καλούνται να δράσουν παράλληλα με άλλες τεχνολογίες αυτού του είδους όπως οι IEEE 802.16e και IEEE 802.16m (αναθεωρήσεις του αρχικού WiMax).

Ειδικότερα στην περίπτωση των πλαισίων IEEE 802.16e, η ροή πακέτων λαμβάνει χώρα προς μια μόνο κατεύθυνση, από τη θύρα πρόσβασης στο δίκτυο προς έναν κινητό σταθμό, με τη διαδρομή να διέπεται από ένα συγκεκριμένο αριθμό χαρακτηριστικών και τη μετάδοση των πακέτων να γίνεται μέσω συγκεκριμένων κανόνων, οι οποίοι καθορίζονται από ταξινομητές που βρίσκονται στην αρχή και στο τέλος της διαδρομής. Επιπρόσθετα, η ύπαρξη ενός σταθμού βάσης, ενισχύει τη μετάδοση. Η απόφαση για την κατανομή των διαφορετικών ροών λαμβάνεται από κατάλληλα προγραμματισμένο ρυθμιστή ο οποίος εντοπίζεται σε υπόστρωμα του MAC, μια διαδικασία που ονομάζεται κατανομή εύρους ζώνης. Οι διαθέσιμοι κάθε φορά πόροι «μοιράζονται» ανάμεσα στο uplink (από τον κινητό σταθμό) και στο downlink (προς τον κινητό σταθμό) έτσι ώστε να επιτυγχάνεται η βέλτιστη κάθε φορά εξυπηρέτηση.

Τα πλαίσια IEEE 802.16m είναι ευκολότερα προσαρμόσιμα στις ανάγκες που προκύπτουν από τις κινητές εφαρμογές διαδικτύου. Ήρθαν να καλύψουν μειονεκτήματα που αφορούν στο διαδικτυακό παιχνίδι σε πραγματικό χρόνο, αλλά και σε εφαρμογές VoIP που απαιτούν αλγορίθμους προσαρμογής και καθυστέρησης, όπως για παράδειγμα το Skype, όπου τη ροή των πακέτων δεδομένων χαρακτηρίζει η απεριοδικότητα τόσο στην κλίμακα του χρόνου όσο και στην κλίμακα της ποσότητας δεδομένων (για παράδειγμα κάποιος μπορεί να σιωπά ή να μιλά για αρκετή ώρα κατά τη διάρκεια μιας κλήσης, χωρίς να μπορεί να προβλεφθεί ένα συγκεκριμένο μοντέλο ομιλίας).

Στην περίπτωση των LTE, τα πλαίσια αναπτύσσονται διαστρωματικά σε φέροντα σήματα ανάμεσα στην πύλη σύνδεσης και στο τερματικό του χρήστη. Κάθε αίτηση εξυπηρετείται από μια ξεχωριστή υπηρεσία ροής δεδομένων, με αυτές που ανήκουν στο ίδιο φέρον να προσφέρουν συμβατικές υπηρεσίες. Σε κάθε φέρον αντιστοιχίζεται μια βαθμωτή τιμή, η οποία αναφέρεται σε έναν ταυτοποιητή, ο οποίος καθορίζει το φέρον της διαστρωμάτωσης.

Πανεπιστήμιο Πειραιώς

Με τη χρήση κατάλληλου φίλτρου κάθε νέα υπηρεσία ροής δεδομένων προστίθεται στα υπάρχοντα φέροντα ανάλογα με τις ανάγκες που εξυπηρετούνται κάθε φορά. Ταυτόχρονα, στην περίπτωση που κάποια ροή υπηρεσιών «πέσει» αδυνατώντας να εξυπηρετήσει τις ανάγκες των χρηστών, το φορτίο που της αναλογούσε επαναδρομολογείται σε νέα υπηρεσία ροής δεδομένων με τη βοήθεια του φίλτρου και του ταυτοποιητή.

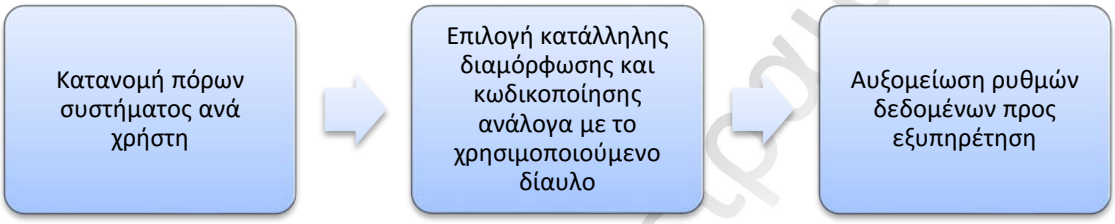
Η σύγκριση των προαναφερόμενων πλαισίων οδηγεί στα εξής συμπεράσματα:

- Τα πρωτόκολλά IEEE χρησιμοποιούν τις ροές υπηρεσιών ως βασική δομική μονάδα για την κατανομή της εξυπηρέτησης των χρηστών ενώ στα LTE το ρόλο αυτό αναλαμβάνουν κατάλληλα ομαδοποιημένα φέροντα.
- Η χρήση των πρωτοκόλλων IEEE μπορεί να εξυπηρετήσει πεπερασμένο όγκο αναγκών (ανάλογα κάθε φορά με τον αρχικό σχεδιασμό) ο οποίος μπορεί να γίνει μεγαλύτερος με χρήση κατάλληλων αλγορίθμων. Στην περίπτωση των LTE, τα περιθώρια είναι πολύ μεγαλύτερα εξαιτίας της ύπαρξης συγκεκριμένων υπηρεσιών ροής δεδομένων που μπορούν να δώσουν λύσεις στην περίπτωση αυξημένου φορτίου.
- Εξαιτίας της δυνατότητας επαναδρομολόγησης μπορούν να καταργηθούν από το διαχειριστή ολόκληρα στρώματα φερόντων ανάλογα κάθε φορά με τη βέλτιστη δυνατή επιλογή εξυπηρέτησης.

Η κεντρική ιδέα των LTE αφορά στη χρήση της πολλαπλής μετάδοσης μέσω πρωτοκόλλου διαδικτύου, αντί για τη χρήση συνδέσεων σημείου προς σημείο, με αποτέλεσμα την εξοικονόμηση χωρητικότητας του δικτύου. Το προς εξυπηρέτηση περιεχόμενο μετασχηματίζεται κατάλληλα έτσι ώστε η μετάδοσή του να είναι δυνατή από ένα τυπικό δίαυλο ραδιοεπαφής σε όλους τους χρήστες που ανήκουν στην ίδια κυψέλη τη δεδομένη χρονική στιγμή. Βασικό μειονέκτημα είναι η απουσία ανάδρασης από τον παραλήπτη σε πραγματικό χρόνο, γεγονός που περιορίζει τους αλγόριθμους προσαρμογής σε μοντέλα πρόβλεψης. Η βασική τεχνική διαμόρφωσης είναι η Orthogonal Freguency Division Multiple Access – OFDMA (χρήση ορθογώνιων κωδικών για διαμόρφωση συχνότητας), τόσο για το DL (downlink) όσο και για το UL (uplink), ενώ βασική διαφορά με την τεχνολογία WiMAX αποτελεί η χρήση υποφέροντος στη συχνότητα των 7,5 kHz για την αντιμετώπιση των καθυστερημένων σημάτων αντίθετα με την WiMAX που

χρησιμοποιεί για το σκοπό αυτό το βασικό φέρον στη συχνότητα των 15 kHz, με αποτέλεσμα τα LTE να παρουσιάζονται ανθεκτικότερα σε φαινόμενα διασποράς τυχόν καθυστερήσεων (Larmo et al. 2009, Ghosh et al. 2010, Alasti et al. 2010, Oyman, and Foerster, 2010).

Για να επιτευχθεί η εξυπηρέτηση των ποικίλων αναγκών των χρηστών ακολουθείται η διαδικασία του ακόλουθου μπλοκ διαγράμματος

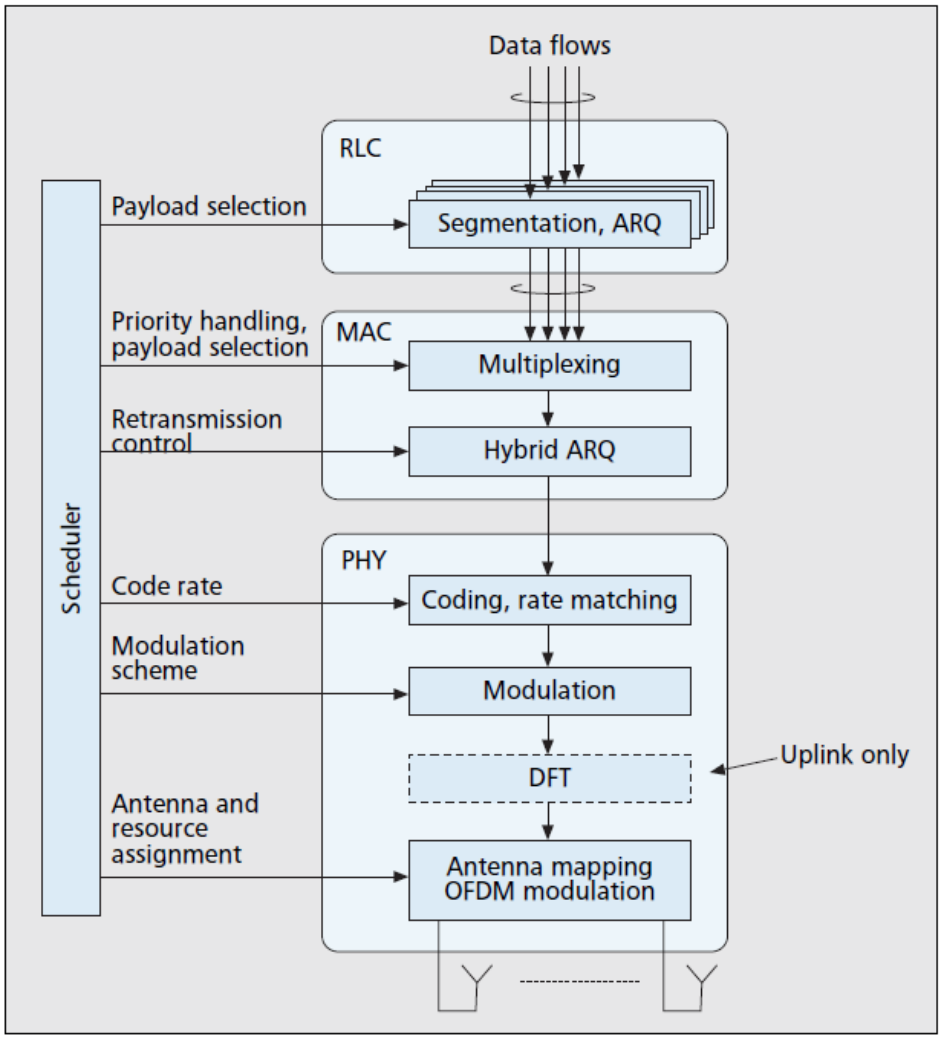


Διάγραμμα 6: Μηχανισμός κάλυψης διαφορετικών αναγκών από τα LTE

Το βασικό πρωτόκολλο δομής LTE παρουσιάζεται στο ακόλουθο διάγραμμα. Οι επιμέρους δομικές μονάδες του συστήματος έχουν ως εξής:

- Radio Link Control (RLC) και Medium Access Control (MAC) επίπεδα: είναι αρμόδια για τον χειρισμό αναμετάδοσης και για την πολυπλεξία των ροών πακέτων δεδομένων.
- Physical Layer (PHY): τα δεδομένα που πρόκειται να διαβιβαστούν είναι κωδικοποιημένα και διαμορφωμένα χρησιμοποιώντας έναν από τους παρακάτω τρόπους: Quadrature-Phase Shift Keying (QPSK), 16-QAM, or 64-QAM, ακολουθούμενο από OFDM διαμόρφωση (Astely et al., 2003).

Πανεπιστήμιο Πειραιώς



Διάγραμμα 7: Δομή LTE πρωτόκολλου (Astely et al., 2003)

Πανεπιστ

ΚΕΦΑΛΑΙΟ 3: Μηχανισμοί Ασφάλειας σε Περιβάλλον Κινητών Επικοινωνιών

3.1 Κρυπτογραφία

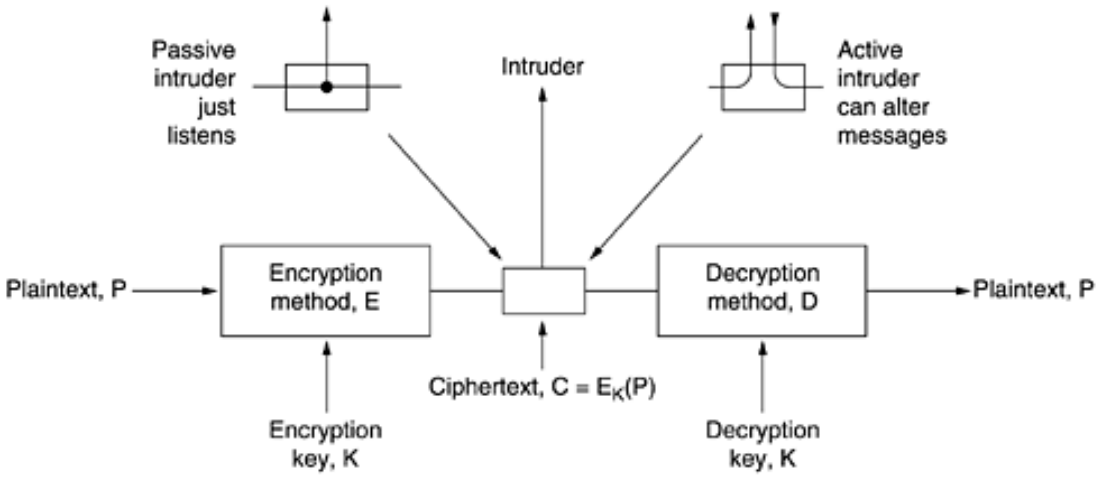
Η κρυπτογραφία αποτελεί ένα μηχανισμό ασφαλείας και βασίζεται στη χρήση κάποιου αλγορίθμου (μαθηματικού ή προγραμματιστικού) που έχει ως βασικό σκοπό να μεταλλάξει και κατ΄ επέκταση να προστατεύσει την ανταλλασσόμενη πληροφορία. Στη σύγχρονη εκδοχή της, επιτρέπει την επικοινωνία μεταξύ δύο μερών εφόσον υφίσταται ένα ζεύγος κλειδιών κρυπτογράφησης (encryption) και αποκρυπτογράφησης (decryption). Η έννοια του κλειδιού έγκειται στο γεγονός ότι η συγκεκριμένη έκφραση – τελεστής είναι απαραίτητη προκειμένου να υπολογιστεί το εκάστοτε κρυπτογράφημα και να γίνει προσβάσιμη η πληροφορία.

Επομένως η τακτική αλλαγή του χρησιμοποιούμενου κλειδιού από το κάθε μέρος της σύνδεσης μπορεί να διατηρήσει την ασφάλεια σε υψηλά επίπεδα. Έτσι, μέσω της κρυπτογραφίας το πρόβλημα διαχείρισης της πληροφορίας που εμπεριέχεται σε μια επικοινωνία και χαρακτηρίζεται από δυσκολία εξαιτίας του όγκου της, ανάγεται σε ένα πρόβλημα διαχείρισης κλειδιών, που είναι σαφώς ευκολότερη και το ίδιο αποδοτική.

Επομένως, είναι λογικό το είδος των κλειδιών να είναι και αυτό που καθορίζει το είδος του κρυπτογραφικού συστήματος. Όταν το κλειδί κρυπτογράφησης και αποκρυπτογράφησης είναι το ίδιο (απαιτείται να είναι μυστικό) πρόκειται για συμμετρικά συστήματα ή συστήματα μυστικού κλειδιού (secret key systems). Όταν τα κλειδιά είναι διαφορετικά η αναφορά γίνεται σε ασύμμετρα συστήματα ή συστήματα δημοσίου κλειδιού (public key systems). Στη δεύτερη περίπτωση, χρησιμοποιείται διαφορετικό κλειδί για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης, με το ένα από αυτά να δημοσιοποιείται (δημόσιο - public) και το άλλο να διατηρείται απόρρητο (ιδιωτικό - private).

Πανεπιστήμιο Πειραιώς

Στο διάγραμμα που ακολουθεί παρατίθεται το μοντέλο ενός συστήματος συμμετρικής κρυπτογραφίας (το κοινό κλειδί είναι το K και εμπεριέχεται στο κρυπτογράφημα C.



Διάγραμμα 8: Μοντέλο συστήματος συμμετρικής κρυπτογραφίας (Tanenbaum, 2003)

Από τους γνωστότερους αλγόριθμους συμμετρικής κρυπτογραφίας είναι οι DES (National Institute of Standards and Technology, 1999), IDEA (Lai, 1992), RC5 (Baldwin, Rivest 1996), CAST-128 (Adams, 1997) και AES (Federal Information Processing Standards Publication, 2001), ενώ στην περίπτωση της κρυπτογραφίας δημοσίου κλειδιού οι πιο γνωστοί αλγόριθμοι είναι οι Rivest Shamir Adleman (RSA), Digital Signature Algorithm (DSA) (RSA Laboratories, 2003), Diffie και Hellman (Diffie, Oorschot and Wiener, 1992), οι Αλγόριθμοι Ελλειπτικών Καμπυλών και ο Αλγόριθμος Κατακερματισμού Secure Hash Algorithm-1 (SHA-1).

3.1.1 Αλγόριθμοι κατακερματισμού

Η διαδικασία του κατακερματισμού έγκειται στη μετατροπή ενός μηνύματος (ανεξαρτήτως του μήκους) σε μια ακολουθία χαρακτήρων. Ο μετασχηματισμός που υλοποιεί τη συγκεκριμένη μετατροπή καλείται συνάρτηση κατακερματισμού (hash

function). Το μήκος της εξόδου της συνάρτησης κατακερματισμού (καλείται και σύνοψη - digest) εξαρτάται από τον αλγόριθμο που χρησιμοποιείται.

Τα βασικά χαρακτηριστικά μιας τέτοιας συνάρτησης είναι ότι είναι μονόδρομη (δεν είναι δηλαδή δυνατός ο υπολογισμός του μηνύματος από την ακολουθία εξόδου) και ότι μπορεί να εξαχθεί συγκεκριμένο μήκος από οποιοδήποτε μήκος εισόδου. Οι πιο γνωστοί αλγόριθμοι κατακερματισμού είναι οι MD5 (σύνοψη 128 bit), SHA-1 (σύνοψη 160 bits), RIPEMD (σύνοψη 160 bits) και οι παραλλαγές τους (οι οποίες σχετίζονται με το μήκος της εξαχθείσας συμβολοσειράς).

3.1.2 Ανταλλαγή κλειδιών

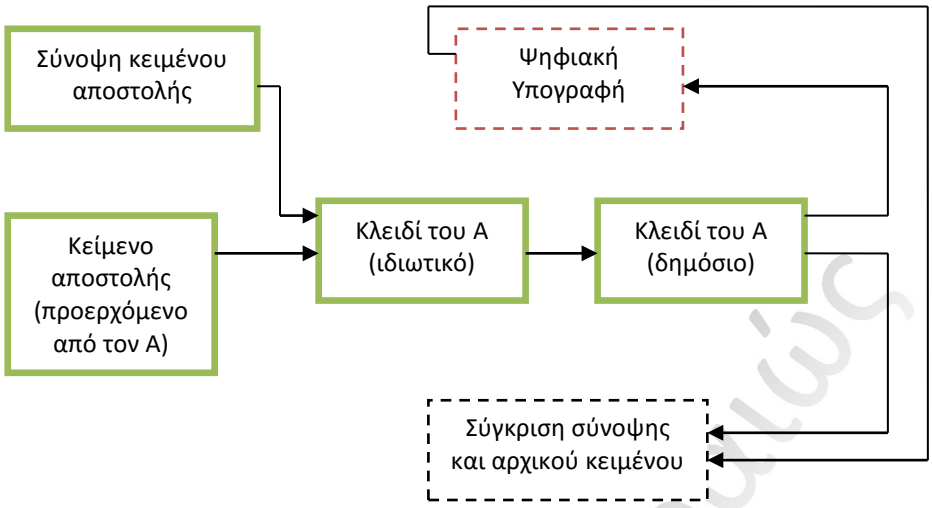
Η διαδικασία της ανταλλαγής κλειδιών έγκειται στο να μοιραστούν δύο δικτυακές οντότητες ένα συμμετρικό κλειδί, το οποίο θα εξασφαλίσει την προστασία της επικοινωνίας τους εφόσον παραμένει άγνωστο στις υπόλοιπες οντότητες του δικτύου. Για την υλοποίηση αυτής της ανταλλαγής μπορεί να πραγματοποιηθεί ο μηχανισμός της μεταφοράς(key transfer) και της συμφωνίας (key agreement). Στην πρώτη περίπτωση το συμμετρικό κλειδί έχει δημιουργηθεί μόνο από τη μία οντότητα ενώ στη δεύτερη περίπτωση η παραγωγή του κλειδιού έχει γίνει και από τα δύο μέρη.

3.2 Ψηφιακή Υπογραφή

Ο ρόλος της ψηφιακής υπογραφής είναι ταυτόσημος με αυτόν της συμβατικής της εκδοχής, αφορά δηλαδή στην πιστοποίηση του προσώπου που υφίσταται πίσω από μια συναλλαγή (υπό την έννοια της γνησιότητας και της ευθύνης για τους συμμετέχοντες στη διαδικασία). Για να γίνει αντιληπτό πως λειτουργεί ο συγκεκριμένος μηχανισμός ασφάλειας ας υποτεθεί το ακόλουθο σενάριο.

.

Πανεπιστήμιο Πειραιώς



Διάγραμμα 9: Ενσωμάτωση ψηφιακής υπογραφής σε αποστολή πληροφορίας

Ο αποστολέας Α για να στείλει το κείμενό του πρώτα το κρυπτογραφεί μέσω του ιδιωτικού του κλειδιού. Προκειμένου να μπορεί το κείμενο να διαβαστεί μόνο από τον Β, γίνεται μια δεύτερη κρυπτογράφηση, με το δημόσιο κλειδί του Β, έτσι ώστε οι αντίστροφοι μηχανισμοί να επιτρέψουν την επικοινωνία μόνο με τον Β. Επειδή η συγκεκριμένη διαδικασία είναι αργή, ο αποστολέας χρησιμοποιεί την ψηφιακή υπογραφή για να αντιστοιχίσει μια σύνοψη του προς αποστολή κειμένου (ουσιαστικά πρόκειται για το αποτέλεσμα της εφαρμογής ενός αλγορίθμου κατακερματισμού) η οποία κρυπτογραφείται ομοίως και αποστέλλεται παράλληλα με το αρχικό κείμενο. Η σύγκριση της σύνοψης και του αρχικού κειμένου πιστοποιεί τον αποστολέα και τη γνησιότητα του κειμένου (Singh, 2008).

Η ισχύς της ψηφιακής υπογραφής έχει κατοχυρωθεί και νομικά, μέσω του ΠΔ.150/2001, σύμφωνα με το οποίο ως ηλεκτρονική υπογραφή εννοούνται δεδομένα σε ηλεκτρονική μορφή, που είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας. Η ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο (ΠΔ.150/2001)

Πανεπιστήμιο Πειραιώς

ΚΕΦΑΛΑΙΟ 4: ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ

Η διαδικασία της αυθεντικοποίησης σε ένα ασύρματο δίκτυο λαμβάνει χώρα όταν μια οντότητα «υποψήφια» προς σύνδεση στο δίκτυο αιτείται άδεια πρόσβασης από τον κεντρικό φορέα ελέγχου του δικτύου (μια άλλη ουσιαστικά οντότητα). Η παροχή της άδειας πρόσβασης και ο έλεγχός της γίνεται μέσω συγκεκριμένου κάθε φορά πρωτοκόλλου. Στη διαδικασία μπορεί να μετάσχει και μια τρίτη οντότητα (Trusted Third Party – TTP), που διαδραματίζει βοηθητικό ρόλο (δεν ανήκει δηλαδή στο δίκτυο).

Μια οντότητα στη συνολική διαδικασία μπορεί να είναι χρήστης (αιτείται την άδεια πρόσβασης), πράκτορα (εκτελεί διάφορες λειτουργίες αυτόνομα) ή κόμβος (πραγματοποιεί ανταλλαγή μηνυμάτων) (Icsa Labs, 2003).

4.1 Καταστάσεις

Στη δυναμική διαδικασία της αυθεντικοποίησης, μια οντότητα διέρχεται από μια συγκεκριμένη διαδοχή καταστάσεων προκειμένου να ολοκληρωθεί. Η διαδικασία άρχεται με την πραγματοποίηση της αίτησης πρόσβασης στο εκάστοτε δίκτυο. Οι διαδοχικές καταστάσεις έχουν ως εξής:

- Αρχικοποίηση (initialization): Στην κατάσταση αυτή η οντότητα εφοδιάζεται με όλα εκείνα τα «εργαλεία» (tools) τα οποία είναι προαπαιτούμενα για τη διαδικασία της αυθεντικοποίησης (authentication functions), όπως πρωτόκολλα ή μηχανισμοί, πιστοποιητικά (συνθηματικά, κλειδιά, ψηφιακά πιστοποιητικά) και ταυτότητες.
- Ανίχνευση (discovery): Όταν η οντότητα βρεθεί στη συγκεκριμένη κατάσταση, εντοπίζει εκείνους τους κόμβους του δικτύου με τους οποίους μοιράζεται τα ίδια «ενδιαφέροντα» (service of interest), έτσι ώστε να ξεκινήσει η ανταλλαγή των πρώτων μηνυμάτων.

Πανεπιστήμιο Πειραιώς

- Επιλογή (selection): Κατά τη διάρκεια παρουσίας μιας οντότητας στη συγκεκριμένη κατάσταση, γίνεται ο συσχετισμός ανάμεσα στα εργαλεία με τα οποία έχει εφοδιαστεί η οντότητα κατά την αρχικοποίησή της και στις κοινές υπηρεσίες – ενδιαφέροντα που έχουν εντοπιστεί παραπάνω.
- Αυθεντικοποίηση (authentication): Αποτελεί μια κατάσταση – «διακόπτη ελέγχου» της ροής διαδοχής καταστάσεων για το σύνολο των οντοτήτων αφού σε ενδεχόμενο έλλειψης των κατάλληλων συνθηματικών, η εκάστοτε οντότητα επιστρέφει στην προηγούμενη κατάσταση, ενώ σε περίπτωση επαρκούς πιστοποίησης, η οντότητα περνά στην επόμενη κατάσταση.
- Αξιολόγηση (evaluation): όταν η οντότητα βρεθεί στη συγκεκριμένη κατάσταση αξιολογείται ως προς τη λειτουργική της συμπεριφορά (έτσι ώστε να εκτιμηθεί τυχόν κακόβουλη παρουσία της στο δίκτυο) (Cisco IOS Software, 2004).

Η διαδοχή των καταστάσεων μιας οντότητας κατά τη συνολική διαδικασία της αυθεντικοποίησης απεικονίζεται στο ακόλουθο διάγραμμα.

Διάγραμμα 10: Διαδοχή των καταστάσεων μιας οντότητας κατά τη συνολική διαδικασία της αυθεντικοποίησης

Πανεπιστήμιο Πειραιώς

4.2 Οντότητες

Όπως αναφέρθηκε παραπάνω μια κατηγοριοποίηση των οντοτήτων αφορά στο ρόλο που διαδραματίζουν εντός του δικτύου κατά τη διαδικασία αυθεντικοποίησης. Ο ρόλος αυτός όμως προσδιορίστηκε σε μεμονωμένη βάση. Αν οι οντότητες θεωρηθούν με βάση την αλληλεπίδραση και τη μεταξύ τους σύγκριση, διακρίνονται σε ομοιογενείς (homogeneous) και ανομοιογενείς (heterogeneous). Στην περίπτωση της ομοιογένειας ο ρόλος των οντοτήτων είναι ίδιος και η απόφαση για την αυθεντικότητα μιας νεοαιτούμενης οντότητας λαμβάνεται από κοινού, σε μια βάση αμοιβαίας εμπιστοσύνης για τις οντότητες – διαχειριστές. Στη δεύτερη περίπτωση, αυτήν της ανομοιογένειας, οι οντότητες έχουν διαφορετικούς ρόλους και απαιτείται η διαχείριση εκ μέρους μιας άλλης, βοηθητικής οντότητας για να ολοκληρωθεί η διαδικασία αυθεντικοποίησης (Yahalom, Klein and Beth 1993).

4.3 Πιστοποιητικά

Όπως προαναφέρθηκε, με πιστοποιητικά εφοδιάζονται οι οντότητες που αιτούνται τη συμμετοχή τους στο ασύρματο δίκτυο κατά το στάδιο της αρχικοποίησης. Το σύνολο των προσαρτούμενων πιστοποιητικών, μπορεί να διαιρεθεί σε δύο κατηγορίες. Στην πρώτη ανήκουν αυτά που βασίζονται στην ταυτότητα (identity) των οντοτήτων και στη δεύτερη ανήκουν αυτά που βασίζονται στα συμφραζόμενα (context).

Όσον αφορά στα πιστοποιητικά ταυτότητας, η λειτουργία τους εξασφαλίζεται με τη συνεργασία μηχανισμών κρυπτογραφίας και αλγορίθμων κατακερματισμού, με διάφορες βέβαια παραλλαγές (χαρακτηριστική είναι η παραλλαγή κοινού μυστικού (shared secret) κατά την οποία οι οντότητες μοιράζονται έναν κοινό φάκελο ο οποίος βρίσκεται στην εκάστοτε συσκευή αυθεντικοποίησης, με τις πληροφορίες να αποδεικνύουν ότι και οι δύο πλευρές γνωρίζουν το κοινό μυστικό).

Στην κατηγορία των βασισμένων στα συμφραζόμενα πιστοποιητικών, η πληροφορία που χρησιμοποιείται έχει να κάνει με τη συμπεριφορά των οντοτήτων και τα χαρακτηριστικά της, τα οποία εφόσον αποτελέσουν ζητούμενα, μπορούν να

αυθεντικοποιήσουν μια συσκευή (για παράδειγμα η συσκευή να έχει συγκεκριμένη αναλογία σήματος προς θόρυβο, ή να βρίσκεται σε μια συγκεκριμένη φυσική τοποθεσία).

4.4 Πρωτόκολλα

Το βασικό πλεονέκτημα των πρωτοκόλλων (με βάση τα οποία γίνεται η ανταλλαγή των μηνυμάτων για την ολοκλήρωση της διαδικασίας αυθεντικοποίησης) είναι η δυναμική τους προσαρμογή στις απαιτήσεις των συσκευών που απαρτίζουν κάθε φορά το ασύρματο δίκτυο. Τέτοιου είδους πρωτόκολλα είναι τα IPSec, VPN, SSL/TLS, SSH, κλπ.

Αυτή η προσαρμογή είναι απαραίτητη για τη μεγιστοποίηση της απόδοσης του δικτύου, η οποία με τη σειρά της εξαρτάται από δύο βασικές παραμέτρους, το φόρτο ροής (load flow) και τον αριθμό των οντοτήτων (number of entities). Ο φόρτος ροής επηρεάζει την απόδοση του δικτύου και επομένως και τις διαδικασίες αυθεντικοποίησης εξαιτίας του ενδεχομένου ύπαρξης καθυστέρησης ή αποτυχίας στην αποστολή πακέτων με αποτέλεσμα να απαιτείται εκ νέου αποστολή τους και να προκαλείται έτσι επιβάρυνση του δικτύου. Ο αριθμός των οντοτήτων επηρεάζει το δίκτυο αφού η ύπαρξη περισσότερων οντοτήτων απαιτεί φυσιολογικά και μεγαλύτερο αριθμό διαδικασιών αυθεντικοποίησης, πόσο μάλλον αν ο αριθμός συνδυαστεί με αυξημένη κινητικότητά τους (Perrig et al. 2002, Rysavy 2003).

Πανεπιστήμιο Πειραιώς

ΚΕΦΑΛΑΙΟ 5: Μηχανισμοί Ασφαλείας ανά τεχνολογία κινητής τηλεφωνίας

Οι βασικές απαιτήσεις ασφαλείας σχετίζονται με την κατά το δυνατό εξασφάλιση των παρακάτω ιδιοτήτων:

- Εμπιστευτικότητα (confidentiality): αφορά στην προστασία δεδομένων που ανταλλάσσονται μέσω μιας ασύρματης σύνδεσης.
- Ανωνυμία (anonymity): αφορά στη διασφάλιση του γεγονότος ότι ο χρήστης θα προστατευτεί τόσο από τον εντοπισμό της θέσης του όσο και από τις κλήσεις που λαμβάνει ή πραγματοποιεί.
- Αυθεντικοποίηση (authentication): αφορά στο να επιβεβαιωθεί κάθε φορά ποιος είναι ο συνδρομητής που συνδέεται στο δίκτυο.
- Έλεγχος πρόσβασης (access control): αφορά ουσιαστικά τον έλεγχο των ταυτοτήτων των συνδρομητών αλλά και των συσκευών που χρησιμοποιούν.

5.1 Μηχανισμοί ασφαλείας κινητής τηλεφωνίας δεύτερης γενιάς

Τα βασικότερα «εργαλεία» που χρησιμοποιεί η τεχνολογία GSM προκειμένου να εξασφαλίσει την ασφάλεια των κινητών επικοινωνιών που εντάσσονται στο πλαίσιό της είναι:

- Η χρήση ταυτοτήτων.
- Η αυθεντικοποίηση.
- Η κρυπτογράφηση των δεδομένων.

Αναλυτικότερα, οι μηχανισμοί αυτοί λειτουργούν ως εξής:

Πανεπιστήμιο Πειραιώς

Χρήση ταυτοτήτων

Σε πρώτο επίπεδο κάθε χρήστης του συστήματος διαθέτει μια μόνιμη (permanent) ταυτότητα, την IMSI (International Mobile Subscriber Identity). Η συγκεκριμένη όμως ταυτότητα θα πρέπει να παραμείνει προστατευμένη, γεγονός που οδήγησε στη χρήση προσωρινών ταυτοτήτων, των TMSI (Temporary Mobile Subscriber Identity). Η προσωρινή ταυτότητα αφενός κρυπτογραφείται σε κάθε της μετάδοση και αφετέρου μεταβάλλεται σε κάθε διαδικασία αυθεντικοποίησης, με αποτέλεσμα ακόμα και αν γίνει γνωστή, να μην απειλείται η ασφάλεια του δικτύου.

Αυθεντικοποίηση και κρυπτογράφηση

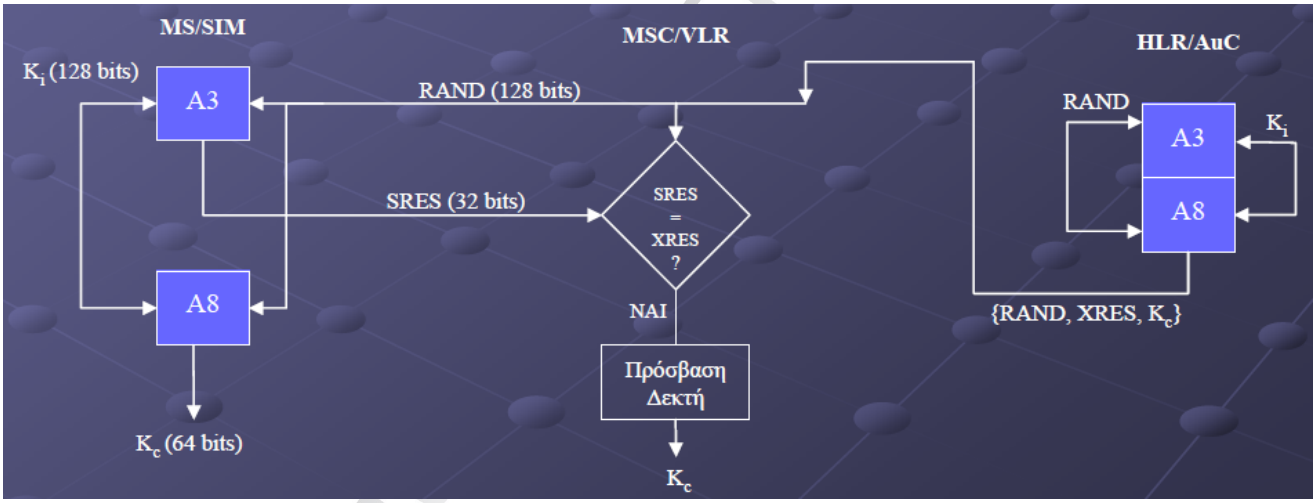
Κάθε συνδρομητής i του δικτύου διαθέτει ένα μοναδικό κλειδί Ki, το οποίο βρίσκεται τόσο στην κάρτα SIM του συνδρομητή όσο και στο κέντρο AuC του δικτύου, το οποίο είναι επιφορτισμένο με το έργο της διαδικασίας αυθεντικοποίησης. Το ζητούμενο είναι ο συνδρομητής να αποδείξει ότι έχει το κλειδί και μάλιστα ότι πρόκειται για το σωστό κλειδί.

Η διαδικασία που ακολουθείται περιλαμβάνει τα εξής στάδια:

- Ο συνδρομητής i αιτείται τη σύνδεσή του στο δίκτυο (attach request).
- Το δίκτυο αναγνωρίζει την περιοχή εντός της οποίας κινείται ο συνδρομητής.
- Μη γνωρίζοντας όμως το κλειδί Ki του συνδρομητή, υπό τη μορφή του τοπικού VLR (Visitor Location Register) ζητά από τον καταχωρητή HLR (Home Location Register) να του αποσταλεί μια διαθέσιμη τριπλέτα αυθεντικοποίησης (authentication triplet) μήκους 224 bits, αποτελούμενη από μια τυχαία (random) ακολουθία 128 bits (RAND), μια αναμενόμενη απάντηση SRES και το κλειδί Kc {RAND, SRES, Kc}.
- Η ακολουθία RAND αποστέλλεται στο συνδρομητή και μεταφέρεται από τη συσκευή στην κάρτα SIM που διαθέτει.

Πανεπιστήμιο Πειραιώς

- Η κάρτα SIM χρησιμοποιεί αυτή την ακολουθία ως είσοδο μιας μονόδρομης συνάρτησης της A3, με την άλλη είσοδο να είναι το κλειδί Ki.
- Η έξοδος της συνάρτησης είναι μια ακολουθία 32-bits, η SRES (Signed Response) που αποστέλλεται πίσω στον VLR.
- Αν αυτή ταυτίζεται με την αναμενόμενη της τριπλέτας, τότε εγκρίνεται η πρόσβαση του συνδρομητή στο δίκτυο.
- Παράλληλα, μέσω μιας άλλης συνάρτησης (A8) με τις ίδιες εισόδους (RAND και Ki) δημιουργείται ένα κλειδί Kc, ίδιο με της τριπλέτας και χρησιμοποιείται για την κρυπτογράφηση των δεδομένων (εμπιστευτικότητα).
- Τέλος, το δίκτυο χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης A5, ο οποίος είναι γνωστός μόνο στους κατασκευαστές του εξοπλισμού του δικτύου.



Διάγραμμα 11: Διαδικασία αυθεντικοποίησης στην κινητή τηλεφωνία 2ης γενιάς (Μαυρίδης, 2008)

5.1.1 Αδύνατα σημεία των μηχανισμών ασφαλείας κινητής τηλεφωνίας δεύτερης γενιάς

- Σε περίπτωση που αποστέλλεται η μόνιμη ταυτότητα του χρήστη (IMSI), αυτό γίνεται χωρίς κρυπτογράφηση. Τέτοιες περιπτώσεις υφίστανται όταν γίνεται αλλαγή περιοχής σε νέο VLR, με το προηγούμενο να μην είναι προσβάσιμο ή να έχει υποστεί απώλεια δεδομένων. Έτσι ένας κακόβουλος χρήστης που μπορεί να προσποιηθεί ένα νόμιμο συνδρομητή (masquerading) μπορεί να αποσπάσει πληροφορίες για τη θέση του χρήστη και με αυτόν τον τρόπο να τον εντοπίσει.
- Ο αλγόριθμος COMP128 που χρησιμοποιείται για την υλοποίηση των συναρτήσεων A3 και A8 είναι μυστικός, χωρίς όμως αυτό να σημαίνει ότι δεν είναι και προσβάσιμος σε κακόβουλες επιθέσεις όπως επιλεγμένου κειμένου (chosen challenge attack) και πλευρικών καναλιών (side channel/partition attacks). Πέφτοντας λοιπόν ο χρήστης «θύμα» μιας τέτοιας επίθεσης, δίνει το δικαίωμα κλωνοποίησης της κάρτας SIM του με ότι αυτό συνεπάγεται (χρέωση νόμιμου συνδρομητή με πραγματοποίηση κλήσεων και υποκλοπή συνομιλιών).
- Το ίδιο συμβαίνει και με τον τελικό αλγόριθμο κρυπτογράφησης (A5) ο οποίος είναι ευάλωτος σε επιθέσεις εξαντλητικής αναζήτησης καθώς και σε κρυπταναλυτικές επιθέσεις, με αποτέλεσμα τα παραγόμενα κάθε φορά κλειδιά να μπορούν να γίνουν γνωστά.
- Η αυθεντικοποίηση λαμβάνει χώρα μόνο από τη μεριά του χρήστη και όχι από αυτή του δικτύου. Αυτό έχει ως αποτέλεσμα, σε μια περίπτωση επίθεσης με τη χρήση ενδιάμεσου σταθμού βάσης (Man-in-the middle attack) και την προώθηση ενός ζεύγους τιμών των παραμέτρων RAND και SRES, να είναι δυνατός ο υπολογισμός του κλειδιού Kc και επομένως η καταγραφή της συνομιλίας.
- Ευάλωτα δεδομένα προσδιορίζονται στη διαδρομή μεταξύ σταθμού βάσης και ελέγχου (BTS – BSC) αφού η μεταξύ τους ανταλλαγή δεδομένων δεν κρυπτογραφείται. Πρόκειται μάλιστα για κρίσιμα δεδομένα αφού

Πανεπιστήμιο Πειραιώς

συμπεριλαμβάνουν, δεδομένα της κλήσης, τις τιμές των παραμέτρων RAND και SRES καθώς και το κλειδί Kc.

- Υπάρχει η πιθανότητα επαναχρησιμοποίησης των τριπλετών ασφαλείας {RAND, SRES, Kc}, σε περιπτώσεις αναποτελεσματικής σύνδεσης μεταξύ VLR και HLR, με αποτέλεσμα να είναι ταυτόχρονα πιθανή και η υποκλοπή τους.

Στις γενικότερες ελλείψεις του συστήματος κινητής τηλεφωνίας δεύτερης γενιάς όσον αφορά στον τομέα της ασφάλειας θα μπορούσαν να αναφερθούν η έλλειψη μηχανισμών ασφάλειας για SMS, η έλλειψη ενημέρωσης χρήστη για παρεχόμενους μηχανισμούς ασφάλειας (lack of visibility), η έλλειψη μηχανισμών ακεραιότητας δεδομένων (data integrity) και η εκ των υστέρων μέριμνα για σύστημα νόμιμων συνακροάσεων (Lawful Interception) (Μαυρίδης, 2008).

5.2 Μηχανισμοί ασφαλείας κινητής τηλεφωνίας τρίτης γενιάς

5.2.1 Διαφορές με μηχανισμούς ασφαλείας δεύτερης γενιάς

Η σχεδίαση των μηχανισμών ασφαλείας της κινητής τηλεφωνίας τρίτης γενιάς βασίζεται ασφαλώς σε εκείνους της δεύτερης γενιάς, με σκοπό τη βελτίωσή τους αλλά και τη διατήρηση της συμβατότητας. Μερικές σημαντικές αλλαγές που έλαβαν χώρα κατά τη μετάβαση στην επόμενη γενιά έχουν ως εξής:

- Η κάρτα SIM αντικαταστάθηκε από την USIM (Universal Subscriber Identity Module, γνωστή και ως Universal Integrated Circuit Chip (UICC)), η οποία μπορεί να θεωρηθεί περισσότερο ως εφαρμογή (application) παρά ως υλικό (hardware).
- Η διαδικασία αυθεντικοποίησης λαμβάνει χώρα αμφίδρομα (ενώ στο GSM η διαδικασία υλοποιούνταν μόνο από τη μεριά του χρήστη).
- Πέρα από το κλειδί Ki, υφίστανται δύο ακόμα κλειδιά των 128 bits τα οποία παράγονται από το αρχικό και βρίσκουν εφαρμογή σε υπηρεσίες εμπιστευτικότητας και ακεραιότητας.

.

Πανεπιστήμιο Πειραιώς

5.2.2 Μηχανισμοί ασφάλειας σε επίπεδο δικτύου πρόσβασης

5.2.2.1 Διαδικασία αυθεντικοποίησης των χρηστών

Η διαδικασία αυθεντικοποίησης υλοποιείται μέσω του μηχανισμού AKA (Authentication and Key Agreement) που παρουσιάζει πολλές ομοιότητες με τον αντίστοιχο της δεύτερης γενιάς. Έτσι, χρησιμοποιεί ομοίως για κάθε συνδρομητή ένα κλειδί Ki μήκους 128 bits, το οποίο βρίσκεται τόσο στην κάρτα UICC του συνδρομητή όσο και στο κέντρο HLR/HSS του HN (Home Network) του δικτύου.

Τα βήματα που περιλαμβάνει η διαδικασία έχει ως εξής:

- Η μόνιμη ή η προσωρινή ταυτότητα του υποψήφιου συνδρομητή αποστέλλεται από το υποδίκτυο RAN στο VLR ή στο SGCN του κεντρικού δικτύου του παρόχου μαζί με μια αίτηση σύνδεσης.
- Το VLR ή το SGCN αφού δεχτεί μια τέτοια αίτηση, στέλνει μια αντίστοιχη αίτηση λήψης δεδομένων αυθεντικοποίησης στο HLR/HSS του οικείου δικτύου
- Το HLR/HSS του οικείου δικτύου, διαθέτοντας το αντίστοιχο κλειδί Ki, εκκινά τη δημιουργία διανυσμάτων αυθεντικοποίησης AV.
- Το διάνυσμα αυθεντικοποίησης αποστέλλεται πίσω στο VLR (ή στο SGCN) μέσω του πρωτοκόλλου MAP (Mobile Application Protocol).
- Σε περίπτωση που το VLR (ή το SGCN) δε λάβει το διάνυσμα, αυτό στέλνεται ξανά, αλλιώς στον επόμενο συνδρομητή αποστέλλεται το επόμενο διάνυσμα.
- Κάθε φορά που το VLR (ή το SGCN) λαμβάνει ένα τέτοιο διάνυσμα επιτυχώς, το αποθηκεύει έτσι ώστε να μη χρειαστεί αυτό να σταλεί ξανά, μειώνοντας έτσι το φόρτο του δικτύου.
- Τη λήψη του διανύσματος αυθεντικοποίησης από το VLR (ή το SGCN) ακολουθεί η αποστολή αίτησης αυθεντικοποίησης στο χρήστη - συνδρομητή.

Πανεπιστήμιο Πειραιώς

- Η αίτηση αυθεντικοποίησης συμπεριλαμβάνει έναν τυχαίο αριθμό RAND (Random Number) και μια σκυτάλη αυθεντικοποίησης AUTN (Authentication Token)
- Οι δύο αυτές παράμετροι αποθηκεύονται στη USIM του χρήστη και χρησιμοποιούνται σε μια υπολογιστική διαδικασία η οποία περιλαμβάνει και το κλειδί Ki προκειμένου να επιβεβαιωθεί ότι η σκυτάλη αυθεντικοποίησης προέρχεται από το VLR (ή το SGCN) και ότι δεν έχει αποσταλεί ξανά.
- Το αποτέλεσμα αυτής της υπολογιστικής διαδικασίας είναι η RES (RESult) και εφόσον είναι επιβεβαιωτική, αποστέλλεται πίσω στο VLR/SGSN.
- Το VLR/SGSN συγκρίνει την πραγματική (ληφθείσα) RES με την αναμενόμενη XRES (Expected Response), η οποία περιέχεται στο αρχικό διάνυσμα αυθεντικοποίησης.
- Τα κλειδιά που χρησιμοποιούνται για υπηρεσίες εμπιστευτικότητας και ακεραιότητας των δεδομένων (CK - Cipher Key και IK - Integrity Key αντίστοιχα), μεταφέρονται μέσω του διανύσματος αυθεντικοποίησης (τα εμπεριέχει) από το VLR/SGSN στο RNC.

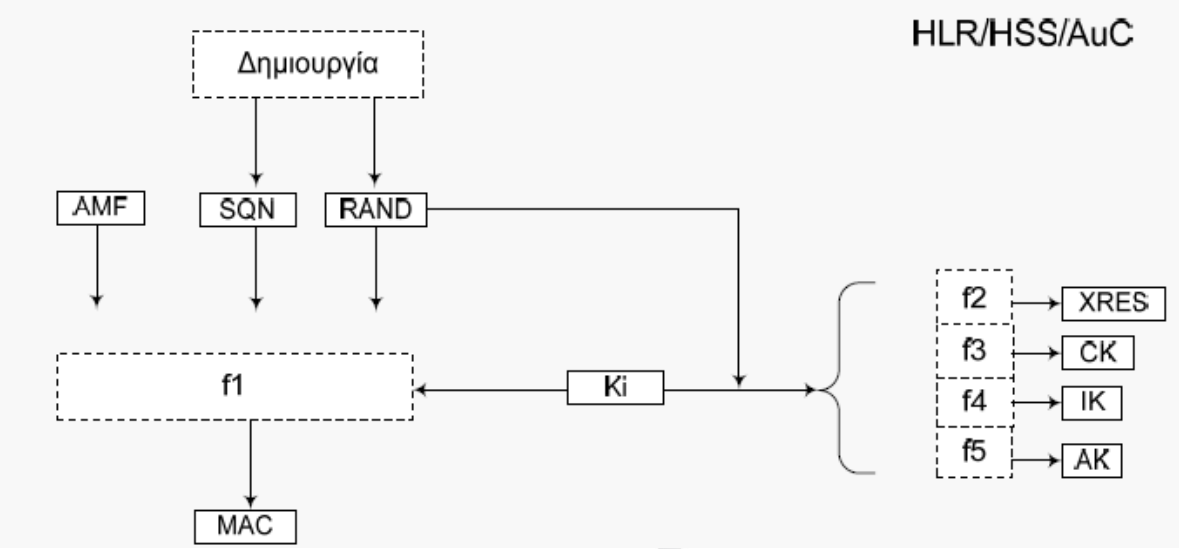
5.2.2.1.1 Παραγωγή των διανυσμάτων αυθεντικοποίησης

Αναλυτικότερα η διαδικασία παραγωγής των διανυσμάτων αυθεντικοποίησης έχει ως εξής:

- Επιλέγεται ο κατάλληλος αριθμός ακολουθίας (SQN - Sequence Number), με την παραγωγή αυτών των αριθμών να γίνεται είτε κατά αύξουσα σειρά είτε να βασίζεται σε μια κάποιου είδους καθολική αρίθμηση, είτε με συνδυασμό τους.
- Η χρησιμότητα των ακολουθιών αυτών είναι ο έλεγχος του «επίκαιρου» του διανύσματος αυθεντικοποίησης.
- Μέσω μιας γεννήτριας ψευδοτυχαίων αριθμών δημιουργείται ένας τυχαίος αριθμός RAND μήκους 128 bits.
- Μέσω πέντε μονόδρομων συναρτήσεων (f1 έως f5) παράγονται πέντε τιμές που συνιστούν το συνολικό διάνυσμα (με την f5 να προηγείται γιατί χρησιμεύει στην απόκρυψη του SQN). Η αντιστοιχία συνάρτησης και

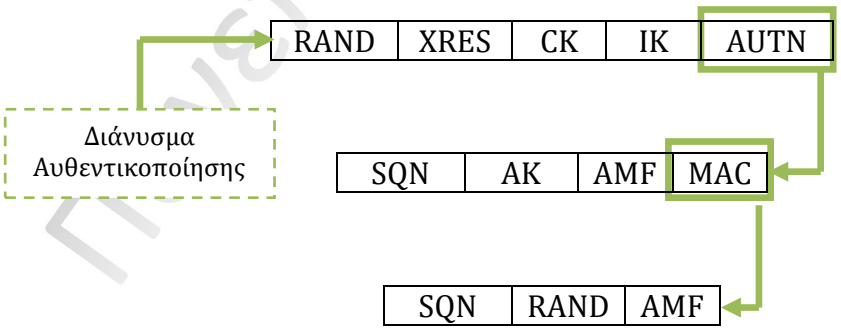
Πανεπιστήμιο Πειραιώς

παραγόμενης τιμής φαίνεται στο ακόλουθο διάγραμμα (όπου το AMF - Authentication Management Field) αποτελεί ένα διαχειριστικό πεδίο.



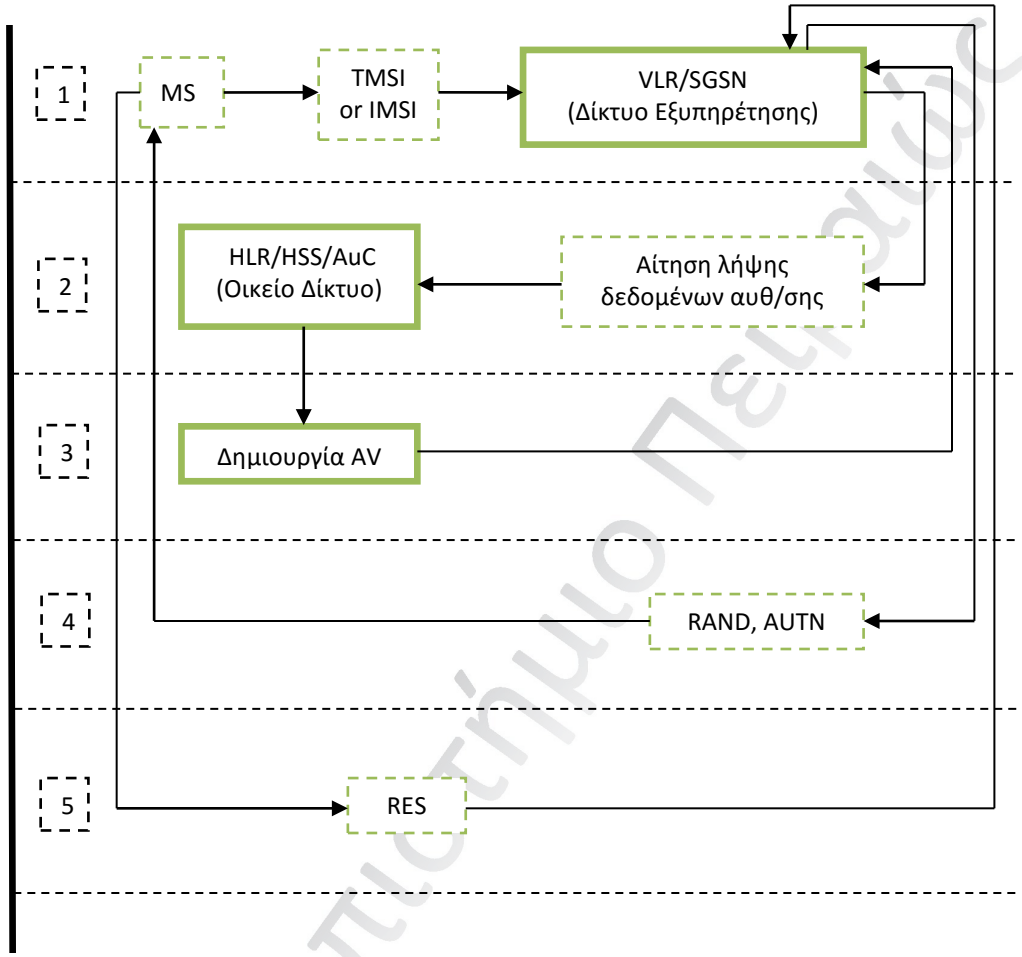
Διάγραμμα 12: Αντιστοιχία μονόδρομων συναρτήσεων και παραγόμενης τιμής για τη δημιουργία του διανύσματος αυθεντικοποίησης (http://www.icsd.aegean.gr)

Τελικά το παραγόμενο διάνυσμα αυθεντικοποίησης περιλαμβάνει τις εξής τιμές (RAND. XRES. CK, IK, AUTN). Οι επιμέρους δομές των πεδίων που απαρτίζουν κατά σειρά το διάνυσμα αυθεντικοποίησης παρουσιάζονται στην παρακάτω εικόνα.



Εικόνα 1: Ανάλυση επιμέρους πεδίων του διανύσματος αυθεντικοποίησης

Στο σημείο αυτό θα πρέπει να αναφερθεί πως ο πάροχος του δικτύου έχει καθολική επιρροή στη διαδικασία, αφού αφενός μπορεί να επιλέξει τις μονόδρομες συναρτήσεις και αφετέρου διατηρεί τον έλεγχο των μονάδων HLR/HSS/AuC και USIM.



Διάγραμμα 13: Αποστολή διανυσμάτων αυθεντικοποίησης

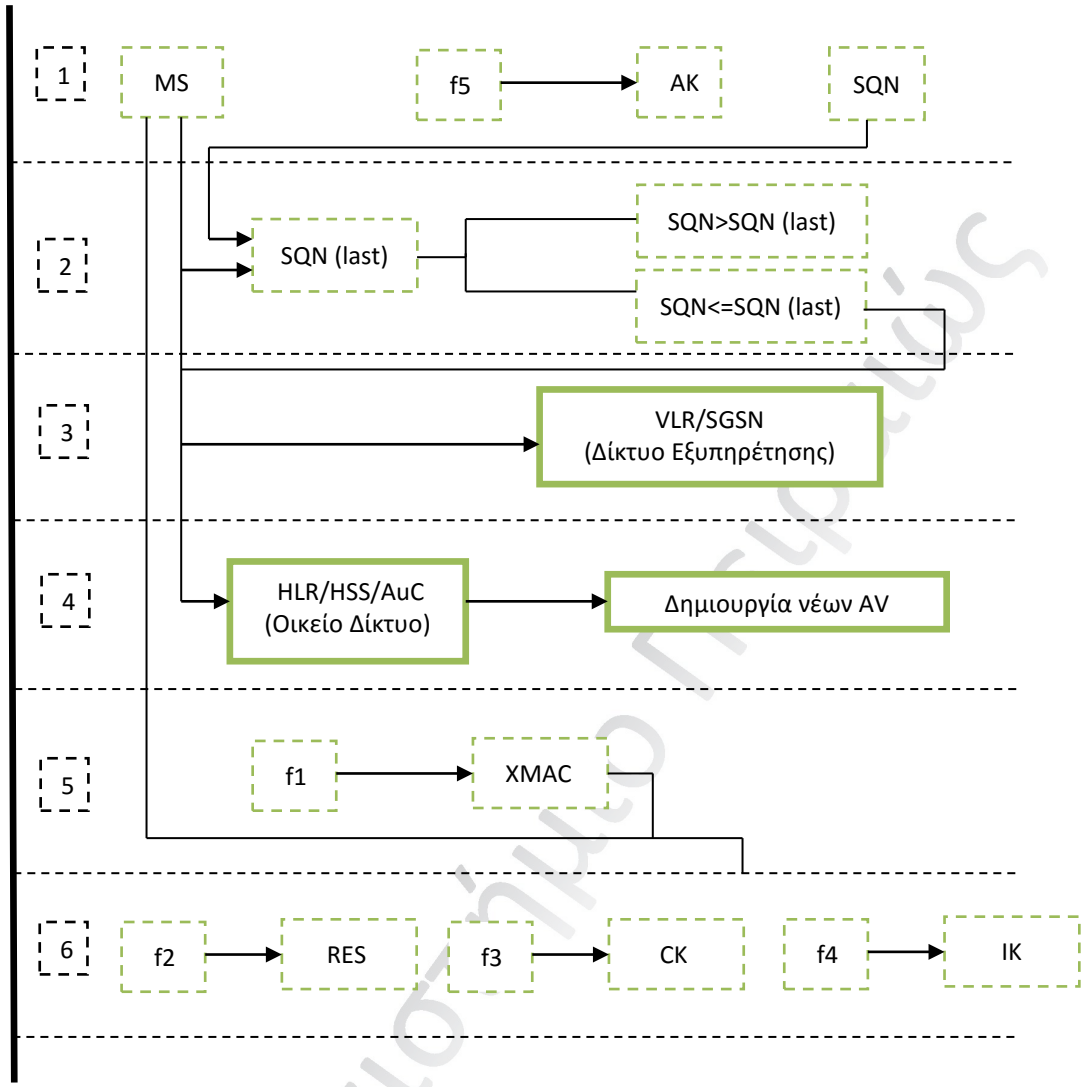
5.2.2.1.2 Διαδικασία που λαμβάνει χώρα στη USIM

- Το ζεύγος τιμών (RAND. AUTN) καταφθάνει στη USIM.
- Υπολογίζονται οι παράμετροι AK (έξοδος της συνάρτησης f5) και SQN (μέσω της λογικής συνάρτησης (SQN XOR AK) XOR AK, με την f5 να εξυπηρετεί την ανάγκη ανωνυμίας του χρήστη.

Πανεπιστήμιο Πειραιώς

- Η υπολογισμένη παράμετρος SQN συγκρίνεται με την τελευταία αποθηκευμένη στη USIM τιμή του SQN και εφόσον είναι μεγαλύτερη θεωρείται έγκυρη.
- Αν δεν είναι μεγαλύτερη, τότε αποστέλλεται με μήνυμα από τη USIM στο VLR/SGSN ο μεγαλύτερος αριθμός SQN που έχει αποθηκευτεί στη USIM για να επέλθει ο επανασυγχρονισμός (re synchronization procedure).
- Ο επανασυγχρονισμός γίνεται με την προώθηση του προηγούμενου μηνύματος στο HLR/HSS/AuC και τη δημιουργία νέων διανυσμάτων αυθεντικοποίησης τα οποία αποστέλλονται ξανά.
- Υπολογίζεται η έξοδος της συνάρτησης f1 είναι η τιμή της μεταβλητής XMAC (Expected MAC), εξυπηρετώντας την ανάγκη αυθεντικοποίησης από τη μεριά του δικτύου.
- Αυτή η αναμενόμενη τιμή της παραμέτρου MAC, συγκρίνεται με τη ληφθείσα (η οποία φτάνει στη USIM ως μέρος της παραμέτρου AUTN όπως φαίνεται στο παραπάνω σχήμα.
- Σε περίπτωση που η αναμενόμενη και η ληφθείσα MAC ταυτίζονται τότε από τη USIM θεωρείται ότι ή αίτηση προέρχεται από το HLR του οικείου δικτύου.
- Τέλος υπολογίζονται οι παράμετροι RES, CK και IK ως έξοδοι των συναρτήσεων f2,f3 και f4, εξυπηρετώντας ουσιαστικά τις ανάγκες της αυθεντικοποίησης της κάρτας του συνδρομητή, της κρυπτογράφησης και της ακεραιότητας αντίστοιχα.

Πανεπιστήμιο Πειραιώς



Διάγραμμα 14: Διαδικασία που λαμβάνει χώρα στη USIM

5.2.2.1.3 Μηχανισμός ανάθεσης προσωρινών ταυτοτήτων

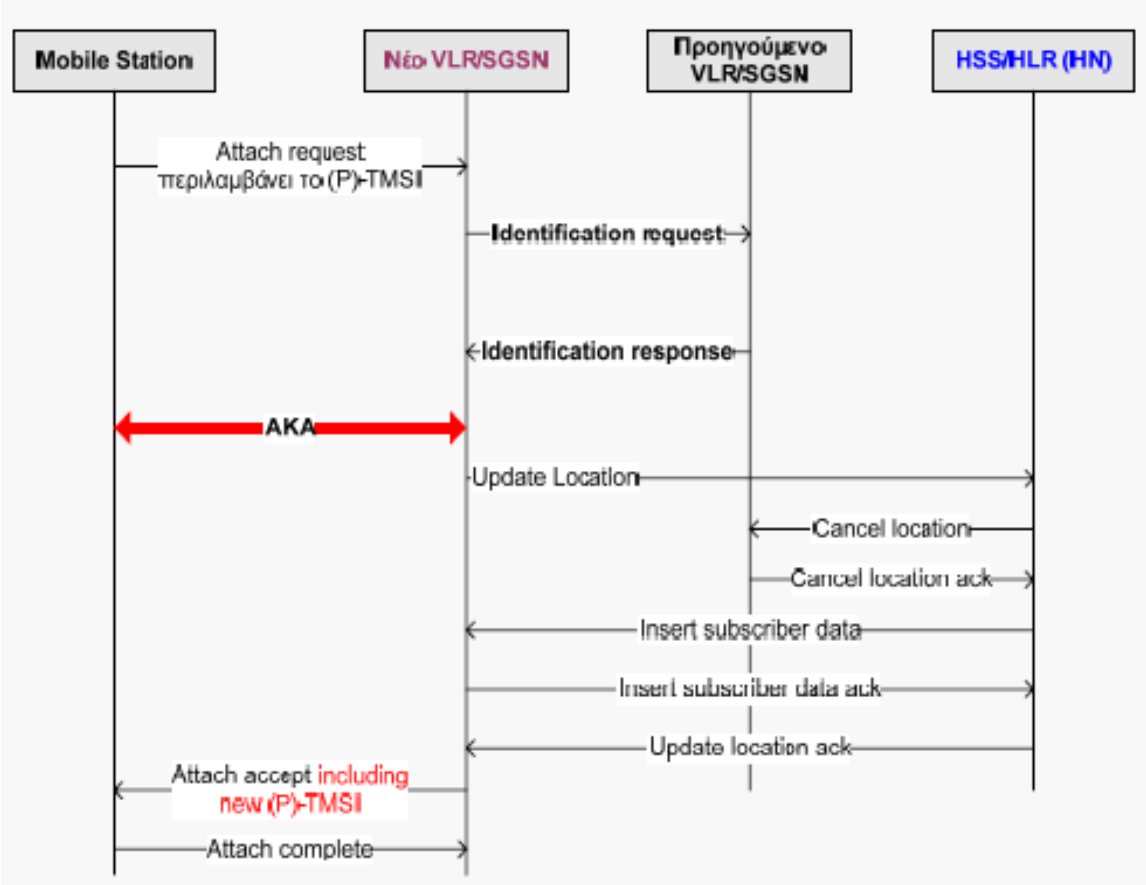
- Εφόσον ο χρήστης συνδέεται για πρώτη φορά, στέλνει στο δίκτυο εξυπηρέτησης (SN - Service Network) τη μόνιμη ταυτότητά του (IMSI).
- Ο χρήστης λαμβάνει με κρυπτογραφημένη μορφή μια προσωρινή ταυτότητα από το στοιχείο που VLR/SGSN.

Πανεπιστήμιο Πειραιώς

- Το στοιχείο VLR/SGSN για να γνωρίζει κάθε φορά σε πιο συνδρομητή απευθύνεται διατηρεί μια σχέση ανάμεσα στη μόνιμη και στην προσωρινή ταυτότητα του χρήστη, μια σχέση που είναι μοναδική για κάθε χρήστη που βρίσκεται εντός της περιοχής που ελέγχεται από το συγκεκριμένο κάθε φορά VLR/SGSN.
- Τη λήψη της προσωρινής ταυτότητας από το χρήστη ακολουθεί η αποστολή μιας επιβεβαίωσης (ACK) αυτής της λήψης.
- Το VLR/SGSN μετά το μήνυμα επιβεβαίωσης αποθηκεύει τη νέα ταυτότητα στη θέση της προηγούμενης (εφόσον υπάρχει).
- Η αποστολή του μηνύματος επιβεβαίωσης είναι σημαντική γιατί αν αυτή υφίσταται τότε διατηρείται τόσο η προηγούμενη όσο και η νέα σχέση. Το σενάριο αυτό «λειτουργεί» μόνο σε περιπτώσεις uplink για το χρήστη. Στην αντίθετη περίπτωση, αυτή του downlink, αυτή η συνύπαρξη παλιάς και νέας προσωρινής ταυτότητας δε λειτουργεί, με αποτέλεσμα να απαιτείται η χρήση της μόνιμης ταυτότητας.
- Εφόσον υλοποιηθεί ένα τέτοιο σενάριο, οι προσωρινές ταυτότητες διαγράφονται και αποστέλλεται νέα μέσω της γνωστής διαδικασίας (reallocation procedure).

Ενδιαφέρον παρουσιάζει η μεταβολή των προσωρινών ταυτοτήτων όταν ο συνδρομητής αλλάζει περιοχή και επομένως απευθύνεται σε διαφορετικό VLR/SGSN. Προκειμένου η προσωρινή ταυτότητα στο νέο VLR/SGSN να μην είναι ίδια με αυτή του προηγούμενου, χρησιμοποιείται ένα πρόθεμα το οποίο έχει άμεση σχέση με την περιοχή, το LAI (Local Area Identity) εφόσον πρόκειται για OS υποσύστημα και το RAI (Routing Area Identity) εφόσον πρόκειται για PS υποσύστημα. Έτσι, η μοναδικότητα της ταυτότητας εξασφαλίζεται κατά πολύ μεγαλύτερο ποσοστό, μια διαδικασία που ενισχύεται από το γεγονός ότι το προηγούμενο VLR/SGSN στέλνει στο επόμενο αχρησιμοποίητα διανύσματα αυθεντικοποίησης. Επίσης, μέσω του προθέματος μπορεί εύκολα να προσδιοριστεί το προηγούμενο VLR/SGSN.

Πανεπιστήμιο Πειραιώς



Διάγραμμα 15: Μηχανισμός ανάθεσης προσωρινών ταυτοτήτων σε συνδρομητές κατά την αλλαγή περιοχής (http://www.icsd.aegean.gr)

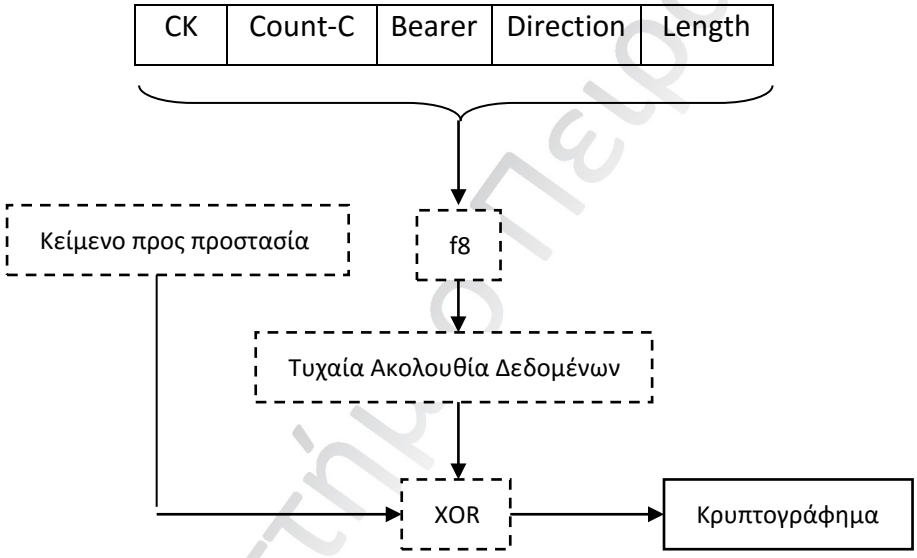
5.2.2.2 Διαδικασία κρυπτογράφησης

Η διαδικασία κρυπτογράφησης μπορεί να υλοποιηθεί σε δύο διαφορετικά επίπεδα, αυτό του ελέγχου πρόσβασης μέσου (Medium Access Control, MAC) ή αυτό του ελέγχου ραδιο-σύζευξης (Radio Link Control, RLC). Τα στάδια της διαδικασίας έχουν ως εξής:

- Το VLR/SGSN αποστέλλει το Cipher Key - CK στο RNC μέσω ενός ειδικού μηνύματος (security mode command) με βάση το πρωτόκολλο Radio Access Network Application Protocol (RANAP).
- Η λήψη του CK, συνεπάγεται την αποστολή μιας εντολής Radio Resource Control (RRC) στο χρήστη ώστε να εκκινηθεί η διαδικασία της κρυπτογράφησης.

- Ο μετρητής COUNT-C μηδενίζεται με την έναρξη της διαδικασίας αυθεντικοποίησης.
- Μια συνάρτηση f8 δημιουργεί μια τυχαία ακολουθία δεδομένων, με τη συνάρτηση να βασίζεται σε ένα νέο κωδικοποιητή ροής (block cipher), που είναι γνωστός ως KASUMI.
- Υλοποιείται μια λογική συνάρτηση XOR ψηφίο προς ψηφίο μεταξύ του προς προστασία κειμένου και της ακολουθίας δεδομένων που έχει παραχθεί στο προηγούμενο στάδιο.

Η χρήση της συνάρτησης f8 παρουσιάζεται στο ακόλουθο διάγραμμα.



Διάγραμμα 16: Υλοποίηση συνάρτησης XOR για δημιουργία κρυπτογραφήματος στο RNC

Αναλυτικότερα, οι παράμετροι εισόδου της συνάρτησης f8 είναι η ταυτότητα του ράδιο-φορέα (radio bearer identity) BEARER, η οποία καταδεικνύει ουσιαστικά την ύπαρξη διαφορετικών μετρητών για διαφορετική υπηρεσία, η παράμετρος DIRECTION η οποία έχει δύο τιμές ανάλογα με την κατεύθυνση κρυπτογράφησης (downlink ή uplink), η παράμετρος LENGTH που υποδηλώνει το μήκος των προς κρυπτογράφηση δεδομένων και ο μετρητής COUNT-C ο μηδενισμός του συμπίπτει με την έναρξη κάθε διαδικασίας αυθεντικοποίησης.

Πανεπιστήμιο Πειραιώς

Στη UICC είναι αποθηκευμένο το κλειδί CK, η παράμετρος START η οποία για κάθε νέα σύνδεση αυξάνεται κατά 2 και αποτελεί το το περισσότερο σημαντικό μέρος (most significant part) του μεγαλύτερου HFN που έχει μέχρι εκείνη τη στιγμή λάβει η USIM και η παράμετρος που ονομάζεται THRESHOLD, μέσω της οποίας ελέγχεται η ανανέωση των κλειδιών CK και IK.

5.2.3 Μηχανισμοί ασφάλειας σε επίπεδο πεδίου δικτύου

MAPsec

Οι συγκεκριμένοι μηχανισμοί σχετίζονται με την εξασφάλιση της προστασίας του Mobile Application Part (MAP) το οποίο κουβαλά όλη εκείνη την πληροφορία προστασίας της ραδιοξεύξης (π.χ κλειδιά αυθεντικοποίησης). Το πρωτόκολλο που περιγράφει τη συγκεκριμένη διαδικασία προστασίας είναι το MAPsec και συμπεριλαμβάνεται στο πρότυπο 3rd Generation Partnership Project (3GPP) (Release 4).

Η βασική ιδέα του πρωτοκόλλου MAPsec έγκειται στην κρυπτογράφηση ενός απροστάτευτου μηνύματος, το οποίο κρυπτογραφείται και το αποτέλεσμα που προκύπτει τοποθετείται μέσα σε ένα άλλο μήνυμα MAP, το οποίο περιέχει επίσης ένα κρυπτογραφημένο άθροισμα ελέγχου.

Το πρωτόκολλο στηρίζεται στην αυτόματη διαχείριση κλειδιών και στην έννοια της Σχέσης Ασφάλειας (Security Association - SA) η οποία συμπεριλαμβάνει πρόσθετη πληροφορία σχετικά με την ασφάλεια (για παράδειγμα τη διάρκεια ζωής των κλειδιών και τους ταυτοποιητές των χρησιμοποιούμενων αλγορίθμων), ενώ σε εφαρμογές διαδικτύου, εφαρμόζεται παράλληλα με το πρωτόκολλο IPsec, σκοπός του οποίου είναι η προστασία των πακέτων IP.

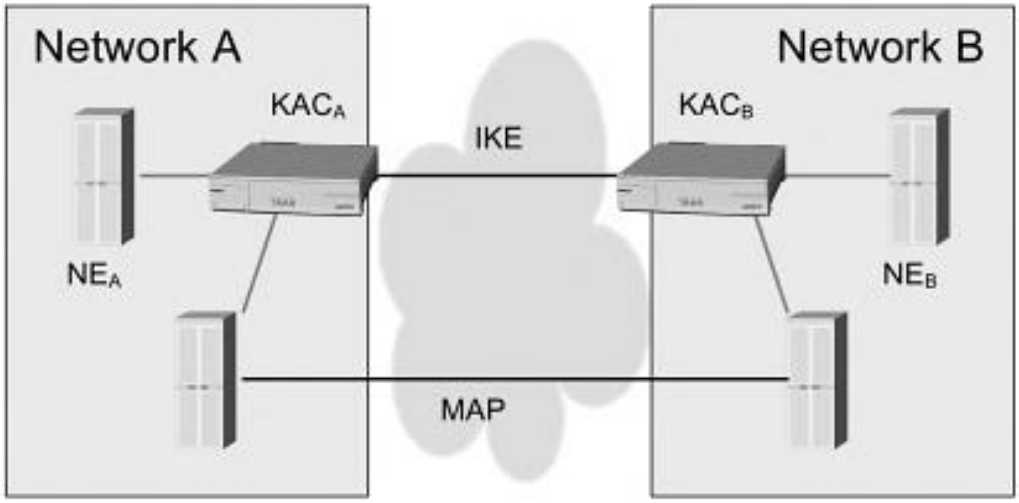
Βασικό στοιχείο της αυτόματης διαχείρισης κλειδιών είναι το στοιχείο Key Administration Centre (KAC) το οποίο χρησιμοποιείται από το πρωτόκολλο Internet Key Exchange (IKE), ως μέρος της γενικότερης πολιτικής ασφαλείας. Το πρωτόκολλο μπορεί να αφορά τρεις διαφορετικές καταστάσεις σε σχέση με την παρεχόμενη προστασία.

- Protection mode 0: Χωρίς προστασία

Πανεπιστήμιο Πειραιώς

- Protection mode 1: Εξασφάλιση Ακεραιότητας
- Protection mode 2: Εξασφάλιση Εμπιστευτικότητας και ακεραιότητας.

Η λειτουργία του πρωτοκόλλου MAPsec περιγράφεται στο ακόλουθο διάγραμμα (όπου NE τα Network Elements του κάθε δικτύου).



Διάγραμμα 17: Λειτουργία του πρωτοκόλλου MAPsec (Niemi and Nyberg, 2003)

5.2.4 Συσχετισμός είδους επίθεσης και σημείου του μηχανισμού ασφαλείας

- Η ύπαρξη του κλειδιού κρυπτογράφησης, εφόσον δεν είναι γνωστή και επιχειρηθεί η αποκρυπτογράφηση των δεδομένων απαιτείται η δοκιμή 2128 διαφορετικών συνδυασμών.
- Η επιλογή συναρτήσεων f1-f5 αυξημένης αντοχής μπορεί να προστατεύσει τη διαδικασία από επιθέσεις εξαντλητικής αναζήτησης (brute force).
- Σε περιπτώσεις που υφίστανται διαδοχικές αυθεντικοποιήσεις, μπορεί το SQN να χρησιμοποιηθεί για να αποκαλυφθεί η ταυτότητα του συνδρομητή. Επομένως η απόκρυψη του SQN μπορεί να προστατεύσει από επιθέσεις αυτού του είδους.
- Σε περιπτώσεις που κάποιος με κακόβουλη διάθεση μπορεί να καταγράψει μια διαδικασία αυθεντικοποίησης και επομένως να γνωρίζει τις τιμές των RAND και AUTN, είναι δυνατό να κάνει μια επαναληπτική επίθεση (replay attack). Η

προστασία έναντι μιας τέτοιας επίθεσης επιτυγχάνεται μέσω του ελέγχου του πεδίου SQN.

- Σε μια επίθεση που υφίσταται κρυφής ακουστικής και παρατήρησης (eavesdrop) με αποτέλεσμα να είναι γνωστό το κρυπτογράφημα και με βάση το γεγονός ότι μπορεί να χρησιμοποιηθεί η ίδια μάσκα για την κρυπτογράφηση δύο διαφορετικών κειμένων, η χρήση δύο μετρητών εξασφαλίζει ότι δεν θα παραχθεί μια ίδια μάσκα για δύο διαφορετικές κρυπτογραφήσεις. Ο πρώτος μετρητής εντοπίζεται στο επίπεδο MAC και είναι ένας αριθμός διόρθωσης πλαισίου (Correction Frame Number, CFN) ή στο επίπεδο (Radio Link Control – RLC) όπου χρησιμοποιείται ένας συγκεκριμένος αριθμός σειράς (RLC sequence number, RLC-SN). Ο δεύτερος μετρητής που συνδυάζεται με τους παραπάνω είναι ο Hyper Frame Number (HFN) και ο οποίος αυξάνεται κάθε φορά που ένας από τους προηγούμενους επανεκκινείται, προλαβαίνοντας έτσι τη γρήγορη μεταβολή αυτών των μετρητών. Με το συνδυασμό αυτών των δύο μετρητών προκύπτει ο μετρητής COUNT-C.

5.3 Μηχανισμοί ασφαλείας κινητής τηλεφωνίας τέταρτης γενιάς

Η ανάπτυξη της τεχνολογίας κινητής τηλεφωνίας τέταρτης γενιάς προήλθε από την ανάγκη αυξημένων απαιτήσεων των χρηστών, όσον αφορά στο χρησιμοποιούμενο εύρος ζώνης αλλά και στον υψηλό ρυθμό μετάδοσης.

5.3.1 Αρχιτεκτονική Δομή Συστήματος Ασφαλείας

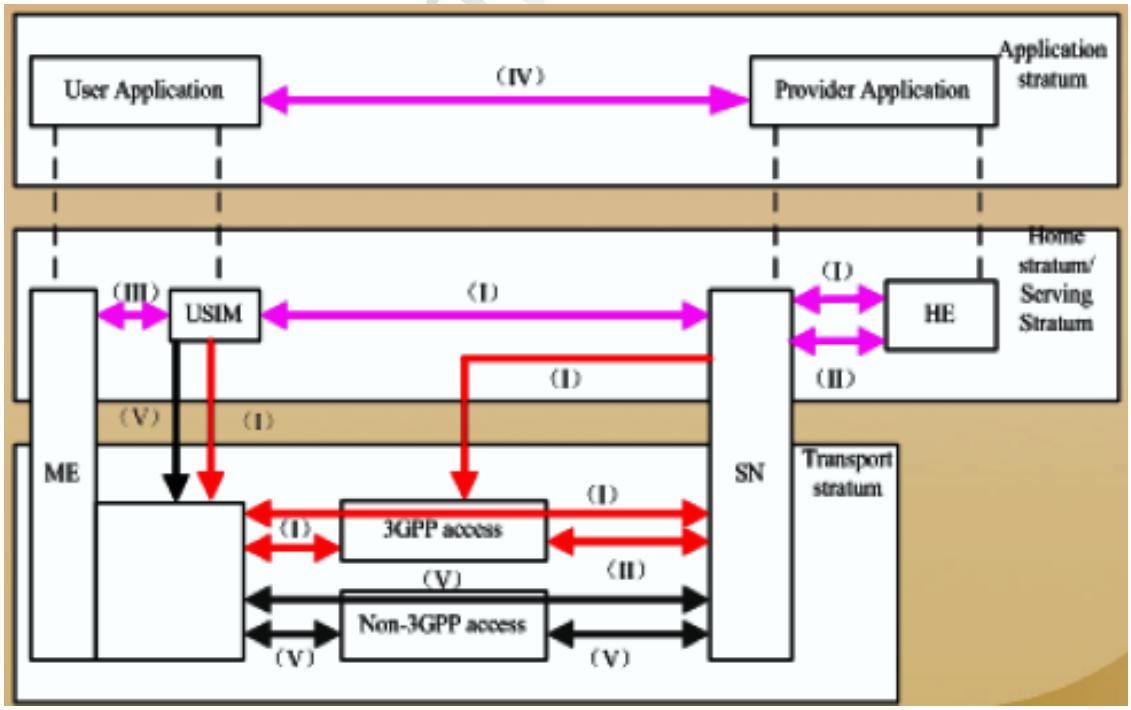
Όσον αφορά στην αρχιτεκτονική του συστήματος ασφαλείας στην τεχνολογία LTE, διακρίνονται πέντε διαφορετικά επίπεδα ασφαλείας.

- Ασφάλεια πρόσβασης δικτύου (Network access security - I): Αφορά το σύνολο των χαρακτηριστικών ασφαλείας που ελέγχουν την πρόσβαση στο δίκτυο Evolved Packet Core - EPC και εξασφαλίζουν την προστασία στη ραδιοζεύξη.

Πανεπιστήμιο Πειραιώς

- Ασφάλεια τομέα δικτύου (Network domain security - II): Αφορά το σύνολο των χαρακτηριστικών ασφαλείας που σχετίζονται με την προστασία του ενσύρματου δικτύου και των κόμβων που ενεργοποιούνται κάθε φορά για την ανταλλαγή των δεδομένων.
- Ασφάλεια τομέα χρήστη (User domain security - III): Αφορά το σύνολο των χαρακτηριστικών ασφαλείας που σχετίζονται με την παροχή αμοιβαίας αυθεντικοποίησης μεταξύ της USIM κσι της κινητής οντότητας ΜΕ.
- Ασφάλεια τομέα εφαρμογών (Application domain security - IV): Αφορά το σύνολο των χαρακτηριστικών ασφαλείας που σχετίζονται με τις εφαρμογές της UE και του παρόχου για την ασφαλή ανταλλαγή δεδομένων.
- Ασφάλεια τομέα Non 3GPP (V): Αφορά το σύνολο των χαρακτηριστικών ασφαλείας που σχετίζονται με την εξασφάλιση της προστασίας δικτύων non-3GPP (τα οποία δηλαδή δε «συμμορφώνονται με τους κανονισμούς του συγκεκριμένου προτύπου) κατά την πρόσβασή τους στο δίκτυο EPC.

Τα προαναφερόμενα επίπεδα και η μεταξύ τους διασύνδεση αποτυπώνονται στο διάγραμμα που ακολουθεί.



Διάγραμμα 18: Αρχιτεκτονική του συστήματος ασφαλείας στην τεχνολογία LTE (Ma, 2012)

5.3.2 Επιμέρους μηχανισμοί ασφαλείας

5.3.2.1 Ασφάλεια πρόσβασης δικτύου

Εμπιστευτικότητα Ταυτότητας Χρήστη

Για να επιτευχθεί η συγκεκριμένη ιδιότητα, απαιτείται από τη Mobility Management Entity (MME) να διαθέσει μια ταυτότητα Globally Unique Temporary Identity (GUTI) στη UE, η οποία χρησιμοποιείται στο Evolved packet system (EPS) για την αποφυγή ανταλλαγής συχνοτήτων της μόνιμης ταυτότητας του χρήστη IMSI μέσω της ραδιοζεύξης. Η GUTI αποτελείται από δύο συνιστώσες, την Globally Unique MME Identity (GUMMEI) που είναι και η ταυτότητα της MME που έχει διαθέσει την GUTI και την M-TMSI η οποία είναι η ταυτότητα της UE που εμπεριέχεται στην MME.

Η GUMMEI με τη σειρά της αποτελείται από τις Public Land Mobile Network PLMN Id (MCC, MNC) και την MME Identifier (MMEI) (η οποία αναλύεται στις MME Group Id (MMEGI) και MME Code (MMEC)) (3GPP TS 23.003, 2008-12).

Εμπιστευτικότητα Συσκευής Χρήστη

Εξασφαλίζεται μέσω της αποστολής (μετά από σχετική αίτηση) της IMEI μέσω διαδικασιών επιπέδου Non-Access Stratum (NAS).

Αυθεντικοποίηση Οντότητας

Πραγματοποιείται μέσω μιας διαδικασίας αυθεντικοποίησης του συστήματος EPS και της διαδικασίας αυθεντικοποίησης και συμφωνίας κλειδιών (Authentication and Key Agreement - AKA), έτσι ώστε χρήστης και δίκτυο να αυθεντικοποιούνται εκατέρωθεν με τη συμφωνία να αφορά το κλειδί Key Access Security Management Entity (K_{ASME}). Το συγκεκριμένο κλειδί – οντότητα αποτελεί τη βάση για τη δημιουργία των κλειδιών

Πανεπιστήμιο Πειραιώς

κρυπτογράφησης και ακεραιότητας των επιπέδων AS και NAS τα οποία θα χρησιμοποιηθούν στον RRC, στο επίπεδο του χρήστη και στην προστασία της ανταλλαγής σημάτων.

5.3.2.1.1 Πλαίσιο ασφαλείας του συστήματος EPS

Το συγκεκριμένο πλαίσιο είναι αποτέλεσμα εφαρμογής του μηχανισμού EPS AKA και ταυτοποιείται μοναδικά από το κλειδί evolved Key Set Identifier (eKSI) το οποίο περιλαμβάνει τις συνιστώσες επιπέδων AS και NAS. Τόσο η UE όσο και η MME διατηρούν ταυτόχρονα το δικό τους πλαίσιο ασφαλείας EPS, με τη λειτουργία τους να λαμβάνει χώρα παράλληλα (για παράδειγμα σε μια διαδικασία επαναυθεντικοποίησης). Ένα πλαίσιο ασφαλείας EPS μπορεί να αποθηκευτεί για μελλοντικό έλεγχο πρόσβασης (cached security context). Μια UE που δε διαθέτει ένα τέτοιο πλαίσιο χρειάζεται μια διαδικασία Extended Pedestrian AKA (EPA) προκειμένου να μπορεί να ενσωματωθεί στο δίκτυο και να «τρέξει».

Ανάκτηση δεδομένων αυθεντικοποίησης

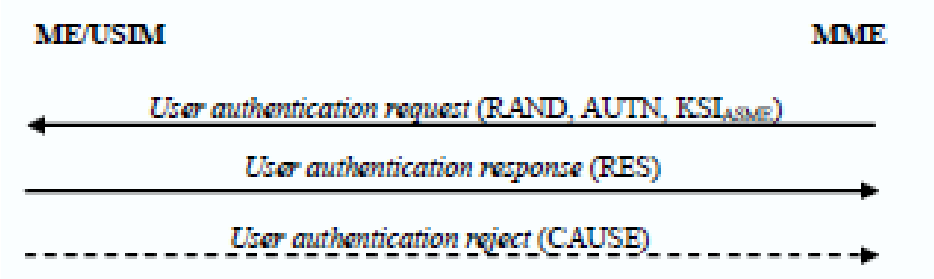
Η σχετική με την αυθεντικοποίηση πληροφορία ανακτάται από τον HSS μέσω της διεπαφής S6a και έπειται από σχετική αίτηση της MME. Η πληροφορία αυτή περιλαμβάνει την IMSI, την ταυτότητα του δικτύου εξυπηρέτησης (κώδικα χώρας και κινητού δικτύου), τον τύπο του δικτύου (E-UTRAN) καθώς και τον αριθμό των διανυσμάτων αυθεντικοποίησης που αναμένεται να ληφθούν από την MME. Περισσότερες πληροφορίες σχετικά με το επίπεδο μηνυμάτων και τους ορισμούς των διανυσμάτων περιλαμβάνονται στα πρωτόκολλα 3GPP TS 29.272 (2009-11) και 3GPP TS 33.102 (2008-12).

Αυθεντικοποίηση UE

Πραγματοποιείται από την εκάστοτε MME μέσω διαδικασιών EPS NAS. Η αίτηση αυθεντικοποίησης EMM αποστέλλεται στην UE συμπεριλαμβάνοντας τις απαραίτητες παραμέτρους (RAND, AUTN και το κλειδί eKSI ή το KSI_{ASME}), όπως φαίνεται στην ακόλουθη εικόνα. Η UE απαντά μέσω της παραμέτρου (RES) ώστε η διαδικασία

Πανεπιστήμιο Πειραιώς

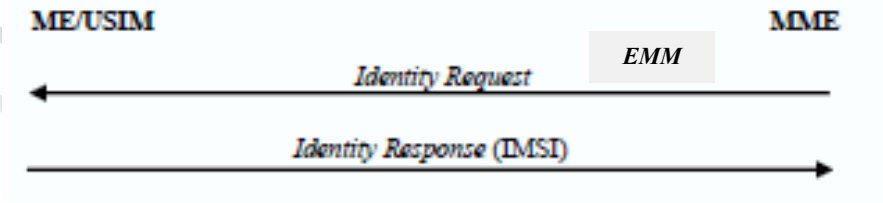
αυθεντικοποίησης να ολοκληρωθεί επιτυχώς (αφού η ορθότητα του αποτελέσματος RES ελεγχθεί από τη MME και αποφασιστεί η τιμή ενδιάμεσου κλειδιού K_{ASME}). Η απόφαση αυτή λαμβάνεται μετά την ολοκλήρωση της εφαρμογής του μηχανισμού EPS AKA με τις προσυμφωνημένες παραμέτρους μεταξύ UE και MME (3GPP TS 24.301, 2008-12).



Διάγραμμα 19: Αυθεντικοποίηση χρήστη συστήματος EPS (Agilent Technologies, 2009)

Ταυτοποίηση UE

Η αίτηση ταυτοποίησης της UE εισάγεται από την MME που εξυπηρετεί κάθε φορά με τη χρήση διαδικασιών EPS NAS. Μια αίτηση ταυτότητας EPS Mobility Management (EMM) αποστέλλεται στην UE σχετικά με τη μόνιμη ταυτότητα της συσκευής, με την αίτηση να δημιουργείται όταν η GUTI δεν είναι διαθέσιμη όσον αφορά στο να παρέχει μια μοναδική ταυτότητα της UE. Η αίτηση ταυτότητας EMM μπορεί επίσης να χρησιμοποιηθεί για την ανάκτηση της IMEI ως μέρος της ταυτότητας του κινητού εξοπλισμού (Mobile Equipment - ME) με την επιστρεφόμενη IMEI να αποστέλλεται στον Equipment Identity Register (EIR) μέσω της διεπαφής S13 (3GPP TS 29.272, 2009-11).



Διάγραμμα 20: Ερώτημα διαπίστωσης ταυτότητας χρήστη (Agilent Technologies, 2009)

Εμπιστευτικότητα και ακεραιότητα των δεδομένων σηματοδότησης και χρήστη

Όπως προαναφέρθηκε, η εξασφάλιση της εμπιστευτικότητας και ακεραιότητας των δεδομένων στο σύστημα EPS επιτυγχάνεται μέσω μηχανισμών ασφαλείας σε δύο διαφορετικά επίπεδα, αυτό της πρόσβασης και αυτό της μη πρόσβασης δικτύου (AS και NAS). Μηχανισμοί κρυπτογράφησης μπορούν να χρησιμοποιηθούν προκειμένου να παρέχεται εμπιστευτικότητα δεδομένων σηματοδοσίας και χρήστη μεταξύ UE και EPS, ενώ η αντίστοιχη ιδιότητα της ακεραιότητας επιτυγχάνεται μέσω μηχανισμών επανάληψης. Η αντιστοιχία των μηχανισμών αυτών με τα στοιχεία του δικτύου καταγράφεται στον ακόλουθο πίνακα.

Μηχανισμός Ασφαλείας	Στοιχεία Δικτύου	
	Επίπεδο Πρόσβασης	Επίπεδο μη πρόσβασης
Σημεία Τερματισμού	UE eNB	UE MME
Κρυπτογραφία	RRC	NAS
Ακεραιότητα και επαναληψιμότητα	RRC	NAS
Επίπεδα πρωτοκόλλων ασφαλείας	PDCP	NAS
Διαδικασίες εντολών ασφαλείας	RRC	NAS

Πίνακας 3: Αντιστοιχία μηχανισμών ασφαλείας και στοιχείων δικτύου στο σύστημα EPS (Agilent Technologies, 2009)

Πανεπιστήμιο Πειραιώς

5.3.2.1.2 Ασφάλεια επιπέδου AS

Ένα πλαίσιο ασφαλείας EPS AS προετοιμάζεται από τον κόμβο eNB μέσω της MME όταν η UE εισέρχεται στην κατάσταση ECMCONNECTED και κατά τη διάρκεια της προετοιμασίας μιας intra-LTE παράδοσης. Τη συγκεκριμένη στιγμή, οι διάφορες παράμετροι ασφαλείας μεταφέρονται από την πηγή στον κόμβο – στόχο της επικοινωνίας. Το πλαίσιο διαγράφεται από τον κόμβο όταν η UE εισέρχεται σε κατάσταση ECM-IDLE ή όταν η παράδοση έχει ολοκληρωθεί.

Μια διαδικασία εντολής ασφαλείας RRC χρησιμοποιείται κατά την αρχική εδραίωση του πλαισίου ασφαλείας AS και δημιουργείται από τον κόμβο eNB προς την UE. Ταυτόχρονα, εδραιώνεται το SRB1 (Signalling Radio Bearer 1) και ακολουθεί η εδραίωση του SRB2 και των DRBs (Data Radio Bearers) (3GPP TS 36.331, 2008-12).

Για την περίπτωση μονάδων πακέτων δεδομένων DRB (Packet Data Units - PDUs), η κρυπτογράφηση στο επίπεδο PDCP (Packet Data Control Plane) εφαρμόζεται με τη χρήση μιας κεφαλίδας – προθέματος (σε συμπιεσμένη μορφή εφόσον δεν πρόκειται για SRBs), ενώ αφορά το τμήμα δεδομένων των SRB ή DRB μέσω του μηνύματος αυθεντικοποίησης MAC-I (Message Authentication Code) για το SRB (3GPP TS 36.323, 2008-12).

5.3.2.1.3 Ασφάλεια επιπέδου NAS

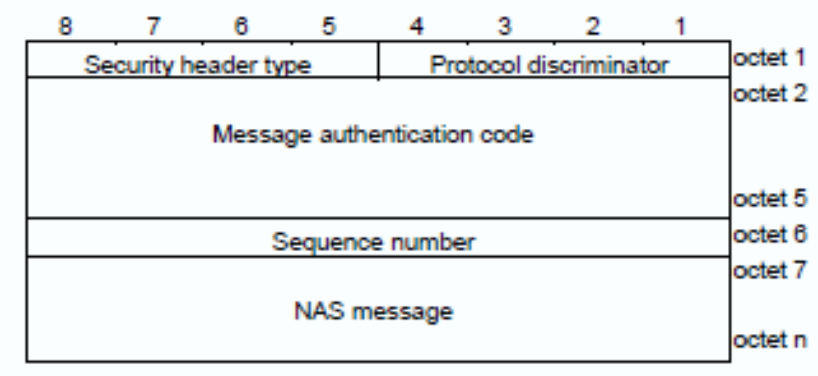
Το πλαίσιο ασφαλείας NAS εδραιώνεται μέσω της αντίστοιχης διαδικασίας ελέγχου κατάστασης η οποία με τη σειρά της δημιουργείται από την MME προς την UE. Η διαδικασία αυτή μπορεί να χρησιμοποιηθεί ακόμα και κατά τη διαμόρφωση του πλαισίου (όπως για παράδειγμα στην αλλαγή ενός αλγορίθμου). Η εφαρμογή της διαδικασίας ξεκινά με την αποστολή ενός μηνύματος εντολής του οποίου η ακεραιότητα είναι προστατευμένη, με το μήνυμα να περιλαμβάνει τις εκάστοτε επιλογές EEA, EIA και eKSI, ανάλογα με τις δυνατότητες ασφαλείας της UE. Το σύστημα επιλέγει κάθε φορά τις υψηλότερης προτεραιότητας EEA και EIA, οι οποίες υποστηρίζονται τόσο από τη MME όσο και από την UE.

Πανεπιστήμιο Πειραιώς

Στη συνέχεια εφαρμόζεται αλγόριθμος κρυπτογράφησης σε όλα τα μηνύματα NAS εκτός από τις αιτήσεις EMM εντοπισμού νέας περιοχής κίνησης (Tracking Area Update - TAU) και την εντολή εφαρμογής πλαισίου ασφαλείας και μέχρι η MME μεταπέσει σε κατάσταση ECM-IDLE.

Στη μετάπτωση από την κατάσταση ECM-IDLE στην ECM-CONNECTED, το σύστημα συνεχίζει να στέλνει τα αρχικά μηνύματα NAS με προστασία ακεραιότητας αλλά χωρίς κρυπτογράφηση.

Η εδραίωση του πλαισίου ασφαλείας NAS ολοκληρώνεται με την απόκριση της MME στο αρχικό μήνυμα της UE. Στην εικόνα που ακολουθεί παρουσιάζεται η οργάνωση ενός μηνύματος NAS προστατευμένου με το προαναφερόμενο πλαίσιο ασφαλείας.



Εικόνα 2: Οργάνωση μηνύματος NAS για την εξασφάλιση της προστασίας του (3GPP TS 24.301, 2008-12)

Στον πίνακα που ακολουθεί καταγράφονται οι κεφαλίδες ασφαλείας οι οποίες περιλαμβάνουν σχετικές πληροφορίες για το πλαίσιο NAS PDU και συμπεριλαμβάνονται σε κάθε μήνυμα EMM.

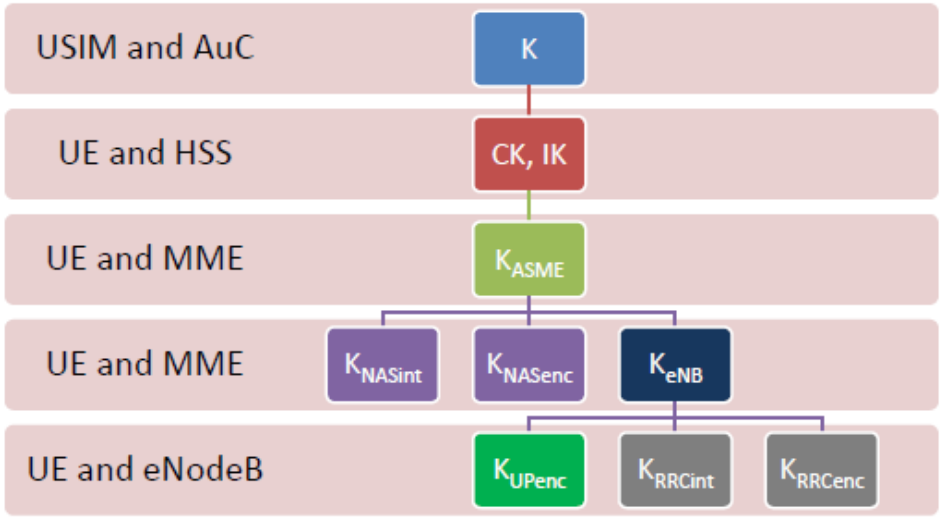
Πανεπιστήμιο Πειραιώς

Είδος κεφαλίδας	*Σημασία κεφαλίδας για το μήνυμα NAS*
0000	Μήνυμα χωρίς προστασία
0001	Προστασία ακεραιότητας
0010	Προστασία ακεραιότητας και κρυπτογραφία
0011	Προστασία ακεραιότητας με νέο περιεχόμενο στο πλαίσιο ασφαλείας EPS
0100	Προστασία ακεραιότητας και κρυπτογραφία με νέο περιεχόμενο στο πλαίσιο ασφαλείας EPS
1100	Κεφαλίδα ασφαλείας για μήνυμα αίτησης εξυπηρέτησης
1101	Δε συμπεριλαμβάνεται στο πρωτόκολλο και ερμηνεύεται ως την αμέσως προηγούμενη

Πίνακας 4: Κεφαλίδες ασφαλείας του πλαισίου NAS PDU (3GPP TS 24.301, 2008-12)

Ιεραρχία κλειδιών συστήματος

Το ακόλουθο διάγραμμα παρουσιάζει την ιεραρχία των κλειδιών ασφαλείας που χρησιμοποιούνται στο σύστημα EPS.



Διάγραμμα 21: Ιεραρχία κλειδιών συστήματος EPS (EventHelix.com Inc, 2012)

Όλα τα κλειδιά του συστήματος έχουν μήκος 256 bits. Εντούτοις, τα κλειδιά κρυπτογράφησης και ακεραιότητας για τους αλγόριθμους AS και NAS χρησιμοποιούν μόνο τα 128 λιγότερο σημαντικά δυαδικά ψηφία (Least Significant Bits - LSB) των αντίστοιχων κλειδιών, τα οποία μετατρέπονται κάθε φορά ανάλογα με τους εν λειτουργία αλγορίθμους. Το κλειδί eKSI χρησιμοποιείται για τη μοναδική ταυτοποίηση του κλειδιού K_{ASME} καθώς και των κλειδιών που προέρχονται από αυτό. Τα κλειδιά KeNB και Next Hop (NH) είναι μεταβατικά και χρησιμοποιούνται κατά τις Intra-LTE handovers και για την εύρεση ενός ανανεωμένου κλειδιού KeNB.

Αλλαγή κλειδιών

Η αλλαγή των κλειδιών σε όλο το εύρος της επικοινωνίας γίνεται δυναμικά. Στην περίπτωση του πλαισίου AS EPS για να γίνει μια τέτοια αλλαγή η MME αποστέλλει το ανανεωμένο KeNB στον κόμβο eNB που εξυπηρετεί κάθε φορά και ο οποίος κατηγοριοποιεί τα κλειδιά ασφαλείας σε SRBs και DRBs. Το νέο πλαίσιο ενεργοποιείται μέσω διαδικασιών AS intra-cell handover.

Παρομοίως, στην περίπτωση του πλαισίου NAS EPS η MME παράγει τα κλειδιά ασφαλείας για το επίπεδο NAS και ο έλεγχος της κατάστασης ασφαλείας του επιπέδου χρησιμοποιείται για να θέσει εκ νέου το σύστημα EPS. Σε περίπτωση που το κλειδί K_{ASME} αλλάξει, η διαδικασία ανανέωσης των κλειδιών στο επίπεδο NAS ακολουθείται από μια αντίστοιχη διαδικασία στο επίπεδο AS.

Η συγκεκριμένη ανανέωση λαμβάνει χώρα όταν ο κόμβος eNB ανιχνεύσει μεταβολή των τιμών PDCP COUNT. Αντίστοιχα, η ανανέωση σε επίπεδο NAS γίνεται όταν η MME ανιχνεύσει μεταβολή των τιμών NAS COUNT. Σε κάθε περίπτωση αρχικοποιείται μια νέα διαδικασία EPS AKA κατά την οποία η αλλαγή των κλειδιών γίνεται σε όλο το εύρος της ιεραρχίας.

Πανεπιστήμιο Πειραιώς

5.3.2.2 Ασφάλεια τομέα δικτύου (Network Domain Security - NDS)

Η προστασία των διεπαφών που βασίζονται σε πρωτόκολλα διαδικτύου περιγράφεται στο πρωτόκολλο 33.210 το οποίο καθορίζει τις επιμέρους λεπτομέρειες σχετικά με την αρχιτεκτονική δομή ασφαλείας των διεπαφών αυτού του είδους *Network Domain IP-based interfaces - NDS/IP) (3GPP TS 33.210 V8.2.0, 2008-12).

Ο πίνακας που ακολουθεί καταγράφει τις υπηρεσίες - χαρακτηριστικά ασφαλείας που παρέχονται από τις διεπαφές NDS/IP διαμέσου του πρωτοκόλλου ασφαλείας IPSec. Τα ελάχιστα χαρακτηριστικά που πρέπει να υποστηρίζονται στη χρήση των διεπαφών NDS/IP μέσω του συγκεκριμένου πρωτοκόλλου, παρουσιάζονται στον ακόλουθο πίνακα.

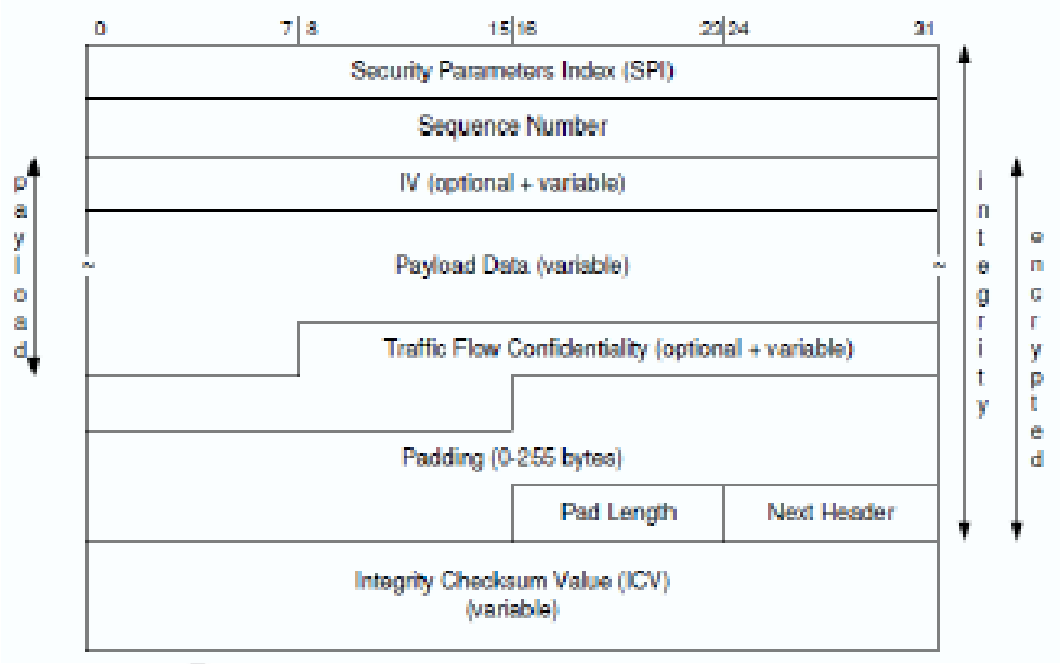
Πρωτόκολλο	ESP (RFC 4303/2406) με υποστήριξη του RFC 4303
Κατάσταση ασφαλείας	Tunnel (υποχρεωτικά) Transport (προαιρετικά)
Αλγόριθμοι κρυπτογράφησης	Null (RFC 2410) 3DES-CBC (RFC 2405/2451) with 3x64-bit key. 64-bit block size AES-CBC (RFC 3602) with 128-bit key. 128 bit block size
Αλγόριθμος αυθεντικοποίησης	HMAC-SHA-1-96 (RFC 2404) with 160-bit key. 512-bit block size
Μηχανισμός ασφαλείας	Single (υποχρεωτικά) Bundle (προαιρετικά)

Πίνακας 5: Χαρακτηριστικά πρωτοκόλλου ασφαλείας IPSec που υποστηρίζονται στο πρωτόκολλο NDS/IP (Agilent Technologies, 2009)

Τα πρωτόκολλα ανταλλαγής κλειδιών IKEv1 και IKEv2 χρησιμοποιούνται στα δίκτυα NDS/IP για τη διαπραγμάτευση, εδραίωση και διατήρηση των συνδέσμων ασφαλείας μεταξύ των Security Gateways (SEGs).

Πανεπιστήμιο Πειραιώς

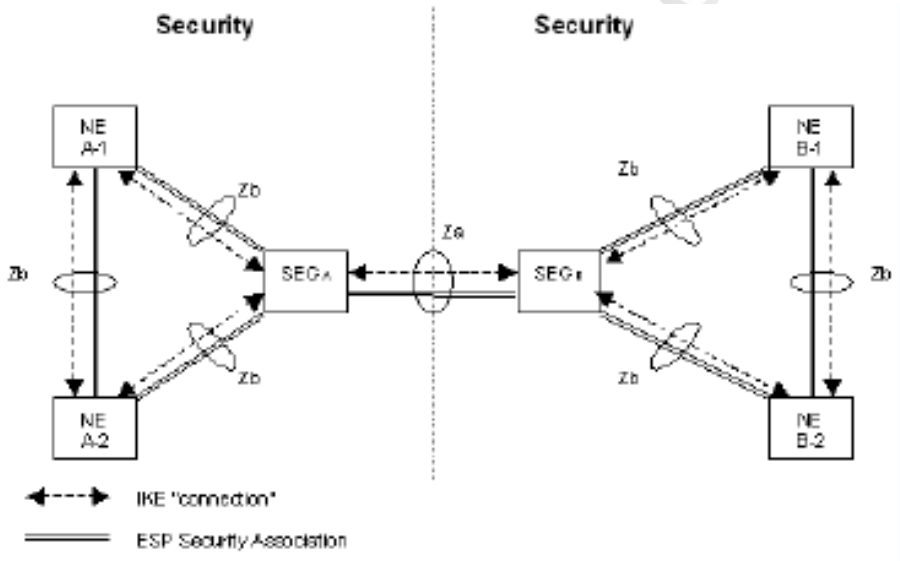
Εικόνα 3: Μορφή πακέτου δεδομένων IPv4 με πρωτόκολλο ασφαλείας ESP (tunnel mode) (RFC 4303, 2005)



Εικόνα 4: Υποδομή χρήσιμων προς μετάδοση δεδομένων με χρήση κεφαλίδας ασφαλείας ESP (RFC 4303, 2005)

Αρχιτεκτονική Ασφαλείας Τομέα Δικτύου

Η ακόλουθη εικόνα περιγράφει την αρχιτεκτονική ασφαλείας του τομέα δικτύου (NDS) για πρωτόκολλα διαδικτύου. Ο τομέας είναι χωρισμένος σε επιμέρους τομείς ασφαλείας οι οποίοι με τη σειρά τους διαχωρίζονται μέσω πυλών ασφαλείας (SEGs) στη διεπαφή Za, με παραπάνω από μία πύλη να είναι δυνατό να χρησιμοποιηθεί για έναν τομέα, όπως παρουσιάζεται στο ακόλουθο διάγραμμα. Η διεπαφή Zb χρησιμοποιείται για την παροχή ασφαλούς πρόσβασης εκτός του τομέα.



Διάγραμμα 22: NDS architecture for IP-based protocols (3GPP TS 33.210, 2008-12)

Στον πίνακα που ακολουθεί παρουσιάζονται οι διαφορές χαρακτηριστικών ασφαλείας για τις διεπαφές Za και Zb όπως καταγράφονται στο πρότυπο 33.210.

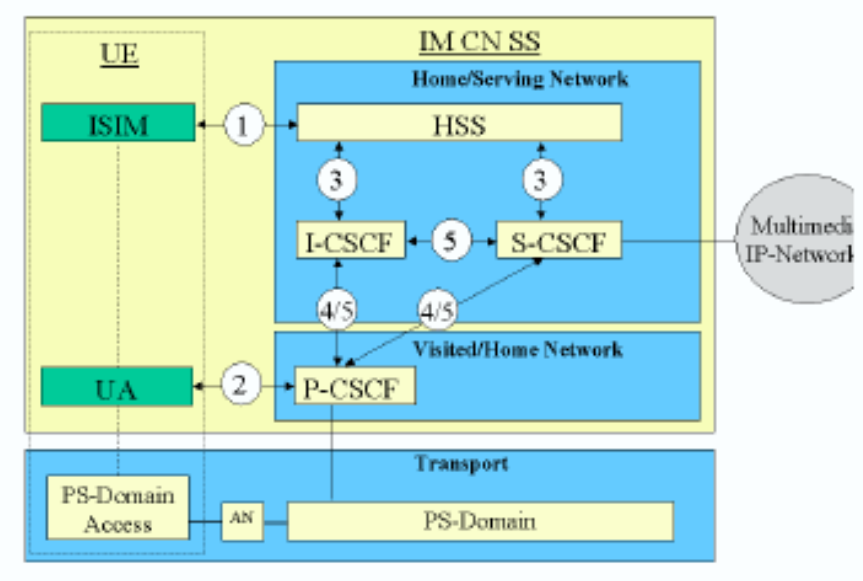
Χαρακτηριστικά ασφαλείας του τομέα δικτύου	Διεπαφή Za	Διεπαφή Zb
Εφαρμογή	Υποχρεωτική	Προαιρετική
Αυθεντικοποίηση / Ακεραιότητα	Υποχρεωτική	Υποχρεωτική
Κρυπτογράφηση	Προαιρετική	Προαιρετική
Πρωτόκολλο ασφαλείας	ESP	ESP
Κατάσταση ασφαλείας	Tunnel	Tunnel & Transport
Πεδίο εφαρμογής ασφαλείας	Εσωτερικά του τομέα	Εξωτερικά του τομέα
Σημεία τερματισμού	SEG-SEG	SEG – NE / NE – NE
Υποστήριξη IKE	IKEv1 & IKEv2	IKEv1/ IKEv2

Πίνακας 6: Διαφορές χαρακτηριστικών ασφαλείας για τις διεπαφές Za και Zb του τομέα δικτύου (3GPP TS 33.210 V8.2.0, 2008-12)

5.3.2.2.1 Αρχιτεκτονική ασφαλείας στο υποσύστημα πολυμέσων IMS

Το υποσύστημα πολυμέσων IMS (IP Multimedia Subsystem) είναι ένα σημαντικό «συστατικό» της ευρύτερης δομής LTE-SAE. Αναλυτικότερα, στο σχετικό πρότυπο (3GPP TS 33.203 V8.5.0, 2008-12) ορίζονται πέντε διαφορετικές σχέσεις - μηχανισμοί ασφαλείας για την προστασία του IMS, με το σύνολό τους να εφαρμόζεται στο υποσύστημα IMS Core Network Subsystem (IM CN SS), όπως απεικονίζεται στην εικόνα που ακολουθεί.

Πανεπιστήμιο Πειραιώς



Εικόνα 5: Αρχιτεκτονική ασφαλείας υποσυστήματος IMS (3GPP TS 33.203 V8.2.0, 2008-12)

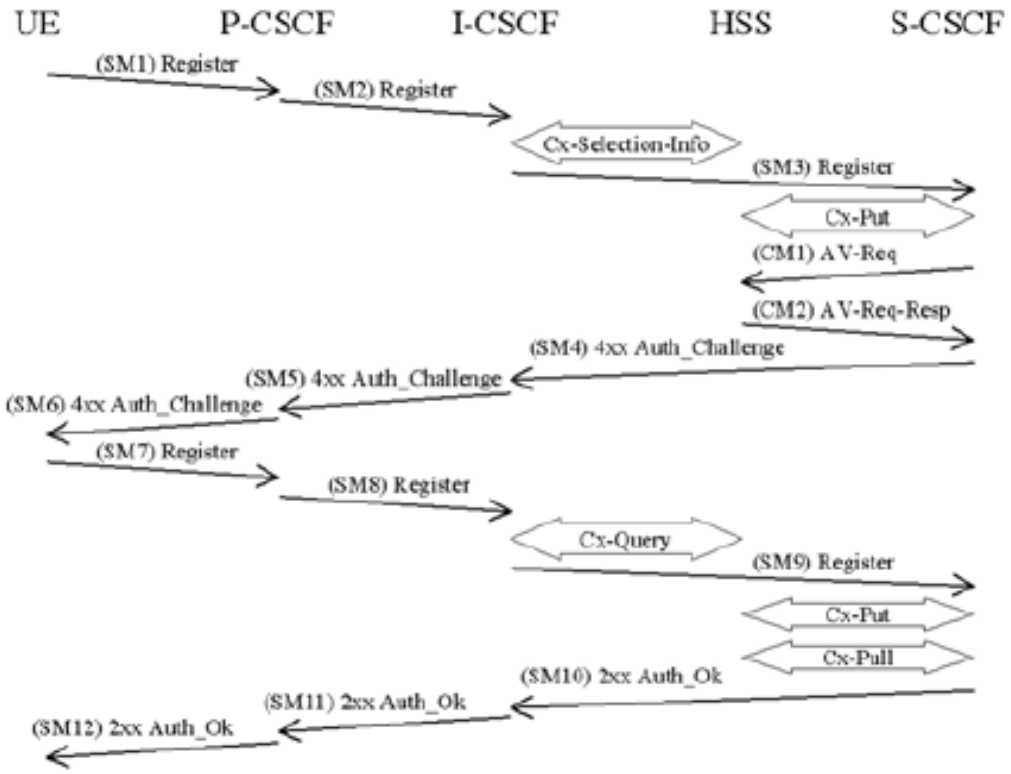
Αναλυτικότερα, η ύπαρξη αυτών των πέντε διαφορετικών συνάψεων αποσκοπεί στην εξυπηρέτηση διαφορετικών αναγκών προστασίας, όπως

- της αμοιβαίας αυθεντικοποίησης μεταξύ των ταυτοτήτων IM Services Identity Module (ISIM) και Home Subscriber Server (HSS) μέσω της συνάρτησης Serving Call Session Control Function (S-CSCF),
- της αυθεντικοποίησης του σημείου αναφοράς πρόσβασης δικτύου (Gm) και της εδραίωσης μιας ασφαλούς σύνδεσης μεταξύ της UE και της συνάρτησης Proxy Call Session Control Function (P-CSCF),
- της ασφαλείας του τομέα δικτύου (Cx) μεταξύ της ταυτότητας HSS και των συναρτήσεων Interrogating Call Session Control Function (I-CSCF) και SCSCF,
- της ασφαλείας του τομέα δικτύου (Mw) και των κόμβων που συνδέονται μέσω του πρωτοκόλλου Session Internet Protocol (SIP) είτε ανήκουν στο δίκτυο Visited Network (VN) είτε στο Home Network (HN).

Πανεπιστήμιο Πειρ

Ασφαλής πρόσβαση στο υποσύστημα IMS

Για να εξασφαλιστεί η αμοιβαία αυθεντικοποίηση μεταξύ του χρήστη και του HN χρησιμοποιείται η διαδικασία IMS AKA, η οποία υλοποιεί ουσιαστικά το ίδιο σενάριο με την προαναφερόμενη διαδικασία UMTS/EPS AKA και βασίζεται στη δημιουργία ενός πλαισίου ασφαλείας, το οποίο με τη σειρά του ενεργοποιείται με την καταχώρηση μιας συσκευής UE στο υποσύστημα IMS CN και πριν από την έγκριση της πρόσβασης, με τη συνολική διαδικασία να απεικονίζεται στο ακόλουθο διάγραμμα, με την αίτηση καταχώρησης να γίνεται με την αποστολή ενός μηνύματος SIP προς το IMS CN και το οποίο δρομολογείται μέσω του S-CSCF.



Εικόνα 6: Successful IMS AKA procedure (3GPP TS 33.203 V8.2.0, 2008-12)

Ανάκτηση δεδομένων αυθεντικοποίησης

Η συγκεκριμένη ανάκτηση λαμβάνει χώρα μετά από σχετική αίτηση της S-CSCF στο υποσύστημα IMS CN, η οποία αποστέλλεται μέσω της διεπαφής Cx. Η αίτηση αυθεντικοποίησης CM1 (CM1: Cx-AV-Req) περιλαμβάνει τις ταυτότητες IP Multimedia Private Identity (IMPI), IP Multimedia Public Identity (IMPU) και τον αριθμό των διανυσμάτων AV τα οποία η συνάρτηση SCSCF είναι προετοιμασμένη κάθε φορά να λάβει.

Ως απόδειξη της λήψης της αίτησης ο HSS επιστρέφει ένα ή περισσότερα διανύσματα IMS AVs μέσω της απόκρισης CM2 (CM2: Cx-AV-Req-Resp) η οποία αποτελείται από τις ακολουθίες RAND, XRES, AUTN, CK και IK σε συγκεκριμένη διάταξη. Κάθε διάνυσμα AV είναι έγκυρο για μια και μόνο συναλλαγή μεταξύ των S-CSCF και UE.

Αυθεντικοποίηση UE

Η διαδικασία αρχικοποιείται από τη S-CSCF, η οποία αν δεν διαθέτει έγκυρο διάνυσμα IMS AV, αποστέλλει μια σχετική αίτηση στον HSS. Στη συνέχεια, η S-CSCF επιλέγει ένα διάνυσμα από τη σχετική λίστα που ανακτάται από τον HSS και αποστέλλει μια πρόκληση αυθεντικοποίησης στον P-CSCF με τις παραμέτρους RAND, AUTN, IK και CK. Η P-CSCF αποθηκεύει το διάνυσμα AV και προωθεί την πρόκληση αυθεντικοποίησης στην UE χωρίς τις παραμέτρους IK και CK. Στη συνέχεια η UE θα πρέπει να απαντήσει σχετικά με την επιτυχία της διαδικασίας (με την απάντηση να περιλαμβάνει την ακολουθία XRES). Ταυτόχρονα, οι ακολουθίες κλειδιών CK και IK υπολογίζονται στην UE.Η απόκριση αυθεντικοποίησης λαμβάνεται από την P-CSCF και προωθείται στην S-CSCF. Η διαδικασία IMS AKA ολοκληρώνεται επιτυχώς με τον έλεγχο της ακολουθίας XRES από την S-CSCF και συνεπάγεται την καταχώρηση της UE στο υποσύστημα IMS CN.

Πανεπιστήμιο Πειραιώς

5.3.3 Τα «βήματα» της συνολικής διαδικασίας

Για να αποσαφηνιστεί το σύνολο των προαναφερόμενων πληροφοριών, επιχειρείται στην παρούσα ενότητα να καταγραφεί το σύνολο των διακριτών βημάτων της διαδικασίας ασφαλείας και κατ' επέκταση αυθεντικοποίησης. Όπως προκύπτει από τη συνολική θεώρηση της διαδικασίας, στον τομέα της ασφάλειας στα δίκτυα LTE, βασικό ρόλο διαδραματίζει η οντότητα Mobility Management Entity (MME) η οποία αποτελεί τον ελεγκτή του δικτύου. Πρόκειται για εκείνη τη μονάδα του συστήματος που όταν ζητηθεί από κάποιο χρήστη – συνδρομητή η σύνδεσή του στο δίκτυο αναλαμβάνει την αυθεντικοποίησή του.

Τα διακριτά λοιπόν βήματα της διαδικασίας έχουν ως εξής:

- Η κάρτα USIM είναι προγραμματισμένη με ένα μυστικό κλειδί K.
- Το συγκεκριμένο κλειδί αποθηκεύεται επίσης στον Home Subscription Server (HSS)
- Η συσκευή του χρήστη User Equipment (UE) προκειμένου να εδραιώσει μια σύνδεση με το δίκτυο, αποστέλλει ένα αρχικό Non- Access Stratum (NAS) μήνυμα στην MME. Τα μηνύματα αυτού του τύπου αφορούν στην αποστολή δεδομένων που γίνεται βάσει πρωτοκόλλων που λειτουργούν διαφανώς ως προς τα επίπεδα ασύρματης μετάδοσης
- Η MME ζητά μέσω του πρωτοκόλλου DIAMETER ζητά πιστοποιήσεις ασφαλείας από τη NME.
- Ο HSS εξάγει τις παραμέτρους K - ASME (Access Security Management Entity), AUTN (Authentication token), XRES (Expected Authentication Result) και RAND (A random number) από το κλειδί K. Αναφορικά με την οντότητα ASME, όπως αυτή ορίζεται στο πρωτόκολλο 3GPP TS 33.401 (2008-12), είναι εκείνη σε επίπεδο ελέγχου πρόσβασης λαμβάνει τα σημαντικότερα κλειδιά από τον HSS.
- Ο HSS διαβιβάζει το συγκεκριμένο σετ παραμέτρων στη MME
- Η MME εξάγει τα κλειδιά K-NAS-enc (κλειδί κρυπτογράφησης του επιπέδου - NAS layer encryption key), K-NAS-int (κλειδί προστασίας ακεραιότητας του επιπέδου NAS layer intergrity protection key) και K-eNB (κλειδί του κόμβου eNodeB).

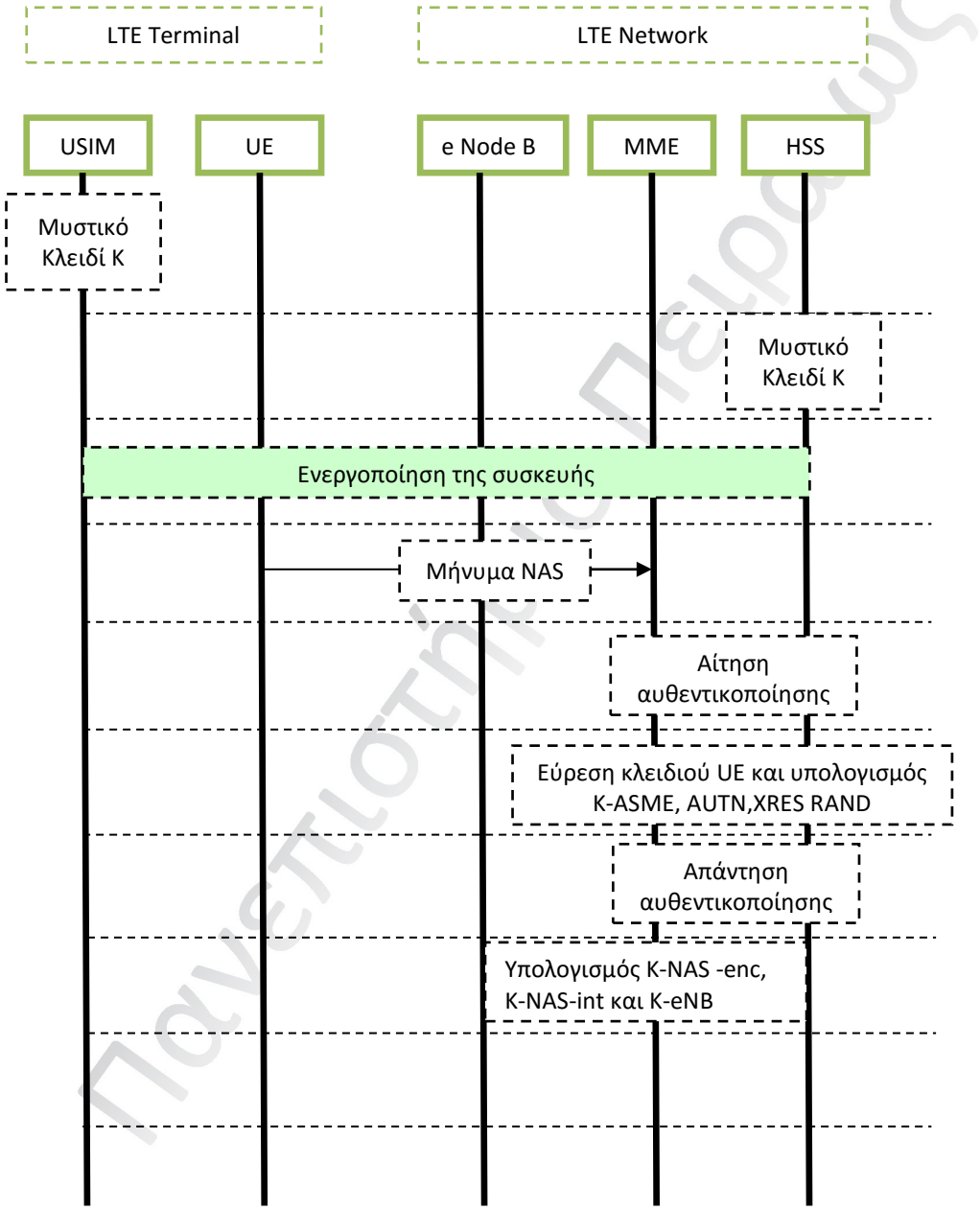
Πανεπιστήμιο Πειραιώς

- Η MME αποστέλλει μια μη κρυπτογραφημένη αίτηση αυθεντικοποίησης στο UE, η οποία περιέχει τις τιμές των παραμέτρων RAND και AUTN.
- Η UE διαβάζει το κλειδί K από τη USIM.
- Η UE υπολογίζει το αποτέλεσμα της αυθεντικοποίησης (RES), σύμφωνα με τις τιμές των K and the received AUTN and RAND values και το αποστέλλει πίσω στη MME.
- Η MME συγκρίνει την τιμή της RES που έλαβε από τη UE και τη συγκρίνει με την τιμή XRES, όπως αυτή ορίζεται από τον HSS. Σε περίπτωση που αυτές οι δύο τιμές είναι ίδιες η MME προχωρά στη διαδικασία ασφαλείας του επιπέδου NAS.

- Η αρχικοποίηση της διαδικασίας ασφαλείας του επιπέδου NAS γίνεται με την αποστολή του κλειδιού K-ASME στη UE, με το μήνυμα που αποστέλλεται να συμπεριλαμβάνει τους αλγόριθμους κρυπτογράφησης και ακεραιότητας.
- Η UE μέσω του κλειδιού K-ASME και του αλγορίθμου ακεραιότητας (Encapsulating Security Payload (EPS) εξάγει το κλειδί ακεραιότητας του επιπέδου NAS. Στη συνέχεια απαντά στη MME αποστέλλοντας το μήνυμα με το μήνυμα NAS να είναι τώρα κρυπτογραφημένο και να έχει προστασία ακεραιότητας.
- Η MME αρχικοποιεί ένα γενικό πλαίσιο ασφαλείας με τον κόμβο eNodeB, με τισδυνατότητες ασφαλείας και το κλειδί K-eNB να αποστέλλονται στον κόμβο eNodeB.
- Ο κόμβος eNodeB εξάγει τα κλειδιά κρυπτογράφησης του ελεγκτή της ραδιοζεύξης RRC και της προστασίας της ακεραιότητας από τα κλειδί K-eNB key.
- Ο κόμβος eNodeB εισάγει την εντολή περί εισόδου σε κατάσταση ασφαλείας στη UE μέσω ενός μηνύματος που περιλαμβάνει την προστασία ακεραιότητας AS, τους αλγόριθμους κρυπτογράφησης και τις παραμέτρους έναρξης (START).
- Η UE χρησιμοποιεί το κλειδί K-ASME και τον αλγόριθμο κρυπτογράφησης AS προκειμένου να δημιουργήσει τα κλειδιά κρυπτογράφησης RRC και User Plane.
- Παράλληλα, χρησιμοποιεί επίσης το κλειδί K-ASME και τον αλγόριθμο ακεραιότητας AS, προκειμένου να «αποφασίσει» το κλειδί προστασίας ακεραιότητας του RRC.

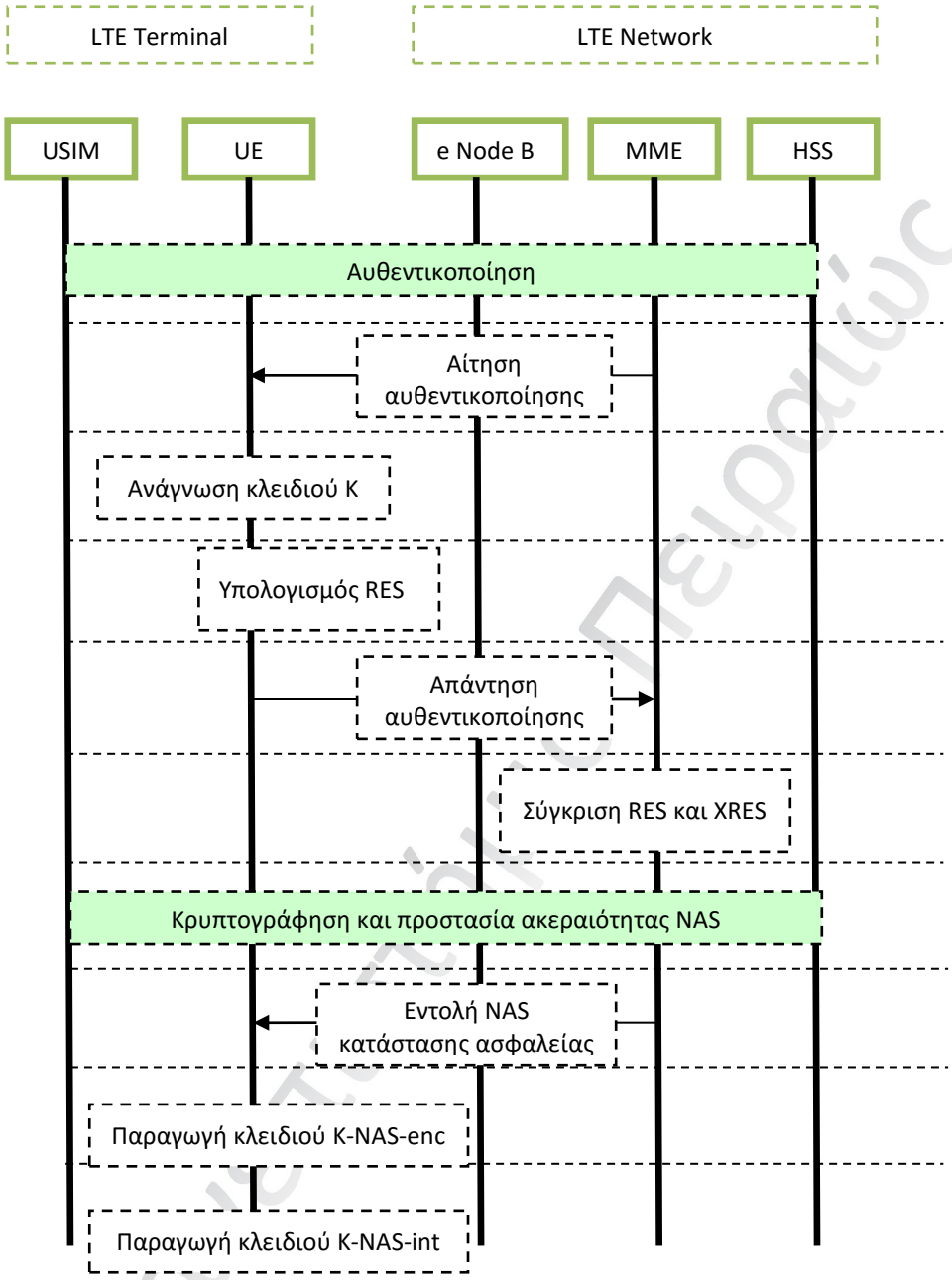
Πανεπιστήμιο Πειραιώς

- Η UE ανταποκρίνεται επιτυχώς, με το μήνυμα να περιλαμβάνει τα πρόσφατα ενεργοποιημένα κλειδιά κρυπτογράφησης και προστασίας ακεραιότητας.
- Ο κόμβος eNodeB απαντά πίσω στη MME σηματοδοτώντας ουσιαστικά την επιτυχή εδραίωση του πλαισίου ασφαλείας.



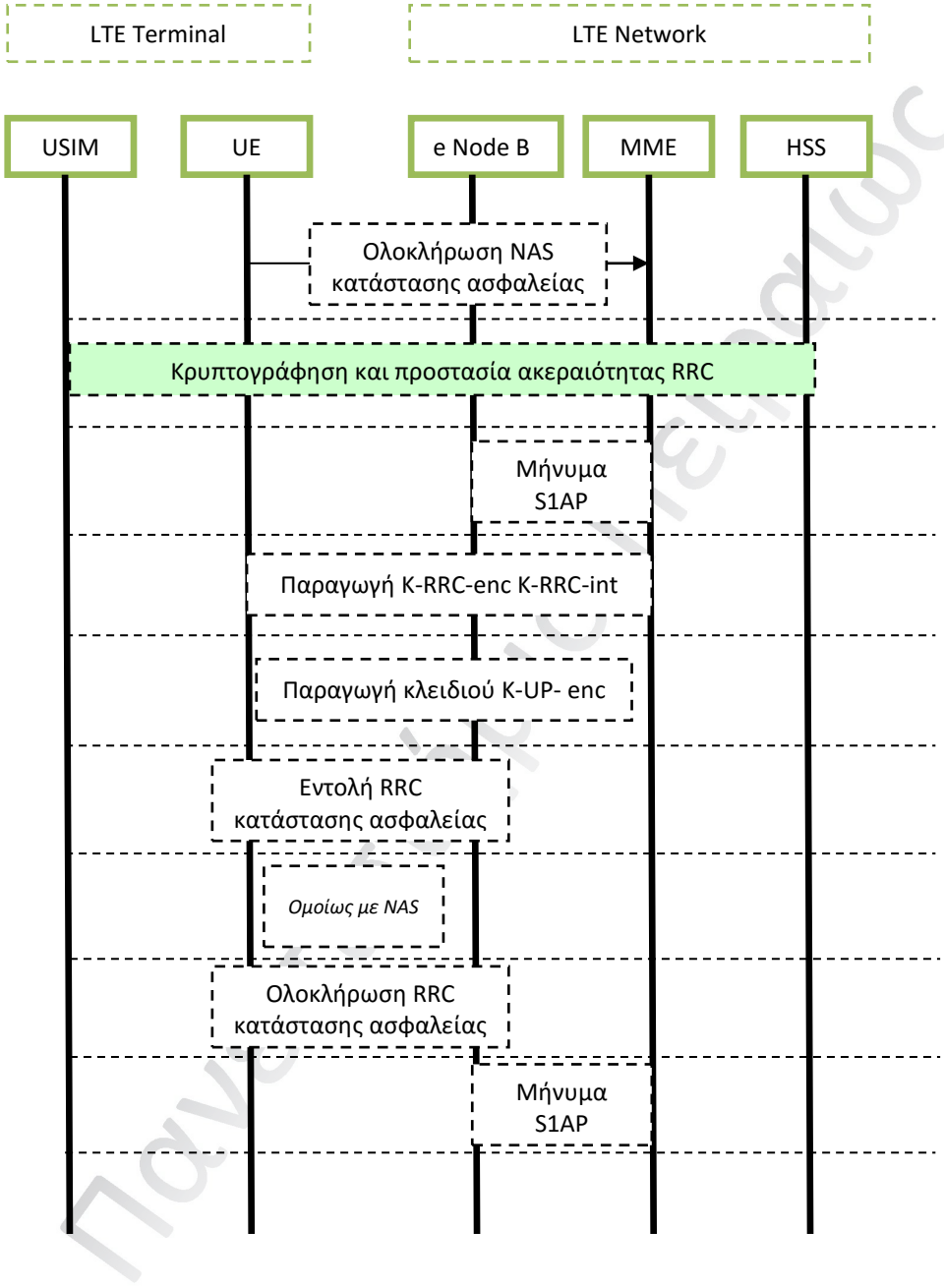
Διάγραμμα 23: Μηχανισμός ασφαλείας σε ένα δίκτυο LTE (1/3)

Πανεπιστήμιο Πειραιώς



Διάγραμμα 24: Μηχανισμός ασφαλείας σε ένα δίκτυο LTE (2/3)

Πανεπιστήμιο Πειραιώς



Διάγραμμα 25: Μηχανισμός ασφαλείας σε ένα δίκτυο LTE (3/3) (EventHelix.com Inc, 2012)

5.3.4 Αδύνατα σημεία μηχανισμών ασφαλείας κινητής τηλεφωνίας τέταρτης γενιάς

Επίπεδη αρχιτεκτονική

Ένα βασικό πρόβλημα του συστήματος ασφαλείας κινητής τηλεφωνίας τέταρτης γενιάς αποτελεί η επίπεδη αρχιτεκτονική του συστήματος, με τον όρο επίπεδη να προκύπτει από το γεγονός ότι μια MME εξυπηρετεί διάφορους κόμβους eNBs (Evolved Node B) εξοπλισμός – σταθμός βάσης που συνδέεται στο κινητό τηλεφωνικό δίκτυο και επικοινωνεί απευθείας με τις κινητές συσκευές UEs). Έτσι, μια επίδοξη επίθεση δεν έχει να εξαπλωθεί σε μια πολύπλοκη διαστρωμάτωση αλλά να ακολουθήσει ευθείες διαδρομές, με τον κίνδυνο να μεγιστοποιείται σε περίπτωση μετάπτωσης μιας UE σε μια νέα σύνδεση Home eNB/eNB.

Προβλήματα στη διαδικασία πρόσβασης

- Η διαδικασία EPS-AKA χαρακτηρίζεται από έλλειψη της προστασίας ιδιωτικότητας, αφού η ταυτότητα IMSI δε μπορεί να ανακτηθεί από την ταυτότητα GUTI.
- Οι επιθέσεις τύπου DoS δεν είναι δυνατό να παρεμποδιστούν επειδή η MME πρέπει να προωθήσει την αίτηση της UE στον HSS/AuC πριν από την αυθεντικοποίηση της UE, μια διαδικασία η οποία ξεκινά μόνο όταν λαμβάνεται η ακολουθία RES από τη MME.
- Το δίκτυο SN θα πρέπει να επιστρέψει στο δίκτυο HN για να αιτηθεί ένα νέο σετ διανυσμάτων αυθεντικοποίησης, όταν η UE παραμένει στο SN για μεγάλη περίοδο, με αποτέλεσμα ανεπιθύμητη κατανάλωση σηματοδότησης και εύρους ζώνης.
- Η διαδικασία EPS-AKA δεν περιλαμβάνει την online αυθεντικοποίηση, αφού η λειτουργία του HN κατά την επικοινωνία UE και SN γίνεται off-line.
- Το ίδιο το πρωτόκολλο EAP-AKA (Extensible Authentication Protocol – AKA) παρουσιάζει σχετικές αδυναμίες όπως η ευπάθεια σε επιθέσεις τύπου MitM (man-in-the-middle), κατά τις οποίες ο κακόβουλος host παρεμβαίνει μεταξύ των δύο προς επικοινωνία μερών και η επαναχρησιμοποίηση της διαδικασίας EAP-AKA για την υλοποίηση της αυθεντικοποίησης.

Προβλήματα στη διαδικασία μεταγωγής

- Έλλειψη ασφαλείας σε διαδρομές «προς τα πίσω»: η αναπαραγωγή νέων κλειδιών από τον κόμβο eNB προς νέους eNBs με την προσθήκη συγκεκριμένων παραμέτρων στα υπάρχοντα κλειδιά.
- Ευπάθεια σε επιθέσεις αποσυγχρονισμού: Μέσω της κακόβουλου eNB μπορεί να διακοπεί η διαδικασία ανανέωσης της τιμής NCC (NH Chaining Count) μέσω ελέγχου του μηνύματος αίτησης μεταγωγής μεταξύ των eNBs ή μεταξύ της MME και του eNB.

Προβλήματα ασφαλεία του συστήματος IMS

- Αυξημένη κατανάλωση πόρων της UE και αυξημένη πολυπλοκότητα του συστήματος αφού η UE χρειάζεται να εκτελέσει δύο διαφορετικές διαδικασίες αυθεντικοποίησης (πρωτόκολλα AKA), μία για το επίπεδο πρόσβασης (EPS AKA) και μία για το σύστημα IMS (IMS AKA).
- Ευπάθεια σε επιθέσεις τύπου DoS (Denial-of-service attack), κατά τις οποίες μια υπηρεσία ή ένας υπολογιστής καθίσταται ανικανος να εξυπηρετήσει άλλους πελάτες. Κατά τη λήψη μιας αίτησης καταχώρησης από μια IMS UE, η P-CSCF/MME αποστέλλει την αίτηση στο δίκτυο (I-CSCF/S-CSCF/HSS) προκειμένου να εφαρμοστεί η διαδικασία αυθεντικοποίησης πρόσβασης με τη συγκεκριμένη υπηρεσία να μπορεί να «προσβληθεί» μέσω της αποστολή μη έγκυρων ταυτοτήτων IMSI/IMPI.

Ευπάθεια στις υπηρεσίες MTC (Machine to Machine (M2M) communication)

- Οι συσκευές MTC είναι εκ κατασκευής ευάλωτες σε διάφορες επιθέσεις αφού χαρακτηρίζονται από ζητούμενα χαμηλής κατανάλωσης ενέργειας και υπολογιστικών πόρων.
- Η ταυτόχρονη αυθεντικοποίηση ενός αριθμού συσκευών MTC επιβαρύνουν τη διαδικασία σηματοδοσίας μεταξύ του HSS και της MME, εξαιτίας των ταυτόχρονων αιτήσεων πρόσβασης στο δίκτυο.

Πανεπιστήμιο Πειραιώς

5.3.5 Προτεινόμενες Λύσεις – Πεδία περαιτέρω έρευνας

- Με την κατάλληλη διαμόρφωση του πρωτοκόλλου EPS-AKA (Koien, 2011), μπορεί να χρησιμοποιηθεί μια ταυτότητα ESIM αντί της USIM προκειμένου να είναι δυνατή μια αμοιβαία απευθείας και online αυθεντικοποίηση μεταξύ της ESIM και της MME/HSS.
- Μια ενισχυμένη μορφή του πρωτοκόλλου EPS-AKA (Purkhiabani and Salahi, 2011) μπορεί να μειώσει την ανεπιθύμητη κατανάλωση εύρους ζώνης με την αύξηση των υπολογισμών στο επίπεδο SN. Οι υπολογισμοί αυτοί περιλαμβάνουν την παραγωγή και την αποθήκευση διανυσμάτων (AVs) από την SN/MME (τα οποία θα προκύπτουν από τα αντίστοιχα διανύσματα του HN/HSS).
- Η εφαρμογή ενός υβριδικού σεναρίου αυθεντικοποίησης και συμφωνίας κλειδιών βασισμένο στην πλατφόρμα Trust Model Platform (TMP) και στην υποδομή Public Key Infrastructure (PKI) (Zheng et al., 2005),, μπορεί να προσφέρει ευρωστία στο σύστημα, ειδικά όσον αφορά στη διαχείριση κινητών χρηστών και ευαίσθητων δεδομένων, με τη χρήση κωδικών ασφαλείας και δακτυλικών αποτυπωμάτων.
- Ένα εναλλακτικό σενάριο αυθεντικοποίησης και συμφωνίας κλειδιών βασισμένο στο κλειδί self-certified public key (SPAKA) (He, Wang and Zheng, 2008), μπορεί να χρησιμοποιηθεί προκειμένου μέσω ενός πρωτοκόλλου δημοσίου κλειδιού μια UE να ταυτοποιήσει έναν αυθεντικό σταθμό βάσης.
- Ένας μηχανισμός αυθεντικοποίησης και συμφωνίας κλειδιών (Security Enhanced Authentication and Key Agreement (SE-EPS AKA)) βασισμένο στην υποδομή Wireless Public Key Infrastructure (WPKI) (Li and Wang, 2011), μπορεί να εξασφαλίσει της ασφάλεια της ταυτότητας του χρήστη και του ανταλλασσόμενου μηνύματος με τη χρήση κρυπτογραφίας Ellipse Curve Cipher (ECC).
- Ενδυνάμωση του μηχανισμού προστασίας μπορεί να επιτευχθεί με τη χρήση του πρωτοκόλλου password authentication key exchange by Juggling (J-PAKE) (Vintila, Patriciu and Bica, 2011), το οποίο μπορεί να αντικαταστήσει το αντίστοιχο EPS-AKA protocol, με βασικό πλεονέκτημά του, τη χρήση ενός μοιρασμένου κλειδιού το οποίο δεν αποστέλλεται στο υφιστάμενο μέσο μετάδοσης.

Πανεπιστήμιο Πειραιώς

- Μια εναλλακτική διαδικασία αυθεντικοποίησης και συμφωνίας κλειδιών μπορεί να εξασφαλίσει παγκόσμια κινητικότητα με χαμηλή υπολογιστική ισχύ και ασφαλή επικοινωνία. Η συγκεκριμένη διαδικασία (Zheng et al., 2005), περιλαμβάνει τη χρήση ενός δυναμικού κωδικού με ένα δημόσιο κλειδί για την επίτευξη αμοιβαίας αυθεντικοποίησης μεταξύ της της UE και ενός foreign network (FN) χωρίς να είνα απαραίτητη η χρήση κάποιου πιστοποιητικού.
- Η χρήση μιας νέας υπηρεσίας αυθεντικοποίησης IMS που χρησιμοποιεί κρυπτογραφία Identity Based Cryptography (IBC) (Abid et al., 2009), μπορεί να ενισχύσει την ασφάλεια της διαδικασίας, επιτρέποντας την εξατομίκευση των υπηρεσιών IMS με τη χρήση των μηχανισμών IBC και ECC.
- Μια βελτιωμένη έκδοση πρωτοκόλλου AKA (Improved AKA (I-AKA)) μπορεί να εξοικονομήσει υπολογιστικούς πόρους (Gu and Gregory, 2011), με τη δέσμευση ασφαλείας μεταξύ του επιπέδου δικτύου και του επιπέδου αυθεντικοποίησης IMS. Σε μια τέτοια έκδοση, η χρήση ταυτότητας (IM Private Identity - IMPI) μπορεί να βοηθήσει στην αποφυγή της ταυτόχρονης διπλής εκτέλεσης του πρωτοκόλλου AKA.
- Μέσω μιας διαδικασίας αυθεντικοποίησης και συμφωνίας κλειδιών που βασίζεται στην ομαδοποίηση των UEs που ανήκουν στο ίδιο HN μπορούν επίσης να εξοικονομηθούν υπολογιστικοί πόροι (Chen et al., 2010), αφού όταν η πρώτη UE μιας τέτοιας ομάδας μετακινηθεί στο SN, το δίκτυο SN αποκτά τις πληροφορίες αυθεντικοποίησης σχετικά όχι μόνο με τη συγκεκριμένη UE αλλά με ολόκληρη την ομάδα. Έτσι, δεν απαιτείται η εκ νέου επικοινωνία με τον HN για την ανάκτηση πληροφοριών αυθεντικοποίησης.

Πανεπιστήμιο Πειραιώς

ΚΕΦΑΛΑΙΟ 6: ΣΥΜΠΕΡΑΣΜΑΤΑ

Η πτυχιακή αυτή έχει σαν σκοπό να παρουσιάσει την εξέλιξη των δικτύων κινητής τηλεφωνίας δεύτερης, τρίτης και τέταρτης γενιάς από την οπτική γωνία της ασφάλειας. Περιλαμβάνει μια εισαγωγή στα 2G, 3G και 4G δίκτυα και περιγράφονται τα βήματα αυθεντικοποίησης του κινητού στην εκάστοτε τεχνολογία.

Το UMTS είναι μια λογική εξέλιξη στον τομέα των τηλεπικοινωνιών και έρχεται να καλύψει την ανάγκη για νέες υπηρεσίες, πολυμεσικό περιεχόμενο και όλα αυτά σε λογικό κόστος και υψηλές για την εποχή ταχύτητες. Δίνει επίσης τη δυνατότητα να έχει ο χρήστης τη δυνατότητα για πρόσβαση στο διαδίκτυο κάτι το οποίο βάζει σε νέο επίπεδο της τηλεπικοινωνίες και τις υπηρεσίες που προσφέρονται, καθώς το κινητό τηλέφωνο γίνεται ένας προσωπικός υπολογιστής τσέπης. Όλα αυτά όμως δημιουργούν και νέες ανάγκες στον τομέα της ασφάλειας.

Η ασφάλεια στο UMTS στηρίζεται στο GSM, με τη διατήρηση και βελτίωση των σημαντικών χαρακτηριστικών γνωρισμάτων ασφάλειας του. Το UMTS έχει πολλά πλεονεκτήματα ασφάλειας σε σχέση με το GSM, παρόλα αυτά όμως δε σημαίνει ότι δεν έχει και αδυναμίες από τη στιγμή που προσφέρει και υπηρεσίες διαδικτύου. Αυτά που μπορούν να συμβούν σε ένα προσωπικό υπολογιστή που είναι συνδεδεμένος στο διαδίκτυο, μπορούν να συμβούν και σε ένα τερματικό UMTS.

Το 4G (LTE) ,είναι ένα διαφορετικής λογικής δομημένο δίκτυο. Έρχεται να καλύψει τις ανάγκες των συνδρομητών για μεγαλύτερες ταχύτητες στο διαδίκτυο και η αρχιτεκτονική του είναι βασισμένη σε All-IP περιβάλλον. Αναλύονται και εδώ τα πλεονεκτήματα και οι αδυναμίες σε σχέση με το UMTS. Τα δίκτυα τέταρτης γενιάς (WiMAC και LTE), έχουν αδυναμίες σε φυσικό επίπεδο από παρεμβολές και τεχνικές κρυπτογράφησης (scrambling techniques). Το LTE, έχει ευπάθειες και σε επίπεδο MAC, όπως παράνομη χρήση κινητού εξοπλισμού και χρήστη, εντοπισμού θέσης (location tracking) ,επιθέσεις άρνησης υπηρεσίας (DoS) και επιθέσεις ακεραιότητας πληροφορίας (data integrity attacks).

Πανεπιστήμιο Πειραιώς

Τέλος, τα δίκτυα τέταρτης γενιάς χρησιμοποιούν ανεπτυγμένες μεθόδους αυθεντικοποίησης (advanced security) σε σχέση με τους προκατόχους του αλλά ακόμα υπάρχουν στοιχεία που χρήζουν βελτίωσης. Θα ήταν χρήσιμο να υπάρξει αύξηση της έρευνας σε δοκιμαστικό περιβάλλον (test-bed), με την οποία θα ήταν πολύ πιθανό να αποκαλυφθούν περαιτέρω ζητήματα και προκλήσεις που θα πρέπει να αντιμετωπιστούν.

Πανεπιστήμιο Πειραιώς

Βιβλιογραφία

- P. Flichy, «Η Ιστορία της Σύγχρονης Επικοινωνίας» Εκδόσεις Κάτοπτρο, Ιούλιος 2004
- Σ. Κωτσόπουλος, Γ.Καραγιαννίδης, «Κινητή Τηλεφωνία» Εκδόσεις Παπασωτηρίου, 1997
- Μάγκος Ε., Παρουσίαση με τίτλο Δίκτυα Η/Υ – Ασύρματα Δίκτυα, Ιόνιο Πανεπιστήμιο, Τμήμα Αρχειονομίας – Βιβλιοθηκονομίας, 2008
- J. P. Castro «The UMTS Network and Radio Access Technology: Air Interface Techniques for Future Mobile Systems» John Wiley & Sons Ltd, p.30-33, 2001
- Εφημερίδα Καθημερινή, Άρθρο με τίτλο «Ο κλάδος κινητής τηλεφωνίας στην Ελλάδα τρίτος σε επενδύσεις στην Ευρώπη, παρά την κρίση», διαθέσιμο στην ηλεκτρονική διεύθυνση, http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_01/10/2012_463908, [Πρόσβαση 19/09/13]
- A. Pashtan, '6.108.10 Wireless Terrestrial Communications : Cellular Telephony', 2006
- S. Redl, 'An introduction to GSM', Artech House Publishers, 1995
- M. Kahabka, "Pocket Guide for Fundamentals and GSM Testing", Wandel & Goltermann GmbH & Co, Communications Test Solutions, 1998
- R. Keller General Packet Radio Service (GPRS), available at http://misnt.indstate.edu/harper/Students/GPRS/GPRS.html [Accessed 10/12/13]
- J. Korhonen «Introduction to 3G Mobile Communications» Second Edition, Artech House Publishers, 2003
- D. Astely, E. Dahlman, A. Furuskar, Y. Jading, M. Lindstrom, S. Parkvall, "LTE – The Evolution of Mobile Broadband" , IEEE Communications Magazine April 2009
- A. Larmo , M. Lindström , M. Meyer , G. Pelletier , J. Torsner , H. Wiemann, "The LTE Link- Layer Design" , IEEE Communications Magazine April 2009

Πανεπιστήμιο Πειραιώς

- A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, and T. Thomas ,"LTE-Advanced Next-Generation Wireless Broadband Technology", IEEE Communications Magazine June 2010
- M. Alasti, B. Neekzad, J. Hui and R. Vannithamb, "Quality of Service in Wi-Max of Service and LTE Networks", IEEE Communications Magazine May 2010
- O. Oyman, J. Foerster, Intel Corporation; Y. Tcha and S. C. Lee, "Toward Enhanced Mobile Video Services" , IEEE Communications Magazine August 2010
- S. Parekh, EE228a - Lecture 6 - Spring 2006 IEEE 802.16 / WiMAX, available at http://walrandpc.eecs.berkeley.edu/228S06/L6.pdf [Accessed 10/12/13]
- GSV R. K. Rao & G. Radhamani, WiMAX, A Wireless Technology Revolution, Auerbach Publications, 2008
- A. S.Tanenbaum, «Computer Networks» Fourth Edition, 2003
- S. Singh, "Κώδικες και μυστικά», Εκδόσεις Τραυλός, 2008
- Federal Information Processing Standards Publication 46-3, "Data Encryption Standard", U.S Department of Commerce/National Institute of Standards and Technology, (1999), available at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf [Accessed 12/12/13]
- X. Lai, "On the design and security of block ciphers", ETH Series in Information Processing (J.L. Massey, ed.), Vol. 1, Hartung-Gorre Verlag Konstanz, Technische Hochschule (Zurich), 1992.
- R. Baldwin, R. Rivest, "The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms" RFC2040, 1996
- C. Adams, "The CAST-128 Encryption Algorithm" RFC2144, May 1997
- Federal Information Processing Standards Publication 197, "Announcing the Advanced Encryption Standard (AES)", NIST, 2001
- RSA Laboratories, PKCS#1 v2.1, "RSA Cryptography Standard, RSA" Security Inc., 2002 available at http://www..rsasecurity.com/rsalabs/node.asp?id=2125 [Accessed 12/12/13]
- W.Diffie, P. van Oorschot and M. Wiener, "Authentication and authenticated key exchanges", Designes, Codes and Cryptography, 1992

Πανεπιστήμιο Πειραιώς

- Icsa Labs, WLAN Testing Reports Debunking the Myth of SSID Hiding, Robert Moskowitz, Senior Technical Director, 2003
- Cisco IOS Software, Configuring Authentication Types, 2004
- R. Yahalom, B. Klein, Th. Beth, Trust Relationships in secure systems –Adistributed Authentication Perspective, IEEE Symposium on Security and Privacy, 1993
- A. Perrig, R. Szewezyk, V. Wen, D. Culler, J D. Tygar, SPINS: Security Protocols for Sensor Networks, ACM, 2002
- P. Rysavy, Secure Mobile Access Using SSL VPNs, Rysavy Research, Sep 2003
- Πανεπιστήμιο Αιγαίου (2007), Παρουσίαση με τίτλο «Ασφάλεια Ασύρματων και Κινητών Επικοινωνιών», Κινητές Επικοινωνίες Μέρος Ι, διαθέσιμη στην ηλεκτρονική διεύθυνση http://www.icsd.aegean.gr/website_files/metaptyxiako/455439940.pdf [Πρόσβαση 18/09/13]
- G. Iosifidis (2013), Άρθρο Smartphones και ασφάλεια/ ανάκτηση δεδομένων, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.digitallife.gr/smartphones-security-89001 [Πρόσβαση 14/12/13]
- Ι.Κ. Μαυρίδης, Ημερίδα ΑΔΑΕ (Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών), Παρουσίαση με τίτλο Υπηρεσίες Ασφαλείας Κινητών Επικοινωνιών, Τμήμα Πληροφορικής Πανεπιστημίου Μακεδονίας, 2008
- V. Niemi, K. Nyberg, "UMTS Security", John Wiley & Sons 2003
- 3GPP TS 33.401 V8.2.1, 3GPP System Architecture Evolution (SAE); Security Architecture, 2008-12
- EventHelix.com Inc (2012), LTE Security Procedures Generated with EventStudio System Designer, available at http://www.EventHelix.com/EventStudio [Accessed 28/12/13]
- EventHelix.com Inc (2012), LTE Security Encryption and Integrity Protection in LTE, available at http://www.eventhelix.com/lte/security/lte-security-presentation.pdf [Accessed 28/12/13]
- M.Ma (2012), Security Investigation in 4G LTE Wireless Networks, School of Electrical and Electronic Engineering Nanyang Technological University, Singapore

Πανεπιστήμιο Πειραιώς

- Agilent Technologies (2009), LTE and the Evolution to 4G Wireless Design and Measurement Challenges Bonus Material: Security in the LTE-SAE Network
- 3GPP TS 33.401 V8.2.1 (2008-12), 3GPP System Architecture Evolution (SAE); Security architecture
- 3GPP TS 33.102 V8.1.0 (2008-12), 3G security; Security architecture
- 3GPP TS 23.003 V8.3.0 (2008-12), Technical Specification Group Core Network and Terminals; Numbering, addressing and identification
- 3GPP TS 24.301 V8.0.0 (2008-12), Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3
- 3GPP TS 29.272 V8.1.1 (2009-11) Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP TS 36.331 V8.4.0 (2008-12), Evolved Universal Terrestrial Radio Access (E-UTRA), Radio Resource Control (RRC); Protocol specification
- 3GPP TS 33.210 V8.2.0 (2008-12) 3G security; Network Domain Security (NDS); IP network layer security
- 3GPP TS 33.203 V8.5.0 (2008-12) 3G security; Access security for IP-based services
- 3GPP TS 23.003 V8.3.0 (2008-12), Technical Specification Group Core Network and Terminals; Numbering, addressing and identification
- RFC 4303 (2005) - IP Encapsulating Security Payload (ESP)
- G. M. Koien (2011), "Mutual Entity Authentication for LTE," Proceedings of 7th International Wireless Communications and Mobile Computing Conference (IWCMC), pp.689-694.
- M. Purkhiabani and A. Salahi (2011), "Enhanced Authentication and Key Agreement Procedure of Next Generation Evolved Mobile Networks," Proceedings of IEEE 3rd International Conference on Communication Software and Networks (ICCSN), pp.557-563.
- Y. Zheng, D. He, X. Tang and H. Wang (2005), "AKA and Authorization Scheme for 4G Mobile Networks Based on Trusted Mobile Platform," Proceedings of Fifth

International Conference on Information, Communications and Signal Processing, pp.976-980.

- D. He, J. Wang and Y. Zheng (2008), "User Authentication Scheme Based on Self-certified Public-key for Next Generation Wireless Network," Proceedings of Biometrics and Security Technologies (ISBAST 2008), pp.1-8.
- X. Li and Y. Wang (2011), "Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network," Proceedings of Wireless Communications, Networking and Mobile Computing (WiCOM), pp.1-4.
- C. Vintila, V. Patriciu and I. Bica (2011), "Security Analysis of LTE Access Network", Proceedings of The Tenth International Conference on Networks (ICN 2011), pp. 29-34.
- Y. Zheng, D. He, L. Xu and X. Tang (2005), "Security Scheme for 4G Wireless Systems," Proceedings of Communications, Circuits and Systems, pp. 397- 401.
- M. Abid, S. Song, H. Moustafa, and H. Afifi (2009), "Efficient Identity-based Authentication for IMS Based Services Access," Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia (MoMM '09), pp. 260-266.
- L. Gu and M.A. Gregory (2011), "A Green and Secure Authentication for the 4th Generation Mobile Network," Proceedings of Australasian Telecommunication Networks and Applications Conference (ATNAC), pp.1-7.
- Y. W. Chen, J. T. Wang, K. H. Chi and C. C. Tseng (2010), "Group-Based Authentication and Key Agreement", Wireless Personal Communications, 2010, pp. 1-15.

Πανεπιστήμιο Πειραιώς