ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΨΗΦΙΩΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΑΣΦΑΛΕΙΑ ΣΤΟ ΚΙΝΗΤΟ ΤΗΛΕΦΩΝΟ

ΚΑΛΙΑΚΟΥΔΑΣ ΧΡΗΣΤΟΣ

ΕΠΙΒΛΕΠΩΝ: ΑΝΑΠΛΗΡΩΤΗΣ ΚΑΘΗΓΗΤΗΣ,
ΞΕΝΑΚΗΣ ΧΡΗΣΤΟΣ

ΠΕΙΡΑΙΑΣ 2017

ΕΥΧΑΡΙΣΤΙΕΣ

Ο τίτλος της παρούσας διπλωματικής είναι: «Ασφάλεια Στο Κινητό Τηλέφωνο». Αυτή πραγματοποιήθηκε, στο πλαίσιο της διπλωματικής εργασίας του τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Στο σημείο αυτό, αισθάνομαι την ανάγκη να εκφράσω τις ειλικρινείς και θερμές ευχαριστίες μου σε όσους συνέβαλαν στην ολοκλήρωση αυτής της προσπάθειας :

Και πρώτα απ' όλα, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα της παρούσας μελέτης Δρ. Χρήστο Ξενάκη, καθηγητή στο τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς και πρόεδρο του μεταπτυχιακού "Ασφάλεια Ψηφιακών Συστημάτων", για την παρότρυνση στην επιλογή του συγκεκριμένου θέματος, την συνεχή καθοδήγηση και ενθάρρυνση, για την επίτευξη του βέλτιστου δυνατού αποτελέσματος, καθώς και για το χρόνο που μου αφιέρωσε.

Επίσης, βαθιά ευχαριστώ όλα τα μέλη της ομάδας του εργαστηρίου ασφάλειας, τόσο για τις πολύτιμες συμβουλές τους στα διάφορα στάδια της εργασίας αυτής. Πιο συγκεκριμένα τον Δρ. Χριστόφορο Νταντογιάν και τον υποψήφιο διδάκτορα Φαίδων Λαλαγιάννη.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου για τη στήριξη που μου προσφέρει από τα πρώτα χρόνια των σπουδών μου, ώστε να μπορώ να αφιερώνω όσο περισσότερο χρόνο,και ενέργεια γίνεται, στην περάτωση των σπουδών μου.

Σημαντικοί όροι:

PDA: Personal Digital Assistant, γνωστός ως φορητός υπολογιστής, είναι μια κινητή συσκευή που λειτουργεί ως διαχειριστής προσωπικών πληροφοριών.
GSM: Global System for Mobile communications (Παγκόσμιο Σύστημα Κινητών Επικοινωνιών), είναι ένα κοινό Ευρωπαϊκό ψηφιακό σύστημα κινητής τηλεφωνίας.
SMS: Short Message Service, είναι υπηρεσία της κινητής τηλεφωνίας, με την οποία ο χρήστης έχει τη δυνατότητα να αποστείλει ή να παραλάβει σύντομο γραπτό μήνυμα από άλλους χρήστες, στην οθόνη του κινητού του τηλεφώνου.
MMS: Multimedia Messaging Service, είναι ένας τυπικός τρόπος για την αποστολή μηνυμάτων που περιλαμβάνουν περιεχόμενο πολυμέσων από και προς κινητό τηλέφωνο μέσω κυψελοειδούς δικτύου.
TDMA: Time-Division Multiple Access, είναι μια μέθοδος πρόσβασης καναλιού για κοινόχρηστα δίκτυα.
HSCSD: High-Speed Circuit-Switched Data, ήταν ένα σύστημα που χρησιμοποιούνταν για κλήσεις δεδομένων σε δίκτυα GSM πριν από τη χρήση πακετοποιημένων συστημάτων όπως το GPRS και το EDGE.
3GPP: 3rd Generation Partnership Project, είναι μια συνεργασία μεταξύ ομάδων οργανισμών τηλεπικοινωνιών, γνωστών ως Οργανωτικοί Συνεργάτες.
RF: Radio Frequency, είναι οποιαδήποτε από τις συχνότητες των ηλεκτρομαγνητικών κυμάτων που κυμαίνονται μεταξύ 3 kHz και 300 GHz και περιλαμβάνουν τις συχνότητες που χρησιμοποιούνται στις ραδιοεπικοινωνίες ή στα ραντάρ.
SS7: Signalling System No. 7, είναι ένα σύνολο πρωτοκόλλων σηματοδοσίας τηλεφωνίας που αναπτύχθηκαν το 1975, το οποίο χρησιμοποιείται για την εγκατάσταση και τη διάδοση των περισσότερων τηλεφωνικών κλήσεων του δημόσιου τηλεφωνικού δικτύου (PSTN) παγκοσμίως.
PDN: Public Data Network, είναι ένα δίκτυο που δημιουργείται και λειτουργεί από μια εταιρία τηλεπικοινωνιών ή από αναγνωρισμένο ιδιωτικό φορέα εκμετάλλευσης, με συγκεκριμένο σκοπό την παροχή υπηρεσιών μετάδοσης δεδομένων για το κοινό.
PLMN: Public Land Mobile Network, είναι ένα δίκτυο το οποίο δημιουργείται και λειτουργεί από έναν αναγνωρισμένο φορέα εκμετάλλευσης για τον συγκεκριμένο σκοπό της παροχής υπηρεσιών εδάφους κινητών τηλεπικοινωνιών στο κοινό.
OFDM: Orthogonal Frequency-Division Multiplexing, είναι μια μέθοδος κωδικοποίησης ψηφιακών δεδομένων σε πολλαπλές συχνότητες φορέων.
WLAN: Wireless Local Area Network, είναι ένα ασύρματο δίκτυο υπολογιστών που συνδέει δύο ή περισσότερες συσκευές που χρησιμοποιούν ασύρματη επικοινωνία σε

μια περιορισμένη περιοχή όπως σπίτι, σχολείο, εργαστήριο ηλεκτρονικών υπολογιστών ή κτίριο γραφείων.

HLR: Home Location Register, είναι μια κεντρική βάση δεδομένων που περιέχει λεπτομέρειες για κάθε συνδρομητή κινητού τηλεφώνου που είναι εξουσιοδοτημένος να χρησιμοποιεί το δίκτυο πυρήνα GSM.

MITM: Man-In-The-Middle, είναι μια επίθεση όπου ο επιτιθέμενος εκπέμπει κρυφά και ενδεχομένως μεταβάλλει την επικοινωνία μεταξύ δύο μερών, που πιστεύουν ότι επικοινωνούν άμεσα μεταξύ τους.

eNB: E-UTRAN Node B, γνωστός επίσης ως Evolved Node B, είναι το στοιχείο στο E-UTRA του LTE που είναι η εξέλιξη του στοιχείου κόμβου B στο UTRA του UMTS.

MME: Mobility Management Entity, είναι ο βασικός κόμβος ελέγχου για το δίκτυο πρόσβασης LTE

UE: User Equipment, είναι οποιαδήποτε συσκευή που χρησιμοποιείται απευθείας από έναν τελικό χρήστη για επικοινωνία.

DoS: Denial-of-Service Attack, είναι μια επίθεση στον κυβερνοχώρο όπου ο δράστης επιδιώκει να καταστήσει μη διαθέσιμη μια πηγή μηχάνημα ή δίκτυο στους επιδιωκόμενους χρήστες, διακόπτοντας προσωρινά ή επ 'αόριστον τις υπηρεσίες ενός κεντρικού υπολογιστή συνδεδεμένου με το Διαδίκτυο.

DDoS: Distributed Denial of Service, είναι ένας τύπος επίθεσης DOS όπου πολλά συμβιβασμένα συστήματα χρησιμοποιούνται για να στοχεύσουν ένα ενιαίο σύστημα που προκαλεί επίθεση Denial of Service (DoS)

UMTS: Universal Mobile Telecommunications System**,** είναι ένα κινητό κυψελοειδές σύστημα τρίτης γενιάς για δίκτυα που βασίζονται στο πρότυπο GSM.

MS: Mobile Station, περιλαμβάνει όλο τον εξοπλισμό του χρήστη και το λογισμικό που απαιτείται για την επικοινωνία με ένα κινητό δίκτυο.

SGSN: Serving GPRS Support Node, είναι ένα κύριο συστατικό του δικτύου GPRS, το οποίο χειρίζεται όλα τα δεδομένα μεταγωγής πακέτων μέσα στο δίκτυο

DPI: Deep Packet Inspection,είναι μια μορφή φιλτραρίσματος πακέτων δικτύου υπολογιστών που εξετάζει το τμήμα δεδομένων (και ενδεχομένως και την κεφαλίδα) ενός πακέτου καθώς περνά ένα σημείο επιθεώρησης

CUSUM: CUmulative SUM control chart, είναι μια τεχνική διαδοχικής ανάλυσης, που χρησιμοποιείται για την ανίχνευση αλλαγών

CQI: Channel Quality Indicator, είναι ένας δείκτης που φέρει τις πληροφορίες σχετικά με το πόσο καλή / κακή είναι η ποιότητα του καναλιού επικοινωνίας.

SON: Self Organising Networks, είναι ουσιαστικής σημασίας για τα περίπλοκα κυψελοειδή δίκτυα σήμερα για να διαμορφώνουν, να οργανώνουν, να βελτιστοποιούν την απόδοση και να παρέχουν δυνατότητες αυτοθεραπείας όταν συμβαίνουν σφάλματα.

E2E: End-to-end encryption, είναι ένα σύστημα επικοινωνίας όπου μόνο οι επικοινωνούντες χρήστες μπορούν να διαβάσουν τα μηνύματα.

Περίληψη

Η εργασία αυτή παρουσιάζει τεχνολογίες δικτύων κινητής τηλεφωνίας και αναλύει την ασφάλεια της κάθε γενιάς. Αποτελείται από δυο μέρη. Στο πρώτο μέρος παρουσιάζονται οι τεχνολογίες δικτύων κινητής τηλεφωνίας, από την πρώτη τους γενιά (1G), μέχρι την τρέχουσα τεχνολογία (4G). Επίσης παρουσιάζεται η τεχνολογία 5G η οποία βρίσκεται σε ερευνητικό στάδιο και προτείνονται σημεία στα οποία θα πρέπει να εστιάσει το μοντέλο ασφάλειας για τις ιδιαίτερες ανάγκες του δικτύου αυτού. Γίνεται ανάλυση της κάθε υποδομής ξεχωριστά και της ασφάλειας που η κάθε μια παρέχει, καθώς και των ευάλωτων τους σημείων. Επίσης έχουμε προτείνει αντίμετρα, που θεωρήσαμε ως τα ιδανικά σε κάθε περίπτωση, για τις αδυναμίες που εντοπίσαμε. Στο δεύτερο μέρος παρουσιάζεται η τεχνολογία OPENBTS- USRP τόσο ως προς την δομή της και τις αδυναμίες της, όσο και στις χρήσεις της υποδομής, για επιθέσεις που έχουν γίνει σε εμπορικά δίκτυα κινητής, με αυτή.

Περιεχόμενα

1.1 Εισαγωγή **11**

1.1.1 Ιστορική Αναδρομή Στα Δίκτυα Κινητής Τηλεφωνίας 11

2. Τα Δίκτυα Κινητής Τηλεφωνίας **14**

2.1 0G - O.5G 14

2.2 Τεχνολογία 0.5G 15

2.3 1G **16**

2.4 2G **16**

2.4.1 Τεχνολογίες 2G 17

2.4.2 Ικανότητες, πλεονεκτήματα και μειονεκτήματα 19

2.4.2.1 Χωρητικότητα 19

2.4.2.2 2G χωρητικότητα μετάδοσης δεδομένων: 19

2.5 2.5G (GPRS) **21**

2.6 2.75G (EDGE) **21**

2.7 3G **22**

2.7.1 Αναλυτικά 23

2.8 4G **27**

2.8.1 Τεχνικές απαιτήσεις 27

2.9 5G **29**

3 Ασφάλεια στα Δίκτυα Κινητής Τηλεφωνίας **31**

3.1 Θέματα ευπαθειών, απειλές και σημεία εισβολής 31

3.1.2 Ενσωματωμένες έξυπνες κινητές συσκευές 32

3.1.3 Το Δίκτυο Πρόσβασης 33

3.1.4 Στο Δίκτυο Κορμού 34

3.1.5 Το εξωτερικό ή τρίτου μέρους δίκτυο (3rd Party Network) 36

3.2 Κατηγοριοποίηση των επιθέσεων σε δίκτυα κινητής τηλεφωνίας 37

4 Αδυναμίες ασφάλειας GSM **42**

4.1 Ιστορική αναδρομή των αλγορίθμων σπασίματος **43**

4.2 Δημοφιλή είδη επιθέσεων **45**

4.2.1 Καταγραφή ενός ή περισσότερων κινητών σταθμών 45

4.2.2 Επιθέσεις κατά της ανωνυμίας των χρηστών GSM 46

4.2.4 Ενεργός παρακολούθηση: 47

4.2.5 Επιθέσεις στον Αλγόριθμο αυθεντικοποίησης: 48
4.2.6 Κλωνοποίηση της SIM κάρτας με φυσική πρόσβαση: 49
4.2.7 Κλωνοποίηση πάνω στον αέρα: 49

4.3 Επιθέσεις στην εμπιστευτικότητα του GSM 51
4.3.1 Brute-Force Attacks 51
4.3.2 Επιθέσεις Κρυπτανάλυσης 52
4.3.3 Μη Κρυπτο-Αναλυτικές επιθέσεις: 54

4.4 Denial of Service (DoS) Attacks 55
4.4.1 Άρνηση παροχής υπηρεσιών - Φυσική παρέμβαση 55
4.4.2 Άρνηση παροχής υπηρεσιών - Λογική παρέμβαση 56

4.5 Ορισμένες χρήσιμες λύσεις κατά των επιθέσεων 57
4.5.1 Χρήση ασφαλών αλγορίθμων για υλοποιήσεις A3 / A8 57
4.5.2 Χρήση ασφαλών αλγόριθμων κρυπτογράφησης 57
4.5.3 Ασφάλεια από άκρη-σε-άκρη 58

5 Επιθέσεις στο 3G 59

5.1 Τι κάνει πιθανές τις επιθέσεις στο Δίκτυο 3G; 59

5.2 Πώς συμβαίνουν οι επιθέσεις σε δίκτυα 3G; 63

5.3 Ταξινόμηση επιθέσεων 64
5.3.1 Διάσταση 1: Φυσική πρόσβαση στο δίκτυο 64
5.3.2 Διάσταση 2: Κατηγορίες επιθέσεων 66
5.3.3 Διάσταση 3: Μέσα επίθεσης 67

6 Απειλές και επιθέσεις σε δίκτυα 4G 68

6.1 Επίθεση κατά της ασφάλειας και της εμπιστευτικότητας 69

6.2 IP-Based Επιθέσεις 77
6.2.1 IP-Based Επιθέσεις Ενάντια στο Backhaul 81
6.2.2 Επιθέσεις που βασίζονται στο GTP 82
6.2.3 VoLTE SIP-Based Attacks 84
6.2.4 Επιθέσεις που βασίζονται σε διάμετρο 85

6.3 Επιθέσεις σηματοδότησης 86

6.4 Επίθεση που βασίζεται σε παρεμβολές 91
6.4.1 Έξυπνη εμπλοκή 92
6.4.2 Μπλοκάρισμα θορύβου 93
6.4.3 Παρεμβολή πάνω σε κανάλι ελέγχου 94

6.5 Θέματα Ανοιχτά προς Έρευνα 98

7 Προκλήσεις ασφάλειας 5G 102

7.1 Παραδοσιακές πρακτικές ασφάλειας 102

7.2 Προκλήσεις ασφάλειας πριν από την 5G 103

7.2.1 Νέα επιχειρηματικά μοντέλα 103

7.2.2 Αρχιτεκτονική δικτύου με γνώμονα τις τεχνολογίες πληροφορικής 103

7.2.3 Ετερογενής πρόσβαση 104

7.2.4 Προστασία προσωπικών δεδομένων 105

7.3 Στόχοι Ασφάλειας στο 5G 105

7.3.1 E2E Ασφάλεια για Κατακόρυφες Βιομηχανίες 106

7.3.2 Ασφάλεια Υποδομών 107

7.4 Προοπτικές ασφάλειας 5G 107

7.4.1 Νέο μοντέλο εμπιστοσύνης και διαχείρισης ταυτότητας 107

7.4.2 Διαχείριση υβριδικού ελέγχου ταυτότητας 108

7.4.3 Διαφοροποιημένη διαχείριση ταυτότητας 109

7.5 Ασφάλεια προσανατολισμένη στις υπηρεσίες 110

7.5.1 Διαφοροποιημένη ασφάλεια για διάφορες υπηρεσίες 110

7.5.2 Ευέλικτη αρχιτεκτονική ασφαλείας για την υποστήριξη χαρακτηριστικών ασφαλείας για διαφορετικές φέτες δικτύου 110

7.5.3 Ένα ενιαίο πλαίσιο διαχείρισης ασφάλειας για περιβάλλον πολλαπλών προμηθευτών 110

8 OPENBTS-USRP 112

8.1 Η Υποδομή του OpenBTS 112

8.2 Voice over IP, VoIP 113

8.3 Quality of services 114

8.4 Layer 2 119

8.5 Ασφάλεια 120

8.6 Εισαγωγή στο Software Defined Radio 121

8.7 Συστατικά μέρη του OpenBTS: 122

8.8 OpenBTS 123

8.8.1 Πομποδέκτης-Transceiver 124

8.8.2 SMQueue 124

8.8.3 SIP router / PBX 124

8.8.4 SIPAuthServe 125

8.9 Ασφάλεια 125

8.9.1 Field tests 125

8.9.2 Burning Man 126

8.9.4 Niue 126

8.9.5 Defcon 20 127

8.10 GNURadio: 127

8.10.1 GNURadio Companion: 128

8.11 Asterisk 129

8.11.1 Χαρακτηριστικά του Asterisk: 129

9 Βιβλιογραφία 132

Μέρος Α΄

Βασικές Αρχές Δικτύων Κινητής Τηλεφωνίας

1.1 Εισαγωγή

1.1.1 Ιστορική Αναδρομή Στα Δίκτυα Κινητής Τηλεφωνίας

- 1918. Πρώτη δοκιμή ασύρματης (κινητής) τηλεφωνίας

Το Γερμανικό σύστημα σιδηροδρόμων αρχίζει να δοκιμάζει ασύρματη τηλεφωνία για το Γερμανικό στρατό σε στρατιωτικά τρένα που εκτελούν το δρομολόγιο μεταξύ Βερολίνου και Ζόσσεν

- 1924. Πρώτη δημόσια δοκιμή ασύρματης (κινητής) τηλεφωνίας

Οι δημόσιες δοκιμές της ασύρματης τηλεφωνίας που πραγματοποιήθηκαν αρχικά το 1918 ξεκίνησαν με τρένα που έτρεχαν μεταξύ Βερολίνου και Αμβούργου

- 1946. Το πρώτο δίκτυο κινητής τηλεφωνίας ξεκίνησε από την Bell Labs

Το πρώτο δίκτυο κινητής τηλεφωνίας ξεκίνησε από την Bell Labs και την AT&T στο Σεντ Λούις του Μισσούρι. Ωστόσο, η κάλυψη ήταν πολύ περιορισμένη και ο αριθμός των ταυτόχρονων χρηστών κινητής τηλεφωνίας ήταν ακόμη πιο περιορισμένος

- 1949. Το MTS (Mobile Telephone Service) κυκλοφορεί απο την AT&T

Αυτή η υπηρεσία ήταν το πρώτο πραγματικό δίκτυο κινητής τηλεφωνίας. Είχε μόνο 5000 συνδρομητές που έκαναν περίπου 30.000 κλήσεις την εβδομάδα. Το κόστος της υπηρεσίας ήταν πάνω από 200 δολάρια το μήνα συν περίπου 5 δολάρια ανά κλήση σε δολάρια Αυστραλίας με τη σημερινή αξία.

- 1956. Η MTS Sweden εγκαινιάζει την πρώτη πλήρως αυτοματοποιημένη κινητή υπηρεσία

Οι κλήσεις μπορούν να πραγματοποιηθούν χωρίς χειριστή που χρησιμοποιεί περιστροφική κλήση

- 1965. Η AT&T εγκαινιάζει την Improved Mobile Telephone Service (IMTS)

Οι βελτιώσεις περιελάμβαναν μια ευρύτερη περιοχή κάλυψης και αυξημένη χωρητικότητα, ωστόσο η ζήτηση σύντομα ήταν μεγαλύτερη από την χωρητικότητα του δικτύου.

- 1973. Το πρώτο εμπορικό κινητό τηλέφωνο

Η Motorola εγκαινιάζει το πρώτο φορητό τηλέφωνο (βάρους 1,1 κιλών)

- 1979. Το πρώτο αναλογικό δίκτυο «κυψελοειδές» (1G) ξεκινά στην Ιαπωνία

Η κυψελοειδής τεχνολογία ανέπτυξε τις δυνατότητες των κινητών και πλέον επιτρέπουν τη μαζική χρήση κινητών τηλεφώνων

- 1987. Η Αυστραλία μπαίνει στην εποχή των κινητών δικτύων

Η Telecom (Telstra) εγκαινιάζει δίκτυο 1G στην Αυστραλία

- 1991. Η πρώτη εμφάνιση του 2G δικτύου

Το πρώτο ψηφιακό δίκτυο δεύτερης γενιάς (2G), ξεκίνησε στη Φιλανδία

- 1992. Η IBM κυκλοφορεί το πρώτο της “smartphone”

Το IBM Simon Personal Communicator (απλά γνωστό ως IBM Simon) ήταν ένα φορητό κινητό τηλέφωνο με οθόνη αφής και PDA που σχεδιάστηκε και κατασκευάστηκε από τη International Business Machines Corp. (IBM) και συναρμολογήθηκε με σύμβαση από τη Mitsubishi Electric Corp. Το Simon Personal Communicator ήταν το πρώτο κινητό τηλέφωνο που περιλαμβάνει χαρακτηριστικά τηλεφώνου και PDA σε μία συσκευή.

- 1999. Οι πρώτες υπηρεσίες ίντερνετ για κινητή συσκευή είναι διαθέσιμες στην Ιαπωνία
- 2001. Το πρώτο ευρυζωνικό δίκτυο 3G ξεκινά στην Ιαπωνία
- 2009. Το πρώτο 4G δίκτυο ενεργοποιείται στην Αυστραλία

2. Τα Δίκτυα Κινητής Τηλεφωνίας

2.1 0G - O.5G

Το OG (Zero Generation) είναι επίσης γνωστό ως κινητό ραδιοτηλεφωνικό σύστημα. Καθώς αυτή η γενιά εφευρέθηκε πριν από το σύστημα κυψελών. Αυτό το σύστημα ήταν αναλογικής φύσης. Γενικά το 0G παρέχει μισοαμφίδρομες επικοινωνίες, δηλαδή μόνο ένα άτομο μπορεί να μιλάει και το άλλο να ακούει την ίδια στιγμή. Το σύστημα κινητής ραδιοφωνικής τηλεφωνίας (Zero generation) αποτελείται από διάφορες τεχνολογίες όπως το προηγμένο σύστημα κινητής τηλεφωνίας (AMTS), το κινητό τηλεφωνικό σύστημα (MTS), το MTD (σύστημα κινητής τηλεφωνίας D), το OLT (Offentlig Landmobile Telefoni) Push To Talk (PTT) και η βελτιωμένη υπηρεσία κινητής τηλεφωνίας (IMTS). Αυτά τα κινητά τηλέφωνα τοποθετήθηκαν σε οχήματα (φορτηγά, αυτοκίνητα κ.λπ.). Το κινητό τηλέφωνο είχε δύο βασικά μέρη: τον πομποδέκτη (πομπός - δέκτης) και κεφαλή (όργανο που είχε πλήκτρα οθόνης και αριθμητικής κλήσης). Ο πομποδέκτης (πομπός-δέκτης) στερεωνόταν στον κορμό του οχήματος. Η κεφαλή στερεωνόταν κοντά στο κάθισμα του οδηγού. Η κεφαλή και ο πομποδέκτης συνδέονταν μεταξύ τους με σύρμα. Η συσκευή (τηλέφωνο) θα συνδεθεί στο τοπικό τηλεφωνικό δίκτυο μόνο αν βρίσκεται στην περιοχή των 20 χιλιομέτρων. Κάθε πόλη είχε έναν κεντρικό πύργο κεραίας με 25 κανάλια. Αυτό σημαίνει ότι ο κινητός πομποδέκτης θα πρέπει να διαθέτει έναν ισχυρό πομπό με εύρος εκπομπής 50-70 Km. Μόνο λίγοι άνθρωποι μπόρεσαν να χρησιμοποιήσουν αυτήν τη συσκευή, καθώς μόνο 25 κανάλια ήταν διαθέσιμα. Η δυνατότητα περιαγωγής δεν υποστηρίχθηκε σε αυτήν την γενιά αναλογικού κυψελοειδούς τηλεφωνικού συστήματος. Το τηλεφωνικό σύστημα κινητής τηλεφωνίας ήταν μια εμπορική υπηρεσία υπό δημόσιο τηλεφωνικό δίκτυο με μοναδικούς τηλεφωνικούς αριθμούς. Ο μεγάλος αριθμός περιορισμών σε αυτή τη γενιά οδήγησε στην έλευση της νέας γενιάς.

2.2 Τεχνολογία 0.5G

Το 0.5G ήταν ο διάδοχος του 0G. Αυτή η τεχνολογία (0.5G) εισήγαγε το ARP (Autoradiopuhelin) ως το πρώτο εμπορικό δημόσιο δίκτυο κινητής τηλεφωνίας. Αυτό το δίκτυο ARP ξεκίνησε το 1971 στη Φινλανδία. Το ARP λειτούργησε σε 8 κανάλια με συχνότητα 150 MHz (ζώνη 147,9 - 154,875 MHz) και η ισχύς μετάδοσης ήταν σε μια περιοχή από 1 έως 5 watts. Το ARP χρησιμοποίησε σύστημα ημιαμφίδρομης μετάδοσης (τα φωνητικά σήματα μπορούν είτε να μεταδοθούν είτε να ληφθούν ταυτόχρονα) με χειροκίνητο σύστημα μεταγωγής. Αυτό το Δίκτυο περιέχει κελιά, (η έκταση χωρίζεται σε μικρούς τομείς, κάθε τομέας είναι γνωστός ως κυψέλη, ένα κελί καλύπτεται από ένα ασύρματο δίκτυο με έναν πομποδέκτη), με μέγεθος κυψέλης 30 km. Καθώς το ARP δεν υποστήριζε την περιαγωγή, οι κλήσεις τερματίζονταν καθώς ο χρήστης μετακινούνταν από το ένα κελί στο άλλο. Η ARP παρείχε κάλυψη 100%, η οποία προσέλκυσε πολλούς χρήστες προς αυτή την κατεύθυνση. Το ARP ήταν επιτυχές και έγινε πολύ δημοφιλές μέχρι να γίνει συμφόρηση του δικτύου. Τα τερματικά κινητής τηλεφωνίας ARP ήταν πολύ μεγάλα για να στερεωθούν σε αυτοκίνητα και πολύ ακριβά. Αυτοί οι περιορισμοί οδήγησαν στην ανακάλυψη του Autotel. Το Autotel είναι επίσης γνωστό ως PALM (Public Automated Land Mobile). Το Autotel είναι μια ραδιοτηλεφωνική υπηρεσία η οποία από την άποψη της τεχνολογίας βρίσκεται μεταξύ MTS και IMTS. Χρησιμοποίησε ψηφιακά σήματα για μηνύματα όπως κλιμάκωση κλήσης, εκχώρηση καναλιού, κουδουνισμό κλπ. Μόνο το κανάλι φωνής ήταν αναλογικό. Αυτό το σύστημα χρησιμοποίησε υπάρχοντα κανάλια VHF υψηλής ισχύος αντί για κυψελοειδές σύστημα. Αναπτύχθηκε στον Καναδά και την Κολομβία.

2.3 1G

Το πρώτο εμπορικά αυτοματοποιημένο κυψελοειδές δίκτυο (η γενιά 1G) ξεκίνησε στην Ιαπωνία από τη Nippon Telegraph and Telephone (NTT) το 1979, αρχικά στη μητροπολιτική περιοχή του Τόκιο. Μέσα σε πέντε χρόνια, το δίκτυο NTT επεκτάθηκε για να καλύψει ολόκληρο τον πληθυσμό της Ιαπωνίας και έγινε το πρώτο παγκόσμιο δίκτυο κινητής 1G.

Το 1981, το σύστημα NMT ξεκίνησε ταυτόχρονα στη Δανία, τη Φινλανδία, τη Νορβηγία και τη Σουηδία. Το NMT ήταν το πρώτο δίκτυο κινητής τηλεφωνίας με διεθνή περιαγωγή. Το 1983, το πρώτο δίκτυο 1G που ξεκίνησε στις ΗΠΑ ήταν το Ameritech με έδρα το Σικάγο χρησιμοποιώντας το κινητό τηλέφωνο Motorola DynaTAC. Στη συνέχεια ακολούθησαν αρκετές χώρες στις αρχές της δεκαετίας του 1980, συμπεριλαμβανομένου του Ηνωμένου Βασιλείου, του Μεξικού και του Καναδά.

2.4 2G

Το 2G (ή το 2-G) είναι η συντομογραφία για την τεχνολογία ασύρματης τηλεφωνίας δεύτερης γενιάς. Τα δίκτυα 2G κυψελοειδών τηλεπικοινωνιών προωθήθηκαν εμπορικά με το πρότυπο GSM στη Φινλανδία από την Radiolinja (τώρα μέρος της Elisa Oyj) το 1991. Τρία βασικά πλεονεκτήματα των δικτύων 2G έναντι των προκατόχων τους ήταν ότι οι τηλεφωνικές συνομιλίες κρυπτογραφούνταν ψηφιακά. Τα συστήματα 2G ήταν σημαντικά πιο αποτελεσματικά στο φάσμα, επιτρέποντας πολύ μεγαλύτερα επίπεδα διείσδυσης σε κινητά τηλέφωνα. Στο 2G εισήχθησαν υπηρεσίες δεδομένων για κινητά, ξεκινώντας με μηνύματα SMS. Οι τεχνολογίες 2G επέτρεψαν στα διάφορα δίκτυα κινητής τηλεφωνίας να παρέχουν υπηρεσίες όπως μηνύματα κειμένου, εικονομηνύματα

και μηνύματα MMS (μηνύματα πολυμέσων). Όλα τα μηνύματα κειμένου που αποστέλλονται μέσω 2G είναι ψηφιακά κρυπτογραφημένα, επιτρέποντας τη μεταφορά δεδομένων με τέτοιο τρόπο ώστε μόνο ο προοριζόμενος δέκτης να μπορεί να τα λάβει και να τα διαβάσει.

Μετά την προώθηση του 2G, τα προηγούμενα συστήματα κινητής τηλεφωνίας (1G) καταργήθηκαν σταδιακά. Ενώ τα ραδιοφωνικά σήματα σε δίκτυα 1G είναι αναλογικά, τα ραδιοφωνικά σήματα σε δίκτυα 2G είναι ψηφιακά. Και τα δύο συστήματα χρησιμοποιούν ψηφιακή σηματοδότηση για τη σύνδεση των σταθμών ραδιοεκπομπής.

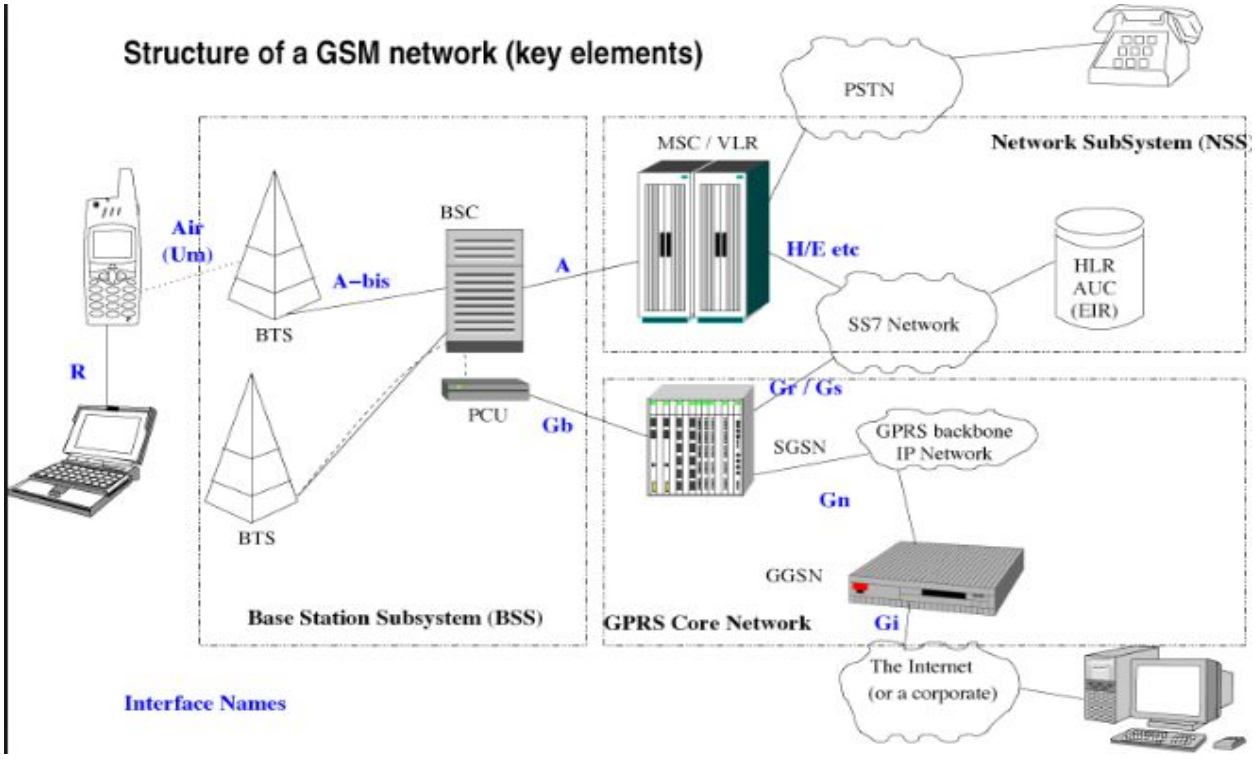
2.4.1 Τεχνολογίες 2G

Οι τεχνολογίες 2G μπορούν να χωριστούν σε πρότυπα βασισμένα σε πολλαπλή πρόσβαση βάσει χρόνου πολλαπλής προσπέλασης (TDMA) και πολλαπλής πρόσβασης (CDMA), ανάλογα με τον τύπο πολυπλεξίας που χρησιμοποιείται. Τα βασικά πρότυπα 2G είναι:

- GSM (βασισμένο σε TDMA), αρχικά από την Ευρώπη, αλλά χρησιμοποιείται στον μεγαλύτερο μέρος του κόσμου εκτός της Βόρειας Αμερικής. Πάνω από 60 φορείς εκμετάλλευσης GSM χρησιμοποιούσαν επίσης το CDMA2000 στη ζώνη συχνοτήτων 450 MHz (CDMA450) μέχρι το 2010.
- Το IS-95, επίσης γνωστό ως cdmaOne (βασισμένο σε CDMA, που συνήθως αναφέρεται ως απλά CDMA στις ΗΠΑ), χρησιμοποιείται στην Αμερική και σε τμήματα της Ασίας, αντιπροσωπεύει περίπου το 17% όλων των συνδρομητών παγκοσμίως.
- Το PDC είναι επίσης γνωστό ως JDC (Japanese Digital Cellular) (βασισμένο σε TDMA) και χρησιμοποιείται αποκλειστικά στην Ιαπωνία

- IDEN (βασισμένο σε TDMA), ιδιόκτητο δίκτυο που χρησιμοποιείται από τη Nextel στις Ηνωμένες Πολιτείες και τη Telus Mobility στον Καναδά
- IS-136 a.k.a Ψηφιακή AMPS ή D-AMPS (βασισμένη σε TDMA, κοινώς αναφερόμενη ως απλά «TDMA» στις ΗΠΑ), ήταν κάποτε διαδεδομένη στην Αμερική, αλλά οι περισσότεροι έχουν μεταφερθεί στο GSM.

Οι υπηρεσίες 2G αναφέρονται συχνά ως υπηρεσίες προσωπικών επικοινωνιών ή PCS στις Ηνωμένες Πολιτείες.



2.4.2 Ικανότητες, πλεονεκτήματα και μειονεκτήματα

2.4.2.1 Χωρητικότητα

Η χρήση ψηφιακών σημάτων μεταξύ των ακουστικών και των πύργων αυξάνει την χωρητικότητα του συστήματος με δύο βασικούς τρόπους:

Τα ψηφιακά φωνητικά δεδομένα μπορούν να συμπιεστούν και να πολυπλέκονται πολύ πιο αποτελεσματικά από τις αναλογικές κωδικοποιήσεις φωνής μέσω της χρήσης διαφόρων κωδικοποιητών, επιτρέποντας περισσότερες κλήσεις να μεταδίδονται στο ίδιο εύρος ζώνης ραδιοσυχνοτήτων.

Τα ψηφιακά συστήματα σχεδιάστηκαν έτσι ώστε να εκπέμπουν λιγότερη ραδιοφωνική ισχύ από τα φορητά ακουστικά. Αυτό σήμαινε ότι οι κυψέλες έπρεπε να είναι μικρότερες, επομένως περισσότερες κυψέλες έπρεπε να τοποθετηθούν στον ίδιο χώρο. Αυτό ήταν δυνατό επειδή οι πύργοι των κυψελών και ο σχετικός εξοπλισμός είχαν γίνει λιγότερο δαπανηροί.

2.4.2.2 2G χωρητικότητα μετάδοσης δεδομένων:

Με τη Γενική Υπηρεσία Πακέτων Ραδιοσυχνοτήτων (GPRS), υπάρχει μια θεωρητική μέγιστη ταχύτητα μεταφοράς 50 kbit / s (40 kbit / s στην πράξη).

Με EDGE (Enhanced Data Rates for GSM Evolution), υπάρχει μια θεωρητική μέγιστη ταχύτητα μεταφοράς 1 Mbit / s (500 kbit / s στην πράξη).

Πλεονεκτήματα

Οι ψηφιακές κλήσεις τείνουν να είναι απαλλαγμένες από θόρυβο λόγω περιβάλλοντος.

Τα ψηφιακά σήματα απαιτούν ελάχιστη ισχύ μπαταρίας για την εκπομπή τους.

Μειονεκτήματα

Σε λιγότερο πυκνοκατοικημένες περιοχές, το ασθενέστερο ψηφιακό σήμα που μεταδίδεται από ένα κινητό τηλέφωνο μπορεί να μην επαρκεί για να φτάσει στην κεραία εμπομπής. Αυτό τείνει να είναι ένα ιδιαίτερο πρόβλημα στα συστήματα 2G που αναπτύσσονται σε υψηλότερες συχνότητες, αλλά όχι σε αυτά που αναπτύσσονται σε χαμηλότερες συχνότητες. Οι εθνικές ρυθμίσεις διαφέρουν σημαντικά μεταξύ των χωρών που υπαγορεύουν το πού μπορεί να αναπτυχθεί το 2G.

Καθώς η απόσταση αυξάνεται, η αναλογική λήψη υποβαθμίζεται βαθμιαία, αλλά η ψηφιακή λήψη μεταβαίνει απότομα από καθαρή λήψη, σε μη λήψη. Αυτό μπορεί να είναι τόσο πλεονέκτημα όσο και μειονέκτημα. Υπό καλές συνθήκες, το ψηφιακό σήμα θα ακούγεται καλύτερα. Υπό ελαφρώς χειρότερες συνθήκες, το αναλογικό θα βιώσει στατικά, ενώ το ψηφιακό θα έχει περιστασιακά διακοπές. Όμως, καθώς οι συνθήκες επιδεινώνονται, το ψηφιακό θα αρχίσει να αποτυγχάνει τελείως, ή δεν θα είναι κατανοητό, ενώ το αναλογικό θα χειροτερεύει, διατηρώντας γενικά μια κλήση περισσότερο ενεργή και επιτρέποντας τουλάχιστον σε μερικούς από τους μεταδιδόμενους ήχους να γίνουν κατανοητοί.

Εάν χρησιμοποιείται συμπίεση απωλειών, μειώνεται η ποιότητα του ήχου, πράγμα που σημαίνει ότι ο καλών μπορεί να ακούσει λιγότερο τον τόνο της φωνής κάποιου.

2.5 2.5G (GPRS)

Το **2.5G** χρησιμοποιείται για την περιγραφή 2G-συστημάτων που έχουν υλοποιήσει έναν τομέα μεταγωγής πακέτων εκτός από τον τομέα μεταγωγής κυκλώματος. Δεν παρέχει απαραιτήτως ταχύτερη εξυπηρέτηση, διότι η ομαδοποίηση χρονικών μηνυμάτων χρησιμοποιείται επίσης για υπηρεσίες δεδομένων μεταγωγής κυκλωμάτων (HSCSD).

Το πρώτο σημαντικό βήμα στην εξέλιξη των δικτύων GSM προς 3G συνέβη με την εισαγωγή της υπηρεσίας General Packet Radio Service (GPRS). Τα δίκτυα CDMA2000 εξελίχθηκαν εξίσου με την εισαγωγή του 2.5G. Η προσέγγισή της 2.5G γενιάς επικεντρώθηκε στη χρήση πακέτων δεδομένων. Μέχρι αυτή τη στιγμή όλα τα κυκλώματα είχαν αφιερωθεί σε ένα δεδομένο χρήστη σε μια προσέγγιση γνωστή ως κύκλωμα μεταγωγής. Αυτό δεν ήταν αποτελεσματικό όταν ένα κανάλι μετέφερε δεδομένα για ένα μικρό ποσοστό του χρόνου. Η νέα προσέγγιση μεταγωγής πακέτων δρομολογεί μεμονωμένα πακέτα δεδομένων από τον πομπό προς τον δέκτη, επιτρέποντας στο ίδιο κύκλωμα να χρησιμοποιείται από διαφορετικούς χρήστες. Αυτό επιτρέπει στα κυκλώματα να χρησιμοποιούνται πιο αποτελεσματικά και τα φορτία να μετριούνται σύμφωνα με τα δεδομένα που μεταφέρονται.

2.6 2.75G (EDGE)

Τα δίκτυα GPRS εξελίχθηκαν σε δίκτυα EDGE με την εισαγωγή κωδικοποίησης 8PSK. Ενώ ο ρυθμός συμβόλων παρέμεινε ο ίδιος στα 270.833 δείγματα ανά δευτερόλεπτο, κάθε σύμβολο φέρει τρία bits αντί για ένα. Τα βελτιωμένα ποσοστά δεδομένων για το

GSM Evolution (EDGE), το Enhanced GPRS (EGPRS) ή το IMT-Single Carrier (IMT-SC) είναι μια τεχνολογία ψηφιακού κινητού τηλεφώνου που επιτρέπει συμβατότητα προς τα πίσω. Το EDGE αναπτύχθηκε σε δίκτυα GSM ξεκινώντας το 2003-αρχικά από την AT & T στις Ηνωμένες Πολιτείες.

Το EDGE είναι τυποποιημένο από το 3GPP ως μέρος της οικογένειας GSM και είναι μια αναβάθμιση που προσφέρει δυνητικά τριπλάσια αύξηση της χωρητικότητας των δικτύων GSM / GPRS. Η ψηφιακή υπηρεσία 2G παρέχει πολύ χρήσιμα χαρακτηριστικά, όπως αναγνωριστικό καλούντος, προώθηση κλήσεων και σύντομα μηνύματα.

2.7 3G

Το 3G,είναι η τρίτη γενιά τεχνολογίας κινητών τηλεπικοινωνιών. Βασίζεται σε ένα σύνολο προτύπων που χρησιμοποιούνται για κινητές συσκευές και υπηρεσίες κινητής τηλεφωνίας και δίκτυα που συμμορφώνονται με τις προδιαγραφές της International Mobile Telecommunications-2000 (IMT-2000) της Διεθνούς Ένωσης Τηλεπικοινωνιών.

Τα δίκτυα τηλεπικοινωνιών 3G υποστηρίζουν υπηρεσίες που παρέχουν ρυθμό μετάδοσης πληροφοριών τουλάχιστον 2 Mbit/s. Οι μεταγενέστερες κυκλοφορίες 3G, οι οποίες συχνά υποδηλώνονται ως 3.5G και 3.75G, παρέχουν επίσης ευρυζωνική πρόσβαση κινητής τηλεφωνίας αρκετών Mbit / s σε smartphones και κινητά μόντεμ σε φορητούς υπολογιστές. Αυτό διασφαλίζει ότι μπορεί να εφαρμοστεί στην ασύρματη φωνητική τηλεφωνία, την πρόσβαση στο κινητό Internet, τη σταθερή ασύρματη πρόσβαση στο Internet, τις βιντεοκλήσεις και τις τεχνολογίες κινητής τηλεόρασης.

Μια νέα γενιά κυψελωτών προτύπων εμφανίζεται περίπου κάθε δέκατο έτος από την εισαγωγή των συστημάτων 1G το 1981/1982. Κάθε γενιά χαρακτηρίζεται από νέες

ζώνες συχνοτήτων, υψηλότερους ρυθμούς δεδομένων και τεχνολογία μετάδοσης που δεν συμβαίνει προς τα πίσω.

2.7.1 Αναλυτικά

Ορισμένες εταιρείες τηλεπικοινωνιών προωθούν ασύρματες υπηρεσίες κινητού Διαδικτύου ως 3G, γεγονός που υποδηλώνει ότι η διαφημιζόμενη υπηρεσία παρέχεται μέσω ασύρματου δικτύου 3G. Οι υπηρεσίες που παρουσιαζόνται ως 3G πρέπει να πληρούν τα τεχνικά πρότυπα IMT-2000, συμπεριλαμβανομένων των προτύπων αξιοπιστίας και ταχύτητας (ποσοστά μεταφοράς δεδομένων). Για την εκπλήρωση των προτύπων IMT-2000, απαιτείται σύστημα για την παροχή μέγιστων ρυθμών δεδομένων τουλάχιστον 200 kbit / s (περίπου 0,2 Mbit / s). Ωστόσο, πολλές υπηρεσίες που διαφημίζονται ως 3G παρέχουν υψηλότερη ταχύτητα από τις ελάχιστες τεχνικές απαιτήσεις για μια υπηρεσία 3G. Οι πρόσφατες κυκλοφορίες 3G, οι οποίες συχνά υποδηλώνονται με 3.5G και 3.75G, παρέχουν επίσης κινητή ευρυζωνική πρόσβαση αρκετών Mbit / s σε smartphones και κινητά μόντεμ σε φορητούς υπολογιστές.

Το 3G ακολουθεί στην αγορά ένα από τα παρακάτω πρότυπα:

Το σύστημα UMTS (Universal Universal Telecommunications Service), που προσφέρεται για πρώτη φορά το 2001, τυποποιημένο από το 3GPP, χρησιμοποιείται κυρίως στην Ευρώπη, την Ιαπωνία, την Κίνα (με διαφορετικό ραδιοφάσμα) και άλλες περιοχές και αντικαθιστά σταδιακά τον πρόγονό του GSM 2G. Τα κινητά τηλέφωνα είναι συνήθως υβριδικά UMTS και GSM. Διάφορες ραδιοσυχνότητες μοιράζονται την ίδια υποδομή:

- Η αρχική και πιο διαδεδομένη διασύνδεση ραδιοσυχνοτήτων ονομάζεται W-CDMA (Πολλαπλή Πρόσβαση σε Κώδικα Ευρείας ζώνης).
- Η ασύρματη διασύνδεση TD-SCDMA διατέθηκε στο εμπόριο το 2009 και προσφέρεται μόνο στην Κίνα.
- Η τελευταία έκδοση UMTS, HSPA +, μπορεί να προσφέρει κορυφαίες ταχύτητες δεδομένων μέχρι 56 Mbit / s στην κατερχόμενη ζεύξη θεωρητικά (28 Mbit / s σε υπάρχουσες υπηρεσίες) και 22 Mbit / s στην ανερχόμενη ζεύξη.

Το σύστημα CDMA2000, το οποίο προσφέρεται για πρώτη φορά το 2002, τυποποιημένο από το 3GPP2, το οποίο χρησιμοποιείται ειδικά στη Βόρεια Αμερική και τη Νότια Κορέα, μοιράζεται υποδομή με το πρότυπο IS-95 2G. Τα κινητά τηλέφωνα είναι συνήθως τα υβρίδια CDMA2000 και IS-95. Η τελευταία έκδοση EVDO Rev B προσφέρει μέγιστες ταχύτητες 14,7 Mbit/s καθόδου.

Τα παραπάνω συστήματα και οι ασύρματες διασυνδέσεις βασίζονται στην τεχνολογία ραδιομετάδοσης ευρέους φάσματος. Ενώ το πρότυπο GSM EDGE ("2.9G"), τα ασύρματα τηλέφωνα DECT και τα πρότυπα Mobile WiMAX πληρούν επίσης τυπικά τις απαιτήσεις IMT-2000 και έχουν εγκριθεί ως πρότυπα 3G από την ITU, αυτά συνήθως δεν είναι επώνυμα 3G και βασίζονται σε εντελώς διαφορετικές τεχνολογίες.

Τα παρακάτω κοινά πρότυπα συμμορφώνονται με το πρότυπο IMT2000 / 3G:

- EDGE, μια αναθεώρηση από τον οργανισμό 3GPP στις παλαιότερες μεθόδους μετάδοσης με βάση το GSM, χρησιμοποιώντας τους ίδιους κόμβους μεταγωγής,

σταθμούς βάσης και συχνότητες όπως στο GPRS, αλλά και νέα κυκλώματα RF σταθμών βάσης και κινητών τηλεφώνων. Βασίζεται στο τρεις φορές πιο αποδοτικό σχήμα διαμόρφωσης 8PSK σε σχέση με το αρχικό σχεδίο διαμόρφωσης GMSK. Το EDGE εξακολουθεί να χρησιμοποιείται ευρέως λόγω της ευκολίας αναβάθμισης από την υπάρχουσα υποδομή GSM.

- Η τεχνολογία EDGE σε συνδυασμό με την τεχνολογία GPRS 2.5G ονομάζεται EGPRS και επιτρέπει κορυφαίες ταχύτητες δεδομένων της τάξης των 200 kbit / s, όπως και οι αρχικές εκδόσεις UMTS WCDMA και έτσι εκπληρώνει τυπικά τις απαιτήσεις IMT2000 σε συστήματα 3G. Ωστόσο, στην πράξη το EDGE σπάνια κυκλοφορεί ως σύστημα 3G, αλλά ως σύστημα 2.9G. Το EDGE παρουσιάζει ελαφρώς καλύτερη φασματική απόδοση του συστήματος από τα αρχικά συστήματα UMTS και CDMA2000, αλλά είναι δύσκολο να επιτευχθούν πολύ μεγαλύτερες ταχύτητες μετάδοσης δεδομένων λόγω του περιορισμένου εύρους ζώνης GSM των 200 kHz.
- Το EDGE ήταν επίσης ένας τρόπος λειτουργίας στο σύστημα IS-136 TDMA,που έχουν καταργηθεί πλέον.
- Evolved EDGE, η τελευταία αναθεώρηση, έχει μέγιστες ταχύτητες 1 Mbit /s καθόδου και 400 kbit / s ανόδου, αλλά δεν χρησιμοποιείται εμπορικά.

- Το Παγκόσμιο Σύστημα Κινητών Τηλεπικοινωνιών, το οποίο δημιουργήθηκε και αναθεωρήθηκε από το 3GPP. Η οικογένεια είναι μια πλήρης αναθεώρηση από το GSM όσον αφορά τις μεθόδους και το υλικό κωδικοποίησης, παρόλο που κάποια

τμήματα του GSM μπορούν να μετατραπούν εκ των υστέρων σε μορφή UMTS / W-CDMA.

- Το W-CDMA είναι η πιο συνηθισμένη ανάπτυξη, που λειτουργεί συνήθως στη ζώνη 2.100 MHz. και κάποιες άλλες ζώνες που είναι οι 850, 900 και 1.900 MHz.
  - Το HSPA είναι μια συγχώνευση αρκετών αναβαθμίσεων στο αρχικό πρότυπο W-CDMA και προσφέρει ταχύτητες 14,4 Mbit/s και 5,76 Mbit/s. Το HSPA είναι συμβατό προς τα πίσω και χρησιμοποιεί τις ίδιες συχνότητες με το W-CDMA.
  - Το HSPA +, είναι μια περαιτέρω αναθεώρηση και αναβάθμιση του HSPA, μπορεί να προσφέρει θεωρητικές μέγιστες ταχύτητες δεδομένων μέχρι 168 Mbit / s στην κατερχόμενη ζεύξη και 22 Mbit / s στην ανερχόμενη ζεύξη, χρησιμοποιώντας έναν συνδυασμό βελτιώσεων της διεπαφής αέρα καθώς και πολλαπλών φορέων HSPA και MIMO . Από τεχνική άποψη, τα MIMO και το DC-HSPA μπορούν να χρησιμοποιηθούν χωρίς τις βελτιώσεις του HSPA +

- Το σύστημα CDMA2000 ή IS-2000, συμπεριλαμβανομένων των CDMA2000 1x και CDMA2000 High Rate Packet Data (ή EVDO), τυποποιημένο από το 3GPP2 (διαφορετικό από το 3GPP), πρόκειται για εξέλιξη του αρχικού συστήματος CDMA IS-95 χρησιμοποιείται κυρίως στη Βόρεια Αμερική, Κίνα, Ινδία, Πακιστάν, Ιαπωνία, Νότια Κορέα, Νοτιοανατολική Ασία, Ευρώπη και Αφρική.

- Το CDMA2000 1x Rev. Ε έχει αυξημένη φωνητική χωρητικότητα (έως και 3 φορές) σε σύγκριση με το Rev. 0. Το EVDO Rev. Β προσφέρει ρυθμούς αιχμής έως 14,7 Mbit/s και βελτιώνει την υπάρχουσα εμπειρία του χρήστη.

2.8 4G

Το 4G είναι η τέταρτη γενιά της τεχνολογίας κινητών τηλεπικοινωνιών. Ένα σύστημα 4G πρέπει να παρέχει δυνατότητες που καθορίζονται από το ITU στο IMT Advanced. Οι δυνητικές και τρέχουσες εφαρμογές περιλαμβάνουν την τροποποιημένη πρόσβαση στο διαδίκτυο μέσω κινητού τηλεφώνου, την IP-τηλεφωνία, τις υπηρεσίες παιχνιδιών, την κινητή τηλεόραση υψηλής ευκρίνειας, την τηλεδιάσκεψη.

Το πρότυπο Long Term Evolution (LTE) έχει αναπτυχθεί εμπορικά στο Όσλο, τη Νορβηγία και τη Στοκχόλμη της Σουηδίας από το 2009. Ωστόσο, συζητήθηκε εάν οι πρώτες εκδόσεις πρέπει να θεωρηθούν ως 4G, όπως αναφέρεται στην παρακάτω ενότητα τεχνικών απαιτήσεων.

2.8.1 Τεχνικές απαιτήσεις

Τον Μάρτιο του 2008, ο Διεθνής Τηλεπικοινωνιακός Οργανισμός Ραδιοεπικοινωνιών (ITU-R) καθόρισε ένα σύνολο απαιτήσεων για τα πρότυπα 4G, με την ονομασία International Advanced Mobile Telecommunications Advanced (IMT Advanced), που καθορίζει τις μέγιστες απαιτήσεις ταχύτητας για υπηρεσίες 4G στα 100 Mbit/s για επικοινωνία υψηλής κινητικότητας (όπως από τρένα και αυτοκίνητα) και 1 Gbit/s για επικοινωνία χαμηλής κινητικότητας (όπως πεζούς και σταθεροί χρήστες).

Δεδομένου ότι οι πρώτες εκδόσεις του Mobile WiMAX και του LTE υποστηρίζουν πολύ μικρότερες ταχύτητες από 1 Gbit/s, δεν είναι πλήρως συμβατές με το IMT-Advanced, αλλά συχνά χαρακτηρίζονται ως 4G από τους παρόχους υπηρεσιών. Σύμφωνα με τους φορείς εκμετάλλευσης, μια γενιά του δικτύου αναφέρεται στην ανάπτυξη μιας νέας μη συμβατής προς τα πίσω τεχνολογίας. Στις 6 Δεκεμβρίου 2010, η ITU-R αναγνώρισε ότι αυτές οι δύο τεχνολογίες, καθώς και άλλες τεχνολογίες μετά το 3G, αν και δεν πληρούν τις απαιτήσεις IMT Advanced, θα μπορούσαν ωστόσο να θεωρηθούν ως "4G", υπό την προϋπόθεση ότι αποτελούν πρόδρομο για την συμβατή IMT έκδοσή τους και "ένα σημαντικό επίπεδο βελτίωσης των επιδόσεων και των δυνατοτήτων σε σχέση με τα αρχικά συστήματα τρίτης γενιάς που αναπτύσσονταν τότε".

Σε αντίθεση με τις προηγούμενες γενιές, ένα σύστημα 4G δεν υποστηρίζει την παραδοσιακή υπηρεσία τηλεφωνίας με κυκλώματα, αλλά επικοινωνία βασισμένη σε πρωτόκολλο Internet (IP), όπως η τηλεφωνία IP. Όπως φαίνεται παρακάτω, η ραδιοφωνική τεχνολογία διασκορπισμένου φάσματος που χρησιμοποιείται σε συστήματα 3G, εγκαταλείπεται σε όλα τα υποψήφια συστήματα 4G και αντικαθίσταται από τη μετάδοση πολλαπλών φορέων OFDMA και από άλλα συστήματα εξισορρόπησης τομέα συχνοτήτων (FDE), επιτρέποντας τη μεταφορά με πολύ υψηλών ρυθμών μετάδοσης δεδομένων παρά το θόρυβο. Ο μέγιστο bit-rate βελτιώνεται περαιτέρω από έξυπνες συστοιχίες κεραιών για επικοινωνίες πολλαπλών εισόδων - πολλαπλών εξόδων (MIMO).

2.9 5G

Τα δίκτυα 5ης γενιάς ή τα ασύρματα συστήματα 5ης γενιάς, συντομογραφημένα 5G, είναι τα προτεινόμενα επόμενα τηλεπικοινωνιακά πρότυπα πέρα από τα τρέχοντα πρότυπα 4G / IMT-Advanced.

Ο σχεδιασμός 5G στοχεύει σε υψηλότερη χωρητικότητα από την τρέχουσα 4G, επιτρέποντας μεγαλύτερη πυκνότητα χρηστών ευρυζωνικών κινητών τηλεφώνων και υποστηρίζοντας από συσκευή σε συσκευή, εξαιρετικά αξιόπιστες και επικοινωνίες μεταξύ πολλών συσκευών.

Η έρευνα και η ανάπτυξη του 5G στοχεύει επίσης σε χαμηλότερη καθυστέρηση από τον εξοπλισμό 4G και χαμηλότερη κατανάλωση μπαταρίας, για την καλύτερη υλοποίηση του Internet of Things.

Προς το παρόν δεν υπάρχει πρότυπο για εφαρμογές 5G.

Η Next Generation Mobile Alliance ορίζει τις ακόλουθες απαιτήσεις που πρέπει να πληροί ένα πρότυπο 5G:

- Ποσοστά δεδομένων δεκάδων megabits ανά δευτερόλεπτο για δεκάδες χιλιάδες χρήστες
- Ποσοστά δεδομένων 100 megabits ανά δευτερόλεπτο για μητροπολιτικές περιοχές
- 1 Gb ανά δευτερόλεπτο ταυτόχρονα σε πολλούς εργαζόμενους στο ίδιο πάτωμα γραφείου
- Αρκετές εκατοντάδες χιλιάδες ταυτόχρονες συνδέσεις για ασύρματους αισθητήρες

- Η φασματική απόδοση σημαντικά βελτιωμένη σε σύγκριση με την 4G
- Βελτιωμένη κάλυψη
- Βελτιωμένη ποιότητα σήματος
- Η καθυστέρηση να είναι σημαντικά μειωμένη σε σύγκριση με το LTE.

Εκτός από την παροχή υψηλότερων ταχυτήτων, έχει προβλεφθεί ότι τα δίκτυα 5G θα πρέπει επίσης να αντιμετωπίσουν νέες περιπτώσεις χρήσης, όπως το Internet of Things (συσκευές συνδεδεμένες με το διαδίκτυο), καθώς και υπηρεσίες τύπου broadcast και επικοινωνίες εκτάκτου ανάγκης σε περιόδους φυσικής καταστροφής. Οι φορείς, οι κατασκευαστές chip, οι OEMS και οι OSAT, όπως η Advanced Semiconductor Engineering (ASE) και η Amkor Technology, Inc., προετοιμάζονται για αυτό το ασύρματο πρότυπο νέας γενιάς (5G), καθώς τα κινητά συστήματα και οι σταθμοί βάσης απαιτούν νέους και γρηγορότερους επεξεργαστές εφαρμογών, ζώνες βάσης και συσκευές ραδιοσυχνοτήτων.

Παρόλο που τα ενημερωμένα πρότυπα που καθορίζουν δυνατότητες πέραν εκείνων που ορίζονται στα τρέχοντα πρότυπα 4G είναι υπό εξέταση, αυτές οι νέες δυνατότητες έχουν ομαδοποιηθεί σύμφωνα με τα ισχύοντα πρότυπα ITU-T 4G. Η Ομοσπονδιακή Επιτροπή Επικοινωνιών των ΗΠΑ (FCC) ενέκρινε το φάσμα για 5G, συμπεριλαμβανομένων των ζωνών 28GHz, 37 GHz και 39 GHz, στις 14 Ιουλίου 2016.

3 Ασφάλεια στα Δίκτυα Κινητής Τηλεφωνίας

3.1 Θέματα ευπαθειών, απειλές και σημεία εισβολής

Λόγω της εισαγωγής νέων τεχνολογιών ραδιοπρόσβασης και της μετάβασης προς την αρχιτεκτονική που βασίζεται στην τεχνολογία IP, νέες ευπάθειες έχουν εισέλθει στην αρχιτεκτονική δικτύου, οι οποίες εκθέτουν τα κινητά δίκτυα σε διαφορετικές απειλές με στόχο τις στοίβες πρωτοκόλλων, τα χαρακτηριστικά ασφαλείας και τις διεπαφές δικτύου. Ένα θέμα ευπάθειας στο δίκτυο κινητής τηλεφωνίας μπορεί να γίνει κατανοητό ως μια αδυναμία που προ-υπάρχει στην αρχιτεκτονική του δικτύου και στα διάφορα μέρη του, τα οποία μπορούν να εκμεταλλευτούν οι κακόβουλοι και να εκτελέσουν μια επίθεση. Ως εκ τούτου, η απειλή καθορίζεται από τη δυνατότητα σκόπιμης προσπάθειας 1) μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες, 2) χειραγώγησης πληροφοριών και 3) μετατροπής ενός συστήματος σε αναξιόπιστο ή άχρηστο.

Η μετάβαση στην επίπεδη αρχιτεκτονική βασισμένη στην IP έχει εισαγάγει μια μετατόπιση στα σημεία εισόδου των απειλών ασύρματης κινητής τηλεφωνίας. Στην πραγματικότητα, τα κινητά δίκτυα 2G και 3G ήταν δύσκολο να στοχευθούν από απειλές που οφείλονται στη χρήση του SS7, το οποίο δύσκολα διεισδύεται σε σύγκριση με τη σηματοδότηση διαμέτρου που χρησιμοποιείται σε όλες τις τεχνολογίες IP και πέρα του 4G, όπου οι συσκευές και τα βασικά δίκτυα φαίνεται να είναι πιο ευάλωτα σε διάφορες επιθέσεις. Αυτό μπορεί να εξηγηθεί από την εξέλιξη των κινητών συσκευών, οι οποίες στρέφονται δυναμικά σε δεδομένα που είναι άμεσα ορατά από το Διαδίκτυο και η αντικατάσταση του πρωτοκόλλου σηματοδότησης SS7 με πρωτόκολλο διαμέτρου, καθώς και η χρήση διαφόρων και ευέλικτων τεχνολογιών πρόσβασης στο RAN (Radio Access Network) όπως οι κυψέλες Femto και τα hotspot ασύρματων τεχνολογιών Ethernet 802.11 (WiFi). Παρόλα αυτά η διάμετρος είναι ένα σημαντικό πρωτόκολλο για τη σηματοδότηση δεδομένων χρέωσης, διαχείρισης κίνησης και συνδρομητών, ελέγχου ταυτότητας συνδρομητών, περιαγωγής και διαχείρισης της κινητικότητας στο LTE, αλλά είναι ευάλωτο στις επιθέσεις σηματοδότησης.

Υπάρχουν διάφορα σημεία εισόδου στα δίκτυα κινητής τηλεφωνίας 4G, όπως οι ενσωματωμένες έξυπνες κινητές συσκευές, το δίκτυο πρόσβασης, το backhaul και το κεντρικό δίκτυο.

3.1.2 Ενσωματωμένες έξυπνες κινητές συσκευές

Οι έξυπνες συσκευές αποτελούν κρίσιμα στοιχεία για την ασφάλεια των κινητών δικτύων, δεδομένου ότι μπορούν να αποτελέσουν στόχους και επίσης να χρησιμοποιηθούν ως αφετηρία για την πραγματοποίηση επιθέσεων προς τα κινητά δίκτυα. Τα σημεία εισόδου για κακόβουλα προγράμματα κινητής τηλεφωνίας μπορούν να κυμαίνονται από υπηρεσίες κινητού δικτύου, πρόσβαση στο διαδίκτυο, έως Bluetooth. Αυτές οι υπηρεσίες μπορούν να χρησιμοποιηθούν για την έναρξη επιθέσεων σε κινητές συσκευές προκειμένου να συλλεχθούν ιδιωτικά δεδομένα, να χρησιμοποιηθούν υπολογιστικοί πόροι ή να εκτελεσθούν επιζήμιες ενέργειες. Διάφοροι τύποι επιθέσεων κακόβουλου λογισμικού μπορούν να εκτελεστούν σε κινητές συσκευές όπως τα κινητά botnet, τα οποία θεωρούνται ως η επόμενη μεγάλη απειλή μεγάλης κλίμακας στοχεύοντας στο δίκτυο κινητής τηλεφωνίας λόγω της ενσωμάτωσης του διαδικτύου στα δίκτυα κινητής τηλεφωνίας. Στην πραγματικότητα, ένα botnet είναι ένα σύνολο εκτεθειμένων συσκευών που μπορούν να ελέγχονται και να συντονίζονται εξ αποστάσεως. Χρησιμοποιώντας κακόβουλο λογισμικό κινητού τηλεφώνου, όπως τον Δούρειο Ίππο (Trojan horse), μια κινητή συσκευή μπορεί να μετατραπεί σε ένα botclient, επιτρέποντάς του έτσι να λαμβάνει εντολές από έναν απομακρυσμένο διακομιστή ελέγχου. Στην πράξη,υπάρχει η δυνατότητα εκκίνησης επιθέσεων Distributed Denial of Service (DDoS) σε δίκτυα κινητής τηλεφωνίας χρησιμοποιώντας κακόβουλα προγράμματα που έχουν διαμοιραστεί σε διαφορετικό εξοπλισμό χρηστών στο WLAN. Τέτοιες επιθέσεις μπορούν να είναι αποτελεσματικές χρησιμοποιώντας κινητά botnets για την πραγματοποίηση επιθέσεων DDoS που στοχεύουν ένα συγκεκριμένο HLR με μεγάλο όγκο κίνησης, εμποδίζοντας έτσι τους νόμιμους χρήστες των κυψελοειδών δικτύων να έχουν πρόσβαση και να χρησιμοποιούν την υπηρεσία.

Άλλες τεχνικές διάδοσης που χρησιμοποιούνται για να υπονομεύσουν μια κινητή συσκευή περιλαμβάνουν τη χορήγηση δικαιωμάτων από κακόβουλες εφαρμογές. Εκτός από τα κακόβουλα προγράμματα, οι κινητές συσκευές μπορούν επίσης να στοχευθούν από μια μεγάλη ποικιλία απειλών, συμπεριλαμβανομένων των απειλών από το διαδίκτυο, το phishing και το MITM

3.1.3 Το Δίκτυο Πρόσβασης

Στο δίκτυο πρόσβασης, η διεπαφή S1 αποτελεί το κύριο σημείο εισόδου, καθώς χρησιμοποιείται για τη σύνδεση και την αυθεντικοποίηση των eNB στο δίκτυο κινητής τηλεφωνίας. Τυπικές ευπάθειες που επηρεάζουν αυτήν τη διασύνδεση σχετίζονται με τη δυνατότητα χρήσης ενός σταθμού κινητής τηλεφωνίας eNB για πρόσβαση και επίθεση στο MME (και ως εκ τούτου την κατάργηση ολόκληρης της βασικής υπηρεσίας), καθώς και τη δυνατότητα εισαγωγής ψευδούς κυκλοφορίας σε εφαρμογές. Άλλες ευπάθειες στην ασφάλεια τομέα πρόσβασης, οι οποίες μπορούν να εκμεταλλευτούν για να απειλήσουν τη λειτουργία των κινητών δικτύων είναι σε σχέση με την έλλειψη κρυπτογράφησης δεδομένων και σηματοδοσίας.

Στην πραγματικότητα, κατά τη διάρκεια της αρχικής διαδικασίας ελέγχου ταυτότητας, τα μηνύματα που ανταλλάσσονται πριν από την εγκατάσταση της εντολής ασφαλούς λειτουργίας, δεν κρυπτογραφούνται ούτε προστατεύονται ως προς την ακεραιότητά τους. Αυτά τα μηνύματα μεταφέρουν δεδομένα όπως ο αριθμός αναγνώρισης ταυτότητας (AUTN), ο τυχαίος αριθμός (RAND), η υπογεγραμμένη απόκριση (RES) και η διεθνής ταυτότητα συνδρομητών κινητής τηλεφωνίας (IMSI) που χρησιμοποιούνται για τον έλεγχο ταυτότητας ενός UE. Συνήθως, ένας εισβολέας μπορεί να εκμεταλλευτεί την έλλειψη προστασίας του μηνύματος απόρριψης σύνδεσης RRC για να ξεκινήσει μια επίθεση DoS σε δίκτυα κινητής τηλεφωνίας. Επιπλέον, η έλλειψη αυθεντικοποίησης μεταξύ του δικτύου εξυπηρέτησης (SN) και του οικιακού δικτύου (HN), καθώς και η έλλειψη κρυπτοσυστήματος στο ασύρματο δίκτυο και η προστασία της ταυτότητας περιοχής εντοπισμού (LAI) στο UMTS-AKA αποτελούν επίσης ευπάθειες που μπορούν να εκμεταλλευθούν για να ξεκινήσουν επιθέσεις σε δίκτυα κινητής τηλεφωνίας. Συγκεκριμένα, οι επιθέσεις ανακατεύθυνσης μπορούν να οδηγήσουν στην αλλαγή του LAI. Για παράδειγμα, η έλλειψη προστασίας ακεραιότητας ορισμένων μηνυμάτων σηματοδότησης UMTS που ανταλλάσσονται μεταξύ του MS και του RNC μπορεί να εκθέσει το δίκτυο σε μια τροποποίηση των μηνυμάτων RRC καθώς αυτά είναι απροστάτευτα.

Μια άλλη ευπάθεια στο δίκτυο πρόσβασης σχετίζεται με το πρωτόκολλο ελέγχου ταυτότητας κατά την ομαλή λειτουργία μεταξύ διαφορετικών τεχνολογιών πρόσβασης όπως GSM, UMTS και LTE

Στην πραγματικότητα, το πρωτόκολλο GSM AKA υποφέρει από μια αδυναμία που σχετίζεται με τη διαλειτουργικότητα του δικτύου πρόσβασης 2G / 3G, γεγονός που μπορεί να εξηγηθεί από διάφορους λόγους. Πρώτον, η έλλειψη αμοιβαίας επαλήθευσης

ταυτότητας μεταξύ των συνδρομητών και του δικτύου αποτελεί σοβαρή απειλή, καθώς μπορεί να οδηγήσει στην αποκάλυψη της ταυτότητας του χρήστη μέσω ενός IMSI catcher. Αυτή η ευπάθεια μπορεί να εκμεταλλευθεί για να ξεκινήσει επίθεση εναντίον ενός συμβατού GSM δικτύου, για παράδειγμα, μέσω του SDR (Software Defined Radio). Δεύτερον, η έλλειψη προστασίας ακεραιότητας των δεδομένων σηματοδότησης μπορεί να χρησιμοποιηθεί για να αναγκάσει το κινητό ή το δίκτυο να συμμετάσχει σε απλή μετάδοση δεδομένων (φωνή ή κείμενο) μετά την αφαίρεση ή την τροποποίηση των επιλογών ασφαλείας. Τέλος, η αποθήκευση της τριπλέτας αυθεντικοποίησης στο Μητρώο τοποθετήσεων επισκεπτών (VLR) μπορεί να οδηγήσει στην έκθεση του συμμετρικού κλειδιού ενός στοχευμένου κινητού σταθμού. Έτσι, ενδέχεται να προκύψουν ορισμένα ζητήματα ασφάλειας κατά την ενσωμάτωση της συσκευής GSM στο δίκτυο UMTS με τα ακόλουθα σενάρια. Για παράδειγμα, κατά τη διάρκεια της περιαγωγής της συσκευής GSM στο δίκτυο UMTS, ένας εισβολέας μπορεί να παρακολουθήσει την επικοινωνία υπό τον όρο ότι έχει ήδη πρόσβαση στο κλειδί κρυπτογράφησης (Kc) ενώ η συσκευή ήταν σε ένα πλήρως GSM δίκτυο. Επιπλέον, είναι δυνατό για ένα Κέντρο Μεταγωγής Κινητού Τηλεφώνου (MSC) να χρησιμοποιεί ένα επικυρωμένο κλειδί κρυπτογράφησης (Kc) για τον έλεγχο ταυτότητας μεταξύ του κινητού και του σταθμού βάσης GSM κατά την περιαγωγή μίας συσκευής UMTS σε ένα υποσύστημα βάσης GSM (BSS). Μια παραλλαγή αυτού του σεναρίου αφορά την κρυπτογράφηση της επικοινωνίας με το κλειδί κρυπτογράφησης GSM (Kc) κατά την περιαγωγή μίας κινητής συσκευής UMTS σε ένα κινητό δίκτυο GSM (BSS και MSC). Επιπλέον, η έλλειψη κρυπτογράφησης ωφέλιμου φορτίου μεταξύ του MS και του SGSN κατά τη σύνδεση με ένα GSM BSS, μπορεί να οδηγήσει στην υποκλοπή της επικοινωνίας.

Τέλος, άλλες αδυναμίες στο δίκτυο πρόσβασης σχετίζονται με την υπερφόρτωση σηματοδοσίας, το περιορισμένο εύρος ζώνης ασύρματης ζεύξης και την βαρία διαδικασία ελέγχου και σηματοδότησης των μηνυμάτων στη διαδικασία RRC για την εγκατάσταση/αποδέσμευση του Radio Access Bearer (RAB), που μπορούν να χρησιμοποιηθούν για την πραγματοποίηση επιθέσεων στο CN, όπως η επίθεση υπερχείλισης του HLR.

3.1.4 Στο Δίκτυο Κορμού

Όπως στο δίκτυο πρόσβασης, υπάρχουν επίσης και ορισμένα τρωτά σημεία που έχουν αναφερθεί στην αρχιτεκτονική του 4G και στο CN (Core Network). Το δίκτυο backhaul αποτελείται από τις φυσικές συνδέσεις και τα δίκτυα που χρησιμοποιούνται για τη

μεταφορά δεδομένων μεταξύ του RAN και του CN, όπου το CN εμπεριέχει την λογική του δικτύου που διαχειρίζεται τη δημιουργία και τη συντήρηση συνδέσεων μεταξύ κινητών συσκευών και εξωτερικών υπηρεσιών δικτύων. Επίσης χειρίζεται τη μεταφορά χρηστών και δεδομένων ελέγχου, καθώς και τον έλεγχο ταυτότητας χρηστών και συσκευών. Παρά το γεγονός ότι η πρόσβαση στο CN μπορεί να είναι ιδιαίτερα δύσκολη, υπάρχουν ακόμα ορισμένες αδυναμίες ασφαλείας. Το backhaul μπορεί να προσφέρει σε έναν εισβολέα πρόσβαση σε όλη την κίνηση ελέγχου και δεδομένων που αποστέλλεται μεταξύ κινητών συσκευών μέσα σε μια περιοχή. Δεδομένου ότι η τεχνολογική εξέλιξη επέτρεψε την ενσωμάτωση διαφορετικών τεχνολογιών πρόσβασης, όπως τα φεμτοκύτταρα και τα ασύρματα δίκτυα 3GPP που ανήκουν στους MNO, εισήχθησαν νέα πιθανά σημεία εισόδου στο CN για επιτιθέμενους. Ιδιαίτερα, στην περίπτωση του LTE, τα νέα σημεία εισόδου απειλών προκύπτουν από την εισαγωγή νέων διεπαφών όπως η διεπαφή X2, η χρήση πρωτοκόλλων σηματοδοσίας διαμέτρου των οποίων η κυκλοφορία αυξάνει την υπερφόρτωση σηματοδοσίας και τη μετάδοση μέσω IP. Στην πραγματικότητα, υπάρχουν αρκετοί σοβαροί παράγοντες απειλής εναντίον του CN, συμπεριλαμβανομένης της IP-based αρχιτεκτονικής, και του υπάρχοντος σταθμού βάσης (BS) με απευθείας σύνδεση ALL-IP στο δίκτυο. Επιπλέον, η έλλειψη προστασίας του ιδιωτικού απορρήτου στο σύστημα EPS-AKA (Extensible Authentication Protocol) στη διαδικασία πρόσβασης και η έλλειψη πρόληψης σε επιθέσεις DoS είναι άλλες σοβαρές απειλές κατά της EPC CN (Evolved Packet *Core)*. Η έλλειψη ασφάλειας προς τα πίσω στη διαδικασία παράδοσης, η έλλειψη προστασίας από αποσυγχρονισμούς και από επιθέσεις επανάληψης, καθώς και η ευπάθεια στην αρχιτεκτονική ασφαλείας MTC και στον Μηχανισμό Ασφαλείας στο IMS και στο Home Evolved Node B (HeNB) συνιστούν επιπλέον σημαντικές απειλές ασφάλειας κατά του δικτύου backhaul.

Μια άλλη αδυναμία που σχετίζεται με την έλλειψη συστημάτων ασφαλείας στο πρωτόκολλο GTP που χρησιμοποιείται στο EPC NAS (Non-Access Stratum), μπορεί να εκθέσει το δίκτυο σε απειλές όπως οι μη φυσιολογικές κινήσεις πακέτων που αποτελούνται από τροποποιημένες ή κατεστραμμένες μονάδες πακέτων (PDU), ή PDU που δεν συμμορφώνονται με το πρωτόκολλο, την ανάλυση κυκλοφορίας και την τροποποίηση κυκλοφορίας.

3.1.5 Το εξωτερικό ή τρίτου μέρους δίκτυο (3rd Party Network)

Το τελευταίο σημείο εισόδου για απειλές που στοχεύουν τα δίκτυα κινητής τηλεφωνίας προέρχονται από το εξωτερικό δίκτυο ή το δίκτυο τρίτων. Στην πραγματικότητα, διάφορες υπηρεσίες χρηστών παρέχονται μέσω εξωτερικών και τρίτων δικτύων, συμπεριλαμβανομένων των υπηρεσιών περιήγησης στο Internet, διασύνδεσης με εταιρικά δίκτυα, δίκτυα συνεργατών περιαγωγής, άλλα συνδεδεμένα δίκτυα δημόσιων δικτύων εδάφους (PLMN), κοινόχρηστο δίκτυο RAN, Δίκτυα πρόσβασης 3GPP.

Στη συγκεκριμένη περίπτωση δικτύων πρόσβασης χωρίς 3GPP, η συνεργασία με το δίκτυο WLAN, το οποίο μπορεί να χρησιμοποιηθεί για παράδειγμα κατά την πρόσβαση σε 3G HN μέσω αρχιτεκτονικής WLAN ή κατά την περιαγωγή 3G μέσω αρχιτεκτονικής WLAN, παρουσιάζει διάφορα ζητήματα ασφάλειας όπως η αποκάλυψη εμπιστευτικών πληροφοριών του χρήστη, ή πληροφορίες σχετικά με την πιστοποίηση ταυτότητας χρήστη που μπορεί να προκύψουν κατά την πρόσβαση σε υπηρεσίες 3G, την πλαστοπροσωπία δικτύου για την απόκτηση προσωπικών πληροφοριών των χρηστών και τη πλαστοπροσωπία νόμιμων χρηστών, η οποία επιτρέπει την πρόσβαση σε δωρεάν υπηρεσίες για την εκτέλεση κακόβουλων δραστηριοτήτων που θα χρεώσουν τον πραγματικό χρήστη. Μια άλλη αδυναμία σχετίζεται με τη δυνατότητα προσπέρασης του ελέγχου πρόσβασης και της διαδικασίας ελέγχου ταυτότητας με σκοπό την παροχή δωρεάν υπηρεσιών, τη δυνατότητα παρεμβολής στη διαδικασία χρέωσης προκειμένου να αποκτηθούν υπηρεσίες χωρίς χρέωση και τη δυνατότητα να αποτραπεί η πρόσβαση των χρηστών σε υπηρεσίες 3G.

Εκτός από τις αδυναμίες που προαναφέρθηκαν, η χρήση διαφορετικών τεχνολογιών σε συγκλίνοντα δίκτυα όπως το WiMAX αποτελεί επίσης ένα άλλο σημείο εισόδου απειλής, δεδομένου ότι το WiMAX εξακολουθεί να παρουσιάζει αδύναμα σημεία στο φυσικό στρώμα και στο στρώμα MAC.

3.2 Κατηγοριοποίηση των επιθέσεων σε δίκτυα κινητής τηλεφωνίας

Σε αυτή την ενότητα, παρουσιάζεται μια κατηγοριοποίηση των διαφόρων επιθέσεων σε δίκτυα κινητής τηλεφωνίας. Στην πραγματικότητα, πολλά έγγραφα έχουν προτείνει διαφορετικές κατηγοριοποιήσεις επιθέσεων, με κριτήρια όπως η δυσκολία της εφαρμογής της επίθεσης, η ανάγκη να απαιτείται πρόσβαση στο δίκτυο, ο δυνητικός αντίκτυπος της επίθεσης, η προέλευση της επίθεσης, ο στόχος της απειλής, η πιθανότητα και ο κίνδυνος της επίθεσης. Στην παρούσα εργασία παρουσιάζονται τέσσερις ομάδες επιθέσεων ανάλογα με την προέλευση της επίθεσης.

Ο Πίνακας 1 παρέχει σύνοψη με τις κατηγορίες απειλών,τις ομάδες προσβολών, την προέλευση, τον τρόπο λειτουργίας και τον στόχο της επίθεσης. Μπορεί να παρατηρηθεί ότι κάθε επίθεση μπορεί να ξεκινήσει εντός του τομέα δικτύου (εσωτερικές επιθέσεις) ή εξωτερικά, χρησιμοποιώντας μια παθητική ή ενεργή αντίστροφη λειτουργία. Η παθητική επίθεση στοχεύει στη συλλογή δεδομένων που ανταλλάσσονται στο δίκτυο χωρίς να διαταράσσει τη λειτουργία των επικοινωνιών, ενώ μια ενεργή επίθεση συνεπάγεται διακοπή, τροποποίηση ή δημιουργία πληροφοριών, διακόπτοντας έτσι την κανονική λειτουργία του δικτύου κινητής τηλεφωνίας.

Ομάδες απειλών	Κατηγορίες Επιθέσεων	Προέλευση Επιθέσεων	Τρόπος Επίθεσης
Διασυνδέσεις διεπαφών	Απώλεια διαθεσιμότητας	Εξωτερική / Εσωτερική	Ενεργός
Καταστροφή στοιχείων δικτύου	Απώλεια διαθεσιμότητας	Εξωτερική / Εσωτερική	Ενεργός
Παρακολούθηση της κυκλοφορίας	Απώλεια εμπιστευτικότητας	Εξωτερική / Εσωτερική	Παθητικός
Μη εξουσιοδοτημένη πρόσβαση δεδομένων	Απώλεια εμπιστευτικότητας	Εξωτερική / Εσωτερική	Ενεργός

Τροποποίηση κυκλοφορίας	Απώλεια ακεραιότητας	Εξωτερική / Εσωτερική	Ενεργός
Τροποποίηση δεδομένων	Απώλεια ακεραιότητας	Εξωτερική / Εσωτερική	Ενεργός
Τροποποιημένα στοιχεία δικτύου	Απώλεια ελέγχου	Εξωτερική / Εσωτερική	Ενεργός
Κακόβουλος εισβολέας	Απώλεια ελέγχου	Εσωτερική	Ενεργός
Κλοπή υπηρεσιών	Κλοπή υπηρεσίας	Εξωτερική / Εσωτερική	Ενεργός

Η πρώτη ομάδα, η οποία αποτελείται από απειλές από το διαδίκτυο, το PDN, την ανταλλαγή περιαγωγής GPRS ή άλλο PLMN, μπορούν να ταξινομηθούν ως εξωτερικές επιθέσεις μέσω δικτύου. Η δεύτερη ομάδα ονομάζεται εξωτερική με φυσική πρόσβαση σε οντότητες δικτύου και περιλαμβάνει επιθέσεις σε διασύνδεση ραδιοσυχνοτήτων, επιθέσεις παραβίασης και μη εξουσιοδοτημένη πρόσβαση σε θύρες δικτύων. Η τρίτη ομάδα περιλαμβάνει τις επιθέσεις που βασίζονται σε κινητές συσκευές και επιθέσεις σε άλλες κινητές συσκευές ή και σε δίκτυα κινητής τηλεφωνίας. Τέλος, η τελευταία ομάδα επιθέσεων μπορεί να χαρακτηριστεί ως εσωτερικές επιθέσεις, οι οποίες συνήθως εκτελούνται από κακόβουλο προσωπικό της εταιρείας παροχής υπηρεσιών που εκμεταλλεύεται τα δικαιώματα του διαχειριστή.

Αυτές οι τέσσερις ομάδες επιθέσεων μπορούν να προκύψουν από πέντε κατηγορίες απειλών που εκμεταλλεύονται τα τρωτά σημεία του δικτύου κινητής τηλεφωνίας. Η πρώτη κατηγορία απειλών είναι η απώλεια διαθεσιμότητας, η οποία μπορεί να οδηγήσει σε επιθέσεις με στόχο την απώλεια της διαθεσιμότητας του δικτύου ή DoS επιθέσεις. Τυπικές επιθέσεις αυτού του είδους συνίστανται στην πλημμύρα μιας διασύνδεσης, στην κατάρρευση ενός στοιχείου δικτύου μέσω ενός ελαττώματος εφαρμογής πρωτοκόλλου ή εφαρμογής, στην καταστροφή πληροφοριών ή / και πόρων δικτύου. Στο φυσικό επίπεδο αυτό μπορεί να επιτευχθεί με το μπλοκάρισμα του ραδιοφωνικού καναλιού. Είναι επίσης πιθανό ότι πολλοί επιτιθέμενοι μπορεί να συντονιστούν για να ξεκινήσουν επιθέσεις μεγάλης κλίμακας που μπορούν να οδηγήσουν σε DDoS. Η δεύτερη ομάδα αφορά την απώλεια εμπιστευτικότητας, η οποία στοχεύει στην πρόσβαση σε εμπιστευτικά δεδομένα χρήστη και μπορεί να πραγματοποιηθεί με την

ανάλυση κρυπτογραφημένης κίνησης, υποκλοπής και μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητα δεδομένα σε ένα στοιχείο δικτύου μέσω διαρροής πληροφοριών.

Μια άλλη κατηγορία είναι η απώλεια της ακεραιότητας που μπορεί να επιτευχθεί μέσω της κίνησης και των τροποποιήσεων δεδομένων σε στοιχεία δικτύου με τη διεξαγωγή επιθέσεων MITM. Στην πραγματικότητα, το MITM αναφέρεται στην ικανότητα ενός εισβολέα να βρεθεί μεταξύ του χρήστη-στόχου και ενός γνήσιου δικτύου και έτσι να είναι σε θέση να παρακολουθεί, να τροποποιεί, να διαγράφει, να ανακατατάσσει, να επαναλαμβάνει τα δεδομένα των χρηστών και τη σηματοδότηση. Η επίθεση αυτή, μπορεί να χρησιμοποιηθεί για να συγκεντρωθούν πληροφορίες, να αποκτηθεί πρόσβαση σε ιδιωτικούς πόρους δικτύου, να αντληθούν πληροφορίες σχετικά με ένα δίκτυο και τους χρήστες του μέσω της ανάλυσης κυκλοφορίας, να αλλοιωθούν μεταδιδόμενα δεδομένα και να εισαχθούν νέες πληροφορίες σε συνεδρίες δικτύου. Η απώλεια της ακεραιότητας μπορεί επίσης να επιτευχθεί μέσω αναγνωρισμένων φορέων επαλήθευσης ταυτότητας στο δίκτυο. Πραγματοποιείται από έναν εισβολέα που αποκτά πρόσβαση σε φορείς επαλήθευσης παρακολουθώντας μηνύματα σηματοδότησης σε συνδέσμους δικτύου. Αυτοί οι εκτεθειμένοι φορείς αυθεντικοποίησης μπορεί να περιλαμβάνουν ζεύγη πρόκλησης / απόκρισης, κλειδιά κρυπτογράφησης και κλειδιά ακεραιότητας.

Η απώλεια ελέγχου αναφέρεται στην κατηγορία απειλών που αποσκοπεί στην απόκτηση του ελέγχου ενός στοιχείου δικτύου, εκμεταλλευόμενοι ελαττώματα υλοποίησης πρωτοκόλλου ή εφαρμογής και παίρνοντας τον έλεγχο μιας διεπαφή διαχείρισης.

Τέλος, η πέμπτη κατηγορία σχετίζεται με την Κλοπή Υπηρεσίας, η οποία μπορεί να επιτευχθεί χρησιμοποιώντας ελαττωματικό μηχανισμό αυθεντικοποίησης και εξουσιοδότησης

Αυτές οι ομάδες επιθέσεων μπορούν να στοχεύσουν το AS και το NAS του E-UTRAN και του EPC. Στο AS, μπορούν να στοχευθούν διαφορετικά χαρακτηριστικά και διαδικασίες βάσει του στρώματος πρωτοκόλλου (Physical, MAC / RLC, και RRC layers). Για παράδειγμα, στο επίπεδο RRC, οι κύριοι στόχοι είναι οι διαδικασίες όπως η σελιδοποίηση, η Εγκατάσταση / Απελευθέρωση σύνδεσης, η παράδοση και η διαχείριση κλειδιών ασφαλείας, οι μετρήσεις UE που σχετίζονται με την ενδοεπιχειρησιακή (inter-RAT) κινητικότητα και το QoS.

Σε σύγκριση με το AS που βασίζεται σε IP, οι απειλές στο NAS στοχεύουν τόσο τον τομέα PS όσο και τον τομέα Switch Circuit (CS Circuit). Για παράδειγμα, στον τομέα του

CS, οι απειλές μπορούν να επικεντρωθούν στη διαχείριση σύνδεσης (CM) και τη διαχείριση της κινητικότητας (MM), αντίθετα με τον τομέα PS, όπου οι απειλές μπορούν να στοχεύσουν στη διαχείριση συνόδων (SM) και GPRS Mobility Management (GMM) χαρακτηριστικά.

Ανάλογα με τον στόχο και τον σκοπό των απειλών, οι κύριες κατηγορίες απειλών σε περιβάλλον κινητών δικτύων που σχετίζονται με τις πέντε ομάδες επιθέσεων που παρουσιάστηκαν παραπάνω μπορούν να συνοψιστούν ως εξής:

- Υπερχείλιση διεπαφής: μπορεί να στοχεύει διαφορετικές διεπαφές στο δίκτυο κινητής τηλεφωνίας, συμπεριλαμβανομένων των διασυνδέσεων ραδιοσυχνοτήτων και των διασυνδέσεων backhaul.

- Συντριβή στοιχείων δικτύου: εκμεταλλεύεται τα πρωτόκολλα ή τα ελαττώματα της εφαρμογής προκειμένου να διαταράξει τη λειτουργία των ενεργών στοιχείων δικτύου.

- Παρακολούθηση της κυκλοφορίας: μπορεί να στοχεύει διαφορετικές διεπαφές συμπεριλαμβανομένης της διασύνδεσης ραδιοσυχνοτήτων, του backhaul, του επιπέδου ελέγχου και του επιπέδου χρήσης. Συνίσταται στην ακρόαση μιας επικοινωνία, στην κατασκοπεία του δικτύου, προκειμένου να συγκεντρωθούν ή να κλαπούν πληροφορίες. Ένας εισβολέας μπορεί να εντοπίσει ευαίσθητα προσωπικά δεδομένα και να τα κλέψει κατά τη διάρκεια της μετάδοσής τους μέσω του εσωτερικού ή του εξωτερικού δικτύου ή από δικτυωμένες συσκευές αποκτώντας μη εξουσιοδοτημένη πρόσβαση. Οι πληροφορίες που συλλέγονται μέσω της παρακολούθησης μπορούν να χρησιμοποιηθούν για την εκτέλεση άλλων επιθέσεων που στοχεύουν τα δίκτυα κινητής τηλεφωνίας. Η υποκλοπή αναφέρεται επίσης στην ικανότητα ενός εισβολέα να παρακολουθεί σηματοδοσίες και δεδομένα που αφορούν άλλους χρήστες μέσω της τροποποίησης του απαιτούμενου εξοπλισμού, όπως ενός MS.

- Μη εξουσιοδοτημένη πρόσβαση δεδομένων: στοχεύει ευαίσθητα δεδομένα σε ένα τμήμα δικτύου και μπορεί να επιτευχθεί μέσω διαρροής δεδομένων.

- Τροποποίηση κίνησης: στοχεύει διαφορετικούς τύπους δεδομένων κίνησης στη ραδιοφωνική διεπαφή, στο backhaul, στο επίπεδο C και στο επίπεδο U.

- Τροποποίηση δεδομένων σε ένα στοιχείο δικτύου: μπορεί να πραγματοποιηθεί με την αξιοποίηση ελαττωμάτων της εφαρμογής πρωτοκόλλου ή της εφαρμογής λειτουργίας.

- Συμβιβασμός ενός στοιχείου δικτύου: μπορεί να επιτευχθεί είτε μέσω ενός ελαττώματος υλοποίησης του πρωτοκόλλου ή της εφαρμογής είτε μέσω διεπαφής διαχείρισης. Χρησιμοποιώντας ένα συμβιβαζόμενο στοιχείο δικτύου, όπως ένα MS, ένας εισβολέας μπορεί να εκτελέσει την πλαστοπροσωπία στέλνοντας δεδομένα χρήστη στο δίκτυο, σε μια προσπάθεια να κάνει το δίκτυο να πιστέψει ότι προέρχονται από το χρήστη-στόχο. Ομοίως, χρησιμοποιώντας έναν τροποποιημένο BS, ένας εισβολέας μπορεί να πραγματοποιήσει την πλαστοπροσωπία δικτύου στέλνοντας σήματα ή/και δεδομένα χρήστη στον χρήστη-στόχο, σε μια προσπάθεια να κάνει το χρήστη-στόχο να πιστέψει ότι προέρχεται από ένα γνήσιο δίκτυο.

- Κακόβουλος χρήστης: αποτελείται από έναν χρήστη που χρησιμοποιεί ακούσια μια κακόβουλη εφαρμογή ή από έναν διαχειριστή με εξουσιοδοτημένη πρόσβαση στο δίκτυο.

- Κλοπή υπηρεσίας: αναφέρεται σε μια λαθραία χρήση της υπηρεσίας χωρίς χρέωση. Μπορεί να επιτευχθεί με την αξιοποίηση ενός ελαττώματος στους μηχανισμούς αυθεντικοποίησης και εξουσιοδότησης ή εντός των διαδικασιών χρέωσης για τη χρήση υπηρεσιών χωρίς χρέωση.

4 Αδυναμίες ασφάλειας GSM

Αδύναμες πλευρές των Μηχανισμών Ασφαλείας

Το GSM δεν διαθέτει τέλειο σύστημα ασφαλείας. Οι αντίπαλοι μπορούν να παρακολουθήσουν το κανάλι σε πραγματικό χρόνο. Οι αδύναμες πλευρές των μηχανισμών ασφάλειας GSM θα συζητηθούν σε αυτό το κεφάλαιο.

Πρώτα απ 'όλα, οι περισσότεροι φορείς εκμετάλλευσης δεν διαθέτουν επαρκή εξειδίκευση για να υιοθετήσουν τους νέους A3/8 αλγορίθμους. Έτσι χρησιμοποιούν τη λειτουργία COMP128 χωρίς να το αλλάξουν. Αυτό είναι ένα μεγάλο πρόβλημα ασφαλείας, επειδή όλες οι λειτουργίες COMP128 έχουν βρεθεί με αντίστροφη μηχανική.

Το μέγεθος bit των αλγορίθμων είναι ασθενές. Ο αλγόριθμος A5 / 1 χρησιμοποιεί 64 bit Kc στην καλύτερη περίπτωση. Οι περισσότεροι χειριστές χρησιμοποιούν COMP128 που έχει 54 bit Kc και τα τελευταία 10 bits είναι πάντα μηδενικά. Επίσης ο A5 / 2 είναι ασθενέστερος από τον A5 / 1.

Επιπλέον, το ερώτημα ελέγχου ταυτότητας υπάρχει μόνο στην επικοινωνία BTS-MS. Δεν υπάρχει έλεγχος ταυτότητας για το MS-BTS. Αυτό σημαίνει ότι οι ψεύτικοι σταθμοί βάσης μπορούν να συμπεριφέρονται σαν πραγματικό BTS και η MS θα απαντήσει σε κάθε αίτημα SRES από αυτούς. Το δίκτυο δεν επαληθεύεται σε ένα τηλέφωνο. Αυτό είναι το πιο σοβαρό σφάλμα στην ασφάλεια του GSM, το οποίο επιτρέπει μια επίθεση MITM. Αυτή η αδυναμία ήταν γνωστή για τους κατασκευαστές GSM κατά την εποχή του σχεδιασμού GSM, αλλά αναμενόταν ότι η κατασκευή ενός ψεύτικου BTS θα ήταν υπερβολικά ακριβή και θα ήταν δύσκολο να καταστούν οι επιθέσεις αυτές αποδοτικές. Ωστόσο, μετά από 20 χρόνια η κατάσταση άλλαξε σημαντικά.

Σήμερα υπάρχουν εταιρείες που παράγουν προϊόν BTS μικρής εμβέλειας, οπότε ο επιτιθέμενος μπορεί απλά να αγοράσει ένα BTS σε χαμηλή τιμή.

Μια άλλη σοβαρή ευπάθεια του GSM είναι η έλλειψη κατάλληλου αναγνωριστικού καλούντος ή αναγνωριστικού αποστολέα επαλήθευσης. Με άλλα λόγια, ο αριθμός του καλούντος ή ο αριθμός αποστολέα SMS θα μπορούσε να παραποιηθεί. Ο αριθμός καλούντος και η φωνή μεταδίδονται σε διαφορετικά κανάλια. Έτσι, το Called ID ή το SMS ID μπορεί να παραποιηθεί.

Μια άλλη αδυναμία που μπορεί ο επιτιθέμενος να εκμεταλλευτεί είναι η ευπάθεια στον μηχανισμό προστασίας του IMSI. Τα δίκτυα χρησιμοποιούν το TMSI για να προστατεύσουν το IMSI, αλλά αν το δίκτυο χάσει κάπως το ίχνος ενός συγκεκριμένου TMSI, τότε πρέπει να ζητήσει από τον συνδρομητή το IMSI του μέσω ραδιοζεύξης. Η σύνδεση δεν μπορεί να κρυπτογραφηθεί επειδή το δίκτυο δεν γνωρίζει την ταυτότητα του χρήστη και επομένως το IMSI αποστέλλεται σε απλό κείμενο. Ο επιτιθέμενος μπορεί να ελέγξει κατά πόσον ένας συγκεκριμένος χρήστης (IMSI) βρίσκεται κοντά.

4.1 Ιστορική αναδρομή των αλγορίθμων σπασίματος

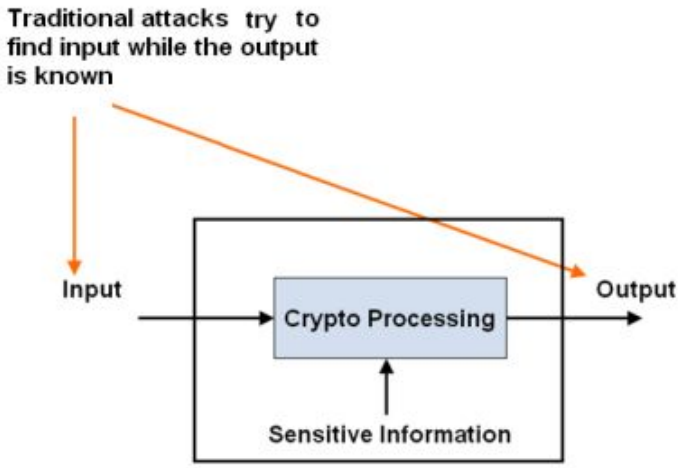
Τον Απρίλιο του 1998, ο Σύνδεσμος Προγραμματιστών Smartcard (SDA) μαζί με δύο ερευνητές του U.K. Berkeley ισχυρίστηκαν ότι έχουν σπάσει τον αλγόριθμο COMP128 που είναι αποθηκευμένος στη SIM. Με την αποστολή μεγάλου αριθμού προκλήσεων στη μονάδα εξουσιοδότησης, μπορούσαν να συμπεράνουν το Ki μέσα σε μερικές ώρες. Ανακάλυψαν επίσης ότι η Kc χρησιμοποιεί μόνο 54 bits από τα 64 bits. Τα υπόλοιπα 10 bits αντικαθίστανται από μηδενικά, γεγονός που καθιστά το κλειδί κρυπτογράφησης αρκετά ασθενέστερο. Πιστεύουν ότι αυτό οφείλεται σε κρατική παρέμβαση. Ένα ασθενέστερο κλειδί κρυπτογράφησης, θα μπορούσε να επιτρέψει στις κυβερνήσεις να παρακολουθήσουν συνομιλίες.

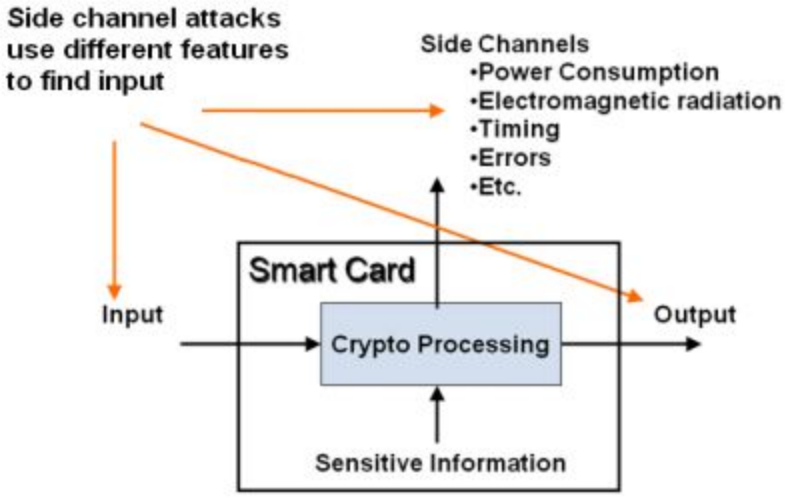
Ο SDA ήταν παρόν όταν έσπασε ο αλγόριθμος της SIM κάρτας. Αν και φοβήθηκαν ότι "μια επίθεση εναέριας κυκλοφορίας" δεν είναι εξεζητημένη, δυστυχώς, δεν ήταν σε θέση να επιβεβαιώσουν τις υποψίες τους, καθώς ο εξοπλισμός που απαιτείται για την πραγματοποίηση μιας τέτοιας επίθεσης ήταν παράνομος στις ΗΠΑ. Η GSM Alliance ανταποκρίθηκε στο περιστατικό, δηλώνοντας ότι ακόμα και αν μια SIM θα μπορούσε να κλωνοποιηθεί, δεν θα εξυπηρετούσε κανένα σκοπό, καθώς το δίκτυο GSM θα επιτρέπει μόνο μία κλήση από οποιοδήποτε αριθμό τηλεφώνου οποιαδήποτε στιγμή. Τα δίκτυα GSM είναι επίσης ικανά να ανιχνεύουν και να κλείνουν διπλούς κωδικούς SIM που βρίσκονται σε πολλά τηλέφωνα.

Τον Αύγουστο του 1999, μια αμερικανική ομάδα ερευνητών ισχυρίστηκε ότι έχει σπάσει τον πιο αδύναμο αλγόριθμο A5 / 2 που χρησιμοποιείται συνήθως στην Ασία, χρησιμοποιώντας ένα μόνο υπολογιστή μέσα σε λίγα δευτερόλεπτα.

Τον Δεκέμβριο του 1999, δύο κορυφαίοι Ισραηλινοί κρυπτογράφοι ισχυρίστηκαν ότι έχουν σπάσει τον ισχυρό αλγόριθμο A5 / 1 που ήταν υπεύθυνος για την κρυπτογράφηση συνομιλιών. Παραδέχονται ότι η εκδοχή που έχουν σπάσει μπορεί να μην είναι η ακριβής έκδοση που χρησιμοποιείται σε κινητά τηλέφωνα GSM, καθώς οι χειριστές GSM επιτρέπεται να πραγματοποιούν μικρές τροποποιήσεις στους αλγόριθμους GSM. Οι ερευνητές χρησιμοποίησαν ψηφιακό σαρωτή και υπολογιστή υψηλής τεχνολογίας για να σπάσουν τον κώδικα. Μέσα σε δύο λεπτά από την παραλαβή μιας κλήσης με ψηφιακό σαρωτή, οι ερευνητές μπόρεσαν να ακούσουν τη συζήτηση. Η GSM Alliance της Βόρειας Αμερικής ισχυρίστηκε ότι κανένα από τα μέλη της δεν χρησιμοποιεί τον αλγόριθμο A5/1, επιλέγοντας πιο πρόσφατα αναπτυχθέντες αλγόριθμους.

Τον Μάιο του 2002, ο όμιλος IBM Research ανακάλυψε έναν νέο τρόπο γρήγορης απόσπασης των κλειδιών COMP128 χρησιμοποιώντας πλευρικά κανάλια.



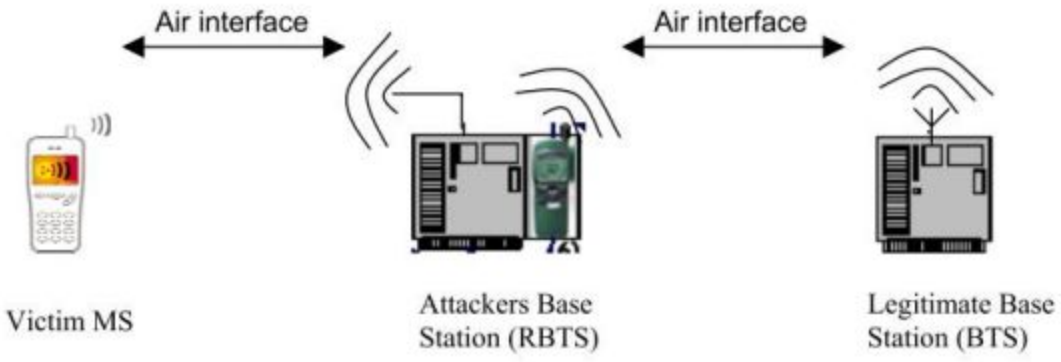


4.2 Δημοφιλή είδη επιθέσεων

Σε αυτό το κεφάλαιο θα περιγραφούν οι σημαντικές επιθέσεις στην ανωνυμία, την αυθεντικοποίηση και την εμπιστευτικότητα.

4.2.1 Καταγραφή ενός ή περισσότερων κινητών σταθμών

Σε πολλές από τις επιθέσεις που περιγράφονται σε αυτό το κεφάλαιο, ο επιτιθέμενος πρέπει να προσποιηθεί το δίκτυο σε ένα MS ή να προσποιηθεί το MS στο δίκτυο ή και τα δύο σε ένα λεγόμενο MITM. Ένας εισβολέας που μιμείται το BS και το MS μεταξύ τους μπορεί να υποκλέψει, να τροποποιήσει, να διαγράψει, να αναπαράγει και να μεταδίδει σήματα / δεδομένα χρήστη μεταξύ δύο επικοινωνούντων οντοτήτων. Ο απαιτούμενος εξοπλισμός είναι μια προσαρμοσμένη και τροποποιημένη δέσμη BTS και MS. Το τροποποιημένο BTS συμπεριφέρεται ως ταυτότητα του δικτύου με το MS, ενώ το τροποποιημένο MS μοιράζεται το MS στο δίκτυο.



Πριν από μια ενεργή επίθεση, ο επιτιθέμενος μπορεί να χρειαστεί να παρακολουθήσει το MS. Ο επιτιθέμενος μπορεί να θέλει να μάθει τις πληροφορίες που περιλαμβάνει η ταυτότητα της κυψέλης, τη ταυτότητα του δικτύου, τη δομή του καναλιού ελέγχου, τη λίστα των καναλιών που χρησιμοποιούνται και λεπτομέρειες του πρωτοκόλλου πρόσβασης. Με αυτόν τον τρόπο, ένας εισβολέας με Fake BTS, που παρέχει υψηλότερα επίπεδα ισχύος από το BTS, μεταξύ του θύματος MS και του νόμιμου BTS, αναγκάζει τα MS να χρησιμοποιούν το FBTS. Το MS καταγράφεται από τον εισβολέα ο οποίος ελέγχει ποια μηνύματα μεταφέρονται από το MS στο BTS καθώς και μηνύματα που ρέουν προς την άλλη κατεύθυνση. Αφού καταγράψει την ταυτότητα του MS, ο εισβολέας θα τη χρησιμοποιήσει στη συνέχεια για να παράσχει κατασκευασμένα μηνύματα για λογαριασμό ενός νόμιμου συνδρομητή.

4.2.2 Επιθέσεις κατά της ανωνυμίας των χρηστών GSM

Η ανωνυμία στο GSM παρέχεται μέσω της χρήσης του προσωρινού αναγνωριστικού TMSI, το οποίο είναι σαν ένα ψευδώνυμο του συνδρομητή τοπικά. Ένας επιτιθέμενος μπορεί να θέλει τις κινήσεις κάποιου συνδρομητή ή/και να ακολουθεί δείγματα κλήσεων και έτσι πρέπει να έχει το IMSI και το TMSI του MS. Αυτές οι πληροφορίες μπορούν επίσης να χρησιμοποιηθούν για την επίθεση άλλων στοιχείων ασφαλείας εκτός από την ανωνυμία, για παράδειγμα, η υποκλοπή σε ένα συγκεκριμένο άτομο. Εάν ο επιτιθέμενος μπορεί να πάρει το IMSI του συνδρομητή ή του συσχετιζόμενου τρέχοντος TMSI ενός συγκεκριμένου ατόμου, τότε η ανωνυμία του χρήστη είναι επισφαλής.

4.2.3 Παθητική παρακολούθηση:

Κάθε φορά που ενεργοποιείται ένα MS, απαιτείται η εισαγωγή του στο δίκτυο. Αυτό γίνεται με ένα συνημμένο IMSI. Η επισύναψη του IMSI συμβαίνει σε περίπτωση ενημέρωσης τοποθεσίας. Δεδομένου ότι το IMSI δεν είναι καταχωρημένο στο δίκτυο και δεν υπάρχει ακόμα έλεγχος ταυτότητας, δεν μπορεί να εφαρμοστεί κρυπτογράφηση. Ως εκ τούτου, το IMSI αποστέλλεται με καθαρό κείμενο. Ένας εισβολέας που ακούει την εναέρια κυκλοφορία μπορεί να αποσπάσει το IMSI του χρήστη.

Η παθητική παρακολούθηση των χρηστών GSM και η απόσπαση της μόνιμης ταυτότητας των χρηστών (IMSI) είναι δυνατή και εύκολη. Αυτές οι πληροφορίες παρέχουν στον εισβολέα ένα λειτουργικό IMSI και τη γνώση του ότι ο ιδιοκτήτης του IMSI είναι στην παρούσα περιοχή. Ωστόσο, η παθητική παρακολούθηση είναι αναποτελεσματική και χρονοβόρα δεδομένου ότι ο επιτιθέμενος πρέπει είτε να περιμένει τα MS να εκτελέσουν την επισύναψη του IMSI όταν είναι ενεργοποιημένο είτε μια βάση δεδομένων να μην εμφανιστεί στο δίκτυο, κάτι που δεν συμβαίνει τόσο συχνά.

4.2.4 Ενεργός παρακολούθηση:

Για την παρακολούθηση ενός συνδρομητή GSM, ο εισβολέας μπορεί να κάνει χρήση της διαδικασίας ταυτοποίησης. Το δίκτυο μπορεί να ξεκινήσει διαδικασία αναγνώρισης, εάν το δίκτυο δεν μπορεί να εντοπίσει το MS χρησιμοποιώντας το TMSI του. Η διαδικασία ταυτοποίησης ξεκινά με τη μετάδοση ενός μηνύματος ΑΙΤΗΣΗΣ ΤΑΥΤΟΤΗΤΑΣ στο MS, ώστε να του ζητηθεί να μεταδώσει μία παράμετρο προσδιορισμού. Το δίκτυο μπορεί να ζητήσει IMSI, IMEI ή TMSI. Δεδομένου ότι το GSM δεν χρησιμοποιεί έλεγχο ταυτότητας μηνυμάτων για να ελέγξει την προέλευση του μηνύματος στη ραδιοζεύξη, ένας εισβολέας με αρκετή λειτουργικότητα σταθμού βάσης μπορεί να χρησιμοποιήσει αυτά τα μηνύματα για να ανακτήσει τις ίδιες πληροφορίες με έναν νόμιμο σταθμό βάσης εξαπατώντας το MS-στόχο. Θα πρέπει να είναι δυνατόν να ζητηθεί από έναν συνδρομητή (του οποίου το IMSI είναι γνωστό από τον εισβολέα) το TMSI που χρησιμοποιείται στην διαδικασία ταυτοποίησης. Όταν ο εισβολέας γνωρίζει τη δέσμη IMSI / TMSI, είναι δυνατό να εντοπίσει έναν συγκεκριμένο συνδρομητή. Ο επιτιθέμενος απλώς σελιδοποιεί το MS με το συγκεκριμένο IMSI / TMSI.

4.2.5 Επιθέσεις στον Αλγόριθμο αυθεντικοποίησης:

Πολλοί φορείς παροχής GSM χρησιμοποιούν την προδιαγραφή σχεδιασμού που δίδεται στο GSM MoU, το COMP128, αντί να σχεδιάσουν τον δικό τους αλγόριθμο για την εξακρίβωση της ταυτότητας (A3) και την παραγωγή κλειδιού συνόδου (A8). Η δυσκολία να αρχίσουμε να δημιουργούμε νέο αλγόριθμο είναι ότι οι συνδρομητές που αγόρασαν κάρτες SIM πριν από την ενδεχόμενη εισαγωγή ενός διαφορετικού αλγορίθμου, χρησιμοποιούν τις παλιές τους κάρτες SIM με τον παλιό αλγόριθμο. Άλλος λόγος αλλαγής / αναθεώρησης του αλγορίθμου είναι το κόστος αλλαγής λογισμικού στη βάση δεδομένων. Από την άλλη πλευρά, είναι δυνατό να χρησιμοποιηθούν νέες και πιο ασφαλείς εκδόσεις του COMP128 σε νέες κάρτες SIM που δίνονται σε νέους συνδρομητές.

Ο σχεδιασμός του COMP128 δεν δημοσιοποιήθηκε ποτέ, αλλά η αρχιτεκτονική του έχει σχεδιαστεί και κρυπτοαναλυθεί με αντίστροφη μηχανική. Σήμερα, είναι αρκετά εύκολο να βρεθεί η εφαρμογή λογισμικού του COMP128 με απλή αναζήτηση στο διαδίκτυο. Δεδομένου ότι οι προδιαγραφές GSM για τις κάρτες SIM είναι ευρέως διαθέσιμες, το μόνο που απαιτείται για την κλωνοποίηση μιας κάρτας SIM είναι το κρυπτογραφημένο κλειδί 128bit του COMP128 και το IMSI που είναι κωδικοποιημένο στην κάρτα SIM.

Αντιγράφοντας το Ki και το IMSI σε μία κενή SIM, ο εισβολέας μπορεί να αυθεντικοποίησει τον εαυτό του στο δίκτυο ως νόμιμος συνδρομητής και έτσι να καλέσει με χρέωση. Ο εισβολέας μπορεί ακόμη και αντί να χρησιμοποιήσει τη συνδρομή, να χρησιμοποιεί το κλειδί Ki για να αποκρυπτογραφήσει όλες τις κλήσεις από και προς τον συνδρομητή.

Η κλωνοποίηση μπορεί να πραγματοποιηθεί είτε με φυσική πρόσβαση στην SIM που πρόκειται να κλωνοποιηθεί είτε μέσω του αέρα. Οι ακόλουθες υποενότητες θα εξετάσουν τις δύο αυτές περιπτώσεις:

4.2.6 Κλωνοποίηση της SIM κάρτας με φυσική πρόσβαση:

Εάν ο εισβολέας έχει φυσική πρόσβαση στη κάρτα SIM, διάφορες επιθέσεις μπορούν να ξεκινήσουν, προκειμένου να κλωνοποιηθεί. Ορισμένες από αυτές τις επιθέσεις βασίζονται στη εκμετάλλευση σφαλμάτων στον κρυπτογραφικό αλγόριθμο που χρησιμοποιεί η έξυπνη κάρτα, ενώ άλλες χρησιμοποιούν ευπάθειες στην ίδια την έξυπνη κάρτα.

Η πιο δημοφιλής επίθεση σε κάρτες SIM είναι οι επιθέσεις στον ίδιο τον κρυπτογραφικό αλγόριθμο (COMP128). Είναι μια επίθεση επιλεγμένης πρόκλησης και χρήσης σφαλμάτων στη λειτουργία κατακερματισμού για να συνταχθεί το μυστικό κλειδί Ki. Ο επιτιθέμενος δημιουργεί μια σειρά από ειδικά επιλεγμένες προκλήσεις και η SIM διερωτάται για κάθε μία από αυτές. Η κάρτα SIM εφαρμόζει το COMP128 στο μυστικό κλειδί και την επιλεγμένη πρόκληση, επιστρέφοντας μια απάντηση πίσω. Μετά την ανάλυση των απαντήσεων, ο επιτιθέμενος μπορεί να καθορίσει το Ki. Το αποτέλεσμα αυτής της επίθεσης είναι ότι ο επιτιθέμενος αποκτά πρόσβαση στο μυστικό κλειδί Ki του MS. Η επίθεση εκμεταλλεύεται την έλλειψη διάχυσης, πράγμα που σημαίνει ότι ορισμένα τμήματα της hash εξόδου εξαρτώνται μόνο από ορισμένα τμήματα της εισόδου στον αλγόριθμο. Η βάση αυτής της επίθεσης απαιτεί, εκτός από την φυσική πρόσβαση στην SIM προορισμού, έναν αναγνώστη έξυπνης κάρτας και έναν υπολογιστή για να κατευθύνει τη λειτουργία. Η επίθεση απαιτεί κάποιον να ερωτά την SIM περίπου 150.000 φορές. Ένας μέσος αναγνώστης SIM μπορεί να εκδώσει 6,25 ερωτήματα ανά δευτερόλεπτο, οπότε η όλη επίθεση διαρκεί περίπου 8 ώρες. Με την ανανέωση της κάρτας SIM ή τη χρήση ταλαντωτή υψηλότερης συχνότητας στον αναγνώστη καρτών SIM ο χρόνος επεξεργασίας θα μπορούσε να μειωθεί σημαντικά. Αυτό αυξάνει ωστόσο τον κίνδυνο αποτυχίας και βλάβης στην αρχική SIM.

4.2.7 Κλωνοποίηση πάνω στον αέρα:

Ο επιτιθέμενος μπορεί να εκτελέσει ακόμη και την επίθεση στον αέρα, κάνοντας χρήση ενός ψεύτικου σταθμού βάσης. Εκτός από αυτόν τον εξοπλισμό, ο επιτιθέμενος πρέπει να γνωρίζει το IMSI ή TMSI του στόχου. Τα σπασμένα MS θα αναγκαστούν αμέσως να πραγματοποιήσουν μια αίτηση ενημέρωσης τοποθεσίας η οποία είναι καθοδηγούμενη.

Αφού ολοκληρωθεί η διαδικασία αυτή, ο εισβολέας ξεκινά διαδικασία αυθεντικοποίησης. Αμέσως μόλις ο εισβολέας έχει ένα ζευγάρι πρόκλησης-απόκρισης, ξεκινά μια νέα διαδικασία επαλήθευσης ταυτότητας. Το MS καλείται να ανταποκριθεί σε κάθε πρόκληση που προκαλείται από το δίκτυο GSM. Αυτή η διαδικασία συνεχίζεται μέχρι ο εισβολέας να έχει τον απαιτούμενο αριθμό ζευγών για να μπορέσει να ξεκινήσει τη διαδικασία κλωνοποίησης.

Θεωρείται ότι το στάδιο εγκατάστασης του καναλιού πρέπει να γίνει μόνο μία φορά. Ο αριθμός των πλαισίων που ανταλλάσσονται μεταξύ του δικτύου και ενός MS, για μια διαδικασία επαλήθευσης ταυτότητας, είναι περίπου 66 καρέ. Δεδομένου ότι η διάρκεια ενός πλαισίου TDMA είναι 4.610 ms, η διάρκεια ολόκληρης της ακολουθίας σηματοδότησης είναι 4.615 ms / frame x 66 frames = 0.30459 s. Ο χρόνος που χρειάζεται για να επιτευχθεί ο αριθμός των ζευγών πρόκλησης-απόκρισης που απαιτούνται για την επίθεση μπορεί να υπολογιστεί. Είναι γνωστό ότι η κρυπτογραφική επίθεση απαιτεί περίπου 150.000 ζεύγη πρόκλησης-απόκρισης. Αυτό σημαίνει ότι η επίθεση διαρκεί περίπου 45.689 δευτερόλεπτα (150.000 προκλήσεις x 0.30459 s), δηλαδή περίπου 13 ώρες. Αυτό συνεπάγεται ότι τα MS πρέπει να είναι διαθέσιμα στον επιτιθέμενο καθ 'όλη τη διάρκεια του χρόνου για να συγκεντρωθούν οι πληροφορίες. Αυτό είναι αρκετά μη ρεαλιστικό, επειδή οι άνθρωποι χρησιμοποιούν τα κινητά τους για να κάνουν κλήσεις ή να λαμβάνουν κλήσεις εκτός από το γεγονός ότι ένας τέτοιος βομβαρδισμός με προκλήσεις μπορεί να προκαλέσει την εξάντληση της μπαταρίας των κινητών, γεγονός που θα έβαζε το θύμα σε υποψίες. Για να απαλλαγούμε από αυτά τα προβλήματα, η επίθεση μπορεί να εκτελεστεί σε μέρη. Αντί να εκτελέσει μια επίθεση 13 ωρών, ο επιτιθέμενος θα μπορούσε να μιλά με το MS για 30 λεπτά κάθε μέρα. Με τον τρόπο αυτό, η μπαταρία δεν θα εξαντληθεί και θα υπήρχε μικρός κίνδυνος να γίνει ύποπτος ο ιδιοκτήτης ή το νόμιμο δίκτυο.

Η άμυνα κατά της κλωνοποίησης μέσω του αέρα είναι να περιορίζεται ο αριθμός των φορών που μπορεί να πιστοποιηθεί μια SIM σε έναν αριθμό σημαντικά μικρότερο από 150.000. Η SIM κλειδώνει εάν το όριο ξεπεραστεί. Το μειονέκτημα αυτής της λύσης είναι ότι πρέπει να εκδοθεί και να διανεμηθεί στον συνδρομητή μια νέα SIM, η οποία έχει ως αποτέλεσμα επιπλέον κόστος τόσο για τον συνδρομητή όσο και για τον πάροχο.

4.3 Επιθέσεις στην εμπιστευτικότητα του GSM

Στις επόμενες υποενότητες οι επιθέσεις διαχωρίζονται σε τρείς κατηγορίες: επιθέσεις βίαιης δύναμης(brute force), κρυπτοαναλυτικές επιθέσεις και μη κρυπτοαναλυτικές επιθέσεις.

4.3.1 Brute-Force Attacks

Η εμπιστευτικότητα του GSM προστατεύεται από την μυστικότητα του Kc. Το Kc είναι 64 bit, αν και τα τελευταία 10 bits είναι μηδενικά. Αυτό μειώνει το χώρο κλειδιών από 2 ^ 64 σε 2 ^ 54. Το A5 / 2 αναπτύχθηκε με τη βοήθεια της NSA και μπορεί να σπάσει σε πραγματικό χρόνο με παράγοντα εργασίας περίπου 2 ^ 16. Το A5 / 1, η ισχυρότερη από τις δύο παραλλαγές, είναι και αυτή επιρρεπής σε επιθέσεις και μπορεί να σπάσει με συντελεστή εργασίας 2 ^ 40.

Το τσιπ Pentium 4 έχει σχεδόν 60 εκατομμύρια τρανζίστορ και η υλοποίηση ενός συνόλου από LFSR (A5 / 1) θα απαιτούσε περίπου 2000 τρανζίστορ, 30.000 παράλληλες υλοποιήσεις A5 / 1 σε ένα τσιπ μπορούν να γίνουν. Εάν το τσιπ χρονίζεται σε 3,2 GHz και κάθε υλοποίηση A5 / 1 θα δημιουργούσε ένα bit εξόδου για κάθε κύκλο ρολογιού τότε χρειάζεται να παράγει δυαδικά ψηφία εξόδου 100 + 114 + 114, κατά συνέπεια περίπου 10M κλειδιά ανά δευτερόλεπτο του A5 / 1 μπορούν να χρησιμοποιηθούν. Ένας χώρος κλειδιού 2^54 θα απαιτούσε επομένως περίπου 18 ώρες, χρησιμοποιώντας όλες τις παράλληλες υλοποιήσεις στο τσιπ. Αν η επίθεση στη μέση περίπτωση επιτύχει μετά από αναζήτηση του μισού του κεντρικού χώρου, το κλειδί βρίσκεται σε περίπου 9 ώρες. Περαιτέρω βελτιστοποίηση μέσω της εγκατάλειψης ενός συγκεκριμένου κλειδιού μετά το πρώτο μη έγκυρο bit και τη διανομή του υπολογισμού μεταξύ των πολλαπλών τσίπ θα μείωνε τον χρόνο υπολογισμού κατά αρκετά μεγέθη. Αυτό, ακόμα και στη καλύτερη περίπτωση, σημαίνει αρκετές ώρες επεξεργασίας και είναι πολύ μακριά από επίθεση σε πραγματικό χρόνο. Έχετε υπόψη ότι η πολυπλοκότητα της επίθεσης είναι ακόμη μεγαλύτερη λόγω του ότι είναι αρκετά

δύσκολο να προσδιοριστεί πότε θα βρεθεί το κλειδί λόγω της φύσης του απλού κειμένου.

Συμπερασματικά, είναι πολύ δύσκολο να επιτύχουμε μια Brute-Force Attack σε πραγματικό χρόνο, αλλά είναι αρκετά δυνατό να βρούμε ένα δοθέν κλειδί σε μερικές ώρες. Οι επιτιθέμενοι με επαρκείς πόρους (υπολογιστική ισχύς) πιθανόν να μπορούν να μειώσουν σημαντικά τον χρόνο επεξεργασίας.

4.3.2 Επιθέσεις Κρυπτανάλυσης

Υπάρχουν αρκετές κρυπτοαναλυτικές επιθέσεις κατά των αλγορίθμων που προστατεύουν διάφορες πτυχές του GSM. Ο αλγόριθμος που χρησιμοποιείται από πολλούς φορείς εκμετάλλευσης για τον έλεγχο ταυτότητας των συνδρομητών (COMP128) σπάει λόγω ελαττωμάτων στο σχεδιασμό της συνάρτησης κατακερματισμού. Το αποτέλεσμα είναι η δυνατότητα των εισβολέων να κλωνοποιήσουν τις συνδρομές είτε με φυσική πρόσβαση στη SIM προορισμού είτε μέσω του αέρα. Η πιο δημοφιλής επίθεση απαιτεί φυσική πρόσβαση στην SIM για κλωνοποίηση και ολοκληρώνεται σε περίπου 8 ώρες. Μπορεί να επιταχυνθεί με τον κίνδυνο να καταστραφεί η κάρτα SIM. Ο πιο αποτελεσματικός τρόπος για να κλωνοποιηθεί μια smartcard GSM είναι μια επίθεση διαμέρισης που προτείνεται από μια ομάδα της IBM. Απαιτεί την πρόκληση της SIM προορισμού μόνο 8 φορές στην καλύτερη περίπτωση, πράγμα που σημαίνει ότι η κλωνοποίηση μπορεί να γίνει σε λεπτά ή και δευτερόλεπτα. Ο εξοπλισμός που απαιτείται για την εκτέλεση αυτής της επίθεσης (ένας ειδικά σχεδιασμένος αναγνώστης και λογισμικό smartcard) είναι διαθέσιμος μόνο σε εργαστήρια. Νέες εκδόσεις του COMP128 έχουν αναπτυχθεί και διανεμηθεί. Ωστόσο, δεν είναι γνωστό σε ποιο βαθμό αυτές οι ισχυρότερες εκδόσεις έχουν προσαρμοστεί από τους παρόχους. Μια εικασία είναι ότι πολλοί πάροχοι εξακολουθούν να χρησιμοποιούν τον παλιό αλγόριθμο λόγω των δαπανών αναβάθμισης. Αυτό που είναι γνωστό είναι ότι οι χρήστες που είχαν COMP128 μέσα στις κάρτες SIM όταν αγοράζουν μια συνδρομή εξακολουθούν να χρησιμοποιούν το COMP128.

Υπάρχουν διάφορες κρυπτοαναλυτικές προτάσεις σχετικά με τον τρόπο επίθεσης των αλγορίθμων κρυπτογράφησης που χρησιμοποιούνται για την προστασία της εμπιστευτικότητας που σπάζουν αυτούς τους αλγόριθμους σε πραγματικό χρόνο. Υπάρχουν αρκετές επιθέσεις εναντίον των A5 / 1 και A5 / 2, αν και οι περισσότερες από

αυτές έχουν μόνο θεωρητική αξία. Οι περισσότερες από τις επιθέσεις απαιτούν ο εισβολέας να γνωρίζει τμήματα της ακολουθίας κλειδιού. Η απόκτηση μικρών τμημάτων απλού κειμένου είναι δυνατή, διότι ο εισβολέας γνωρίζει συχνά τη δομή και το περιεχόμενο των μηνυμάτων σηματοδότησης (ειδικά αν ο εισβολέας μοιράζεται το δίκτυο με το θύμα MS και ως εκ τούτου μπορεί να ζητήσει πληροφορίες από το MS για πληροφορίες). Επιπλέον το γεγονός ότι η κωδικοποίηση καναλιών εφαρμόζεται στα δεδομένα πριν από την κρυπτογράφηση. Ένας επιτιθέμενος που πραγματοποιεί μια MITM μπορεί να ζητήσει από τον συνδρομητή-θύμα να μεταδώσει ορισμένα μηνύματα σηματοδοσίας (των οποίων το περιεχόμενο είναι γνωστό ή σχεδόν γνωστό) μετά την έναρξη της κρυπτογράφησης. Ο επιτιθέμενος έχει στη συνέχεια πρόσβαση στο κρυπτογραφικό κείμενο επιπλέον των γνωστών τμημάτων του απλού κειμένου και μπορεί έτσι να αντλεί τμήματα της ακολουθίας κλειδιού που χρησιμοποιείται στη διαδικασία κρυπτογράφησης. Είναι, ωστόσο, δύσκολο να ληφθούν τα μεγέθη του καθαρού κειμένου που απαιτούνται από κάποιες από αυτές τις επιθέσεις. Η επίθεση που απαιτεί λιγότερο γνωστό καθαρό κείμενο είναι μια επίθεση εναντίον του A5 / 2. Απαιτεί ότι ο εισβολέας γνωρίζει από το απλό κείμενο δύο καρέ περίπου έξι δευτερόλεπτα μεταξύ τους και βρίσκει το κλειδί της συνδιάλεξης σε περίπου 10 ms. Η γνωστή απαίτηση ελεύθερου κώδικα μπορεί να είναι δυνατόν να ικανοποιηθεί με τη χρήση της προαναφερθείσας μεθόδου, επομένως αυτή η επίθεση στον A5 / 2 έχει χρησιμοποιηθεί σε μία από τις επιθέσεις κατά του απορρήτου. Αξίζει να σημειωθεί ότι χρειάστηκαν μόνο μερικές ώρες για να σπάσουν το A5 / 2, κάτι που φανερώνει τις αδυναμίες αυτού του αλγορίθμου.

Η πιο πρόσφατη επίθεση στον A5 / 1, είναι μια επίθεση με τη χρήση μόνο κρυπτογραφημένου κειμένου. Αυτή είναι μια εντυπωσιακή επίθεση που απαιτεί μόνο τη γνώση ενός μικρού αριθμού κρυπτογραφημένων καρέ, επιτρέποντας στον εισβολέα να ακούει τα δεδομένα κρυπτογραφημένων συνομιλιών σε πραγματικό χρόνο. Περαιτέρω, οι συγγραφείς προτείνουν μια ανάλογη επίθεση που βελτιώνει την προηγούμενη επίθεση στον A5 / 2. Το πρόβλημα του γνωστού απλού κειμένου δεν αποτελεί πλέον ανησυχία με τη χρήση αυτής της επίθεσης. Αυτό όμως αποτελεί επίθεση που απαιτεί τεράστιες ποσότητες υπολογιστικής ισχύος.

Διαθέσιμα δεδομένα (κρυπτοκείμενα)	Βήματα προεργασίας	Αριθμός υπολογιστών για συμπλήρωση της προεργασίας σε ένα έτος	Αριθμός δίσκων μεγέθους 200GB	Χρόνος	Αριθμός υπολογιστών για να ολοκληρωθεί η επίθεση σε πραγματικό χρόνο
2^12 (περίπου 5 λεπτα)	2^52	140	22	2^28	1
2^6.7 (8 δευτ/τα)	2^41	5000	176	2^32.6	1000
2^6.7 (8 δευτ/τα)	2^42	5000	350	2^30.6	200
2^14 (20 λεπτα)	2^35	35	3	2^30	1

Δεδομένου ότι πρόκειται για επίθεση μόνο με κρυπτογράφημα, δεν απαιτείται απλό κείμενο για την εύρεση του κλειδιού συνεδρίας σε πραγματικό χρόνο. Ωστόσο, οι απαιτήσεις υπολογισμού και αποθήκευσης για αυτήν την επίθεση είναι πολύ υψηλές καθιστώντας πολύ απίθανο ότι ένας μεμονωμένος χάκερ θα έχει τους απαραίτητους πόρους για να πραγματοποιήσει την επίθεση. Οι απαιτήσεις για την κρυπτοανάλυση μόνο του A5 / 2 πληρούνται ωστόσο από τους περισσότερους προσωπικούς υπολογιστές του σήμερα.

4.3.3 Μη Κρυπτο-Αναλυτικές επιθέσεις:

Είναι γνωστό ότι τα περισσότερα κινητά τηλέφωνα GSM μπορούν να επικοινωνούν με τους περισσότερους σταθμούς βάσης και δίκτυα. Αυτό είναι δυνατό επειδή όλοι οι κατασκευαστές ακολουθούν τις ίδιες προδιαγραφές και πρότυπα για τον τρόπο λειτουργίας του GSM. Οι προδιαγραφές αυτές έχουν αναπτυχθεί από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI). Είναι δυνατόν να μελετηθούν οι

προδιαγραφές σχετικά με τον τρόπο διεξαγωγής της επικοινωνίας μεταξύ του δικτύου και του MS και να ληφθούν λεπτομερείς πληροφορίες σχετικά με τα πρωτόκολλα επικοινωνίας και τους μηχανισμούς που χρησιμοποιούνται όταν ένα MS πιστοποιείται από το δίκτυο.

Το ίδιο κλειδί Kc χρησιμοποιείται για τους διαφορετικούς αλγορίθμους κρυπτογράφησης A5 / 1, A5 / 2 και A5 / 3. Αυτό σημαίνει ότι το σπάσιμο ενός από τους τρεις αυτούς αλγόριθμους και η ανάκτηση του κλειδιού συνεδρίας απειλεί την εμπιστευτικότητα της συνομιλίας ακόμη και όταν οι ισχυρότερες εκδόσεις του αλγορίθμου χρησιμοποιούνται αργότερα.

Ο σταθμός βάσης δεν χρειάζεται να επικυρώνει τον εαυτό του στο MS στο οποίο επικοινωνεί. Επιπλέον, τα μηνύματα δεν έχουν πιστοποιηθεί και η ακεραιότητά τους δεν προστατεύεται.

4.4 Denial of Service (DoS) Attacks

Οι επιθέσεις DoS μπορούν να εκτελεστούν με φυσικά ραδιοσήματα παρεμβολής ή με λογικά μέσα. Αυτές οι δύο δυνατότητες θα αναλυθούν παρακάτω.

4.4.1 Άρνηση παροχής υπηρεσιών - Φυσική παρέμβαση

Οι φυσικές επιθέσεις είναι οι πιο άμεσες επιθέσεις. Ο εισβολέας εμποδίζει τη μετάδοση του χρήστη ή την σηματοδοσία της κίνησης από οποιαδήποτε διεπαφή συστήματος, είτε ενσύρματη, είτε ασύρματη με φυσικά μέσα. Ένα παράδειγμα φυσικής παρέμβασης σε μια ενσύρματη διεπαφή είναι η κοπή του σύρματος. Ο επιτιθέμενος θα μπορούσε, για παράδειγμα, να κόψει το σύρμα αφήνοντας ένα σταθμό βάσης. Ένα παράδειγμα φυσικής παρέμβασης σε μια ασύρματη διεπαφή είναι το μπλοκάρισμά της. Η κατοχή του κατάλληλου εξοπλισμού για να μπλοκάρουμε σήματα GSM, είναι εφικτή. Ο εξοπλισμός τοποθετείται στην περιοχή όπου πρέπει να διαταραχθεί η κυκλοφορία και

οι συσκευές GSM εντός της εμβέλειας της συσκευής δεν θα λειτουργούν σωστά. Η αναπήδηση συχνοτήτων καθιστά το μπλοκάρισμα δυσκολότερο από το συνηθισμένο.

Υπάρχουν παραδείγματα μπλοκαρίσματος που προκαλούν προβλήματα στους παρόχους GSM. Πρόσφατα, ένας φορέας εκμετάλλευσης κινητής τηλεφωνίας στη Μολδαβία υπέστη σοβαρές παρενοχλήσεις, γεγονός που προκάλεσε ουσιαστικά αύξηση των αποτυχημένων κλήσεων κατά περίπου 7%. Ο πάροχος και οι αρχές είχαν σοβαρά προβλήματα στην παύση των επιθέσεων.

4.4.2 Άρνηση παροχής υπηρεσιών - Λογική παρέμβαση

Ένας εισβολέας μπορεί να εκτελέσει επιθέσεις DoS με λογικά μέσα επίσης όπως τα ακόλουθα παραδείγματα δείχνουν:

- Ο επιτιθέμενος παραβιάζει ένα αίτημα κατάργησης εγγραφής (IMSI-detach) στο δίκτυο. Το δίκτυο αποκρύπτει τον συνδρομητή από την περιοχή τοποθεσίας που επισκέπτεται και δίνει οδηγίες στο HLR να κάνει το ίδιο. Ο χρήστης στη συνέχεια δεν είναι προσβάσιμος για άλλους συνδρομητές. Ο επιτιθέμενος χρειάζεται ένα τροποποιημένο MS και το IMSI του χρήστη να αποσυρθεί.

- Ο επιτιθέμενος πραγματοποιεί ένα αίτημα ενημέρωσης τοποθεσίας σε μια διαφορετική περιοχή τοποθεσίας από εκείνη στην οποία ο συνδρομητής βρίσκεται σε περιαγωγή. Το δίκτυο καταχωρεί τον συνδρομητή στη νέα περιοχή τοποθεσίας και ο χρήστης-στόχος θα μπει σε αυτή τη νέα περιοχή. Ο χρήστης στη συνέχεια δεν είναι προσβάσιμος για υπηρεσίες κινητής τηλεφωνίας.

- Ένας επιτιθέμενος που έχει στην κατοχή του έναν τροποποιημένο σταθμό βάσης, μεταδίδοντας το κανάλι βάσης με υψηλότερη ισχύ σήματος θα αναγκάσει τα κινητά τηλέφωνα της περιοχής να χρησιμοποιούν τα ραδιοφωνικά κανάλια του εσφαλμένου σταθμού βάσης, καθιστώντας τα μη προσβάσιμα για το δίκτυο εξυπηρέτησης.

4.5 Ορισμένες χρήσιμες λύσεις κατά των επιθέσεων

Ανεξάρτητα από τις βελτιώσεις ασφάλειας στα νέα δίκτυα κινητής, είναι απαραίτητο να παρέχονται λύσεις για τη βελτίωση της ασφάλειας των επί του παρόντος διαθέσιμων συστημάτων 2G. Ορισμένες πρακτικές λύσεις παρουσιάζονται παρακάτω.

4.5.1 Χρήση ασφαλών αλγορίθμων για υλοποιήσεις A3 / A8

Αυτό μπορεί να εμποδίσει την επικίνδυνη επίθεση κλωνοποίησης της κάρτας SIM. Η λύση αυτή είναι κερδοφόρα, δεδομένου ότι οι φορείς εκμετάλλευσης δικτύων μπορούν να επιτελέσουν αυτές τις βελτιώσεις οι ίδιοι και χωρίς να χρειαστούν οι κατασκευαστές λογισμικού και υλικού. Ωστόσο, αυτή η λύση απαιτεί την παροχή και τη διανομή νέων καρτών SIM και την τροποποίηση του λογισμικού του HLR. Επί του παρόντος, αμφότεροι οι αλγόριθμοι COMP128-2 και COMP128-3 εμποδίζουν την κλωνοποίηση της κάρτας SIM και το σπάσιμο του Ki από τον αέρα. Επειδή το COMP128-3 ενισχύει το πραγματικό μήκος κλειδιού συνεδρίας με επιπλέον 10 bits, επιτρέπει στον αναπτυγμένο κρυπτογραφικό αλγόριθμο να έχει μια αποδεκτού επιπέδου ασφάλεια. Αν και σύντομα θα κρίνουμε την πραγματική ασφάλεια των COMP128-2 και COMP128-3, έχουν προφανή πλεονεκτήματα έναντι του παραδοσιακού COMP128-1 για τον οποίο οι συσκευές κλωνοποίησης SIM είναι διαθέσιμες σε πολύ χαμηλές τιμές.

4.5.2 Χρήση ασφαλών αλγόριθμων κρυπτογράφησης

Οι χειριστές μπορούν να χρησιμοποιούν πιο πρόσφατους και πιο ασφαλείς αλγορίθμους, όπως τον A5 / 3, υπό την προϋπόθεση ότι αυτές οι βελτιώσεις επιτρέπονται από την κοινοπραξία GSM. Οι αναπτυγμένοι κρυπτογραφικοί αλγόριθμοι θα πρέπει να εφαρμοστούν τόσο σε BTS όσο και σε κινητά τηλέφωνα. Οποιαδήποτε αλλαγή στους κρυπτογραφικούς αλγορίθμους απαιτεί συμφωνία και συνεργασία κατασκευαστών λογισμικού και υλικού, δεδομένου ότι θα πρέπει να πραγματοποιήσουν τις κατάλληλες αλλαγές στα προϊόντα τους. Δεδομένου ότι οι κρυπτογραφικοί αλγόριθμοι πρέπει να εφαρμοστούν στα κινητά τηλέφωνα, απαιτείται επίσης η συμφωνία κατασκευαστών κινητών τηλεφώνων. Ωστόσο, μια μοναδική αναβάθμιση

των αναπτυγμένων κρυπτογραφικών αλγορίθμων δεν μπορεί να είναι τόσο χρήσιμη. Ακόμα κι αν οι αλγόριθμοι κρυπτογράφησης αντικατασταθούν από τους ισχυρότερους, ο επιτιθέμενος μπορεί απλώς να παραποιήσει το πραγματικό δίκτυο και να αναγκάσει την MS να απενεργοποιήσει τη λειτουργία κρυπτογράφησης, οπότε είναι επίσης απαραίτητο να τροποποιηθούν τα πρωτόκολλα ελέγχου ταυτότητας.

4.5.3 Ασφάλεια από άκρη-σε-άκρη

Η καλύτερη, ευκολότερη και πιο κερδοφόρα λύση είναι η ανάπτυξη της ασφάλειας από το ένα άκρο στο άλλο σε επίπεδο εφαρμογής. Τα περισσότερα από τα τρωτά σημεία ασφαλείας του GSM (εκτός από την κλωνοποίηση SIM και τις επιθέσεις DoS) δεν στοχεύουν τους απλούς ανθρώπους και οι στόχοι τους συνήθως περιορίζονται σε ειδικές ομάδες, επομένως είναι εύλογο και οικονομικό ότι τέτοιες ομάδες πρέπει να καταστήσουν τις επικοινωνίες τους ασφαλείς από άκρο σε άκρο. Δεδομένου ότι η κρυπτογράφηση και η εγκατάσταση ασφάλειας πραγματοποιούνται στις άκρες, δεν απαιτείται καμία αλλαγή στο υλικό του GSM. Με αυτόν τον τρόπο, ακόμα και αν η συνομιλία παρακολουθείται από την αστυνομία ή από νομικές οργανώσεις, δεν μπορούν να αποκρυπτογραφούν τα μεταδιδόμενα δεδομένα χωρίς να έχουν το αληθινό κλειδί κρυπτογράφησης, υπό την προϋπόθεση ότι χρησιμοποιείται ένας αρκετά ασφαλής κρυπτογραφικός αλγόριθμος. Επομένως, προκειμένου να αποφευχθούν παράνομες δραστηριότητες, θα πρέπει να είναι διαφανής τόσο για τον φορέα εκμετάλλευσης GSM όσο και για τον πάροχο υπηρεσιών.

5 Επιθέσεις στο 3G

5.1 Τι κάνει πιθανές τις επιθέσεις στο Δίκτυο 3G;

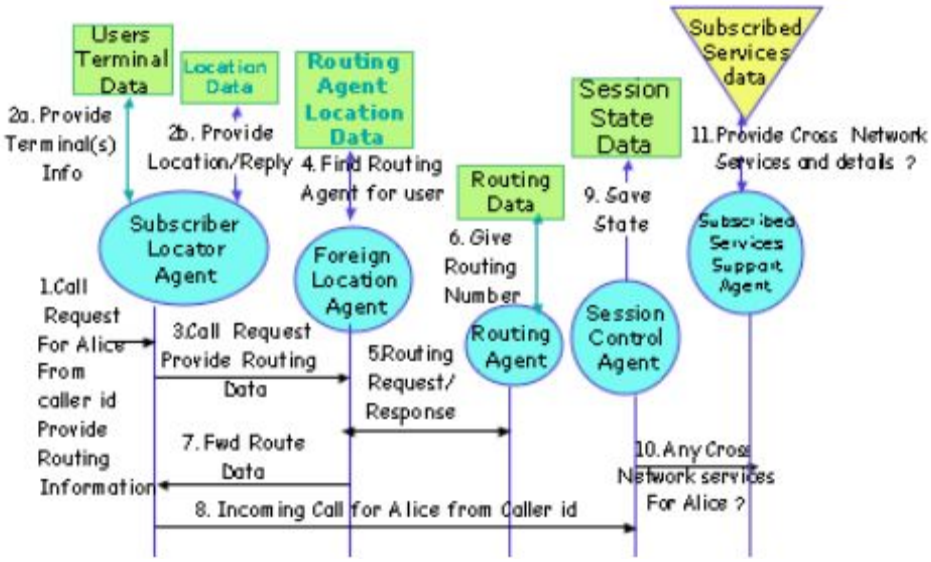
Τα πρώιμα ασύρματα τηλεπικοινωνιακά δίκτυα 1G και 2G και τα δίκτυα PSTN απέτυχαν καθώς τα μηνύματα σηματοδοσίας ανταλλάσσονταν σε ιδιωτικά απομονωμένα δίκτυα SS7. Αυτά τα απομονωμένα δίκτυα δεν συνδέονταν με κανένα δημόσιο δίκτυο και επομένως οι κακόβουλοι χάκερς δεν μπορούσαν να έχουν εύκολη πρόσβαση στο ασύρματο τηλεπικοινωνιακό δίκτυο. Οι επιθέσεις που ήταν δυνατές σε αυτά τα απομονωμένα δίκτυα μελετήθηκαν καλά και εξετάστηκαν στην ταξινόμησή μας. Ένα παράδειγμα για το τι καθιστά δυνατή την επίθεση αυτή είναι η εύκολη διαθεσιμότητα πρότυπου φθηνού εξοπλισμού δοκιμής κινητού ραδιοσήματος. Αυτός ο εξοπλισμός θα μπορούσε να χρησιμοποιηθεί για την πλαστοπροσωπία τμημάτων του δικτύου. Άλλες απειλές είναι οι δυσαρεστημένοι εργαζόμενοι και οι τρομοκράτες, που μπορούν να αποκτήσουν πρόσβαση σε κεντρικά γραφεία και σε οντότητες δικτύου πυρήνα 3G.

Με την ενσωμάτωση των βασικών δικτύων 3G, τα δίκτυα έχουν ανοίξει πρόσθετα τρωτά σημεία και έδωσαν στους κακόβουλους επιτιθέμενους εύκολη πρόσβαση μέσω των Cross Network Servers. Το Διαδίκτυο είναι ανοικτό και προσβάσιμο σε όλους με απλό εξοπλισμό. Είναι επίσης πολύ εύκολο για τους κακόβουλους επιτιθέμενους να σπάσουν τους διακομιστές Internet λόγω των πολλών τρωτών του σημείων. Το σπάσιμο ενός διακομιστή Διαδικτύου που παρέχει υπηρεσία Cross Network ανοίγει δυνατότητες για εισβολή στα κεντρικά δίκτυα 3G και PSTN. Το Cyber Attack Cross Infrastructure είναι εύκολο να εκτελεστεί και μπορεί να είναι αρκετά σοβαρό για να προκαλέσει την καταστροφή του τηλεπικοινωνιακού δικτύου. Ορισμένα παραδείγματα Cross Network Services, τα οποία λειτουργούν ως υποστύλωμα εκτόξευσης για τις επιθέσεις Cyber Attack Cross Infrastructure, είναι η Υπηρεσία Προώθησης Κλήσεων (CFS), το Instant Messaging βάσει θέσης (LB-IM) και οι Υπηρεσίες Χρεώσεων Πελατών (CBS).

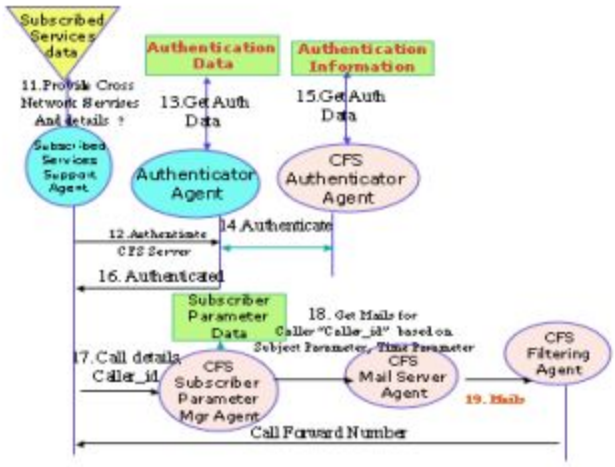
Οι υπηρεσίες CFS και CBS ενεργοποιούνται όταν φτάσει ένα μήνυμα σηματοδότησης στο HLR που έχει εκχωρηθεί στον συνδρομητή. Ο Subscriber Locator Agent θα στείλει ένα ερώτημα στη βάση δεδομένων της πηγής δεδομένων του τερματικού χρήστη και θα

βρει τα τερματικά που έχουν καταχωρηθεί για το χρήστη και στη συνέχεια θα ερωτήσει την προέλευση δεδομένων τοποθεσίας και θα βρει το VLR όπου είναι εγγεγραμμένος ο συνδρομητής. Ο MSC θα παράσχει έναν αριθμό δρομολόγησης για τη δρομολόγηση της κλήσης στο MSC, όπου ο συνδρομητής βρίσκεται σε περιαγωγή. Ο αριθμός δρομολόγησης επιστρέφεται στον παράγοντα εντοπισμού συνδρομητών (HLR). Η κλήση δρομολογείται στον παράγοντα ελέγχου σύνδεσης (MSC). Ο υπεύθυνος ελέγχου σύνδεσης (MSC) θα καλέσει τον Διαχειριστή Υποστήριξης Υπηρεσιών Συνδρομητών (MSC) για να ελέγξει αν υπάρχουν καταχωρημένες υπηρεσίες Διαδικτύου για τον δέκτη κλήσης. Ο Διαχειριστής Υποστήριξης Υπηρεσιών Συνδρομητών (MSC), μέσω ερωτήματος για cached Δεδομένα Συνδρομητικών Υπηρεσιών από το HLR, γνωρίζει ότι ο δέκτης κλήσης εγγράφεται στις υπηρεσίες CFS και CBS.

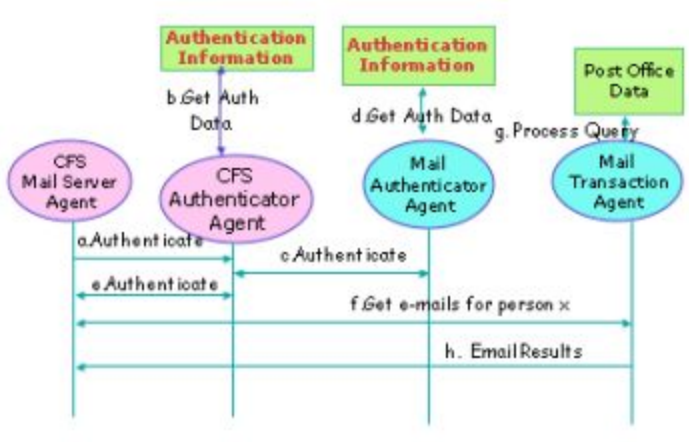
Το παρακάτω σχήμα δείχνει τις ροές σήματος για την ανίχνευση υπηρεσιών διασταυρούμενων δικτύων που βασίζονται στη ταυτότητα καλούντος. Ο Διαχειριστής Υποστήριξης Υπηρεσιών Συνδρομητών (MSC) ρωτάει, μέσω εσωτερικού ερωτήματος της βάσης δεδομένων του, παραμέτρους που απαιτούνται για την κλήση του CFS / CBS και ζητάει από τον Authenticator Agent (HLR) να πιστοποιήσει τον έλεγχο ταυτότητας με τον Cross Network Server. Σε υπηρεσίες όπως το CBS και το CFS, όπου χρησιμοποιείται το αναγνωριστικό του καλούντος για τον προσδιορισμό του τύπου υπηρεσίας που πρέπει να παρασχεθεί, μόνο το δίκτυο εξυπηρέτησης (MSC / VLR) μπορεί να επικαλεστεί την υπηρεσία Cross Network. Υποθέτουμε ότι ο συνδρομητής δεν ενεργοποιεί συνδρομή σε καμία άλλη συμπληρωματική υπηρεσία και ως εκ τούτου το αναγνωριστικό καλούντος είναι διαθέσιμο μόνο στο μήνυμα σηματοδοσίας που λαμβάνεται στο MSC και όχι στο HLR.



Εάν ο Cross Network Server είναι ο CFS, μετά τον έλεγχο ταυτότητας, ο Παράγοντας Διαχειριστή παραμέτρων συνδρομητή CFS καλεί τον διακομιστή αλληλογραφίας CFS να ελέγξει το αποθηκευμένο αρχείο ηλεκτρονικού ταχυδρομείου του για να διαπιστώσει αν ικανοποιεί τους περιορισμούς που ορίζει ο χρήστης. Τα μηνύματα ηλεκτρονικού ταχυδρομείου από τον προσωρινό χώρο αποθήκευσης δεδομένων ηλεκτρονικού ταχυδρομείου μεταφέρονται στον διακομιστή αλληλογραφίας από τον παράγοντα διακομιστή αλληλογραφίας CFS σε διαστήματα που ορίζονται από τον συνδρομητή. Ανάλογα με τους περιορισμούς που θέτει ο συνδρομητής και η προσωρινή μνήμη ηλεκτρονικού ταχυδρομείου από τον παράγοντα διακομιστή αλληλογραφίας CFS, ο Φορέας φιλτραρίσματος CFS επιστρέφει τον αριθμό προώθησης στον Διαχειριστή Υποστήριξης Υπηρεσιών Συνδρομητών (MSC), ο οποίος θα καλέσει άλλες οντότητες δικτύου να προωθήσουν την κλήση. Το παρακάτω σχήμα δείχνει τις παραπάνω ροές σηματοδοσίας.



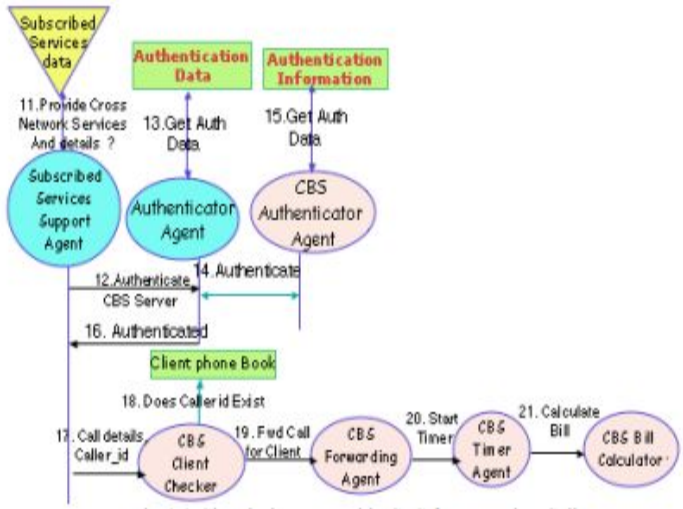
Ροές σημάτων: Παροχή CFS για εισερχόμενη κλήση



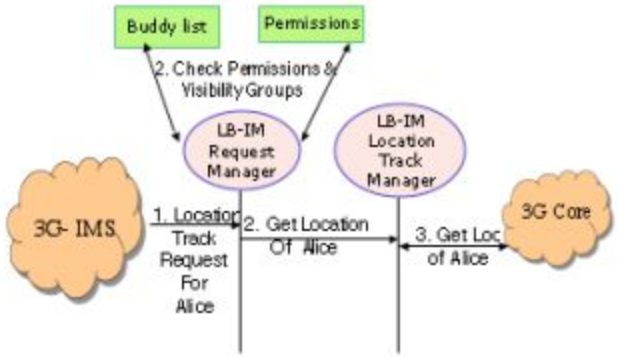
Ροές σημάτων: Ο διακομιστής CF λαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου από τον διακομιστή αλληλογραφίας

Εάν ο Cross Network Server είναι ο CBS, μετά τον έλεγχο ταυτότητας, ο Client Checker Agent CBS ελέγχει αν υπάρχει πελάτης που αντιστοιχεί στο αναγνωριστικό του καλούντος στο χώρο αποθήκευσης δεδομένων βιβλιοθήκης πελάτη. Αν υπάρχει αντιστοιχία, γίνεται κλήση του CBS Forwarding Agent, ο οποίος θα προωθήσει την κλήση στον κατάλληλο αριθμό και θα καλέσει τον παράγοντα χρονοδιακόπτη CBS. Το σχήμα δείχνει τις ροές σηματοδότησης για την παραπάνω διαδικασία. Στην Υπηρεσία Διασύνδεσης CBS Cross Network, οι επιθέσεις Cyber Infrastructure Cyber μπορούν να εμφανιστούν στο διακομιστή CB.

Το LB-IM ενεργοποιείται όταν φτάσει ένα αίτημα track στο LB-IM Request Manager. Ο διαχειριστής αίτησης LB-IM θα ελέγξει αν ο αιτών ανήκει στην ομάδα ορατότητας θέσης και ώρας, ελέγχοντας το χώρο αποθήκευσης δεδομένων δικαιωμάτων. Εάν ο αιτών ικανοποιήσει τους περιορισμούς, ο παράγοντας εντοπισμού θέσης LB-IM ανακτά την τοποθεσία του συνδρομητή ζητώντας τις οντότητες δικτύου 3G.



Ροές σημάτων: Παρέχετε CBS για εισερχόμενη κλήση



Ροές σημάτων: Διαχείριση αίτησης LB-IM

5.2 Πώς συμβαίνουν οι επιθέσεις σε δίκτυα 3G;

Επιθέσεις μπορεί να προκύψουν από διάφορα σημεία του δικτύου. Σε γενικές γραμμές, οι επιθέσεις μπορούν να χωριστούν σε επιθέσεις συγκεκριμένης υποδομής και ολόκληρης της υποδομής.

Οι περισσότερες Επιθέσεις Συγκεκριμένης Υποδομής θα πραγματοποιηθούν μέσω αέρα στα δίκτυα 3G. Αυτές μπορεί να προέρχονται από πρότυπους φθηνούς κινητούς

ραδιοεξοπλισμούς δοκιμής "off-the-shelf" για την πλαστοπροσωπία τμημάτων του δικτύου. Ο εισβολέας μπορεί να αναλύσει την κυκλοφορία, να παρακολουθήσει, να υποκλέψει μηνύματα σηματοδότησης, να τροποποιήσει μηνύματα σηματοδότησης και να μπλοκάρει τη διεπαφή ραδιοσυχνοτήτων.

Εάν ένας εισβολέας εισχωρήσει σε μια οντότητα δικτύου στον πυρήνα του 3G, τότε μπορεί να εισάγει, να τροποποιήσει και να καταστρέψει πηγές δεδομένων, έτσι ώστε οι κακόβουλοι συνδρομητές να μπορούν να διαπράξουν απάτη συνδρομής, να συλλέξουν εμπιστευτικές πληροφορίες από άλλες οντότητες και να τροποποιήσουν τη λογική των υπηρεσιών για να διακόψουν τη λειτουργία του. Ωστόσο, είναι πολύ δύσκολο να εισέλθει κάποιος σε μια βασική οντότητα δικτύου 3G.

Το σπάσιμο σε έναν Διακομιστή Διαδικτύου που παρέχει Cross Network Service, ανοίγει δυνατότητες για τον επιτιθέμενο να εκτελεί Cross Infrastructure Cyber Attacks. Θα εξετάσουμε τώρα πώς μπορούν να συμβούν οι επιθέσεις χρησιμοποιώντας τα παραπάνω παραδείγματα Σταυροειδών Υπηρεσιών Δικτύου.

5.3 Ταξινόμηση επιθέσεων

Για να ταξινομήσουμε τις επιθέσεις στο Δίκτυο 3G, λαμβάνουμε υπόψη την φυσική πρόσβαση του εισβολέα στο δίκτυο, τον τύπο των κατηγοριών επίθεσης και τα μέσα που χρησιμοποιούνται για να προκαλέσουν την επίθεση. Κατατάσσουμε τις επιθέσεις σε τρεις διαστάσεις: Διάσταση 1: Φυσική Πρόσβαση στο Δίκτυο, Διάσταση 2: Κατηγορίες Επίθεσης και Διάσταση 3: Μέσα επίθεσης.

5.3.1 Διάσταση 1: Φυσική πρόσβαση στο δίκτυο

Σε αυτή τη διάσταση, οι επιθέσεις ταξινομούνται με βάση το επίπεδο φυσικής πρόσβασης που έχει ο εισβολέας στο δίκτυο ασύρματων τηλεπικοινωνιών 3G. Η

διάσταση 1 μπορεί να ταξινομηθεί περαιτέρω ως επίθεση μεμονωμένης υποδομής (Επίπεδο 1-3) και επίθεση μεγάλου εύρους υποδομής (Επίπεδο 4-5)

Επίπεδο 1: Πρόσβαση στη διεπαφή με τη φυσική συσκευή: Ο επιτιθέμενος έχει πρόσβαση σε τυποποιημένο φτηνό εξοπλισμό "off-the-shelf" που θα μπορούσε να χρησιμοποιηθεί για την πλαστοπροσωπία τμημάτων του δικτύου. Ο επιτιθέμενος μπορεί να τοποθετήσει έναν ψευδεπίγραφο σταθμό βάσης. Τα θύματα που εισέρχονται στον ψεύτικο σταθμό βάσης υπόκεινται σε επιθέσεις από αυτόν. Οι επιτιθέμενοι μπορούν επίσης να χρησιμοποιούν τροποποιημένους κινητούς σταθμούς για να εκπέμπουν σε υψηλή συχνότητα, να παρακολουθούν και να πραγματοποιήσουν MITM επιθέσεις .

Επίπεδο 2: Πρόσβαση σε καλώδια που συνδέουν κεντρικά γραφεία (οντότητες δικτύου πυρήνα 3G): Τα κεντρικά γραφεία στεγάζουν τις οντότητες δικτύου πυρήνα 3G. Συνήθως εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση σε αυτά τα κεντρικά γραφεία. Εάν ο εισβολέας έχει πρόσβαση σε καλώδια που συνδέουν αυτά τα κεντρικά γραφεία, μπορεί να προκαλέσει ζημιά διακόπτοντας την κανονική μετάδοση μηνυμάτων σηματοδότησης.

Επίπεδο 3: Πρόσβαση σε οντότητες δικτύου πυρήνα 3G στην κεντρική υπηρεσία: Σε αυτή την περίπτωση ο επιτιθέμενος μπορεί να είναι ένας δυσαρεστημένος υπάλληλος ή ένας τρομοκράτης που κατάφερε να αποκτήσει πρόσβαση στο κεντρικό γραφείο. Εδώ ο επιτιθέμενος μπορεί να προκαλέσει ζημιά επεξεργάζοντας τη λογική των υπηρεσιών ή τροποποιώντας τα δεδομένα συνδρομητών (προφίλ, ασφάλεια και υπηρεσίες) που είναι αποθηκευμένα στην οντότητα του δικτύου.

Επίπεδο 4: Πρόσβαση σε συνδέσμους που συνδέουν το Διαδίκτυο και το δίκτυο πυρήνα 3G: Πρόκειται για μια διαδικτυακή επίθεση σε πολλαπλές υποδομές του δικτύου. Ο επιτιθέμενος έχει πρόσβαση σε συνδέσμους που συνδέουν το δίκτυο πυρήνα 3G και τις υπηρεσίες Διαδικτύου που βασίζονται σε αυτό. Σε αυτή την περίπτωση ο εισβολέας μπορεί να προκαλέσει ζημιά διακόπτοντας την κανονική μετάδοση μηνυμάτων σηματοδότησης που διέρχονται από τη ζεύξη, εισάγοντας μηνύματα σηματοδότησης στη σύνδεση μεταξύ των δύο δικτύων. Το επίπεδο 4 μπορεί να υποδιαιρεθεί με βάση τις προσεγγίσεις αλληλεπίδρασης που χρησιμοποιούνται για τη σύνδεση του κεντρικού δικτύου 3G και του Διαδικτύου.

Επίπεδο 5: Πρόσβαση σε διακομιστές Διαδικτύου ή Διακομιστές Διασταυρούμενων Δικτύων (παρέχει πολυμέσα ή άλλες υπηρεσίες σε συνδρομητές κινητής τηλεφωνίας) που είναι συνδεδεμένα με δίκτυα 3G: Πρόκειται για Cross Infrastructure Cyber Attack. Σε αυτή την περίπτωση, ο εισβολέας μπορεί να προκαλέσει ζημιά, επεξεργάζοντας τη λογική υπηρεσίας, τροποποιώντας τα δεδομένα συνδρομητών (προφίλ, ασφάλεια και υπηρεσίες) που είναι αποθηκευμένα στους Cross Servers. Αυτό το επίπεδο επίθεσης είναι ευκολότερο να επιτευχθεί από το επίπεδο 2 και το επίπεδο 3.

5.3.2 Διάσταση 2: Κατηγορίες επιθέσεων

Σε αυτή τη διάσταση, οι επιθέσεις ταξινομούνται με βάση τον τύπο της επίθεσης. Οι κατηγορίες επίθεσης βασίζονται σε:

Υποκλοπή: Ο εισβολέας παρακολουθεί πληροφορίες, π.χ. διαβάζει μηνύματα σηματοδότησης σε ένα καλώδιο (Επίπεδο 2), αλλά δεν τα τροποποιεί ή τα διαγράφει. Αυτή είναι μια παθητική επίθεση. Αυτό επηρεάζει την ιδιωτικότητα του συνδρομητή και του χειριστή του δικτύου. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει τα δεδομένα που λαμβάνονται από την παρακολούθηση, για την ανάλυση της κυκλοφορίας και την εξάλειψη του ανταγωνισμού που παρέχει ο πάροχος του δικτύου.

Κατασκευή / αναπαραγωγή: Σε αυτή την περίπτωση ο εισβολέας μπορεί να εισάγει ψευδή αντικείμενα στο σύστημα. Αυτά τα αντικείμενα εξαρτώνται από το επίπεδο της φυσικής πρόσβασης του εισβολέα στο σύστημα. Π.χ. στο επίπεδο 2, ο εισβολέας μπορεί να εισάγει ψεύτικα μηνύματα σηματοδότησης, στο επίπεδο 3, ο εισβολέας μπορεί να εισάγει ψευδή λογική υπηρεσίας ή ψεύτικα δεδομένα συνδρομητών σε αυτό το σύστημα. Το αποτέλεσμα θα ήταν, ο επιτιθέμενος να φαίνεται στο σύστημα ως ρυθμιστική αρχή.

Τροποποίηση πόρων: Ο εισβολέας προκαλεί ζημιά τροποποιώντας τους πόρους του συστήματος. Π.χ. στο επίπεδο 2, ο εισβολέας μπορεί να τροποποιήσει τα μηνύματα σηματοδοσίας μέσα και έξω από το καλώδιο. Στο επίπεδο 3, ο εισβολέας μπορεί να

τροποποιήσει τη λογική της υπηρεσίας ή να τροποποιήσει δεδομένα συνδρομητή στην οντότητα.

Άρνηση παροχής υπηρεσιών: Ο εισβολέας προκαλεί υπερφόρτωση ή διακοπή του συστήματος, έτσι ώστε το δίκτυο να λειτουργεί με μη φυσιολογικό τρόπο. Η μη φυσιολογική συμπεριφορά μπορεί να είναι νόμιμοι συνδρομητές που δεν λαμβάνουν υπηρεσία, παράνομοι συνδρομητές που λαμβάνουν υπηρεσία ή ολόκληρο το δίκτυο να απενεργοποιηθεί ως αποτέλεσμα της επίθεσης.

Διακοπή: Ο εισβολέας προκαλεί διακοπή καταστρέφοντας πόρους. Π.χ. σε επίπεδο 2, ο επιτιθέμενος μπορεί να διαγράψει μηνύματα σηματοδοσίας μέσα και έξω από το καλώδιο. Σε επίπεδο 3, ο εισβολέας μπορεί να διαγράψει δεδομένα συνδρομητή στην αντίστοιχη καταχώρηση, όπως HLR. Σε αυτή την περίπτωση και ο εισβολέας μπορεί να μην λάμβάνει υπηρεσίες.

5.3.3 Διάσταση 3: Μέσα επίθεσης

Σε αυτή τη διάσταση, οι επιθέσεις ταξινομούνται με βάση τα μέσα που χρησιμοποιούνται για να προκαλέσουν την επίθεση. Τα μέσα επίθεσης είναι τα ακόλουθα.

Δεδομένα: Ο εισβολέας επιτίθεται στα δεδομένα που είναι αποθηκευμένα στο σύστημα. Η ζημιά προκαλείται τροποποιώντας, εισάγοντας και διαγράφοντας τα δεδομένα που είναι αποθηκευμένα στο σύστημα.

Μηνύματα: Ο εισβολέας επιτίθεται στο σύστημα μέσω των μηνυμάτων σηματοδότησης. Έτσι μπορεί να εισάγει, να τροποποιεί, να διαγράφει και να επαναλαμβάνει μηνύματα σηματοδότησης που εισέρχονται και εξέρχονται από το δίκτυο.

Λογική υπηρεσίας: Ο εισβολέας προκαλεί ζημιά προσβάλλοντας τη λογική της υπηρεσίας που εκτελείται στις διάφορες οντότητες του δικτύου πυρήνα 3G.

6 Απειλές και επιθέσεις σε δίκτυα 4G

Σε αυτή την ενότητα, διερευνόνται επιθέσεις ασφάλειας και εμπιστευτικότητας, επιθέσεις που βασίζονται σε IP, επιθέσεις σηματοδότησης και επιθέσεις εμπλοκής. Σχεδιάζουμε επίσης μια κατηγοριοποίηση των διαφορετικών επιθέσεων με βάση τα στοιχεία του δικτύου. Οι επιθέσεις στο δίκτυο κινητής τηλεφωνίας 4G μπορούν να προκύψουν από την αποτυχία των απαιτήσεων ασφαλείας, οι οποίες επικεντρώνονται στα εξής:

- **Η ασφάλεια εφαρμογών**: σχετίζεται με την ακεραιότητα του υλικού, του λογισμικού, των δεδομένων και του λειτουργικού συστήματος (OS).

- **Η ασφάλεια πρόσβασης στο δίκτυο**: σχετίζεται με την εμπιστευτικότητα, την ακεραιότητα, την αυθεντικοποίηση και την εξουσιοδότηση (CIAA) των δεδομένων.

- **Η Ασφάλεια Χρήστη**: σχετίζεται με την ταυτότητα, την εμπιστευτικότητα και την εξουσιοδότηση του χρήστη.

- **Η ασφάλεια της περιοχής του δικτύου**: σχετίζεται με την εξακρίβωση της ταυτότητας και την εμπιστευτικότητα της τοποθεσίας ΜΕ.

- **Η συντήρηση QoS**: σχετίζεται με την ασφάλεια ενάντια στις επιθέσεις άρνησης παροχής υπηρεσιών (DoS).

- **Η Ασφάλεια Φυσικού Επιπέδου**: σχετίζεται με την αντίσταση κατά της παραβίασης.

Η αποτυχία των απαιτήσεων ασφάλειας μπορεί να αξιοποιηθεί από έναν εισβολέα για την εκτέλεση διαφόρων τύπων επιθέσεων, όπως επιθέσεις εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, οι οποίες ενδέχεται να έχουν ως αποτέλεσμα τη δημιουργία DoS ή DDoS.

6.1 Επίθεση κατά της ασφάλειας και της εμπιστευτικότητας

Οι επιθέσεις κατά της ασφάλειας και της εμπιστευτικότητας παρουσιάζονται στον παρακάτω πίνακα. Αυτές οι επιθέσεις σχετίζονται με απειλές με στόχο την εμπιστευτικότητα του χρήστη και της ταυτότητας των συσκευών, την αμοιβαία αυθεντικοποίηση και την συμφωνία κλειδιού (πρωτόκολλα AKA).

Αναφορικός χάρτης επιθέσεων σε δίκτυα κινητής τηλεφωνίας 4G		
Στόχοι Επιθέσεων	Τύπος επιθέσεων	Προτεινόμενη Λύση
Ασφαλεια LTE	Απειλές στην ταυτότητα του χρήστη και στην ιδιωτικότητα : ● Τροποποίηση δεδομένων σε επιπέδου ελέγχου ● Μη εξουσιοδοτημένη πρόσβαση στο δίκτυο, επιθεσεις στο eNB, παρακολούθηση των UE USIM	Καμία προτεινόμενη λύση
Ασφαλεια LTE	Αναλυμένες διάφορες επιθέσεις ● Επιθέσεις εναντίον της εμπιστευτικότητας ● Επιθέσεις εναντίον της ακεραιότητας ● Επιθέσεις εναντίον της διαθεσιμότητας	Καμία προτεινόμενη λύση μείωσης των απειλών

DoS	WLAN-LTE επιθέσεις ● Εσωτερικές επιθέσεις ● Εξωτερικές επιθέσεις χωρίς συνεργασία ● Εξωτερικές επιθέσεις με την συνεργασία μολυσμένων συσκευών ή με αναμετάδοση	Συστήματα ανάλυσης κίνησης
DoS	Επιθέσεις ανακατεύθυνσης/ Επιθέσεις ψεύτικου σταθμού βάσης: ● Μη προστατευμένος φορέας αυθεντικοποίησης EPS-AKA ● Κακόβουλες δραστηριότητες χρηστών	Βελτιωμένα EPS-AKA συνδυαστικά διανύσματα και KASME μη προσβάσιμα από ένα εισβολέα που προσπαθεί να πραγματοποιήσει επίθεση στο τομέα του δικτύου μεταξύ MME και HSS
DoS	MITM επιθέσεις εναντίον της τοποθεσίας του χρήστη ● Μη προστατευμένος φορέας αυθεντικοποίησης μεταξύ HSS και ΜΕ ● Μη προστατευμένο SNID ● Παρακολούθηση του SNID και Επιθέσεις ψεύτικου σταθμού βάσης	Προτείνονται: ● SE-EPS-AKA ● Ψηφιακά πιστοποιητικά ● Απόκτηση δημόσιου κλειδιού από τους HSS/MME και απο το UE
DoS	Τα τρωτά σημεία διαχείρισης κλειδιού παράδοσης ● Επίθεση βασικών σταθμών βάσης ● Πλαστογραφία ταυτότητας	Η επιλογή του βέλτιστου αλγορίθμου ανανέωσης κλειδιού εσωτερικά

	• Παρακολούθηση • Επίθεση αποσυγχρονισμού • Προσθήκη και παραποίηση πακέτων	
Ψευδής σταθμός βάσης	Επιθέσεις εναντίον του IMSI στο LTE: • Μια διαδικασία αρχικής προσάρτησης • Εσωτερική μεταφορά MME	Βελτιστοποίηση του EPS-AKA βασισμένη πάνω σε ένα DMSI: • Μεταφορά του DMSI μέσω του UE αντί του IMSI • Ανανέωση του DMSI με την χρήση ενός τυχαία παραχθέντος αριθμού μετά από μια επιτυχημένη διαδικασία EPS-AKA • Η πρόσβαση του IMSI είναι περιορισμένη στα UE και HSS

Αν και το EPS-AKA χρησιμοποιείται για έλεγχο ταυτότητας μεταξύ UE και 4G EPC CN, εξακολουθεί να παρουσιάζει προβλήματα ασφάλειας όπως η μη προστασία των φορέων επαλήθευσης ταυτότητας μεταξύ HSS και ME, την αποκάλυψη ταυτότητας χρήστη λόγω έλλειψης προστασίας IMSI κατά την εγγραφή ME (μπορεί να είναι δυνατή η παρακολούθηση του IMSI) και την έλλειψη προστασίας του SNID. Στην πραγματικότητα, η διαδικασία αυθεντικοποίησης ενεργοποιείται κατά τη διάρκεια διαδικασιών διαχείρισης της κινητικότητας, όπως η παράδοση, η τηλεειδοποίηση και η ενημέρωση τοποθεσίας, τα οποία χειρίζονται τα MME.

Οι διαδικασίες ελέγχου ταυτότητας εμφανίζονται σε κάθε Update Tracking Area (TAU), στην εγγραφή κινητού τηλεφώνου, στην προέλευση κλήσης, στον τερματισμό και την παράδοση κλήσεων. Ωστόσο, στην περίπτωση της ανταλλαγής κλειδιών, εντοπίστηκαν ορισμένα τρωτά σημεία, τα οποία μπορεί να οδηγήσουν σε πιθανή επισφαλή

επικοινωνία μεταξύ χρήστη και δικτύου, σε επιθέσεις ψεύτικων σταθμών βάσης. Στην πραγματικότητα, η επίθεση ψεύτικου σταθμού βάσης επιτρέπει σε μια κινητή συσκευή να αναπαράγει τη λειτουργικότητα ενός σταθμού βάσης εκμεταλλευόμενη τα τρωτά σημεία πρωτοκόλλου δικτύου, όπως στη στοίβα IP. Στην πράξη, ο βασικός σταθμός βάσης μπορεί να χρησιμοποιηθεί για την επίθεση πλαστοπροσωπίας ταυτότητας χρήστη, επίθεση υποκλοπής, επίθεση πακέτου, επίθεση τροποποίησης πακέτου και επίθεση αποσυγχρονισμού. Η επίθεση αποσυγχρονισμού μπορεί να προκαλέσει αποτυχία της διαχείρισης κλειδιού παραλαβής, εμποδίζοντας έτσι το eNB του στόχου να διατηρήσει τη φρεσκάδα των κλειδιών μετάδοσης. Στην πραγματικότητα, υπάρχουν δύο τύποι μεταβιβάσεων στο EPS: οι ενδοεπιχειρησιακές και οι μεταβιβάσεις μεταξύ των MME. Στην παράδοση εντός του MME, η προετοιμασία της μεταβίβασης λαμβάνει χώρα μεταξύ της πηγής και του στόχου eNB στην ίδια MME μέσω της διεπαφής X2. Στην περίπτωση μεταβίβασης μεταξύ MME, η προετοιμασία πραγματοποιείται εξ ολοκλήρου στο MME χωρίς καμία άμεση σηματοδοσία μεταξύ σταθμών βάσης.

Εφόσον ο κύριος σκοπός της διαχείρισης κλειδιού παραλαβής είναι να εξασφαλίσει τον διαχωρισμό των κλειδιών συνόδου σε μια μεταβίβαση μεταξύ των σταθμών βάσης με τέτοιο τρόπο ώστε ένα συμφωνημένο κλειδί συνόδου να περιορίζεται σε έναν σταθμό βάσης και κατά συνέπεια η αποτυχία στη διαχείριση κλειδιού παραλαβής, να μπορεί να καταστήσει δυνατή την αποκρυπτογράφηση μηνυμάτων μεταξύ eNB και UE, καθώς και την σηματοδότηση RRC.

Διάφορες επιθέσεις που μπορούν να εκτελεστούν χρησιμοποιώντας έναν βασικό σταθμό βάσης περιλαμβανομένων και των επιθέσεων ανακατεύθυνσης, επιθέσεις MITM κατά της τοποθεσίας συνδρομητών, ψευδείς επιθέσεις σταθμού βάσης με υποκλοπές του SNID και επιθέσεις με γνωστά Authentication Vectors (AV). Για να μετριαστούν αυτές τις επιθέσεις, προτάθηκε ένας αλγόριθμος για την επιλογή ενός βέλτιστου διαστήματος ενημέρωσης βασικού κλειδιού, προκειμένου να μετριαστεί η επίδραση του αποσυγχρονισμού και οι επιθέσεις με γνωστά κλειδία.

Επιπλέον, όπως προαναφέρθηκε, η ιδιωτική ταυτότητα χρήστη μπορεί να αποκαλυφθεί στο EPS-AKA κατά τη διαδικασία αρχικής επισύναψης στο LTE, καθώς το IMSI μεταδίδεται με απλό κείμενο. Επιπλέον, άλλες αδυναμίες στο EPS-AKA μπορούν να χρησιμοποιηθούν για την πραγματοποίηση ενεργών επιθέσεων, συμπεριλαμβανομένης της αδυναμίας ανάκτησης του IMSI από τον GUTI (Globally Unique Temporary Identifier), τις μεταφορές μεταξύ MME, καθώς και την καθυστέρηση υπολογισμού και την καθυστέρηση λόγω αυθεντικοποίησης. Στην πραγματικότητα, ο σκοπός του GUTI

είναι να ταυτοποίησει το UE σε παγκόσμιο επίπεδο χωρίς να αποκαλύψει την ταυτότητά του όταν επισκέπτεται ένα νέο MME ή όταν ένα ψεύτικο eNB ζητάει IMSI από τον UE.

Για να ξεπεραστούν οι ευπάθειες στο EPS-AKA, προτάθηκε από ερευνητές ένα νέο ασφαλές πρωτόκολλο AKA καθώς επίσης και ένα νέο σχήμα που μπορεί να βελτιώσει την απόδοση του EPS-AKA. Αυτή η λύση είναι ένα ενισχυμένο πρωτόκολλο EPS-AKA δύο βημάτων, το οποίο αυξάνει το υπολογιστικό κόστος στο SN και μπορεί να μειώσει: 1) την φόρτωση κατά την ανταλλαγή μηνυμάτων, 2) την κατανάλωση εύρους ζώνης, 3) το κόστος υπολογισμού των hash fuctions, οι οποίες αποτελούνται από ένα σύνολο αλγορίθμων f1, f2, f3, f3, f5 και λειτουργίες εξαγωγής κλειδιού (KDF) μεταξύ οντοτήτων σε σύγκριση με το αρχικό πλαίσιο EPS-AKA. Οι αλγόριθμοι f1 και f2 είναι γνωστοί ως λειτουργίες επαλήθευσης ταυτότητας μηνυμάτων, ενώ οι f3, f4 και f5 είναι οι λεγόμενες λειτουργίες δημιουργίας κλειδιών. Ένα βασικό σημείο αυτής της λύσης είναι ότι μπορεί να βελτιώσει την απόδοση αυθεντικοποίησης και την ασφάλεια, συνδυάζοντας το φορέα και το κλειδί KASME, το οποίο δεν μπορεί να προσεγγιστεί από έναν εισβολέα που πραγματοποιεί επίθεση στον τομέα του δικτύου μεταξύ MME και HSS και αποτρέπει τις ενεργές επιθέσεις.

Μια άλλη προτεινόμενη λύση είναι η κρυπτογράφηση ECC (Ellipse Curve Cipher), η οποία παρέχει προστασία αυθεντικοποίησης και συμφωνία κλειδιών (SE-EPS-AKA) βασισμένη στο WPKI (Wireless Public Key Infrastructure) με την χρήση της Ellipse Curve Cipher κρυπτογράφησης, η οποία παρέχει προστασία στην ασφάλεια ταυτότητας χρήστη και μειωμένη ενεργειακή κατανάλωση κατά την ανταλλαγή πληροφοριών και εισαγάγει την χρήση ψηφιακών πιστοποιητικών και δημόσια κλειδιά τα οποία μπορούν να χρησιμοποιηθούν από τα HSS, MME και UE. Το νέο σύστημα παρέχει προστασία κατά της επίθεσης MITM και της Sequence Number (SQN) DoS, αμοιβαία αναγνώριση ταυτότητας μεταξύ UE, MME και HSS, προστασία μετάδοσης ιδιωτικών και εμπιστευτικών πληροφοριών μεταξύ οντοτήτων, καθώς και επίλυση προβλημάτων ασφάλειας που προκύπτουν από τη διαρροή IMSI και SNID και αύξηση της αντοχής ασφαλείας του κρυπτογραφικού κλειδιού συνεδρίας.

Παρομοίως, προτείνεται ένα ενισχυμένο σύστημα EPS-AKA προκειμένου να ξεπεραστούν τα τρωτά σημεία που σχετίζονται με την ιδιωτική ταυτότητα των χρηστών, εισάγοντας ένα DMSI που μεταδίδεται από τον UE αντί του IMSI. Το DMSI ενημερώνεται βάσει ενός τυχαίου αριθμού που λαμβάνεται σε κάθε επιτυχημένη

διαδικασία EPS-AKA και μπορεί να επιτύχει την ιδιωτικότητα της ταυτότητας χρήστη περιορίζοντας τη γνώση του IMSI στο UE και στο HSS.

Επιπλέον, η ετερογένεια των τεχνολογιών πρόσβασης είναι σημαντική πρόοδος στο LTE. Παρ 'όλα αυτά, δημιουργεί νέες πιθανές απειλές που πρέπει να αντιμετωπιστούν, καθώς η ταχεία και ασφαλής μεταβίβαση αποτελεί βασική προϋπόθεση για την ενσωμάτωση ετερογενών τεχνολογιών δικτύωσης.

Στην πραγματικότητα, η αρχιτεκτονική SAE / LTE χρησιμοποιεί τη μέθοδο αυθεντικοποίησης Extensible Authentication Protocol (EAP) -AKA για να εξασφαλίσει την ασφαλή μετάδοση μέσω 3G-WLAN και να αυθεντικοποιήσει την UE που είναι προσαρτημένη σε WLAN με την αρχιτεκτονική 3G-WLAN. Παρά το γεγονός ότι η UE πρέπει να επικυρωθεί από την HSS, την HLR και την Home Authentication Authorization and Accounting (HAAA), έχουν παρουσιαστεί διάφορες απειλές κατά του EAP-AKA, όπως:

- Απειλές κατά της ταυτότητας και της ιδιωτικής ζωής των χρηστών,
- Απειλές παρακολούθησης των UE / USIM,
- Απειλές που σχετίζονται με τους σταθμούς βάσης και τις μεταβιβάσεις,
- Απειλές που σχετίζονται με σηματοδότηση εκπομπής ή πολυεκπομπής,
- Απειλές που σχετίζονται με το DoS,
- Απειλές κακόβουλου χειρισμού δεδομένων σε επιπέδου ελέγχου,
- Απειλές μη εξουσιοδοτημένης πρόσβασης στο δίκτυο,
- Η διαρροή των διαπιστευτηρίων του eNB καθώς και οι φυσικές επιθέσεις σε ένα eNB,
- Επιθέσεις πρωτοκόλλου σε ένα eNB,
- Επιθέσεις στο κεντρικό δίκτυο, συμπεριλαμβανομένων των επιθέσεων eNB που βασίζονται στην τοποθεσία.

Ειδικότερα, αυτές οι απειλές μπορούν να οδηγήσουν στην αποκάλυψη της ταυτότητας που αποστέλλεται σε απλό κείμενο, το DoS που σχετίζεται με την έλλειψη κρυπτογράφησης μηνυμάτων επαλήθευσης ταυτότητας (μηνύματα όπως EAPoL-Start, EAP-success και EAP-failure), η επίθεση MITM, η επίθεση SQN και η πρόσθετη κατανάλωση εύρους ζώνης που εκθέτουν τους νόμιμους χρήστες σε κίνδυνο και αυξάνουν την καθυστέρηση της αυθεντικοποίησης. Έχουν αναλυθεί ιδιαίτερα τα ζητήματα της διασύνδεσης LTE-AKA με το WiFi. Έχουν επίσης εξετασθεί σημαντικές

απειλές ιδιωτικού απορρήτου κατά των χρηστών που συνδέονται με ασύρματο τοπικό δίκτυο (LAN) σε σχέση με την αποκάλυψη της ταυτότητας χρήστη που αποστέλλεται με ένα απλό κείμενο που επιτρέπει την επίθεση ταυτότητας χρήστη. Ως αντιστάθμισμα, η προτεινόμενη λύση είναι ένα νέο σχήμα LTE-AKA που δεν επιτρέπει τη σαφή μετάδοση του IMSI και χρησιμοποιεί τα WiFi-AP που είναι συνδεδεμένα στο διαδίκτυο για να δημιουργήσουν ένα ασφαλές πλευρικό κανάλι. Το κανάλι WiFi λειτουργεί ως ασφαλές τούνελ μέσω του οποίου θα ανταλλάσσεται μια νέα τυχαία ταυτότητα (RID). Το RID θα χρησιμοποιείται στο HSS για τον εντοπισμό του χρήστη και θα συνδέεται με ένα IMSI και ένα μυστικό κλειδί K που βρίσκεται μόνο στη USIM και στο HSS.

Επιπλέον, οι διαλειτουργίες μεταξύ LTE, UMTS και GSM παρουσιάζουν επίσης αρκετές αδυναμίες που σχετίζονται με τα αντίστοιχα συστήματα AKA, τα οποία μπορούν να χρησιμοποιηθούν για την εκτέλεση διαφορετικών τύπων επιθέσεων. Πρώτον, η αδυναμία στην κρυπτογράφηση του GSM και η έλλειψη προστασίας ακεραιότητας κατά την κίνηση του χρήστη στο 4G μπορούν να αξιοποιηθούν για την εκτέλεση επιθέσεων παρακολούθησης και πλαστοπροσωπίας δικτύου στο UMTS. Επιπλέον, η έλλειψη ελέγχου αυθεντικοποίησης στο GSM μπορεί επίσης να αξιοποιηθεί για την πραγματοποίηση εσφαλμένων επιθέσεων σταθμού βάσης κατά του 4G κατά τη διάρκεια της διαδικασίας AKA. Αυτό τυπικά περιλαμβάνει το 4G SN, το 4G MME και το 3G HN. Το γεγονός ότι το 3G HN μπορεί να δημιουργήσει μόνο 2G και 3G διανύσματα αθυεντικοποίησης, καθιστά δυνατή αυτή την επίθεση, δεδομένου ότι οι φορείς γνησιότητας 4G δεν παράγονται από το 3G HN.

Ομοίως, όταν το 4G AKA εκτελείται από μικτά SN (2G BS και 4G MME), 4G MS και 4G HN, ο επιτιθέμενος μπορεί επίσης να εκτελέσει επίθεση ψεύτικου σταθμού βάσης. Επιπλέον, η διαλειτουργικότητα μεταξύ GSM και UMTS είναι επίσης ευάλωτη σε επιθέσεις MITM. Αυτά τα τρωτά σημεία μπορούν επίσης να οδηγήσουν σε επίθεση κατά του Cipher Mode Command (CMC) μυνήματος μεταξύ του 2G BS και του MS, λόγω της έλλειψης προστασίας ακεραιότητας του μηνύματος CMC.

Όπως στις διεργασίες μεταξύ των 4G και των προκατόχων της (3G και 2G), το DoS μπορεί επίσης να προκύψει από την ενσωμάτωση δικτύων WLAN και 4G / LTE, καθώς φέρνει νέες απειλές και ευπάθειες. Ως αντιστάθμισμα, προτείνεται να αποθηκεύονται οι πληροφορίες συμπεριφοράς των σημείων πρόσβασης που εκδίδονται από τις απαντήσεις αυθεντικοποίησης, παράδοσης και αποσύνδεσης για την ανάπτυξη αποδοτικών αντιμέτρων, όπως εκσυγχρονισμένα συστήματα ανάλυσης και ελέγχου, ικανά να ανιχνεύσουν το κατεστραμμένο σημείο πρόσβασης (PoA) και οποιαδήποτε

αλλαγή στο δίκτυο. Αυτό μπορεί να βοηθήσει στην προστασία από εσωτερικές επιθέσεις, όπως η διακριτική διαρροή μηνυμάτων, η οποία μπορεί να οδηγήσει σε υποκλοπή μηνυμάτων, αποκάλυψη πληροφοριών, παραποίηση δεδομένων, κρυπτογραφικές και άλλες εξωτερικές επιθέσεις.

Μια άλλη αδυναμία στα 4G κινητά δίκτυα σχετίζεται με τα ασύρματα συγκλίνοντα δίκτυα, ιδιαίτερα στο WiMAX, το οποίο είναι ευάλωτο σε απειλές στο φυσικό στρώμα και στο στρώμα Mac . Οι τυπικές απειλές που αντιμετωπίζει το WiMAX είναι οι επιθέσεις DoS λόγω της απροστάτευτης εισόδου στο δίκτυο,της μη κρυπτογραφημένης επικοινωνίας διαχείρισης, των μη προστατευμένων πλαισίων διαχείρισης και του αδύναμου μηχανισμού διαμοιρασμού κλειδιών σε λειτουργίες πολυεκπομπής και εκπομπής. Ως πιθανά αντίμετρα, προτείνονται:

- Η χρήση της αυθεντικοποίησης και της ψηφιακής υπογραφής για την άμβλυνση της πλαστογραφίας και του MITM,
- Η χρήση κρυπτογράφησης ενάντια στην υποκλοπή
- Η χρήση ευρέως διαδεδομένου φάσματος για την προστασία από επιθέσεις φυσικού στρώματος

Επιπλέον, προτάθηκε η επέκταση του μηχανισμού ελέγχου ταυτότητας σε όλα τα πλαίσια διαχείρισης, καθώς και η κρυπτογράφηση RRC, προκειμένου να αμβλυνθούν οι απειλές που σχετίζονται με το μη προστατευμένο UE ID στο LTE. Η λύση αυτή βασίζεται στην αυθεντικοποίηση και την ψηφιακή υπογραφή κατά της πλαστογράφησης και του MITM και χρησιμοποιεί κρυπτογράφηση για την καταπολέμηση της υποκλοπής, της εξάπλωσης του φάσματος, για την προστασία από επιθέσεις φυσικού επιπέδου.

Τέλος, η έλλειψη εμπιστευτικότητας των δεδομένων των χρηστών αποτελεί σημαντική απειλή για τις επιθέσεις φυσικού επιπέδου και της ανάλυσης κυκλοφορίας. Προκειμένου να μετριαστεί αυτή η απειλή, προτείνεται να γενικευθεί η κρυπτογραφική φάση σε οποιοδήποτε σύστημα επικοινωνίας ανεξάρτητα από το κείμενο καθεστώς διαφοροποίησης. Αυτή η λύση μπορεί να αντισταθεί στην επίθεση της ανάλυσης κυκλοφορίας, η οποία δεν μπορεί να προληφθεί από οποιαδήποτε πρότυπο ασφαλείας στα ανώτερα στρώματα.

Προκειμένου να αντιμετωπιστούν τα τρωτά σημεία και οι επιθέσεις που περιγράφηκαν παραπάνω, προτείνεται ορισμένες βελτιώσεις στην αρχιτεκτονική ασφάλειας καθώς και περισσότερη έρευνα σε θέματα όπως:

- **Αρχιτεκτονική συστήματος LTE:** πρέπει να σχεδιαστούν περισσότεροι μηχανισμοί ασφαλείας για την προστασία των επικοινωνιών από επιθέσεις παραδοσιακών πρωτοκόλλων και φυσικών εισβολών στα δίκτυα LTE,
- **LTE κυψελοειδής ασφάλεια:** απαιτείται ενίσχυση του συστήματος EPS-AKA, καθώς και σχεδιασμός μηχανισμών ελέγχου ταυτότητας ασφαλούς πρόσβασης που θα χρησιμοποιηθούν κατά την πρόσβαση του UE στο EPC μέσω μη-3GPP δικτύων, προκειμένου να προστατευθεί από την αποκάλυψη ταυτότητας χρήστη, από επιθέσεις DoS και άλλες κακόβουλες επιθέσεις,
- **LTE security:** Απαιτείται περαιτέρω βελτίωση στους μηχανισμούς διαχείρισης κλειδιού και διαδικασίες παράδοσης ταυτότητας για την αποτροπή επιθέσεων πρωτοκόλλου, επιθέσεων αποσυγχρονισμού και επιθέσεων επανάληψης,
- **Ασφάλεια IMS:** Απαιτείται σχεδιασμός γρήγορων και ισχυρών μηχανισμών ελέγχου ταυτότητας πρόσβασης IMS για την απλούστευση της διαδικασίας ελέγχου ταυτότητας και την πρόληψη των επιθέσεων DoS και άλλων κακόβουλων επιθέσεων στα δίκτυα LTE,
- **Ασφάλεια HeNB:** Απαιτείται σχεδιασμός απλών και ισχυρών μηχανισμών αμοιβαίας επαλήθευσης ταυτότητας μεταξύ των UEs και των HeNBs για την αποτροπή διαφόρων επιθέσεων πρωτοκόλλου,
- **Ασφάλεια MTC:** ο σχεδιασμός των μηχανισμών ασφαλείας MTC στο LTE / Long Term Evolution-Advanced (LTE-A) είναι υπό ερευνητική εργασία.

6.2 IP-Based Επιθέσεις

Σε αυτή την ενότητα παρουσιάζουμε IP-Based επιθέσεις σε δίκτυα κινητής τηλεφωνίας 4G. Καθώς οι πρόσφατες εξελίξεις στις τεχνολογίες κινητών δικτύων ευνόησαν τη μετάβαση στην τεχνολογία που βασίζεται στην τεχνολογία IP στο δίκτυο μεταφορών, έχουν δημιουργηθεί νέες απειλές στα δίκτυα. Θα παρουσιάσουμε τις επιθέσεις που βασίζονται σε IP κατά του backhaul, του GTP και των πρωτοκόλλων διαμέτρου.

Χάρτης αναφοράς επίθεσης σε δίκτυα κινητής τηλεφωνίας 4G		
Στόχοι Επιθέσεων	Τύποι Επιθέσεων	Προτεινόμενες Λύσεις
	Καταιγισμός σηματοδοσίας στο C-plane ● Διαδικασία πρόσβασης NAS ● Επιθέσεις αποσυγχρονισμού ● IMS και HeNB μηχανισμοί ασφάλειας	Προτεινόμενη έρευνα για ενίσχυση των: ● Μηχανισμοί ασφάλειας ενάντια σε επιθέσεις πρωτοκόλλου και φυσικές εισβολές ● EPS-AKA μηχανισμοί ενάντια στην ιδιωτικότητα της ταυτότητας χρήστη, αποσυγχρονισμούς, και επιθέσεις επανάληψης ● Γρήγορους και ισχυρούς μηχανισμούς επαλήθευσης για την πρόσβαση στο IMS και μεταξύ UEs - eNBs
Επιθέσεις στο GTP	Οι επιθέσεις σχετίζονται με: ● Αλλοίωση πακέτων ● Διαρροή πληροφοριών ● Μη φυσιολογικά GTP πακέτα	Προτείνεται ένα σύστημα ανίχνευσης για να: ● Συλλάβει τον έλεγχο δικτύου 4G και την κυκλοφορία δεδομένων για να παράγει χρήσιμες πληροφορίες και μη φυσιολογική αναγνώριση προτύπων ● Εντοπισμός επιθετικής κινητικότητας στο 4G δίκτυο ● Παρακολούθηση και έλεγχος του 4G δικτύου για

		επιθέσεις ασφάλειας
VoLTE επιθέσεις	Απειλές ασφάλειας στο SIP: ● Σκανάρισμα του δικτύου ● Επίθεση εξάντλησης πόρων ● Διαγραφή και αλλοίωση μηνυμάτων ● Υπερχείληση του SIP	Προτείνονται: ● Διαχείριση ελέγχου συνεδριών ● Σύστημα ανίχνευσης VoLTE βάσει ροής ● VoLTE IPS βασισμένο σε υπογραφές
VoLTE επιθέσεις	Επιθέσεις που βασίζονται στη σηματοδότηση: ● Επιθέσεις προσθήκης δεδομένων στον φορέα σηματοδοσίας VoLTE ● Επιθέσεις κακής χρήσης στον φορέα σηματοδοσίας VoLTE ● Επιθέσεις κατάχρησης του QoS στον φορέα σηματοδοσίας VoLTE	Προτείνονται: ● Επιβολή αυστηρής ρύθμισης δρομολόγησης ● Αναβάθμιση της πύλης 4G με φίλτρα VoLTE ● Μηχανισμός μείωσης προτεραιότητας όταν οι ζητούμενοι πόροι υπερβαίνουν τους υπάρχοντες
VoLTE επιθέσεις	Ευπάθειες του VoLTE που σχετίζονται με: ● Υποκλοπή κλήσεων, Αλλαγή θύρας προέλευσης SIP ● Η έλλειψη διακομιστή μεσολάβησης πολυμέσων στο δίκτυο κινητής τηλεφωνίας ● Η έλλειψη	Προτείνονται: ● Το DPI να εφαρμόζεται στο P-GW ● Αυστηρή διαχείριση συνεδριών ● Επαλήθευση του UE

	διαχείρισης συνεδριών σε διακομιστές SIP ● Η έλλειψη ελέγχου ταυτότητας μηνυμάτων SIP ● Αποστολή δεδομένων μέσω φορέα VoLTE	
DoS	Ευπάθειες στην μεταγωγή του LTE: ● Εξαπάτηση του eNB ● Παρακολούθηση της κίνησης του χρήστη ● Μη εξουσιοδοτημένη πρόσβαση στον εξοπλισμό του δικτύου	Προτείνεται η χρήση των μηχανισμών ασφάλειας: ● Πύλες ασφαλείας ● Αρχή πιστοποίησης
DoS	IP spoofing	Προτείνεται ενσωμάτωση IPS στο GTP
DoS	Συνωστισμός επιθέσεων στην διαμετρική διεπαφή	ροτάθηκε ένα ECN για την άμβλυνση της διασυνδεδεμένης διασύνδεσης με διάμετρο
DoS	Διαμετρικές επιθέσεις DoS ● Μηνύματα σε κακή μορφή ● Υπερχείλιση μηνυμάτων ● Κακόβουλες δραστηριότητες χρήστη	Οι προτεινόμενες λύσεις βασίζονται σε: ● Κρυπτογράφηση των μηνυμάτων διαμετρικής σηματοδοσίας ● ανίχνευση ανωμαλιών και ανίχνευση με βάση την υπογραφή χρησιμοποιώντας τον CUSUM
DoS	IP-based επιθέσεις στο backhaul του LTE: ● Υπερχείληση με	Προτείνονται δυο λύσεις βασισμένες στο VPN: ● L3 IPsec VPN με

	πακέτα TCP SYN/ RESET • TCP RESET επίθεση	την τροποποίηση IKEv2 • L3 IPsec BEET VPN βασισμένη στο HIP

6.2.1 IP-Based Επιθέσεις Ενάντια στο Backhaul

Το backhaul αποτελείται από στοιχεία ελέγχου και διασυνδέσεις που βασίζονται στην IP, καθιστώντας το ευάλωτο σε επιθέσεις που βασίζονται σε IP. Αυτή η ευπάθεια μπορεί να εξηγηθεί από την έλλειψη αμοιβαίας αυθεντικοποίησης των eNB, την έλλειψη πρόληψης των επιθέσεων που βασίζονται σε IP, την έλλειψη κρυπτογράφησης δεδομένων και την κίνηση σημοτοδοσίας σε μη αξιόπιστα δίκτυα. Τα S1-U, S1-C, X2-U και X2-C είναι διασυνδέσεις LTE backhaul όπου πρέπει η μεταφερόμενη κυκλοφορία να γίνεται με ασφάλεια. Οι πιθανές επιθέσεις σε αυτές τις διασυνδέσεις μπορούν να εκτελεστούν ως επίθεση κατά του eNB, υποκλοπή της κίνησης των χρηστών, επιθέσεις μη εξουσιοδοτημένης πρόσβασης, επίθεση υπερχείλισης με πακέτα TCP SYN και επιθέσεις επαναφοράς TCP RESET.

Η επίθεση πλαστογράφησης IP αναφέρεται επίσης ως επίθεση μεταμφιέσεων και συνίσταται στη χειραγώγηση των πακέτων TCP / IP και στην παραποίηση της διεύθυνσης IP πηγής, κάνοντας έτσι τον εισβολέα να εμφανίζεται ως άλλος χρήστης. Είναι δυνατό για τον εισβολέα να χρησιμοποιεί μια διεύθυνση IP μέσα στο εύρος διευθύνσεων IP του δικτύου ή να χρησιμοποιεί μια εξουσιοδοτημένη αξιόπιστη εξωτερική διεύθυνση IP που παρέχει πρόσβαση σε πόρους δικτύου. Συνήθως, αυτή η επίθεση μπορεί να οδηγήσει σε υπερβολικές χρεώσεις και υπερβολική κατανάλωση ενέργειας για ορισμένες UE (επίθεση εξάντλησης μπαταρίας) και να προκαλέσει μη ομαλή κίνηση σε στοιχεία του δικτύου κινητής τηλεφωνίας όπως το GPRS, το GGSN και το P-GW.

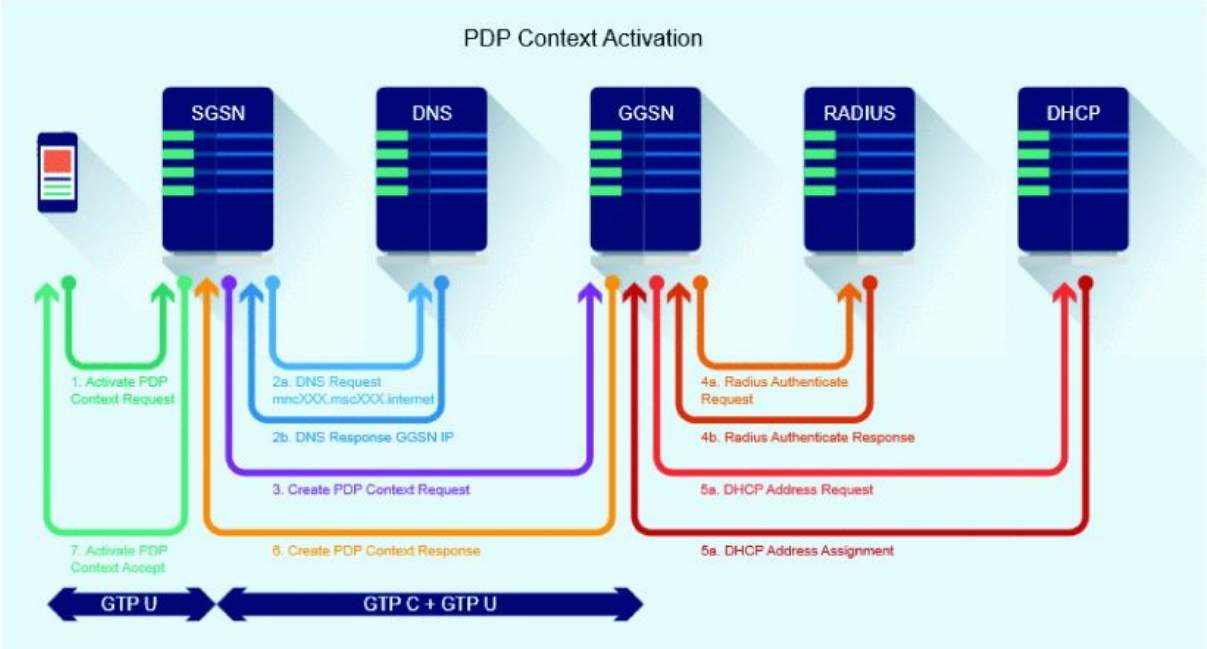
Για να μετριαστούν οι απειλές που βασίζονται στο πρότυπο 3GPP, προτάθηκε μια λύση ασφαλείας η οποία θα μπορούσε να χρησιμοποιηθεί κατά την ανάπτυξη του δικτύου LTE και την τροφοδότηση των eNB. Αυτή η λύση βασίζεται σε δυο βασικά στοιχεία, τις πύλες ασφαλείας για το φιλτράρισμα συνδέσεων και τη κρυπτογράφηση της

κυκλοφορίας βάσει IPsec, καθώς και μια αρχή έκδοσης πιστοποιητικών για την αποτροπή μη εξουσιοδοτημένης πρόσβασης στα δεδομένα ή σε στοιχεία δικτύου και την παροχή κλειδιών για την κρυπτογράφηση της κυκλοφορίας. Το DPI μπορεί να θεωρηθεί ως μελλοντική βελτίωση ασφάλειας.

Για να μετριαστούν τα ζητήματα ασφάλειας στο δίκτυο backhaul του LTE, υπάρχουν δύο λύσεις. Η πρώτη λύση αποτελείται από μια αρχιτεκτονική VPN τύπου IPsec σε επίπεδο 3, χρησιμοποιώντας ένα τροποποιημένο πρωτόκολλο IKEv2 για την παροχή προστασίας κατά των DoS επιθέσεων. Η δεύτερη λύση είναι μια αρχιτεκτονική VPN επιπέδου 3 που βασίζεται στο πρωτόκολλο HIP και παρέχει προστασία από επιθέσεις κατά της πλαστογράφησης. Χρησιμοποιείται για τη δημιουργία IPsec BEET (Bound End-to-End Tunnel) βασισμένα σε VPNs που επικαλύπτουν το δίκτυο backhaul. Ως αποτέλεσμα, η προτεινόμενη λύση VPNs μπορεί να προσφέρει προστασία ταυτότητας και εξουσιοδότησης χρηστών, κρυπτογράφηση ωφέλιμου φορτίου και προστασία ιδιωτικού απορρήτου από επιθέσεις που βασίζονται σε IP στο LTE backhaul.

6.2.2 Επιθέσεις που βασίζονται στο GTP

Μια άλλη τυπική επίθεση που βασίζεται σε IP είναι η επίθεση κατά του GTP, η επίδραση του οποίου στα δίκτυα LTE αποδείχθηκε μέσω προσομοιώσεων. Στην πραγματικότητα, το GTP είναι ένα tunneling πρωτόκολλο που χρησιμοποιείται για τη μεταφορά δεδομένων στο δίκτυο 4G και την εκχώρηση IP ή τη διαχείριση των πόρων του δικτύου.



Επιπλέον, το GTP είναι ένα πρωτόκολλο βασισμένο σε User Datagram Protocol (UDP), γεγονός που το εκθέτει σε επιθέσεις αλλοίωσης πακέτων. Ως παραδείγματα των επιθέσεων στο GTP, οι πιο κάτω επιθέσεις είναι πιο συχνές:

1. **Οι επιθέσεις σάρωσης GTP:** συνίστανται στην αποστολή μηνυμάτων echo για τη σάρωση στοιχείων δικτύου και μπορούν να προκαλέσουν διαρροή πληροφοριών σε δίκτυα κινητής τηλεφωνίας 4G, καθώς τα GTP echo/request μπορεί να αποκαλύψουν την ταυτότητα των στοιχείων του δικτύου
2. **Δημιουργία επιθέσεων αίτησης συνόδου:** συνίστανται σε επαναλαμβανόμενα αιτήματα δημιουργίας συνόδου σύνδεσης που μπορούν να προκαλέσουν εξάντληση πόρων λόγω μη φυσιολογικής χρήσης του μηνύματος αίτησης περιόδου σύνδεσης GTP για τον καθορισμό πόρων κατά την αρχική αποστολή του MS. Καθώς οι διευθύνσεις IP διανέμονται από το P-GW στο μήνυμα απάντησης δημιουργίας συνόδου σύνδεσης, μπορούν να εξαντληθούν εάν αποσταλούν υπερβολικά αιτήματα για τη δημιουργία συνεδριών. Μια διακοπή υπηρεσίας μπορεί να προκύψει από έναν ψευδή αριθμό κανονικών χρηστών που αποστέλλουν αιτήσεις δημιουργίας περιόδου σύνδεσης.
3. **Ασυνήθιστες επιθέσεις πακέτων GTP:** μπορεί να έχουν ως αποτέλεσμα το fuzzing του GTP σε κινητό δίκτυο 4G και δυσλειτουργία των συνιστωσών του GTP μετά τη λήψη μη φυσιολογικών μηνυμάτων GTP. Αυτές οι επιθέσεις

μπορούν να εκτελεστούν από το δίκτυο 3G και το Evolved Packet Data Gateway (ePDG) του WLAN.

4. **Οι επιθέσεις φωνητικών κλήσεων:** μπορεί να πραγματοποιηθούν με παραβίαση του πρωτοκόλλου SIP.
5. **Επιθέσεις υποδομής:** ένας εισβολέας μπορεί να τροποποιήσει τη δική του διεύθυνση IP και να συνδεθεί σε στοιχεία του CN όπως το GGSN και να στοχεύσει άλλες κινητές συσκευές εσωκλείωντας πακέτα προσβολής του GTP

6.2.3 VoLTE SIP-Based Attacks

Το SIP είναι ένα πρωτόκολλο βασισμένο σε κείμενο, το οποίο υποφέρει από διάφορες ευπάθειες.

Οι απειλές ασφαλείας SIP στο VoLTE, κατηγοριοποιούνται σε απειλές κατά του δικτύου και απειλές εναντίον του χρήστη. Τυπικές απειλές περιλαμβάνουν την έκθεση πληροφοριών λόγω της σάρωσης του δικτύου VoLTE, πλαστογράφησης μηνυμάτων, παραβιάσεων μηνυμάτων και υπερχείληση του SIP. Μπορούν να οδηγήσουν σε εξάντληση πόρων, υποβάθμιση ή διακοπή υπηρεσίας VoLTE, υπερχρέωση υπηρεσιών VoLTE, phishing VoLTE και DoS. Ως αντιστάθμισμα, πρότεινεται η διαχείριση ελέγχου των συνεδριάσεων, το σύστημα ανίχνευσης VoLTE βάσει ροής για την προστασία από επιθέσεις εξάντλησης δικτύου και εξάντλησης πόρων και το IPS VoLTE βασισμένο σε υπογραφές.

Επισημαίνεται ότι οι αδυναμίες του VoLTE που σχετίζονται με την έλλειψη ελέγχου πρόσβασης σε κινητό λογισμικό και υλικό για την πρόληψη της προσθήκης δεδομένων στον φορέα σηματοδοσίας VoLTE, τη μη σωστή δρομολόγηση και προώθηση από την πλευρά του κινητού δικτύου, το οποίο δεν παρέχει μηχανισμό επαλήθευσης της κίνησης που μεταφέρεται από τους φορείς σηματοδότησης μέσω του VoLTE, ούτε επαρκή άμυνα σε επίπεδο αδειών πρόσβασης στο κινητό τηλέφωνο. Εκμεταλλευόμενος αυτά τα τρωτά σημεία ο επιτιθέμενος, είναι δυνατόν να καταχραστεί τον φορέα σηματοδοσίας VoLTE είτε παρακάμπτοντας τον μηχανισμό χρέωσης προκειμένου να ληφθούν δεδομένα δωρεάν, είτε εκμεταλλευόμενος την υψηλή προτεραιότητα του φορέα σηματοδοσίας VoLTE ώστε να καταχραστεί το υψηλού επιπέδου QoS σηματοδότησης στο VoLTE . Τέτοιες επιθέσεις μπορούν να πραγματοποιηθούν με την ενσωμάτωση πακέτου δεδομένων ως πακέτου ICMP

(Internet Message Control Protocol) με τη χρήση ενθυλάκωσης ICMP για την παράδοση δεδομένων μέσω του φορέα σηματοδοσίας, αφού τα πακέτα ICMP προωθούνται από την πύλη 4G στο διαδίκτυο ή σε άλλο κινητό τηλέφωνο. Για να μετριασθούν οι παραπάνω επιθέσεις, προτείνονται αρκετές λύσεις: αυστηρή ρύθμιση της δρομολόγησης του 4G για να επιτρέψει την αναμετάδοση της κίνησης μέσω VoLTE μόνο μεταξύ του τηλεφώνου και του εξυπηρετητή φορέα σηματοδοσίας ή της πύλης μέσων στο IMS. Αναβάθμιση της πύλης 4G με την προσθήκη φίλτρων VoLTE. Χρέωση σημάτων παρόμοιων με την κίνηση δεδομένων. Μηχανισμό αναβολής, προκειμένου να μειωθεί η προτεραιότητα κατά το χρόνο εκτέλεσης όταν ο αιτούμενος πόρος υπερβαίνει την ποσόστωση.

6.2.4 Επιθέσεις που βασίζονται σε διάμετρο

Τέλος, μία από τις κρίσιμες απειλές στο 4G κινητό δίκτυο είναι η διαμετρική προσθήκη σημάτων θορύβου, η οποία έχει μεγάλη επίδραση στα δίκτυα LTE.

Στην πραγματικότητα, η διάμετρος αναμένεται να γίνει το πιο σημαντικό πρωτόκολλο για τη σηματοδότηση του επιπέδου ελέγχου στο IMS που χρησιμοποιείται για την παροχή υπηρεσιών Αυθεντικοποίησης, Εξουσιοδότησης και Χρέωσης. Είναι υπεύθυνη για τη διαχείριση της κινητικότητας των συσκευών, της περιαγωγής, των σύνθετων μοντέλων τιμολόγησης βάσει πολιτικής, του QoS και νέων υπηρεσιών (υπηρεσίες βασισμένες στο IMS, συμπεριλαμβανομένων των Rich Communication Services (RCS) και Voice Over LTE (VoLTE). Οι απειλές ασφάλειας και διακοπής του δικτύου που σχετίζεται με τη σηματοδότηση της διαμέτρου επηρεάζουν όλα τα δίκτυα κινητής τηλεφωνίας που βασίζονται σε IP. Τα μηνύματα σηματοδοσίας που βασίζονται στη διάμετρο μπορούν να χρησιμοποιηθούν από έναν εισβολέα για την πραγματοποίηση επιθέσεων εναντίον συνδρομητών και εξαρτημάτων του δικτύου. Ως λύση για την ανίχνευση και τον μετριασμό των ζητημάτων ασφάλειας και των επιθέσεων που σχετίζονται με τη διάμετρο, προτείνονται μια προληπτική και αντιδραστική προσέγγιση βασισμένη στις υπηρεσίες, η οποία περιλαμβάνει ένα σύστημα ανίχνευσης ανωμαλιών χρησιμοποιώντας έναν μηχανισμό κανόνων που επιτρέπει τον καθορισμό προδιαγραφών, εφαρμόζοντας διαφορετικούς κανόνες για τα δεδομένα εισερχόμενων κλήσεων. Μια λύση βασισμένη σε υπογραφές για την ανίχνευση του προφίλ των επιθέσεων και την τεχνική CUSUM. Η λύση αυτή, μπορεί να μετριάσει τις κακόβουλες δραστηριότητες και τις απειλές που σχετίζονται με τη διάμετρο με στόχο να ανιχνεύσει κακόβουλα μηνύματα.

6.3 Επιθέσεις σηματοδότησης

Σε αυτή την ενότητα, εξετάζουμε τις επιθέσεις σηματοδότησης, οι οποίες αποτελούν μείζονα απειλή στο δίκτυο κινητής τηλεφωνίας 4G, ιδιαίτερα στο επίπεδο σηματοδοσίας LTE. Ο παρακάτω Πίνακας παρουσιάζει μια επισκόπηση των τυπικών επιθέσεων DoS στο 4G.

Χάρτης αναφοράς επιθέσεων σε δίκτυα κινητής τηλεφωνίας 4G		
Στόχος Επίθεσης	Τύπος Επίθεσης	Προτεινόμενη Λύση
DoS	Επίθεση Επαναλαμβανόμενων MME Δημιουργίας αιτήματων φορέα για ενεργοποίηση διαδικασίας TAU	Προτάθηκε ένα νέο πρόγραμμα ενίσχυσης ασφάλειας για να γίνει διάκριση μεταξύ νόμιμου και παράνομου χρήστη
DoS	Ραδιοφωνική διασύνδεση LTE και έλεγχος σηματοδότησης φορέα	Προτάθηκε ένος βελτιστοποιημένος ελέγχος σηματοδότησης συνόδου, λειτουργίας και ελέγχου κομιστή, η οποία συνίσταται σε διαδικασίες ενεργοποίησης, τροποποίησης και απενεργοποίησης της αρχικοποιημένης σύνδεσης δικτύου
DoS	Το MS ξεκίνησε DoS σηματοδοσία	Προτάθηκε μία νέα μέθοδος εντοπισμού βασισμένη στα ίχνη των IP πακέτων που αντιλαμβάνεται κακόβουλες εφαρμογές
DoS	Η διεπαφή του LTE είναι ευάλλωτη στο Botnet	Καμία προτεινόμενη λύση
DoS	DoS επίθεση σηματοδοσίας	Προτάθηκε ένα σύστημα

	με επαναλαμβανόμενα δικτυακά πακέτα σύνδεσης/ αποσύνδεσης	ανίχνευσης DoS 3 βημάτων
DoS	• DoS χαμηλής έντασης • DDoS επίθεση σε δίκτυο LTE • Επιθέσεις ενίσχυσης σήματος • Επιθέσεις υπερχείλισης σηματοδοσίας με διαμετρική προσθήκη	Προτάθηκε ένα σύστημα βασισμένο σε ECN για την μείωση της συμφόρησης
DoS	RRC LTE επιθέσεις σημοτοδοσίας: • Επίθεση κατάληψης πόρων • Επαναλαμβανόμενες αιτήσεις για κομιστές που χρησιμοποιούν εσφαλμένη τιμή δείκτη MCS	Προτάθηκε ένα προσαρμοσμένο ελάχιστο όριο MCS με το οποίο τα υψηλά bandwidth απορρίπτονται από τον φορέα
DoS	HSS/AuC επίθεση υπερχείλισης που χρησιμοποιούν μη προστατευμένα μηνύματα κατά τις διαδικασίες του LTE	Καμία προτεινόμενη λύση

Στην πραγματικότητα, το LTE σε επίπεδο σηματοδοσίας μπορεί να στοχεύει με επιθέσεις σηματοδότησης, ιδιαίτερα με την εκμετάλλευση των τρωτών σημείων που σχετίζονται με την ενεργοποίηση και την απενεργοποίηση του κομιστή. Ο φορέας είναι βασικό στοιχείο του QoS σε δίκτυα LTE και συνίσταται σε μια εικονική σύνδεση μεταξύ του P-GW και του UE.

Οι απαιτήσεις 3GPP για το σχεδιασμό του ελέγχου σύνδεσης και του φορέα στο LTE επικεντρώνονται στην παροχή μιας υπηρεσίας προεπιλεγμένης IP πρόσβασης “πάντα

ανοιχτής” , η οποία επιτρέπει την σύνδεση με έναν προεπιλεγμένο φορέα εγκατάστασης και παροχής υπηρεσιών ενεργοποίησης πλαισίου κατά τη διάρκεια της προσάρτησης δικτύου, την σηματοδοσία δημιουργίας συνόδων που ξεκινούν από το δίκτυο. Η πολλαπλή πρόσβαση PDN απαιτεί επίσης σηματοδότηση εγκατάστασης που ξεκινά από το UE, συσσωμάτωση QoS και αλληλεπίδραση μηνυμάτων (για τη μείωση καθυστερήσεων στην εγκατάσταση υπηρεσιών).

Προκειμένου να εκπληρωθούν οι απαιτήσεις για τους φορείς συνεδριών, προτάθηκε μια βελτιστοποιημένη σηματοδότηση ελέγχου περιόδου λειτουργίας και ελέγχου του κομιστή, η οποία συνίσταται σε διαδικασίες ενεργοποίησης, τροποποίησης και απενεργοποίησης της διαδικασίας σύνδεσης, με μια προεπιλεγμένη υπηρεσία πρόσβασης IP και πολλαπλή υποστήριξη πρόσβασης PDN και μια διαδικασία ενεργοποίησης της περιόδου συνόδου, ικανή να παρέχει αλληλοσύνδεση μηνυμάτων για τη βελτιστοποίηση της σηματοδότησης ελέγχου λειτουργίας και ελέγχου σηματοδοσίας.

Ανάλογα με το επίπεδο QoS που πρέπει να επιτευχθεί, αρκετοί φορείς είναι τυποποιημένοι, κάθε φορέας έχει τις δικές του παραμέτρους QoS με βάση τον τύπο της εφαρμογής. Οι τυπικοί φορείς είναι:

- E-RAB: είναι ραδιο-φορέας μεταξύ UE και eNB,
- S1 φορέας: είναι φορέας μεταξύ eNB και S-GW,
- S5-S8 φορέας: είναι φορέας μεταξύ S-GW και P-GW.

Για να ενεργοποιηθεί / απενεργοποιηθεί ένας κομιστή, απαιτούνται δώδεκα μηνύματα σηματοδότησης, έξι από τα οποία επεξεργάζονται στο eNB. Έτσι, η προκύπτουσα επιβάρυνση σηματοδοσίας μπορεί να αξιοποιηθεί για να ξεκινήσουν επιθέσεις σηματοδοσίας LTE, όπως η επίθεση η οποία εξαρτάται από την επανειλημμένη και ταυτόχρονη αποστολή μεγάλου αριθμού αιτήσεων αξιόπιστων φορέων προκειμένου να αναγκαστεί η ενεργοποίηση και η απενεργοποίηση του κομιστή.

Μια άλλη τυπική επίθεση στον κομιστή, γνωστή ως επίθεση κράτησης πόρων, μπορεί να εκτελεστεί από ένα μικρό αριθμό χρηστών που δεσμεύουν κακόβουλα τους πόρους στο eNB ζητώντας από τους φορείς υψηλό εύρος ζώνης, ενώ αυτοί συνήθως απαιτούν χαμηλό εύρος ζώνης για τέτοιες εργασίες, προκαλώντας έτσι άρνηση εξυπηρέτησης για όλους τους άλλους χρήστες στο ίδιο κελί που εκτελούν αιτήματα εφαρμογών TCP. Για να μετριαστούν τέτοιες επιθέσεις, προτείνεται να ορισθεί ένα ελάχιστο όριο MCS κάτω από το οποίο θα απορρίπτονται οι υψηλές αιτήσεις για Bandwindth. Το όριο αυτό μπορεί να οριστεί από τους φορείς.

Μια άλλη κατηγορία σηματοδοτικών επιθέσεων σε φορείς LTE μπορεί να πραγματοποιηθεί με την εκμετάλλευση των τρωτών σημείων στη διαδικασία TAU, η ασφάλεια της οποίας εξαρτάται εξ' ολοκλήρου από το MME. Λόγω της έλλειψης επαλήθευσης από τον χρήστη και της έλλειψης μηχανισμών προστασίας στο S-GW για την TAU, οι παράνομοι χρήστες ενδέχεται να είναι σε θέση να ξεκινήσουν διάφορες επιθέσεις εναντίον του MME, όπως επίθεση αποστολής αιτημάτων δημιουργίας φορέα, υπερφόρτωση S-GW ή χρήση κακόβουλου UE για τη συνεχή ενεργοποίηση της TAU. Ως αντίμετρο εναντίον αυτών των επιθέσεων, μπορεί να χρησιμοποιηθεί ένα πρόγραμμα ενίσχυσης της ασφάλειας για την αντιμετώπιση των επιθέσεων DoS, το οποίο μπορεί να αποτρέψει το S-GW από κακόβουλα αιτήματα κατά τη διαδικασία TAU όταν η UE εισέρχεται σε νέα περιοχή παρακολούθησης. Το σύστημα αυτό μπορεί να κάνει διάκριση μεταξύ νόμιμων χρηστών και παράνομων. Στην πραγματικότητα, αξιοποιώντας το γεγονός ότι το IMSI είναι παρόν σε κάθε Αίτηση TAU, το MME μπορεί να στείλει ένα αίτημα Δημιουργίας Φορέα στο S-GW με το IMSI, ο οποίος με τη σειρά του ελέγχει εάν έχει λάβει περισσότερες από μία Αιτήσεις Δημιουργίας για τον Χρήστη, ή με τη χρήση μηνύματος αιτήματος-ερωτήματος που αποστέλλεται στο παλιό S-GW για να ελέγξει την αυθεντικότητα του χρήστη σε περίπτωση επίθεσης από μη αυθεντικοποιημένο χρήστη.

Ένα σημαντικό σημείο είναι η δυνατότητα εκτέλεσης DDoS σε δίκτυα κινητής τηλεφωνίας 4G χρησιμοποιώντας συντονισμένες σηματοδοτικές επιθέσεις DoS από τα botnets, οι οποίες μπορεί να έχουν τεράστιες επιπτώσεις στη διεπαφή του LTE. Το DDoS από τα botnets μπορεί να επιτευχθεί μέσω επιθέσεων ενίσχυσης σήματος (πλημμύρες σηματοδοσίας μηνυμάτων) προκειμένου να εξαντληθούν οι πόροι του δικτύου και να επηρεαστούν οι επιδόσεις του. Ως αντιστάθμισμα, προτείνεται η μείωση του κινδύνου συμφόρησης βάσει του ECN για την αποφυγή συμφόρησης στις διεπαφές διαμέτρου. Αυτή η λύση είναι μια επέκταση του TCP / IP και χρησιμοποιεί έναν

αλγόριθμο αποφυγής συμφόρησης επιπέδου μεταφοράς, προκειμένου να αποφευχθεί η αύξηση των μηνυμάτων στο δρομολογητή μέσω σημάτων ECN. Μετά την παραλαβή πακέτου που θεωρείται ότι προκαλεί συμφόρηση, ο δέκτης TCP ενημερώνει τον αποστολέα στο ακόλουθο μήνυμα επιβεβαίωσης (ACK) σχετικά με επικείμενη συμφόρηση, η οποία με τη σειρά του θα ενεργοποιήσει τον αλγόριθμο αποφυγής συμφόρησης στον αποστολέα.

Το LTE εισήγαγε μια απότομη αύξηση της κυκλοφορίας βίντεο σε δίκτυα κινητής τηλεφωνίας, η οποία μπορεί να χρησιμοποιηθεί για την συμφόρηση του δικτύου. Για να αντιμετωπιστούν τα γενικά έξοδα σηματοδότησης που σχετίζονται με τον υψηλό όγκο ροής κίνησης βίντεο, ο οποίος μπορεί να αυξήσει το OPEX για τους φορείς εκμετάλλευσης κινητής τηλεφωνίας, προτείνεται ένα σύστημα σήμανσης προτεραιότητας για το περιεχόμενο, QoE. Στο LTE, αυτό το σχήμα μπορεί να εφαρμοστεί σε δύο ενότητες: μια ενότητα σήμανσης προτεραιότητας CA που επισημαίνει κάθε πακέτο στρώματος βίντεο με την προτεραιότητα του ανταποκριτή και ένα CA που κατεβάζει το layer, το οποίο με τη σειρά του ρίχνει την παραλαβή του πακέτου στο eNB με βάση την προτεραιότητά του.

Τέλος, μια άλλη τυπική επίθεση σηματοδοσίας σχετίζεται με την επίθεση αιτημάτων NAS με στόχο το HSS / AuC. Αυτή η επίθεση μπορεί να πραγματοποιηθεί με την εκμετάλλευση των τρωτών σημείων στο NAS του E-UTRAN λόγω των μη προστατευμένων ανταλλαγών μηνυμάτων RRC κατά τη διαδικασία προσάρτησης: RRCConnectionRequest, RRCConnectionSetup, RRCConnectionSetupComplete, RRCConnectionReject και RRCConnectionRelease. Επιπλέον, η μη προστατευμένη μετάδοση του IMSI κατά τη δημιουργία της σύνδεσης και η απροστάτευτη μετάδοση του Cell Radio Network Temporary Identifier (C-RNTI) κατά τη διάρκεια της διαδικασίας προώθησης επιπέδου 1 μπορούν επίσης να χρησιμοποιηθούν για να ξεκινήσουν μια τέτοια επίθεση. Στην πραγματικότητα, δεδομένου ότι το C-RNTI είναι ένα προσωρινό αναγνωριστικό ενός κινητού εντός του δικτύου κυψελωτού ραδιοσυστήματος που έχει ανατεθεί από το δίκτυο μέσω σημάτων ελέγχου RRC, αυτό το τρωτό σημείο μπορεί να αξιοποιηθεί για να προκαλέσει επίθεση DoS με υπερχείληση του HSS / AuC.

6.4 Επίθεση που βασίζεται σε παρεμβολές

Σε αυτή την ενότητα, περιγράφουμε κυρίως τις επιθέσεις DoS με παρεμβολές σε δίκτυα 4G που επικεντρώνονται στο LTE και αναθεωρούμε τις τρέχουσες λύσεις που βασίζονται στην επιστημονική βιβλιογραφία. Οι επιθέσεις παρεμπόδισης είναι γνωστές ως επιθέσεις παρεμβολών και μπορούν να πραγματοποιηθούν σε διαφορετικές στρώσεις, ιδιαίτερα στο φυσικό στρώμα, όπου η κύρια απειλή αφορά την εμπλοκή ραδιοσυχνοτήτων. Η εμπλοκή ραδιοσυχνοτήτων μπορεί να γίνει κατανοητή ως η σκόπιμη μετάδοση ραδιοφωνικών σημάτων προκειμένου να διαταραχθούν οι επικοινωνίες μειώνοντας τον λόγο σήματος προς θόρυβο (SNR) του ληφθέντος σήματος.

Έχουν εντοπιστεί και εξετασθεί διάφορες μορφές εμπλοκής σε ασύρματα δίκτυα, οι οποίες συνοψίζονται ως εξής:

- **Συνεχής παρεμβολή:** συνίσταται στη συνεχή μετάδοση σήματος παρεμβολής μέσω του κοινόχρηστου ασύρματου μέσου. Μπορεί να οδηγήσει σε αύξηση των επιπέδων παρεμβολών και θορύβου και σε υποβάθμιση της ποιότητας λήψης σήματος. Ως πρόσθετο αποτέλεσμα, το ασύρματο κανάλι είναι πάντα απασχολημένο, γεγονός που εμποδίζει τον νόμιμο πομπό να αποκτήσει πρόσβαση στο κανάλι. Ως εκ τούτου, η συνεχής επίθεση θορύβου, έχει την ικανότητα να διαταράσσει τις νόμιμες επικοινωνίες.

- **Διαλείπουσα παρεμβολή:** συνίσταται στην εκπεμπόμενη παρεμβολών κατά διαστήματα.

- **Παρεμβολή επανενεργοποίησης:** για να καταστραφούν τα δεδομένα στη λήψη, ξεκινάει μια μετάδοση σήματος παρεμβολής όταν η νόμιμη μετάδοση ανιχνεύεται ότι είναι ενεργή. Σε σύγκριση με τη σταθερή και τη διαλείπουσα εμπλοκή, η ενεργός εμπλοκή έχει λιγότερες επιπτώσεις εξαιτίας του γεγονότος ότι μόνο τα δεδομένα στη λήψη είναι κατεστραμμένα ενώ ο νόμιμος πομπός εξακολουθεί να έχει πρόσβαση στο ασύρματο κανάλι.

- **Προσαρμοστική παρεμβολή:** σε αυτήν την επίθεση, το μεταδιδόμενο σήμα εμπλοκής ρυθμίζεται στο επίπεδο της λαμβανόμενης ισχύος του νόμιμου δέκτη. Μια ομοιότητα με την αντιδραστική παρεμβολή είναι το γεγονός ότι η προσαρμοστική παρεμβολή δεν μεταδίδεται όταν η νόμιμη μετάδοση δεν ανιχνεύεται και είναι ανενεργή. Ωστόσο, η σκληρότητα για την ανίχνευση μιας τέτοιας επίθεσης εξαιτίας της δυναμικής ρύθμισης του μπλοκαρίσματος είναι ένα από τα χαρακτηριστικά της.

- **Ευφυής παρεμβολή:** αυτή συνήθως εκμεταλλεύεται τις αδυναμίες των πρωτοκόλλων ανώτερου στρώματος προκειμένου να εμποδίσει τη νόμιμη μετάδοση. Για να εκτελεσθεί μια τέτοια επίθεση, απαιτείται μια λεπτομερής κατανόηση των πρωτοκόλλων ανώτερου στρώματος, προκειμένου να στοχευθούν τα κρίσιμα πακέτα ελέγχου δικτύου αντί των πακέτων δεδομένων, με βάση τα τρωτά σημεία του σχετικού πρωτοκόλλου. Οι τυπικές επιθέσεις περιλαμβάνουν παρεμβολές των πακέτων ελέγχου MAC σε WiFi, τα οποία μπορούν να ομαδοποιηθούν σε επίθεση εμπλοκής έτοιμων προς αποστολή (RTS), επίθεση παρεμβολής Clear To Send (CTS) και επίθεση παρεμβολής ACK.

6.4.1 Έξυπνη εμπλοκή

Εξαρτάται από την τοπική διακοπή των επικοινωνιών LTE χωρίς να προκαλεί προειδοποιήσεις, με κορεσμό καναλιών ελέγχου ανερχόμενης και κατερχόμενης ζεύξης και τείνει να μην εντοπίζεται και να μετριάζεται. Υπάρχουν δύο μορφές επιθέσεων έξυπνης παρεμβολής: έξυπνη παρεμβολή καθοδικής και ανοδικής ζεύξης.

Σε επιθέσεις έξυπνης παρεμβολής κατερχόμενης ζεύξης, παράγεται ένα κακόβουλο ραδιοφωνικό σήμα προκειμένου να παρεμβαίνει στη λήψη των κρίσιμων πληροφοριών καναλιών ελέγχου κατερχόμενης ζεύξης. Σε επιθέσεις έξυπνης παρεμβολής ανερχόμενης ζεύξης, αντίθετα, το κανάλι ελέγχου ανερχόμενης ζεύξης είναι ο κύριος στόχος. Με τη στόχευση του καναλιού ελέγχου ανερχόμενης ζεύξης, μπορεί να εμποδισθεί το eNB να λαμβάνει βασικά μηνύματα σηματοδότησης που απαιτούνται για τη σωστή λειτουργία της κυψέλης. Η εκτέλεση μιας τέτοιας επίθεσης απαιτεί προηγούμενη γνώση του Φυσικού Φορέα (PRB) που έχει ανατεθεί σε ένα κανάλι

ελέγχου ανερχόμενης ζεύξης στο φυσικό στρώμα, το οποίο μπορεί να ληφθεί από μη προστατευμένα μηνύματα SIB που μεταφέρονται από το PBCH και το Physical Downlink Shared Channel (PDSCH). Στην πραγματικότητα, τα μη προστατευμένα μηνύματα MIB και SIB μεταφέρονται στο κανάλι PBCH κατά την αρχική διαδικασία πρόσβασης στο δίκτυο LTE και μπορεί να παρακολουθούνται όπως αναφέρεται σε προηγούμενες ενότητες. Από πρακτική άποψη, η επίθεση σταθμού βάσης μπορεί να βελτιστοποιηθεί συνδυάζοντας έξυπνο μπλοκάρισμα στο δίκτυο LTE προκειμένου πρώτα να ληφθούν πληροφορίες από τα μη κρυπτογραφημένα μηνύματα MIB και SIB και στη συνέχεια να αναγκαστεί ο UE να εγγραφεί σε μια ψεύτικη κυψέλη GSM, χωρίς να χρειαστεί έλεγχος ταυτότητας.

Ο αντίκτυπος της έξυπνης παρεμβολής στην απόδοση των δικτύων LTE παραμένει ανοιχτό πρόβλημα. Ένας επιτιθέμενος μπορεί να εκτελέσει έξυπνες παρεμβολές DoS στα κοινά κανάλια ελέγχου και OFDM πειραματικά σύμβολα όπως το CS-RS σε LTE, χρησιμοποιώντας απλές τεχνικές παρεμβολής στενής ζώνης, χωρίς να απαιτείται hacking του δικτύου ή των χρηστών του. Αυτό μπορεί να επιτευχθεί μέσω ενός έξυπνου παρεμποδιστή περιορισμένης ισχύος που στοχεύει το CS-RS, το PBCH ή το PCFICH και μπορεί να οδηγήσει σε απώλεια του δείκτη μορφής ελέγχου (CFI). Ένας άλλος αντίκτυπος είναι η απώλεια της παρακολούθησης των πληροφοριών κρίσιμης ανάδρασης από τις μονάδες UE στο PUCCH.

6.4.2 Μπλοκάρισμα θορύβου

Εξαρτάται από την εισαγωγή του θορύβου στον δέκτη και λαμβάνει διάφορες μορφές όπως:

- **Μπαράζ επιθέσεων παρεμβολής:** αυτή η μορφή εμπλοκής αναφέρεται επίσης ως επίθεση παρεμβολής θορύβου ευρείας ζώνης και συνίσταται στην παρεμβολή σε όλο το εύρος ζώνης που καταλαμβάνεται από τους φορείς OFDM με υψηλό επίπεδο θορύβου.

- **Επίθεση παρεμβολής θορύβου μερικής ζώνης:** αυτή η τεχνική εμπλοκής συνίσταται στην εμπλοκή ενός τμήματος του BW με τη μετάδοση του πρόσθετου

λευκού Gaussian Noise (AWGN) επάνω του. Μπορεί να εκτελείται ως επίθεση παρεμβολής με ένα ήχο ή επίθεση με παρεμβολές πολλαπλών τόνων. Η παρεμβολή ενός τόνου απαιτεί να μεταδίδεται ένας μόνο υψηλός τροφοδοτούμενος παλμός του θορύβου AWGN έτσι ώστε να παρεμβαίνει σε μια συγκεκριμένη ζώνη ενδιαφέροντος. Αυτό μπορεί να επηρεάσει μόνο το LTE καθόδου ενός υπο-φορέα. Η εμπλοκή πολλαπλών τόνων μπορεί να θεωρηθεί ως μια παραλλαγή της παρεμβολής μερικής φραγής, στην οποία μεταδίδονται πολλαπλοί αριθμοί εξίσου ισχυρού θορύβου προκειμένου να αφαιρεθεί ένας πολλαπλός αριθμός υποφορέων συχνότητας εντός των ζωνών LTE. Αυτή η επίθεση τείνει να είναι ιδιαίτερα αποτελεσματική σε περίπτωση περιορισμένης ισχύος στην πλευρά μετάδοσης.

- **Επίθεση παρεμβολής με τιτιβίσματα:** πρόκειται για έναν συνεχή κυματοειδή τόνο με συνεχώς μεταβαλλόμενη συχνότητα στην πάροδο του χρόνου. Αυτός ο τύπος παρεμβολής είναι ο πιο δύσκολος για να μετριαστεί.

6.4.3 Παρεμβολή πάνω σε κανάλι ελέγχου

Είναι μια τυπική μορφή παρεμβολής που στοχεύει το 4G LTE στο κανάλι ελέγχου. Αυτή η επίθεση μπορεί να εκτελεστεί εκμεταλλευόμενη τις ευπάθειες που σχετίζονται με τα κανάλια PCFICH και PUCCH στα σήματα καθόδου και ανόδου, την αναλογία J / S στα φυσικά κανάλια OFDM (PDSCH / PUSCH, PCFICH, PUCCH, PBCH, Physical Hybrid-ARQ Indicator Channel (PHICH)), το σήμα φυσικού επιπέδου LTE, πρωτογενή και δευτερογενή σήματα συγχρονισμού (PSS) και τα σήματα αναφοράς Downlink (RS)). Στην πραγματικότητα, τα κανάλια ελέγχου όπως το PUCCH παίζουν βασικό ρόλο στη μετάδοση LTE, καθώς χρησιμοποιούνται για τη μετάδοση σημάτων ζωτικής σημασίας ελέγχου. Συνεπώς, το μπλοκάρισμα του φάσματος που διατίθεται στο PUCCH μπορεί να οδηγήσει στη μείωση της διαθεσιμότητας σύνδεσης LTE μέσα σε μια ή περισσότερες κυψέλες λόγω των επιπτώσεων αυτής της επίθεσης. Ως παραδείγματα επιπτώσεων αυτής της επίθεσης, υπάρχει η αδυναμία της σηματοδότησης ελέγχου να φθάσει στα eNB, η περιττή επαναμετάδοση και οι καθυστερήσεις των δεδομένων κατερχόμενης ζεύξης σε συνδυασμό με τα λανθασμένα ACK και μη αναγνώριση (NACK), και τα αιτήματα προγραμματισμού phantom που σχετίζονται με λανθασμένα SR προκαλώντας το eNB να κατανείμει το PUSCH σε μια UE που δεν ζητά μετάδοση. Άλλες επιπτώσεις περιλαμβάνουν την κακή προσαρμογή της σύνδεσης λόγω

εσφαλμένων CQIs και την αλλοιωμένη ανατροφοδότηση MIMO λόγω εσφαλμένου CSI που ελήφθη στο eNB.

Επιπλέον, επιθέσεις σε κανάλια ελέγχου μπορούν επίσης να πραγματοποιηθούν με παρεμβολή τμήματος των σημάτων ανερχόμενης ή κατερχόμενης ζεύξης. Στην περίπτωση αυτή οι τυπικές επιθέσεις περιλαμβάνουν:

- **HARQ Επιβεβαίωση Επίθεση:** μπορεί να προκαλέσει καθυστερήσεις και περιττή επανάδοση.

- **Επίθεση καναλιού τυχαίας προσπέλασης:** εξαρτάται από την παρέμβαση στο τμήμα του εύρους ζώνης ανερχόμενης ζεύξης που έχει εκχωρηθεί σε αιτήσεις τυχαίας πρόσβασης. Με την υπερχείλιση του καναλιού τυχαίας προσπέλασης, αυτή η επίθεση μπορεί να οδηγήσει στην αδυναμία του σταθμού βάσης να επιτρέψει σε ένα χρήστη να ξεκινήσει την επικοινωνία.

- **Επίθεση στον Δείκτη Διαμόρφωσης:** αυτή η επίθεση μπορεί να πραγματοποιηθεί με εμπλοκή του δείκτη σχήματος διαμόρφωσης (MSI) προκειμένου να προκληθεί λανθασμένη αποδιαμόρφωση δεδομένων στον δέκτη, υψηλότερη ταχύτητα σφάλματος δυαδικών ψηφίων (BER) και κατεστραμμένο CQI. Στην πραγματικότητα, οι διαταραχές CQIs μπορούν να οδηγήσουν είτε σε μια κατώτερης διάταξης διαμόρφωση σε έναν υποφορέα που διαφορετικά θα μπορούσε να χειριστεί περισσότερα, είτε σε μια υπερβολικά υψηλή διάταξη διαμόρφωσης η οποία θα αυξήσει τον BER στον υποφορέα.

- **Επίθεση στην κατανομή των πόρων:** Αυτός ο τύπος επιθέσεων μπορεί να εκτελεστεί με την αλλοίωση των πληροφοριών κατανομής πόρων, οι οποίες μπορούν να οδηγήσουν σε DoS.

Προκειμένου να μετριαστούν ο θόρυβος AWGN και παρεμβολές θορύβου στο OFDM, προτάθηκαν διάφορες λύσεις που ακολουθούν τις παρακάτω τεχνικές:

- Οι επιθέσεις εξισορρόπησης μπορούν να μετριαστούν με τη μετάδοση πιλοτικών τόνων των οποίων οι τιμές είναι άγνωστες στους επιτιθέμενους ή την τυχαία επιλογή των πιλοτικών θέσεων.

- Οι επιθέσεις στο κανάλι ελέγχου μπορούν να μετριαστούν συμπεριλαμβάνοντας ευάλωτες πληροφορίες ελέγχου σε άδειους πόρους δεδομένων, την παρακολούθηση των πρόσθετων ενεργειών στα κανάλια ελέγχου, την τυχαία ρύθμιση των καναλιών ελέγχου στο χρόνο και στη συχνότητα και τη χρήση ενός κοινόχρηστου κλειδιού για τη μετάδοση πληροφοριών θέσης στον χρήστη.

Άλλες λύσεις μετριασμού και προσεγγίσεις κατά των επιθέσεων εμπλοκής σε LTE, συμπεριλαμβάνουν την αυθεντικοποίηση, την δημιουργία κλειδιού και την κρυπτογράφηση σε φυσικό επίπεδο. Δεδομένου ότι οι μηχανισμοί φυσικής ασφάλειας LTE επικεντρώνονται στην αυθεντικοποίηση σε φυσικό επίπεδο, στην παραγωγή γεννήτριας κλειδιών σε φυσικό επίπεδο στρώματος και στην κρυπτογράφηση σε φυσικό επίπεδο. Οι μετριαστικές επιθέσεις στο φυσικό στρώμα μπορούν να επιτευχθούν μέσω διαδικασίας πιστοποίησης βασισμένης στις τεχνικές ασφαλείας φυσικού στρώματος, προκειμένου να απλοποιηθεί η αλληλεπίδραση σηματοδότησης καθώς και να ενισχυθεί η ασφάλεια του συστήματος και να μειωθούν τα γενικά έξοδα της ανταλλαγής πληροφοριών και της μετάδοσης σημάτων. Επιπλέον, η λύση αυτή δεν απαιτεί συμμετρικό κλειδί στο σύστημα λόγω της δημιουργία του κλειδιού σύμφωνα με τα χαρακτηριστικά του καναλιού και εξασφαλίζει την ασφάλεια μετάδοσης μέσω τεχνικών μορφοποίησης δέσμης και προκαθορισμού.

Επιπλέον, ως λύση έναντι της απώλειας ορθογωνιότητας μεταξύ των συνδεδεμένων ή κατακερματισμένων ζωνών φάσματος, οι οποίες μπορούν να χρησιμοποιηθούν για να προκαλέσουν διακοπή υπηρεσίας σε δίκτυα DSA με βάση το IEEE 802.22, δίκτυα LTE και High Access Packet Access (HSPA) +, μπορούν να λάβουν μέτρα ανίχνευσης με βάση την εκτιμώμενη ισχύ του παραληφθέντος σήματος. Για να είναι αποτελεσματικός, ένας τέτοιος μηχανισμός ανίχνευσης εξαρτάται από τη διαφορά μεταξύ της μέσης ισχύος μετάδοσης των καλών χρηστών και της ισχύος μετάδοσης των εισβολέων και μπορεί να ενισχυθεί με την ανάπτυξη μιας συνεταιριστικής ανίχνευσης.

Για τον μετριασμό των επιπτώσεων των επιθέσεων εμπλοκής στο πρωτόκολλο PUCCH αναλύθηκαν πιθανές μέθοδοι ανίχνευσης και μετριασμού και προτάθηκε η

παρακολούθηση της περίσσειας ενέργειας PUCCH, η οποία επιτρέπει την ανίχνευση επίθεσης με βάση την παρουσία ενέργειας σε στοιχεία πόρων στην περιοχή PUCCH που δεν έχει εκχωρηθεί. Επιπλέον, η παρακολούθηση μπορεί απλώς να ανιχνεύσει μια ασυνήθιστα υψηλή ποσότητα ενέργειας στην περιοχή PUCCH συνολικά, να ανιχνεύσει μια ανώμαλη ποσότητα σφαλμάτων PUCCH παρακολουθώντας το eNB για μια ξαφνική αύξηση των σφαλμάτων στο PUCCH, καθώς και εσφαλμένα Bit βλέποντας τις ληφθείσες τιμές CQI που δεν είναι έγκυρες.

Ως αντισταθμιστικά μέτρα προτάθηκαν, να δίνονται στον χρήστη πόροι PUSCH για κάθε υποπλαίσιο που έχει πληροφορίες ελέγχου ανερχόμενης ζεύξης για αποστολή, καθώς και για τους περιοδικούς πόρους PUSCH ή για τη χρήση δυναμικού μεγέθους PUCCH και για τη χορήγηση περιοδικών PUSH για υποσύστηματα με την παρουσία των phantom-SRs, μεταβιβάζοντας την αξιόπιστη μετάδοση σε υψηλότερα επίπεδα και αναγκάζοντας όλες τις PDUs στο RLC να χρησιμοποιούν μη αναγνωρισμένο τρόπο (RLC-UM) για να μετριάσουν τις επιπτώσεις της παρεμβολής PUCCH στις διαδικασίες HARQ.

Για να επιτευχθεί η πλήρης διαθεσιμότητα και η ανθεκτικότητα των κυψελοειδών δικτύων από επιθέσεις ασφάλειας, μελλοντικές κατευθύνσεις έρευνας πρέπει να είναι:

- **Προστασία εκπομπής και ελέγχου καναλιών:** θα χρειαστεί για βελτιωμένη ανθεκτικότητα παρεμβολών.

- **Αρχική πρόσβαση στο δίκτυο:** οι γνώσεις από παλαιότερα ραδιοσυστήματα και η επαναχρησιμοποίηση των παλαιότερων δικτύων θα μπορούσαν να εφαρμοστούν για τον σχεδιασμό ισχυρότερων αρχιτεκτονικών κατανομής ραδιό-πόρων.

- **RRC διαχείριση φορέα:** κατανεμημένη διαδικασία διαχείρισης κομιστή, προκειμένου να διανείμει το φορτίο σηματοδότησης EPC και να ελαχιστοποιήσει τον αντίκτυπό του είναι απαραίτητη.

- **Εφαρμογή κατανεμημένων λύσεων:** μείωση της εξάρτησης κεντρικού κόμβου.

- **Σηματοδότηση δικτύου πυρήνα:** Ισχυροί κόμβοι δικτύου SoN και λογισμικού θα μπορούσαν να ελαχιστοποιήσουν το φορτίο σηματοδοσίας NAS στο EPC και να παράσχουν χαρακτηριστικά μετριασμού για την εξισορρόπηση, την επαναδρομολόγηση ή το φιλτραρίσμα της κυκλοφορίας ελέγχου δικτύου και θα μπορούσαν να εφαρμοστούν σε μια ευέλικτη και προσαρμόσιμη αρχιτεκτονική.

6.5 Θέματα Ανοιχτά προς Έρευνα

Σε αυτήν την ενότητα, εντοπίζουμε ανοικτά ζητήματα στην ασφάλεια δικτύων κινητών τηλεφώνων επισημαίνοντας τομείς στους οποίους χρειάζεται περισσότερη έρευνα.

Α. Μείωση επιθέσεων διαθεσιμότητας και ασφάλειας στο 4G

Οι επιθέσεις DoS και DDoS στο κινητό 4G εξακολουθούν να είναι ένα ανοιχτό ζήτημα και μπορούν να εκτελεστούν αξιοποιώντας τις ευπάθειες που παρουσιάζονται σε προηγούμενες ενότητες. Έχουν επισημανθεί οι πιθανότητες πραγματοποίησης επιθέσεων σε συγκλίνοντα δίκτυα LTE (Physical and MAC layer of WiMAX). Ωστόσο, υπάρχει ακόμη ανάγκη να σχεδιαστούν νέοι μηχανισμοί προστασίας και κρυπτογράφησης που θα εφαρμόζονται στο φυσικό στρώμα.

Οι επιθέσεις DoS μπορούν επίσης να προκύψουν από την ενσωμάτωση δικτύων WLAN και 4G / LTE. Οι λύσεις που προτείνονται κατά των απειλών αυτών βασίζονται σε ένα καινοτόμο σύστημα παρακολούθησης της κίνησης. Στην περίπτωση επιθέσεων στη διάμετρο, προτάθηκαν προληπτικές και αντιδραστικές προσεγγίσεις βασισμένες στις υπηρεσίες, συμπεριλαμβανομένων συστημάτων ανίχνευσης που βασίζονται σε υπογραφές. Η αποδοτικότητα αυτών των λύσεων σε λειτουργικά δίκτυα κινητής τηλεφωνίας δεν έχει αποδειχθεί. Η μελλοντική έρευνα ασφάλειας σχετικά με την ανίχνευση επίθεσης δικτύου κινητικότητας, προκειμένου να παρέχεται προηγμένο σύστημα ανίχνευσης επίθεσης σε επίπεδο RAN, προτείνεται.

Στην αρχιτεκτονική ασφάλειας LTE, υπάρχουν ορισμένα θέματα που αξίζει να διερευνηθούν. Στην πραγματικότητα, πρέπει να σχεδιαστούν περισσότεροι μηχανισμοί ασφαλείας στην αρχιτεκτονική του συστήματος, προκειμένου να προστατευθούν οι επικοινωνίες από επιθέσεις λόγω παλαιομένων πρωτοκόλλων και φυσικές εισβολές στα δίκτυα LTE.

Απαιτούνται πρόσθετες βελτιώσεις στο σχήμα EPS AKA καθώς και σχεδιασμός ασφαλούς πρόσβασης σε συστήματα αυθεντικοποίησης που θα χρησιμοποιηθούν κατά τη διάρκεια της πρόσβασης του UE στο EPC μέσω μη-3GPP δικτύων, προκειμένου να προστατευθεί από την αποκάλυψη ταυτότητας χρήστη, επιθέσεων DoS και άλλων κακόβουλων επιθέσεων. Επιπλέον, η ασφάλεια της διαδικασίας LTE Handover εξακολουθεί να είναι ένα ανοιχτό ζήτημα που απαιτεί περαιτέρω βελτιώσεις στους μηχανισμούς διαχείρισης κλειδιών και στις διαδικασίες ανταλλαγής ταυτότητας με σκοπό την αποτροπή επιθέσεων πρωτοκόλλου, αποσυγχρονισμού και επανάληψης.

Μια νέα τάση είναι η ενσωμάτωση του Machine to Machine (M2M) στα δίκτυα κινητής τηλεφωνίας. Στο πλαίσιο αυτό, πρέπει να διεξαχθούν ορισμένες έρευνες σχετικά με τις απειλές επικύρωσης ταυτότητας που ενδέχεται να προκύψουν. Στην πραγματικότητα, υπήρξαν αρκετές εργασίες σχετικά με θέματα που σχετίζονται με τις αδυναμίες του EPS AKA, όπως η κατανάλωση εύρους ζώνης και γενικά τα έξοδα σηματοδότησης μεταξύ εξυπηρετητικών και οικιακών δικτύων. Ωστόσο, λίγες από αυτές έχουν αντιμετωπίσει πιθανές απειλές και επιθέσεις από το M2M σε δίκτυα κινητής τηλεφωνίας 4G.

Στο E-UTRAN NAS, οι αδυναμίες στο E-UTRAN εξακολουθούν να είναι μερικά ανοικτά ζητήματα που σχετίζονται με το σήμα ελέγχου για τις επιθέσεις υπερχείλησης των HSS / AuC. Οι πιθανοί τομείς έρευνας περιλαμβάνουν κόμβους δικτύου που βασίζονται σε λογισμικό, προκειμένου να ελαχιστοποιηθεί το φορτίο σηματοδοσίας NAS στο EPC και να παρασχεθούν χαρακτηριστικά μετριασμού για τη μόχλευση της κυκλοφορίας ελέγχου δικτύου.

Β. Μείωση επιθέσεων LTE Backhaul

Οι απειλές στο backhaul είναι κυρίως επιθέσεις που βασίζονται σε IP που στοχεύουν στοιχεία ελέγχου και διεπαφές.

Το GTP θα εξακολουθήσει να χρησιμοποιείται ως πρωτόκολλο σήραγγας σε δίκτυα κινητής τηλεφωνίας 4G, παρά την πιθανή επίθεση εναντίον του. Η λύση που βασίζεται στο σύστημα ανίχνευσης κίνησης ελέγχου δεν μπορεί να αποτρέψει και να προστατεύσει πλήρως από την παραβίαση πακέτων και την εξάντληση των πόρων, καθώς δεν είναι αποτελεσματική ενάντια σε μη φυσιολογική χρήση του μηνύματος αίτησης περιόδου σύνδεσης GTP κατά την αρχική αποστολή του MS.

Για την αντιμετώπιση απειλών που βασίζονται σε IP στα δίκτυα backhaul LTE, πολλές υπάρχουσες λύσεις περιλαμβάνουν τις πύλες ασφαλείας που χρησιμοποιούνται για το φιλτράρισμα συνδέσεων, την κρυπτογράφηση κυκλοφορίας με βάση IPsec και την αρχή έκδοσης πιστοποιητικών. Η αρχή έκδοσης πιστοποιητικών, μπορεί να αποτρέψει την μη εξουσιοδοτημένη πρόσβαση σε δεδομένα και εξαρτήματα δικτύου και να παράσχει κλειδιά για την κρυπτογράφηση της κυκλοφορίας. Πιθανή μελλοντική βελτίωση μπορεί να επιτευχθεί στο DPI.

Επιπλέον, έχουν προταθεί και άλλες λύσεις, οι οποίες συνίστανται σε αρχιτεκτονική VPN τύπου IPsec της στρώσης 3, βασισμένη σε τροποποιημένο πρωτόκολλο IKEv2 και πρωτόκολλο HIP. Αυτό επιτρέπει τη δημιουργία VPN που βασίζονται σε IPsec BEET (Bound End-to-End Tunnel) που επικαλύπτεται πάνω στο δίκτυο backhaul, προκειμένου να παράσχει προστασία από επιθέσεις spoofing, έλεγχο ταυτότητας χρήστη και εξουσιοδότηση, κρυπτογράφηση ωφέλιμου φορτίου και προστασία ιδιωτικού απορρήτου. Ιδιαίτερα ενδιαφέρον είναι να διερευνηθεί η αποτελεσματικότητα αυτής της λύσης στο πλαίσιο της υποδομής εικονικού δικτύου βασισμένο στο cloud και το Software Defined Network (SDN).

Τα botnets θεωρούνται ως μείζονες απειλές στα δίκτυα κινητής τηλεφωνίας 4G, δεδομένου ότι μπορούν να χρησιμοποιηθούν για την εκτόξευση DDoS μεγάλης κλίμακας (επιθέσεις ενίσχυσης σηματοδοσίας). Ορισμένα προτεινόμενα αντίμετρα περιλαμβάνουν τον μετριασμό της συμφόρησης με βάση το ECN. Μια τυπική απειλή που σχετίζεται με τα Botnets είναι η επίθεση σηματοδότησης κατά της διαδικασίας

διαχείρισης του κομιστή. Οι προτεινόμενες λύσεις μετριασμού είναι η αρχικοποίηση του δικτύου κατά τις διαδικασίες συνόδου ενεργοποίησης, τροποποίησης και απενεργοποίησης.

Μέσα από την ανάλυση, δείξαμε ότι το E-UTRAN είναι ευάλωτο σε επιθέσεις ψευδούς σταθμού βάσης, υποκλοπές, επιθέσεις ανακατεύθυνσης, επιθέσεις MITM και επιθέσεις DoS. Διάφορες λύσεις και αντίμετρα, που έχουν προταθεί για τον μετριασμό αυτών των ζητημάτων, περιλαμβάνουν μηχανισμούς ασφάλειας σε φυσικό επίπεδο (δημιουργία και κρυπτογράφηση κλειδιών), ισχυρό έλεγχο ταυτότητας, ενισχυμένα συστήματα κρυπτογράφησης και αρχιτεκτονική ασφαλείας. Ωστόσο, αυτές οι τρέχουσες λύσεις δεν είναι πλήρως αποδοτικές, για παράδειγμα στο σενάριο επιθέσεων κατά της διαδικασίας σελιδοποίησης (εντοπισμός χρήστη ή επίθεση εντοπισμού). Ως εκ τούτου, θα πρέπει να ενισχυθούν οι μηχανισμοί ασφαλείας προκειμένου να μετριαστεί αυτός ο τύπος επίθεσης.

Στο backhaul και το EPC, απειλές που σχετίζονται με μη εξουσιοδοτημένη πρόσβαση, DoS, υπερχείληση σηματοδοσίας, IP spoofing κ.λπ. εξακολουθούν να επηρεάζουν την ικανότητα των στοιχείων του δικτύου να εξυπηρετούν νέα κίνηση και μπορούν να οδηγήσουν σε μη διαθεσιμότητα υπηρεσιών, παρά τις υφιστάμενες προτεινόμενες λύσεις όπως η αρχιτεκτονική ασφαλείας, τα VPN, η κρυπτογράφηση, η παρακολούθηση δικτύου και κυκλοφορίας, τα IPS. Τυπικές επιθέσεις σηματοδοσίας, επιθέσεις στην σελιδοποίηση και προσάρτησης αιτήσεων στο σενάριο της υπερχείλισης του HSS δεν μπορεί να αποτραπεί και να εντοπιστεί. Καθώς αυτές οι απειλές μπορούν να έχουν μεγάλες επιπτώσεις στα MME, HSS και HLR, ο σχεδιασμός ενός νέου ολοκληρωμένου μηχανισμού στην 4G LTE για να εξασφαλίσει την αρχική αίτηση αποστολής εξακολουθεί να είναι ένα ανοιχτό ζήτημα.

Επιπλέον, στο φυσικό στρώμα του E-UTRAN, οι επιθέσεις Jamming εξακολουθούν να αποτελούν σοβαρή απειλή και χρειάζονται περισσότερη έρευνα. Οι ερευνητές πρότειναν λύσεις βασισμένες σε τεχνητή ασφάλεια θορύβου, προσεγγίσεις ασφάλειας με τη βοήθεια της ποικιλίας και δημιουργία μυστικών κλειδιών σε φυσικό επίπεδο, αλλά εξακολουθούν να βρίσκονται σε ερευνητικό επίπεδο, για να μπορέσουν να βρουν πρακτική εφαρμογή.

Τέλος, με την εξέλιξη προς τα δίκτυα LTE-A, οι επικοινωνίες M2M αναμένεται να ενσωματώνονται και να μεταφέρονται μέσω κινητών δικτύων. Οι νέες απειλές που

σχετίζονται με την ασφάλεια εφαρμογής τους και την προστασία της ιδιωτικής ζωής των χρηστών αναδεικνύονται ως μείζον πρόβλημα. Συνεπώς, η διερεύνηση του αντίκτυπου των συντονισμένων κοινών επιθέσεων που ξεκινούν από τις δυναμικά συνδεδεμένες συσκευές, αποτελεί ένα δύσκολο θέμα που πρέπει να αντιμετωπιστεί από τη μελλοντική έρευνα.

7 Προκλήσεις ασφάλειας 5G

7.1 Παραδοσιακές πρακτικές ασφάλειας

Τα συστήματα κινητής τηλεφωνίας εξελίχθηκαν μέσω της καινοτομίας ασύρματων τεχνολογιών σε 2G, 3G και στη συνέχεια 4G για να συμβαδίζουν με την ολοένα αυξανόμενη κίνηση φωνής και δεδομένων. Βελτιωμένοι μηχανισμοί ασφαλείας υπάρχουν για τη διασφάλιση των σημερινών συστημάτων κινητής επικοινωνίας. Για παράδειγμα, ο έλεγχος ταυτότητας μονής κατεύθυνσης στο 2G έχει αυξηθεί σε αμοιβαίο έλεγχο ταυτότητας στα 3G & 4G. Το μήκος του κλειδιού και οι αλγόριθμοι γίνονται όλο και πιο ισχυροί. Καθώς βελτιώνεται η διαχείριση της κινητικότητας, έχει προστεθεί στο 4G ένας διαχωρισμός κλειδιών στο εμπρόσθιο τμήμα των χειρισμών. Επίσης, εξετάζεται η αποτελεσματικότερη προστασία της ιδιωτικής ζωής.

Οι παραδοσιακές αρχιτεκτονικές ασφάλειας επικεντρώνονται στην προστασία της φωνής και των δεδομένων και έχουν όλα τα κοινά χαρακτηριστικά ασφαλείας:

• Διαχείριση ταυτότητας χρήστη βασισμένη στην (U)SIM

• Αμοιβαία επαλήθευση ταυτότητας μεταξύ δικτύων και χρηστών

• Διασφάλιση της διαδρομής μεταξύ των επικοινωνούντων μερών hop-by-hop

7.2 Προκλήσεις ασφάλειας πριν από την 5G

7.2.1 Νέα επιχειρηματικά μοντέλα

Στα παραδοσιακά δίκτυα κινητών επικοινωνιών, ο πρωταρχικός στόχος είναι να εμπλουτισθεί η ζωή των ανθρώπων μέσω της επικοινωνίας. Οι χρήστες μπορούν να επικοινωνούν με μηνύματα κειμένου, φωνητικές κλήσεις και βιντεοκλήσεις ή να πλοηγηθούν στο Διαδίκτυο ή να έχουν πρόσβαση σε υπηρεσίες εφαρμογών χρησιμοποιώντας έξυπνα τηλέφωνα. Ωστόσο, η 5G δεν περιορίζεται πλέον σε μεμονωμένους πελάτες. Δεν πρόκειται απλά για ένα ταχύτερο κινητό δίκτυο ή μια πλουσιότερη λειτουργία σε έξυπνα τηλέφωνα. Η 5G θα εξυπηρετεί επίσης ολόκληρες βιομηχανίες, από τις οποίες θα προκύψει ποικιλία νέων υπηρεσιών.

Στο πλαίσιο της κάθετης βιομηχανίας, τα αιτήματα ασφάλειας θα μπορούσαν να διαφέρουν σημαντικά μεταξύ των υπηρεσιών. Για παράδειγμα, οι κινητές συσκευές Internet of Things (IoT) απαιτούν ελαφριά ασφάλεια ενώ οι κινητές υπηρεσίες υψηλής ταχύτητας απαιτούν υψηλή ασφάλεια κινητής τηλεφωνίας. Η δικτυακή προσέγγιση ασφάλειας hop-by-hop μπορεί να μην είναι επαρκώς αποδοτική ώστε να δημιουργήσει διαφοροποιημένη ασφάλεια από άκρο σε άκρο (E2E) για διάφορες υπηρεσίες. Καθώς το IoT κερδίζει δυναμική, περισσότεροι άνθρωποι θα μπορούν να λειτουργούν εξ αποστάσεως ή να "μιλάνε" σε δικτυωμένες συσκευές, για παράδειγμα,η καθοδήγηση διαδικασιών σε ένα έξυπνο σπίτι εξ αποστάσεως. Συνεπώς, υπάρχει ανάγκη για μια πιο αυστηρή μέθοδο ελέγχου ταυτότητας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε συσκευές IoT. Για παράδειγμα, η βιομετρική ταυτοποίηση θα μπορούσε να αποτελεί μέρος της αυθεντικοποίησης σε έξυπνα σπίτια.

7.2.2 Αρχιτεκτονική δικτύου με γνώμονα τις τεχνολογίες πληροφορικής

Οι νέες τεχνολογίες πληροφορικής, όπως το virtualization και το Network Defined Network (SDN) / Virtualization Functions Network (NFV), θεωρούνται ως ένας τρόπος για να καταστούν τα δίκτυα 5G πιο έξυπνα και αποδοτικά, αλλά και λιγότερο δαπανηρά.

Ενώ οι πάροχοι βλέπουν ευχάριστα την εισαγωγή νέων τεχνολογικών δυνατοτήτων μέσω των δικτύων τους, νέες ανησυχίες όσον αφορά την ασφάλεια δημιουργούνται.

Η ασφάλεια δεν μπορεί να κατασκευαστεί για υπηρεσίες 5G εκτός αν η υποδομή δικτύου είναι ισχυρή. Στα δίκτυα παλαιού τύπου, η ασφάλεια των στοιχείων δικτύου λειτουργίας (NEs) εξαρτάται σε μεγάλο βαθμό από το πόσο καλά θα μπορούσαν να απομονωθούν οι φυσικές οντότητες μεταξύ τους. Ωστόσο, στο 5G, η απομόνωση θα λειτουργήσει διαφορετικά ως εικονικά NEs σε υποδομές που βασίζονται σε σύννεφο. Είναι λοιπόν πλέον ο χρόνος, για να ληφθεί σοβαρά υπόψη η ασφάλεια υποδομής 5G. Το SDN αποδεικνύεται ότι βοηθά στη βελτίωση της αποτελεσματικότητας μετάδοσης και του διαμοιρασμού πόρων. Από την άλλη πλευρά, είναι σημαντικό να εξεταστεί στο σχεδιασμό ασφάλειας 5G αν θα μπορούσε να διαχειριστεί από την άποψη της απομόνωσης τους κόμβους δικτύου, όπως κόμβους ελέγχου και κόμβους προώθησης και την ασφαλή και σωστή εφαρμογή του πίνακα ροής SDN.

Με βάση την τεχνολογία virtualization δικτύου, ένα δίκτυο θα μπορούσε να δημιουργήσει διαφορετικές εικονικές δικτυακές φέτες. Κάθε εικονική φέτα δικτύου θα μπορούσε να ικανοποιήσει μια συγκεκριμένη απαίτηση υπηρεσίας και συνεπώς μπορεί να απαιτεί διαφοροποιημένες δυνατότητες ασφάλειας. Στο σχέδιο ασφάλειας του 5G θα χρειαστεί να εξετασθούν θέματα σχετικά με τον τρόπο απομόνωσης, εγκατάστασης και διαχείρισης των εικονικών φετών δικτύου με ασφάλεια.

7.2.3 Ετερογενής πρόσβαση

Η ετερογένεια θα είναι ένα από τα χαρακτηριστικά της επόμενης γενιάς δικτύων. Η ετερογενής φύση προέρχεται όχι μόνο από τη χρήση διαφορετικών τεχνολογιών πρόσβασης (WiFi και LTE), αλλά και από περιβάλλον των πολλαπλών δικτύων, γεγονός που μπορεί να σημαίνει ότι η αρχιτεκτονική του δικτύου πρόσβασης από διαφορετικά δίκτυα είναι διαφορετική. Επομένως, οι σχεδιαστές ασφάλειας θα πρέπει να δημιουργήσουν αρχιτεκτονική ασφάλειας κατάλληλη για διαφορετικές τεχνολογίες πρόσβασης.

Οι συσκευές IoT έχουν πολλές επιλογές στον τρόπο πρόσβασης σε δίκτυα. Για παράδειγμα, μπορούν να συνδεθούν απευθείας σε δίκτυα ή μέσω πύλης ή με τη μέθοδο D2D ή Relay. Σε σύγκριση με το κινητό τηλέφωνο, η διαχείριση της ασφάλειας

της συσκευής IOT στο 5G μπορεί να είναι αποδοτική και ελαφριά για να δημιουργηθούν σχέσεις εμπιστοσύνης μεταξύ συσκευών και δικτύων.

7.2.4 Προστασία προσωπικών δεδομένων

Με την πρόοδο του κινητού Διαδικτύου, όλο και περισσότερες κάθετες βιομηχανίες, συμπεριλαμβανομένης της υγειονομικής περίθαλψης, της έξυπνης οικίας και των έξυπνων μεταφορών, θα καταφύγουν σε δίκτυα 5G. Ως πλατφόρμες ανοικτού δικτύου, τα δίκτυα 5G εγείρουν σοβαρές ανησυχίες για τη διαρροή της ιδιωτικής ζωής. Σε πολλές περιπτώσεις, η διαρροή απορρήτου μπορεί να προκαλέσει σοβαρές συνέπειες.

Ως κύρια μέθοδος για την πρόσβαση στο δίκτυο, τα κινητά δίκτυα μεταφέρουν δεδομένα και σηματοδότηση που περιέχουν πολλές προσωπικές πληροφορίες απορρήτου (για παράδειγμα, ταυτότητα, θέση και ιδιωτικό περιεχόμενο). Προκειμένου να προσφέρουν διαφοροποιημένη ποιότητα εξυπηρέτησης, τα δίκτυα μπορεί να χρειαστεί να αντιληφθούν τον τύπο υπηρεσίας που χρησιμοποιεί ο χρήστης. Η ανίχνευση τύπου υπηρεσίας μπορεί να αφορά την ιδιωτικότητα του χρήστη. Συνεπώς, η προστασία της ιδιωτικής ζωής στο 5G είναι πιο δύσκολο.

7.3 Στόχοι Ασφάλειας στο 5G

Καθώς πλησιάζει η εποχή του 5G, ο όγκος της κυκλοφορίας δεδομένων και η ποικιλία των υπηρεσιών θα αυξηθούν σε επίπεδα που δεν έχουν φτάσει στο παρελθόν. Η υπηρεσία IoT είναι μόνο μία από τις πολλές. Όταν μιλάμε για το 5G, δεν αναφερόμαστε απλώς σε ένα μέσο επικοινωνίας. Μπορεί να θεωρηθεί καταλύτης για την ελαχιστοποίηση των ορίων μεταξύ του ψηφιακού κόσμου και του φυσικού κόσμου. Ο σχεδιασμός ασφάλειας 5G είναι ένας πανίσχυρος σχεδιασμός που παρέχει προστασία ασφάλειας για τον κόσμο που συνδέεται με τα πάντα.

7.3.1 E2E Ασφάλεια για Κατακόρυφες Βιομηχανίες

• Διαφορετική προστασία ασφάλειας

Το σχέδιο ασφάλειας E2E εξυπηρετεί διαφορετικές κάθετες βιομηχανίες. Στην περίπτωση αυτή, ο σχεδιασμός της προστασίας της ασφάλειας πρέπει να εξετάσει τον τρόπο με τον οποίο θα εκπληρωθούν οι διάφορες απαιτήσεις ασφαλείας.

• Ευελιξία

Προκειμένου να παρέχεται καλύτερη υποστήριξη και ταχεία ανταπόκριση στην απαίτηση της κάθετης βιομηχανίας, είναι σημαντικό ότι οι δυνατότητες ασφάλειας της E2E θα μπορούσαν να ευθυγραμμιστούν γρήγορα με τις αλλαγές στις επιχειρήσεις. Σε αυτή την περίπτωση, θα απαιτηθεί ευέλικτη και υψηλής απόδοσης ανάπτυξη και προσαρμογή της ασφάλειας του E2E.

• Προστασία απορρήτου

Στο 5G θα δούμε τις υπηρεσίες της APP να αναπτύσσονται δυναμικά. Μαζί με αυτό, τα προσωπικά δεδομένα απορρήτου αυξάνονται μαζικά επίσης, συμπεριλαμβανομένων των αναγνωριστικών συσκευών, των αναγνωριστικών χρήστη και των προτιμήσεων των χρηστών. Λαμβάνοντας υπόψη ότι η προστασία της ιδιωτικής ζωής θα μπορούσε να χτιστεί από άκρη σε άκρη, χωρίς να παραμείνει κάποιο μέρος της αλυσίδας ασφάλειας ευάλωτο στη διαρροή της ιδιωτικής ζωής.

• Ασφάλεια ως υπηρεσία

Ενόψει της σύγκλισης των τεχνολογιών πληροφορικής και τηλεπικοινωνιών, η βιομηχανία τηλεπικοινωνιών επιδιώκει να ενισχύσει τη δύναμή της και να εξυπηρετήσει καλύτερα τις κάθετες βιομηχανίες. Τα συστήματα τηλεπικοινωνιών τα έχουν καταφέρει καλά στην προστασία της ιδιωτικής ζωής των χρηστών και οι χρήστες έχουν δημιουργήσει σχετικά καλό επίπεδο εμπιστοσύνης με την ασφάλεια των συστημάτων επικοινωνίας. Το 5G θα μπορούσε να συνεχίσει να επεκτείνει την εμπιστοσύνη των χρηστών ανοίγοντας τις δυνατότητες ασφάλειας ως υπηρεσία για μεμονωμένους χρήστες και κάθετες βιομηχανίες.

7.3.2 Ασφάλεια Υποδομών

• Διαφοροποιημένη προστασία επιπέδου πληροφοριακής υποδομής

Μετά την έναρξη χρήσης τεχνολογιών πληροφορικής (π.χ. NFV και SDN), υπάρχει μια τεράστια ποικιλία συστημάτων προστασίας σε επίπεδο συστήματος για την υπεράσπιση της κατανεμημένης άρνησης υπηρεσίας (DDoS) και άλλων ενεργών επιθέσεων που ενδέχεται να αυξηθούν.

• Διαχείριση ταυτότητας

Τόσο οι υποδομές λογισμικού όσο και του υλικού λειτουργούν σε περιβάλλον πολλαπλών προμηθευτών. Προκειμένου να μετριαστεί η μη εξουσιοδοτημένη πρόσβαση σε πόρους δικτύου, η αυστηρή διαχείριση ταυτότητας είναι μια πιθανή ανάγκη.

• Προστασία δεδομένων

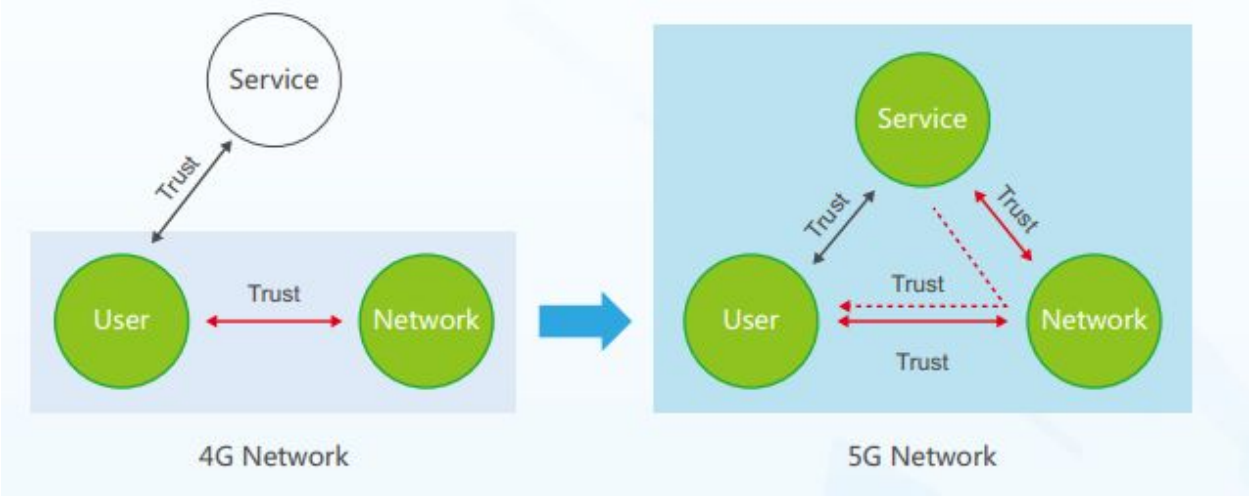
Η προστασία της ακεραιότητας και της εμπιστευτικότητας παρέχεται καθ 'όλη τη διάρκεια της διαβίβασης δεδομένων, προκειμένου να αποφευχθεί η ανάσχεση ή η αναδρομολόγηση δεδομένων σε μη εξουσιοδοτημένους προορισμούς.

7.4 Προοπτικές ασφάλειας 5G

7.4.1 Νέο μοντέλο εμπιστοσύνης και διαχείρισης ταυτότητας

Στα δίκτυα κινητής τηλεφωνίας παλαιού τύπου, τα δίκτυα τηλεπικοινωνιών είναι υπεύθυνα για τον έλεγχο της ταυτότητας του χρήστη μόνο για πρόσβαση στο δίκτυο. Δημιουργείται ένα μοντέλο εμπιστοσύνης με δύο στοιχεία, μεταξύ χρηστών και δικτύων. Ο έλεγχος ταυτότητας μεταξύ χρηστών και υπηρεσιών δεν καλύπτεται από τα δίκτυα. Ωστόσο, στα δίκτυα 5G, ένα μοντέλο εμπιστοσύνης με ένα πρόσθετο στοιχείο, τον κάθετο πάροχο υπηρεσιών, θεωρείται ως ο πιο πιθανός σχεδιασμός. Τα δίκτυα

μπορούν να συνεργάζονται με τους παρόχους υπηρεσιών για την επίτευξη ακόμη πιο ασφαλούς και αποτελεσματικότερης διαχείρισης ταυτότητας.



7.4.2 Διαχείριση υβριδικού ελέγχου ταυτότητας

Τα δίκτυα 5G είναι ανοικτές πλατφόρμες με πληθώρα υπηρεσιών. Οι έξυπνες μεταφορές, το έξυπνο δίκτυο, το βιομηχανικό διαδίκτυο είναι μερικές από αυτές. Τόσο τα δίκτυα όσο και οι πάροχοι υπηρεσιών αντιμετωπίζουν προκλήσεις για απλούστερη και λιγότερο δαπανηρή επαλήθευση της πρόσβασης και της εξυπηρέτησης. Τρία μοντέλα επαλήθευσης θα μπορούσαν να συνυπάρχουν στο 5G για να καλύψουν τις ανάγκες των διαφορετικών επιχειρήσεων.

• Έλεγχος ταυτότητας μόνο από δίκτυα

Ο έλεγχος ταυτότητας υπηρεσίας συνεπάγεται σημαντικό κόστος για τους παρόχους υπηρεσιών. Οι πάροχοι υπηρεσιών μπορούν να πληρώνουν δίκτυα για έλεγχο ταυτότητας υπηρεσιών, έτσι ώστε οι χρήστες να μπορούν να έχουν πρόσβαση σε πολλές υπηρεσίες αφού ολοκληρώσουν έναν μόνο έλεγχο ταυτότητας. Αυτό απαλλάσσει τους χρήστες από το δυσκίνητο καθήκον να αυθεντικοποιούνται επανειλημμένα για να έχουν πρόσβαση σε διάφορες υπηρεσίες.

• Έλεγχος ταυτότητας μόνο από παρόχους υπηρεσιών

Από την άλλη πλευρά, τα δίκτυα μπορούν να βασίζονται στις αποδεδειγμένες δυνατότητες επαλήθευσης ταυτότητας από κάθετες βιομηχανίες και να απαλλάσσουν συσκευές από έλεγχο ταυτότητας πρόσβασης μέσω ασύρματου δικτύου,. Γεγονός που μπορεί να βοηθήσει τα δίκτυα να μειώσουν το λειτουργικό κόστος.

• Έλεγχος ταυτότητας από δίκτυα και παρόχους υπηρεσιών

Για μερικές από τις υπηρεσίες, μπορεί να υιοθετηθεί ένα μοντέλο παλαιού τύπου. Τα δίκτυα φροντίζουν την πρόσβαση στο δίκτυο και οι πάροχοι υπηρεσιών ασχολούνται με την πρόσβαση στις υπηρεσίες.

7.4.3 Διαφοροποιημένη διαχείριση ταυτότητας

Τα κυψελοειδή δίκτυα Legacy βασίζονται σε κάρτες (U)SIM για τη διαχείριση ταυτότητας χρήστη και κλειδιών. Οι συσκευές 5G, συσκευές όπως αισθητήρες, φορητές συσκευές και έξυπνες οικιακές συσκευές είναι πολύ μικρές και φτηνές για να φιλοξενήσουν (U) SIM. Τώρα έχει έρθει ο καιρός να βρούμε έναν νέο τρόπο διαχείρισης των ταυτοτήτων των συσκευών, για παράδειγμα, να παράγουμε, να αναθέσουμε και να εφαρμόσουμε τη διαχείριση του κύκλου ζωής σε ταυτότητες συσκευών.

• Συνδυασμός ταυτότητας συσκευής και ταυτότητας υπηρεσίας

Στο νέο πλαίσιο διαχείρισης ταυτότητας, η ταυτότητα αποτελείται από ταυτότητα συσκευής και ταυτότητα υπηρεσίας. Κάθε ταυτότητα συσκευής (αποκαλούμενη επίσης φυσική ταυτότητα) είναι παγκοσμίως μοναδική και μπορεί να αποδοθεί σε μια συσκευή κατά τη φάση της κατασκευής. Οι ταυτότητες υπηρεσιών ανατίθενται από παρόχους υπηρεσιών ή δίκτυα. Η φυσική ταυτότητα μπορεί να αντιστοιχεί σε μία ή περισσότερες ταυτότητες υπηρεσιών.

• Από διαχείριση βάσει συσκευών έως διαχείριση βάσει χρηστών

Αφήνει στους χρήστες να αποφασίσουν ποια από τις συσκευές τους επιτρέπεται να έχουν πρόσβαση στο δίκτυο και ποια υπηρεσία επιτρέπεται να χρησιμοποιούν. Για παράδειγμα, οι συσκευές ενός ίδιου χρήστη μπορούν είτε να είναι σε σύνδεση με το δίκτυο είτε εκτός σύνδεσης.

7.5 Ασφάλεια προσανατολισμένη στις υπηρεσίες

- **Δημιουργία ασφάλειας E2E**

7.5.1 Διαφοροποιημένη ασφάλεια για διάφορες υπηρεσίες

Τα συστήματα 5G πρόκειται να προσανατολιστούν στην υπηρεσία. Αυτό σημαίνει ότι θα δοθεί ιδιαίτερη έμφαση στις απαιτήσεις ασφαλείας που απορρέουν από τη γωνία των υπηρεσιών. Για παράδειγμα, η απομακρυσμένη υγειονομική περίθαλψη απαιτεί ανθεκτική ασφάλεια ενώ το IoT απαιτεί ελαφριά ασφάλεια. Είναι λογικό να προσφέρουμε διαφοροποιημένη ασφάλεια σε διαφορετικές υπηρεσίες.

7.5.2 Ευέλικτη αρχιτεκτονική ασφαλείας για την υποστήριξη χαρακτηριστικών ασφαλείας για διαφορετικές φέτες δικτύου

Εάν προσφέρεται διαφοροποιημένη ασφάλεια, τότε απαιτείται ευέλικτη αρχιτεκτονική ασφαλείας για την υποστήριξη της προστασίας E2E για διαφορετικές υπηρεσίες, βασισμένες στην αρχιτεκτονική του δικτύου. Το δίκτυο διαχειρίζεται διάφορες δυνατότητες ασφάλειας E2E, συμπεριλαμβανομένης της αντοχής των αλγορίθμων ασφαλείας, τρόπους εξαγωγής και διαπραγμάτευσης μυστικών κλειδιών και μηχανισμούς προστασίας της εμπιστευτικότητας και της ακεραιότητας. Μέσα σε μια εικονική φέτα του δικτύου, οι δυνατότητες ασφάλειας θα μπορούσαν να διανεμηθούν περαιτέρω.

7.5.3 Ένα ενιαίο πλαίσιο διαχείρισης ασφάλειας για περιβάλλον πολλαπλών προμηθευτών

Στο περιβάλλον του cloud, το λογισμικό και ο εξοπλισμός της υποδομής δικτύου προέρχονται από περισσότερους προμηθευτές εξοπλισμού, οι οποίοι περιπλέκουν

σχετικά τα ζητήματα ασφάλειας. Για τις υπηρεσίες και τους χρήστες, η οικοδόμηση μιας αλυσίδας ασφάλειας δεδομένων E2E θα μπορούσε να είναι ένας τρόπος για να μειωθεί η εξάρτηση από την ατομική ασφάλεια σύνδεσης και να απλοποιηθεί η διαχείριση της ασφάλειας.

ΜΕΡΟΣ Β΄

8 OPENBTS-USRP

Το OpenBTS (Open Base Transceiver Station) είναι ένα access point που βασίζεται στο λογισμικό GSM, επιτρέποντας στα κινητά τηλέφωνα συμβατά με το GSM να χρησιμοποιούνται ως τελικά σημεία SIP σε δίκτυα Voice over IP (VoIP). Το OpenBTS είναι ένα λογισμικό ανοιχτού κώδικα που αναπτύχθηκε και διατηρείται από τα δίκτυα Range. Η δημόσια κυκλοφορία του OpenBTS είναι αξιοσημείωτη για το γεγονός ότι είναι η πρώτη εφαρμογή ελεύθερου λογισμικού των κατώτερων τριών επιπέδων της στοίβας πρωτόκολλο GSM. Είναι γραμμένο σε C ++ και κυκλοφορεί ως ελεύθερο λογισμικό υπό τους όρους της έκδοσης 3 της Γενικής Δημόσιας Άδειας GNU Affero.

8.1 Η Υποδομή του OpenBTS

Το OpenBTS αντικαθιστά την συμβατική υποδομή δικτύου πυρήνα του φορέα εκμετάλλευσης GSM από το επίπεδο 3 προς τα πάνω. Αντί να βασίζονται σε εξωτερικούς ελεγκτές σταθμών βάσης για διαχείριση ραδιοφωνικών πόρων, οι μονάδες OpenBTS εκτελούν αυτή τη λειτουργία εσωτερικά. Αντί της προώθησης της κίνησης κλήσεων προς το κέντρο μεταγωγής κινητού τηλεφώνου, το OpenBTS παρέχει κλήσεις μέσω SIP σε ένα soft-switch VOIP (όπως FreeSWITCH ή yate) ή PBX (όπως το Asterisk). Αυτός ο διακόπτης VOIP ή λογισμικό PBX μπορεί να εγκατασταθεί στον ίδιο υπολογιστή που χρησιμοποιείται για την εκτέλεση του ίδιου του OpenBTS, σχηματίζοντας ένα αυτόνομο κυψελοειδές δίκτυο σε ένα μόνο σύστημα υπολογιστή. Πολλές μονάδες OpenBTS μπορούν επίσης να μοιράζονται έναν κοινό διακόπτη VOIP ή ένα PBX για να σχηματίσουν μεγαλύτερα δίκτυα

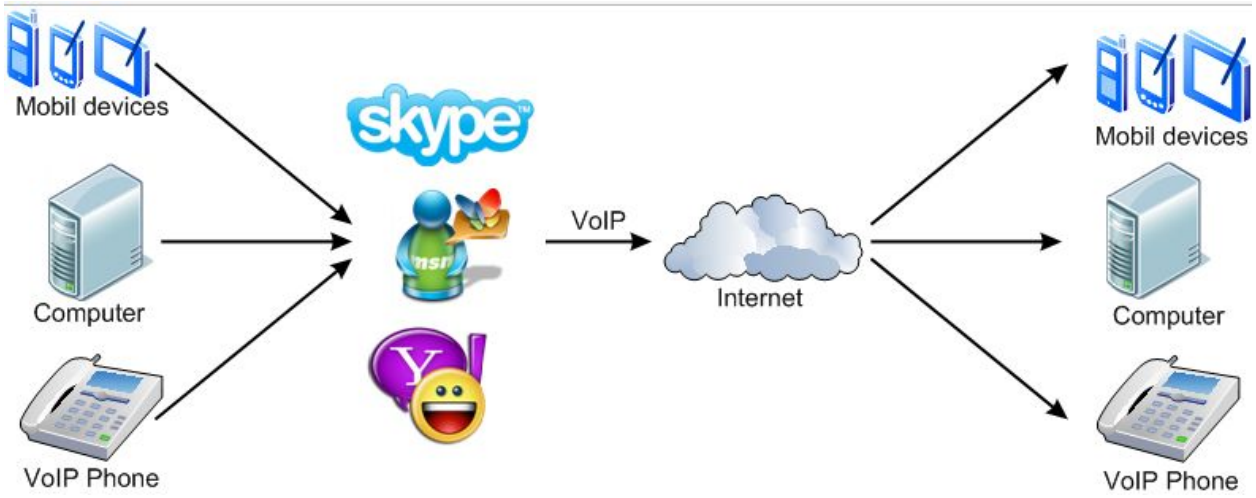
Η εξωτερική διεπαφή του OpenBTS Um χρησιμοποιεί έναν πομποδέκτη καθορισμένο από λογισμικό χωρίς εξειδικευμένο υλικό GSM. Η αρχική εφαρμογή χρησιμοποίησε ένα USRP από την Ettus Research, αλλά έκτοτε επεκτάθηκε για να υποστηρίξει αρκετές ψηφιακές ραδιοσυσκευές σε υλοποιήσεις που κυμαίνονται από σταθμούς βάσης πλήρους κλίμακας έως ενσωματωμένα φεμτοκύτταρα.

8.2 Voice over IP, VoIP

Η φωνή μέσω Internet πρωτοκόλλου (Voice over IP, VoIP) είναι μια μεθοδολογία και ανήκει στην ομάδα των τεχνολογιών μετάδοσης φωνής και πολυμέσων μέσω IP δικτύων, όπως το Internet. Άλλοι όροι που συνδέονται συνήθως με το VoIP είναι η IP τηλεφωνία, Internet τηλεφωνία, ευρυζωνική τηλεφωνία και ευρυζωνική τηλεφωνική υπηρεσία.

Ο όρος τηλεφωνία μέσω του Διαδικτύου αναφέρεται στην παροχή των υπηρεσιών επικοινωνίας (φωνή, φαξ, SMS, μηνυμάτων φωνής) μέσω του Διαδικτύου, αντί μέσω του δημόσιου τηλεφωνικού δικτύου μεταγωγής (PSTN). Τα βήματα και οι αρχές που εμπλέκονται στην πραγματοποίηση των VoIP τηλεφωνικών κλήσεων είναι παρόμοια της παραδοσιακής ψηφιακής τηλεφωνίας και περιλαμβάνουν σηματοδότηση, ρύθμιση του καναλιού, ψηφιοποίηση των αναλογικών σημάτων φωνής, και κωδικοποίηση. Ωστόσο αντί να μεταδίδονται μέσω ενός δικτύου κυκλωματομεταγωγής, η ψηφιακή πληροφορία πακετάρεται, και μεταδίδεται ως IP πακέτα μέσω δικτύου πακετομεταγωγής. Η διαβίβαση αυτή απαιτεί προσεκτική εκτίμηση σχετικά με τη διαχείριση των πόρων. Διαφορετική από αυτή των δικτύων πολυπλεξίας διαίρεσης χρόνου (TDM).

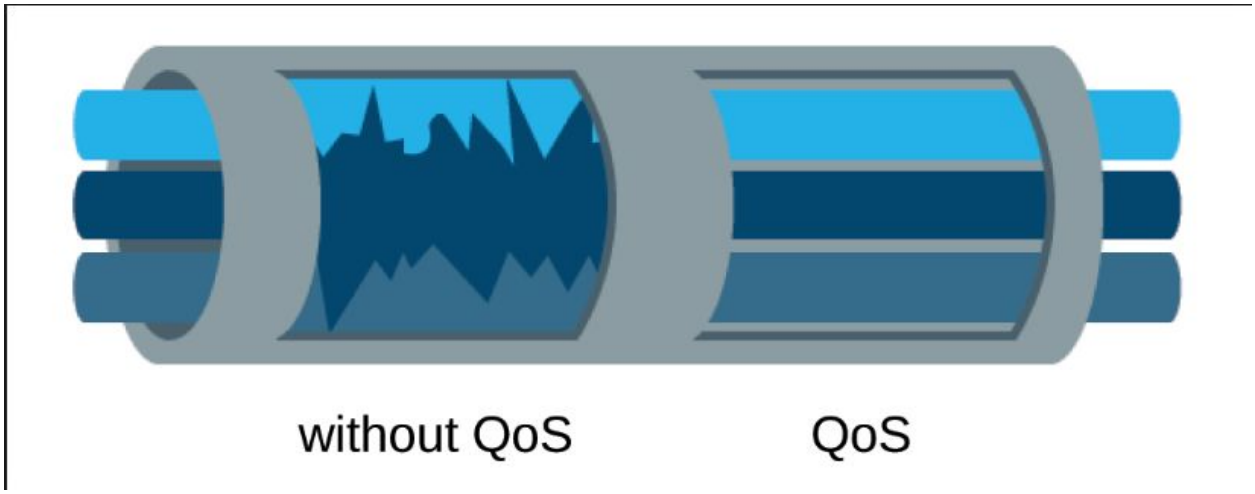
Οι αρχικοί πάροχοι υπηρεσιών voice-over-IP προσέφεραν επιχειρηματικά μοντέλα και τεχνικές λύσεις που αντικατοπτρίζονταν στην αρχιτεκτονική του νόμιμου τηλεφωνικού δικτύου. Οι παρόχοι δεύτερης γενιάς, όπως το Skype, έχουν κατασκευαστεί ως κλειστά δίκτυα για τις ιδιωτικές βάσεις χρηστών, προσφέροντας το πλεονέκτημα των δωρεάν κλήσεων και άλλες ευκολίες, ενώ δυνητικά γίνεται χρέωση για την πρόσβαση σε άλλα δίκτυα επικοινωνιών, όπως το PSTN. Αυτό έχει περιορίσει την ελευθερία των χρηστών στην ανάμιξη και το ταίριασμα υλικού και λογισμικού τρίτων οντοτήτων. Οι πάροχοι τρίτης γενιάς, όπως το Google Talk, έχουν υιοθετήσει την έννοια της σύμπραξης ομόσπονδων VoIP - η οποία είναι μια απόκλιση από την αρχιτεκτονική των νομικά κατοχυρωμένων δικτύων. Οι λύσεις αυτές επιτρέπουν συνήθως τη δυναμική διασύνδεση μεταξύ των χρηστών σε ένα από τα δύο domains στο Διαδίκτυο, όταν ένας χρήστης επιθυμεί να πραγματοποιήσει μια κλήση.



Τα VoIP συστήματα χρησιμοποιούν έλεγχο συνόδου και πρωτόκολλα σηματοδοσίας για τον έλεγχο της σηματοδότησης, την εγκατάσταση, και την πραγματοποίηση των κλήσεων. Μεταφέρουν ροές ήχου μέσω δικτύων IP, χρησιμοποιώντας ειδικά πρωτόκολλα παράδοσης μέσων που κωδικοποιούν φωνή, ήχο, βίντεο με κωδικοποιητές ήχου και κωδικοποιητές βίντεο. Διάφορα codecs υπάρχουν που βελτιστοποιούν τη ροή πολυμέσων με βάση τις απαιτήσεις της εφαρμογής και το εύρος ζώνης του δικτύου. Μερικές υλοποιήσεις βασίζονται σε “στενής” ζώνης και συμπιεσμένης ομιλίας, ενώ άλλες υποστηρίζουν στερεοφωνικούς κωδικοποιητές υψηλής πιστότητας. Μερικά δημοφιλή codecs περιλαμβάνουν μ-law και a-law εκδόσεις των G.711, G.722, ένα δημοφιλές open source codec φωνής γνωστό ως iLBC, ενός κωδικοποιητή που χρησιμοποιεί μόνο 8 kbit / s προς κάθε μέρος, που ονομάζεται G.729, και πολλά άλλα .

8.3 Quality of services

Η επικοινωνία στο δίκτυο IP χαρακτηρίζεται ως λιγότερο αξιόπιστη σε αντίθεση με το κύκλωμα μεταγωγής του δημόσιου τηλεφωνικού δικτύου, διότι δεν παρέχει μηχανισμούς που να βασίζονται σε δίκτυο για να εξασφαλιστεί ότι τα πακέτα δεδομένων δεν χάνονται, και παραδίδονται σε διαδοχική σειρά. Πρόκειται για ένα δίκτυο βέλτιστης προσπάθειας χωρίς θεμελιώδεις Quality of Service (QoS) εγγυήσεις. Ως εκ τούτου, οι εφαρμογές VoIP μπορεί να αντιμετωπίσουν προβλήματα καθυστέρησης, απώλεια πακέτων και jitter.



Από προεπιλογή, οι δρομολογητές του δικτύου χειρίζονται την κυκλοφορία σε μια first-come, first-served βάση. Οι δρομολογητές του δικτύου για τις συνδέσεις κυκλοφορίας υψηλής έντασης μπορούν να εισάγουν καθυστέρηση που υπερβαίνει τα επιτρεπόμενα όρια για VoIP. Οι σταθερές καθυστερήσεις δεν μπορούν να ελεγχθούν, όπως αυτές που προκαλούνται από τη φυσική απόσταση κατά την μετάδοση των πακέτων. Ωστόσο, ο λανθάνων χρόνος μπορεί να ελαχιστοποιηθεί με τη σήμανση “πακέτα φωνής” στα ευαίσθητα προς την καθυστέρηση πακέτα με μεθόδους όπως DiffServ.

Τα τελικά σημεία του VoIP συνήθως πρέπει να περιμένουν την ολοκλήρωση της μετάδοσης των προηγούμενων πακέτων για την αποστολή των νέων δεδομένων. Αν και είναι δυνατόν να γίνει ακύρωση λιγότερο σημαντικών πακέτων στα μέσα μεταφοράς, αυτό δεν γίνεται συνήθως, ειδικά στις συνδέσεις υψηλής ταχύτητας όπου οι χρόνοι μετάδοσης είναι μικροί, ακόμα και για πακέτα που είναι στο μέγιστο επιτρεπόμενο μέγεθος. Μια εναλλακτική λύση στην ακύρωση πακέτων για πιο αργές συνδέσεις, όπως dialup και ψηφιακή συνδρομητική γραμμή (DSL), είναι η μείωση του μέγιστου χρόνου μετάδοσης, μειώνοντας τη μέγιστη μονάδα μετάδοσης. Αλλά κάθε πακέτο πρέπει να περιέχει κεφαλίδες πρωτοκόλλου για να εξασφαλισθεί το QoS. Ο τρόπος όμως, αυτός αυξάνει το μέγεθος της επικεφαλίδας σε κάθε πακέτο που πρέπει να μεταδοθεί και αυτό μπορεί να προκαλέσει bottleneck στη σύνδεση.

Τα DSL μόντεμ παρέχουν Ethernet (ή Ethernet μέσω USB) σύνδεση με τοπικό εξοπλισμό, αλλά στο εσωτερικό τους είναι στην πραγματικότητα σε λειτουργία ασύγχρονης μεταφοράς (ATM). Χρησιμοποιούν ATM Προσαρμογή Layer 5 (AAL5) για να κατακερματίσουν το κάθε πακέτο Ethernet σε μια σειρά τμημάτων ATM, 53-byte για

τη μετάδοση, τα οποία θα επανασυνδεθούν πίσω σε πλαίσια στο τελικό άκρο λήψης. Ένα αναγνωριστικό εικονικού κυκλώματος (VCI) αποτελεί μέρος του header των 5-byte σε κάθε κελί ATM, έτσι ώστε ο πομπός να μπορεί να πολυπλέξει τα ενεργά εικονικά κυκλώματα (VCs) σε οποιαδήποτε αυθαίρετη σειρά. Κυψέλες από την ίδια VC αποστέλλονται πάντα διαδοχικά.

Ωστόσο, η πλειοψηφία των παρόχων DSL παρέχουν μόνο ένα VC για κάθε πελάτη, ακόμη και σε εκείνους με συνδυασμένη VoIP υπηρεσία. Κάθε πλαίσιο Ethernet πρέπει να διαβιβάζεται πλήρως πριν ένα άλλο να μπορεί να αρχίσει. Αν δημιουργηθεί ένα δεύτερο VC, με υψηλή προτεραιότητα και προορίζεται για αποστολή μέσω VoIP, τότε το πακέτο χαμηλής προτεραιότητας θα ανασταλεί ως προς τη μεταφορά του και το πακέτο VoIP με την υψηλή προτεραιότητα VC θα προηγηθεί. Επειδή οι ATM συνδέσεις πολυπλέκονται σε μια βάση “κυψέλη-προς-κυψέλη”, ένα πακέτο υψηλής προτεραιότητας θα πρέπει να περιμένει το πολύ 53 byte για να ξεκινήσει τη μετάδοση. Δεν υπάρχει ανάγκη της μείωσης της διέπαφης του MTU και αποδοχής της προκύπτουσας αύξησης της προτεραιότητας, ενώ δεν χρειάζεται να εγκαταλειφθεί ένα πακέτο χαμηλής προτεραιότητας και να ξανασταλεί αργότερα.

Η δυναμική αυτή των ATM για την μείωση των καθυστερήσεων προσφέρει περισσότερα πλεονεκτήματα στις αργές συνδέσεις, γιατί στη χειρότερη περίπτωση οι καθυστερήσεις μπορούν να μειωθούν με την αύξηση της ταχύτητας σύνδεσης. Ένα πλαίσιο πλήρους μεγέθους Ethernet (1500 byte) διαρκεί 94 ms για τη μετάδοση στα 128 kbit / s, αλλά μόνο 8 ms στα 1,5 Mbit / s. Αν έχουμε μία σύνδεση με bottleneck, αυτή η καθυστέρηση είναι μάλλον αρκετά μικρή για να εξασφαλιστεί η καλή απόδοση VoIP χωρίς μειώσεις MTU ή πολλαπλά ATM VCs. Οι τελευταίες γενιές των DSL, VDSL και VDSL2, φέρουν Ethernet χωρίς ενδιάμεσα στρώματα / AAL5 ATM, και γενικά υποστηρίζουν IEEE 802.1p tags προτεραιότητας ώστε το VoIP να μπορεί να βρίσκεται μπροστά στην ουρά σε σχέση με τις λιγότερο χρόνο-κρίσιμες ροές.

Η φωνή, και όλα τα άλλα δεδομένα, ταξιδεύουν σε πακέτα πάνω από IP δίκτυα με σταθερή μέγιστη χωρητικότητα. Αυτό το σύστημα μπορεί να είναι πιο επιρρεπές σε συμφόρηση και επιθέσεις DoS σε σχέση με τα παραδοσιακά συστήματα μεταγωγής κυκλώματος. Ένα κύκλωμα μεταγωγής κυκλώματος με ανεπαρκή διαθέσιμο χώρο θα αρνηθεί νέες συνδέσεις, και θα μεταφέρει τα υπόλοιπα χωρίς βλάβες, ενώ η ποιότητα των δεδομένων σε πραγματικό χρόνο, όπως τηλεφωνικές συνδιαλέξεις σε δίκτυα μεταγωγής πακέτων υποβαθμίζεται δραματικά.

Σταθερές καθυστερήσεις, όπως αυτές που προκαλούνται από τη φυσική απόσταση των πακέτων που ταξιδεύουν, δεν μπορούν να ελεγχθούν. Η μεταφορά είναι ιδιαίτερα

προβληματική όταν εμπλέκονται δορυφορικά κυκλώματα, λόγω της μεγάλης απόστασης προς τον δορυφόρο και πίσω. Καθυστερήσεις των 400-600 ms είναι συνηθισμένες.

Όταν ο φόρτος σε ένα σύνδεσμο μεγαλώνει τόσο γρήγορα, που οι διακόπτες ελέγχου ουράς του υπερχειλίζουν, τα αποτελέσματα της κυκλοφοριακής συμφόρησης αυξάνονται και πακέτα δεδομένων χάνονται. Αυτό απαιτεί την χρήση ενός πρωτοκόλλου μεταφοράς όπως το TCP για την μείωση του ρυθμού μετάδοσης και έλεγχο της συμφόρησης. Αλλά το VoIP χρησιμοποιεί συνήθως UDP και όχι TCP επειδή η επιδιόρθωση από τη συμφόρηση μέσω αναμετάδοσης συνεπάγεται συνήθως πάρα πολύ μεγάλη καθυστέρηση. Έτσι, με τους μηχανισμούς QoS που εφαρμόζονται στον σύνδεσμο, μπορούμε να αποφύγουμε την ανεπιθύμητη απώλεια των VoIP πακέτων με την άμεση μεταβίβασή τους μπροστά από κάθε σειρά αναμονής κυκλοφορίας, ακόμα και όταν ότι η ουρά κίνησης έχει υπερχειλίσει.

Ο δέκτης πρέπει να επανασυντάξει IP πακέτα που φθάνουν εκτός της σωστής διάταξης και να τα ανακτήσει όταν φτάνουν πολύ αργά ή και καθόλου. “Jitter” συμβαίνει από τις ταχείες και τυχαίες (δηλαδή απρόβλεπτες) μεταβολές στα μήκη ουράς κατά μήκος μιας συγκεκριμένης διαδρομής του Διαδικτύου, λόγω του “ανταγωνισμού” με άλλους χρήστες για τις ίδιες συνδέσεις μετάδοσης. Δέκτες VoIP αντιμετωπίζουν τα jitter με την αποθήκευση των εισερχόμενων πακέτων για μικρό χρονικό διάστημα σε ένα "de-jitter" ή "playout” buffer. Έτσι, αυξάνεται σκόπιμα η καθυστέρηση για να βελτιωθεί η πιθανότητα ότι κάθε πακέτο θα είναι σε ετοιμότητα, για την στιγμή που θα έρθει η ώρα της μηχανής να το μεταδώσει. Η προστιθέμενη καθυστέρηση είναι επομένως ένας συμβιβασμός μεταξύ της υπερβολικής καθυστέρησης και των υπερβολικά πολλών χαμένων πακέτων, δηλαδή στιγμιαίων διακοπών ήχου.

Αν και το jitter θεωρείται μια τυχαία μεταβλητή, είναι το άθροισμα αρκετών άλλων τυχαίων μεταβλητών που είναι, κατά κάποιο τρόπο, ανεξάρτητες - μεμονωμένες καθυστερήσεις αναμονής των δρομολογητών, κατά μήκος της διαδρομής του Διαδικτύου. Έτσι, σύμφωνα με το κεντρικό οριακό θεώρημα, μπορούμε να μοντελοποιήσουμε το jitter ως Gaussian τυχαία μεταβλητή. Αυτό δείχνει συνεχώς την εκτίμηση της μέσης καθυστέρησης, την τυπική απόκλιση και τον καθορισμό της καθυστέρησης playout, έτσι ώστε μόνο τα πακέτα που είναι χρήσιμα να επιτρέπεται να καθυστερούν περισσότερο σε σχέση με την τυπική απόκλιση και πάνω από τη μέση τιμή. Στην πράξη, ωστόσο, η διακύμανση στην καθυστέρηση σε πολλά μονοπάτια στο Διαδίκτυο οφείλεται σε ένα μικρό αριθμό (συχνά ένα) σχετικά αργών και συμφορημένων συνδέσεων. Οι περισσότερες συνδέσεις κορμού του Διαδικτύου είναι πλέον τόσο γρήγορες (π.χ. 10 Gbit / s) που το μέσο μετάδοσης (π.χ. οπτικές ίνες) ξεπερνά τις

καθυστερήσεις και οι δρομολογητές τους δεν έχουν αρκετό buffering που να μπορεί να προκαλέσει καθυστερήσεις.

Έχει προταθεί η “πακετοποιημένη” φύση των μέσων επικοινωνιών του VoIP και μετάδοση των ροών των πακέτων από το τηλέφωνο της πηγής στο τηλέφωνο του προορισμού ταυτόχρονα σε διαφορετικές διαδρομές (multi-path routing). Με τον τρόπο αυτό, οι προσωρινές αποτυχίες έχουν μικρότερη επίπτωση στην ποιότητα της επικοινωνίας. Η τριχοειδής δρομολόγηση έχει προταθεί για χρήση σε επίπεδο πακέτου με Fountain κωδικούς ή συγκεκριμένους κώδικες Raptor για τη μετάδοση επιπλέον πρόσθετων πακέτων που μπορούν να κάνουν την επικοινωνία πιο αξιόπιστη.

Μια σειρά από πρωτόκολλα έχουν οριστεί για την υποστήριξη της υποβολής της ποιότητας των υπηρεσιών (QoS) και την ποιότητα της εμπειρίας (QoE) για κλήσεις VoIP. Αυτά περιλαμβάνουν RTCP Extended Report (RFC 3611), συνοπτικές εκθέσεις SIP RTCP, H.460.9 παράρτημα B (για H.323), H.248.30 και MGCP επεκτάσεις. Το RFC 3611 VoIP Metrics block παράγεται από ένα τηλέφωνο IP ή μια πύλη κατά τη διάρκεια μιας ζωντανής κλήσης και περιέχει πληροφορίες σχετικά με τον ρυθμό απώλειας πακέτων, το ποσοστό απόρριψης πακέτων (λόγω του jitter), το πηλίκο απώλειας πακέτων / απορριπτέων, μετρήσεων που έχουν σκάσει (μήκος ριπής / πυκνότητα, μήκος χάσματος / πυκνότητας), καθυστέρηση του δικτύου, τέλος καθυστέρησης του συστήματος, σήμα / θόρυβος / επίπεδο ηχούς, μέσης βαθμολογίας γνώμεων (MOS), τους συντελεστές R και τη διαμόρφωση των πληροφοριών που σχετίζονται με το jitter buffer.

Οι RFC 3611 VoIP μετρικές αναφορές που ανταλλάσσονται μεταξύ των τελικών σημείων IP σε περιστασιακή βάση κατά τη διάρκεια μιας κλήσης, και ενός ηχητικού μηνύματος ολοκλήρωσης κλήσης αποστέλλεται μέσω SIP RTCP Summary Report ή μέσω κάποιας από τις άλλες επεκτάσεις πρωτοκόλλων σηματοδοσίας. Οι RFC 3611 VoIP μετρικές αναφορές προορίζονται να στηρίξουν σε πραγματικό χρόνο την ανατροφοδότηση που σχετίζεται με προβλήματα QoS, την ανταλλαγή πληροφοριών μεταξύ των τελικών σημείων για τη βελτίωση του υπολογισμού ποιότητας της κλήσης και μια ποικιλία άλλων εφαρμογών.

Στις επαρχιακές, ιδίως, περιοχές παρεμποδίζεται σε μεγάλο βαθμό η δυνατότητα των χρηστών, να επιλέξουν ένα σύστημα VoIP μέσω PBX. Αυτό είναι σύνηθες, στις φτωχές σε πρόσβαση Superfast ευρυζωνικών δικτύων, περιοχές της υπαίθρου χώρας. Με την κυκλοφορία των δεδομένων 4G, υπάρχει η δυνατότητα για εταιρικούς χρήστες, που κατοικούν έξω από κατοικημένες περιοχές να αλλάξουν τη σύνδεσή τους στο διαδίκτυο σε δίκτυο 4G, το οποίο είναι συγκριτικά τόσο γρήγορα όσο μια κανονική υπερταχεία ευρυζωνική σύνδεση. Αυτό βελτιώνει σημαντικά τη συνολική ποιότητα και την εμπειρία

χρήστη ενός συστήματος VoIP σε αυτές τις περιοχές. Αυτή η μέθοδος έχει ήδη δοκιμαστεί στην επαρχιακή Γερμανία, ξεπερνώντας κάθε προσδοκία.

8.4 Layer 2

Μια σειρά πρωτοκόλλων που ασχολούνται με το στρώμα ζεύξης δεδομένων και το φυσικό στρώμα, περιλαμβάνουν QoS μηχανισμούς που μπορούν να χρησιμοποιηθούν ώστε να εξασφαλιστεί η καλή λειτουργία των εφαρμογών ακόμα και σε σενάρια συμφόρησης όπως το VoIP.

Μερικά παραδείγματα περιλαμβάνουν:

- IEEE 802.11e είναι μια εγκεκριμένη τροποποίηση του 802.11 πρότυπου IEEE που ορίζει ένα σύνολο QoS βελτιώσεων για ασύρματες LAN εφαρμογές μέσω τροποποιήσεων στο στρώμα ελέγχου πρόσβασης μέσου (MAC). Το πρότυπο θεωρείται κρίσιμης σημασίας για εφαρμογές ευαίσθητες σε καθυστέρηση, όπως η φωνή μέσω IP ασύρματα.

- IEEE 802.1p καθορίζει 8 διαφορετικές κατηγορίες των υπηρεσιών (συμπεριλαμβανομένης και της φωνής) για την κυκλοφορία στο στρώμα-2 ενσύρματου Ethernet.

- Το πρότυπο ITU-T G.hn, το οποίο παρέχει έναν τρόπο δημιουργίας μιας υψηλής ταχύτητας (έως 1 gigabit ανά δευτερόλεπτο) σύνδεσης τοπικού δικτύου (LAN) με χρήση των υφιστάμενων καλωδιώσεων του σπιτιού (γραμμές ηλεκτρικού ρεύματος, τηλεφωνικές γραμμές και ομοαξονικά καλώδια). Το G.hn παρέχει QoS μέσω της "Ελεύθερης από “Διαμάχες” Ευκαιρίες μετάδοσης" (CFTXOPs), οι οποίες κατανέμονται σε ροές (όπως μια κλήση VoIP) που απαιτούν QoS και τα οποία έχουν διαπραγματευθεί ένα «συμβόλαιο» με τους ελεγκτές του δικτύου.

8.5 Ασφάλεια

Οι ανησυχίες για την ασφάλεια των τηλεφωνικών συστημάτων VoIP είναι παρόμοιες με εκείνες της οποιαδήποτε συσκευής με σύνδεση στο Internet. Αυτό σημαίνει ότι οι hackers που γνωρίζουν τις αδυναμίες αυτές μπορούν να προκαλέσουν denial-of-service επιθέσεις, να συλλέξουν δεδομένα των πελατών,να καταγράψουν συνομιλίες και μηνύματα του χρήστη. Η ποιότητα της σύνδεσης στο internet καθορίζει την ποιότητα των κλήσεων. Οι VoIP τηλεφωνικές υπηρεσίες επίσης, δεν θα λειτουργήσουν εάν υπάρχει διακοπή ρεύματος και όταν η σύνδεση στο internet είναι πεσμένη. Οι έκτακτες τηλεφωνικές υπηρεσίες επίσης που παρέχονται από VoIP τηλεφωνική υπηρεσία είναι διαφορετική από το αναλογικό τηλέφωνο που συνδέεται με μια σταθερή διεύθυνση. Το κέντρο έκτακτης ανάγκης ενδέχεται να μην είναι σε θέση να προσδιορίσει τη θέση σας με βάση τον εικονικό αριθμό τηλεφώνου σας. Εκτεθειμένα στο VoIP στοιχεία χρηστών, ή διαπιστευτήρια συνόδου μπορεί να επιτρέψουν σε έναν εισβολέα να επιφέρει σημαντικές χρεώσεις από υπηρεσίες τρίτων, όπως υπεραστικές ή διεθνείς τηλεφωνικές κλήσεις.

Οι τεχνικές λεπτομέρειες των πολλών πρωτοκόλλων VoIP δημιουργούν προκλήσεις στη δρομολόγηση της κυκλοφορίας VoIP μέσω firewalls, που χρησιμοποιούνται για τη διασύνδεση με τα δίκτυα διαμετακόμισης ή στο Διαδίκτυο. Ιδιωτικοί ελεγκτές ελέγχου συνόδου χρησιμοποιούνται συχνά για να πραγματοποιούνται οι VoIP κλήσεις προς και από προστατευόμενα δίκτυα. Άλλες μέθοδοι για να διασχίσθουν οι NAT συσκευές, περιλαμβάνουν βοηθητικά πρωτόκολλα όπως το STUN και το Interactive Connectivity Establishment (ICE).

Πολλές εμπορικές λύσεις VoIP δεν υποστηρίζουν την κρυπτογράφηση της διαδρομής σηματοδοσίας ή των μέσων μετάδοσης, ωστόσο, το να ασφαλίσεις ένα τηλέφωνο VoIP είναι θεωρητικά ευκολότερο από ό,τι ένα παραδοσιακό τηλεφωνικό κυκλώμα. Ένα αποτέλεσμα της έλλειψης κρυπτογράφησης είναι η σχετική ευκολία με την οποία μπορούμε να αφουγκραστούμε κλήσεις VoIP, όταν είναι δυνατή η πρόσβαση στο δίκτυο δεδομένων. Δωρεάν λύσεις ανοιχτού κώδικα, όπως το Wireshark, διευκολύνουν την καταγραφή συνομιλιών VoIP.

Πρότυπα για την θωράκιση του VoIP είναι διαθέσιμα στο Secure Real-time Transport Protocol (SRTP) και το πρωτόκολλο ZRTP για προσαρμογείς αναλογικής τηλεφωνίας, καθώς και για ορισμένα softphones. Το IPsec είναι διαθέσιμο για να εξασφαλίσει

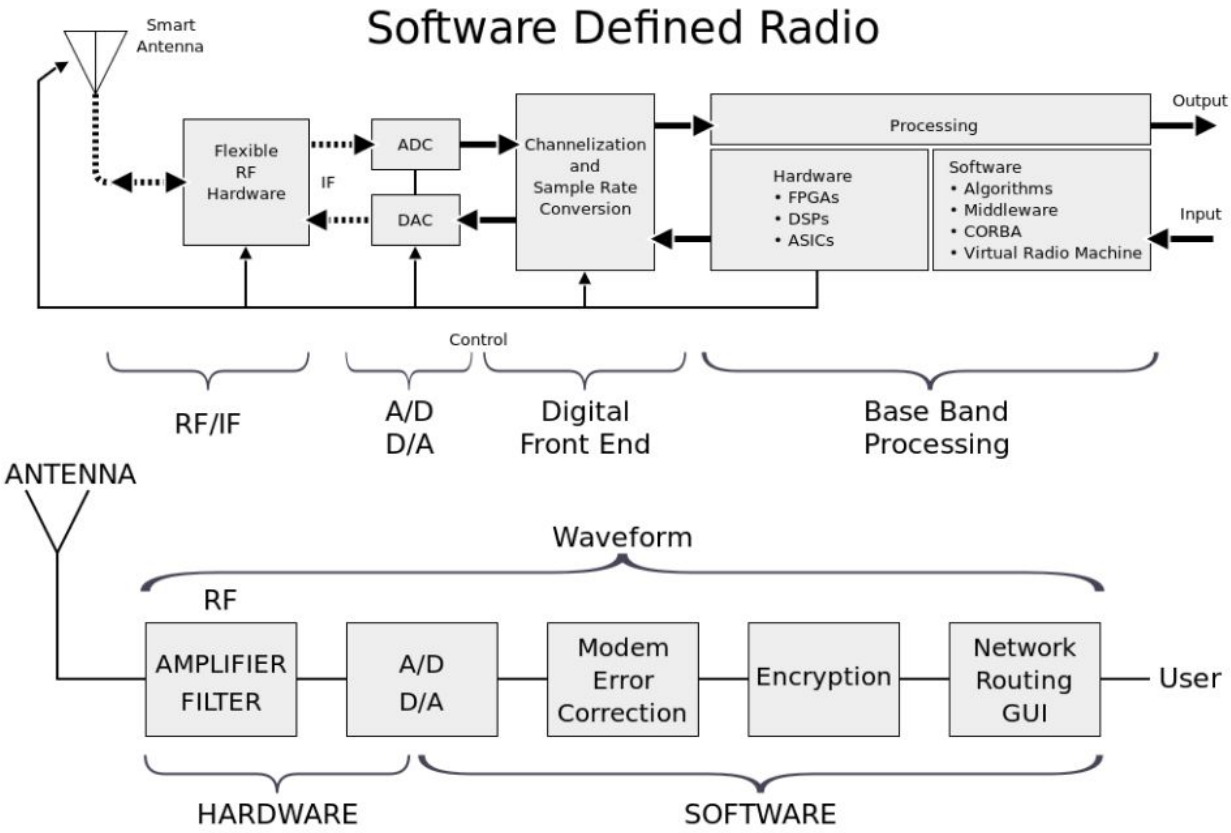
σημείο-προς-σημείο VoIP σε επίπεδο μεταφοράς, χρησιμοποιώντας περιστασιακά κρυπτογράφηση.

Κυβέρνηση και στρατιωτικές οργανώσεις χρησιμοποιούν διάφορα μέτρα ασφαλείας για την προστασία της κυκλοφορίας VoIP, όπως η φωνή μέσω ασφαλούς IP (VoSIP), ασφαλή voice over IP (SVoIP), και ασφαλή voice over ασφαλή IP (SVoSIP). Η διάκριση έγκειται στο κατά πόσον η κρυπτογράφηση εφαρμόζεται στο τηλέφωνο ή στο δίκτυο ή και τα δύο. Ασφαλής φωνής μέσω ασφαλούς IP επιτυγχάνεται με την κρυπτογράφηση VoIP με πρωτόκολλα όπως SRTP ή ZRTP. Ασφαλής voice over IP σύνδεση επιτυγχάνεται με τη χρήση κρυπτογράφησης τύπου 1 σε διαβαθμισμένο δίκτυο, όπως το Siprnet.

8.6 Εισαγωγή στο Software Defined Radio

Ένα software defined ραδιο-σύστημα, ή SDR, είναι ένα σύστημα ραδιοεπικοινωνίας, όπου όλα τα συστατικά που συνήθως ενσωματώνονται με υλικά (όπως μείκτες, φίλτρα, ενισχυτές, διαμορφωτές/ αποδιαμορφωτές, ανιχνευτές κ.λ.π) υλοποιούνται με λογισμικό σε έναν προσωπικό υπολογιστή ή ενσωματωμένες υπολογιστικές συσκευές. Ενώ η έννοια του SDR δεν είναι νέα, οι ταχέως εξελισσόμενες δυνατότητες των ψηφιακών ηλεκτρονικών καθιστούν πρακτικά πολλές διαδικασίες δύσκολες να εφαρμοσθούν πρακτικά, αν και θεωρητικά είναι εφικτές.

Μπορείτε να σκεφτείτε το SDR ως πομποδέκτη που μπορεί να λειτουργήσει σε ολόκληρο το φάσμα από DC έως το άπειρο, συμβατό με όλα τα στάνταρ ανεξάρτητα από οποιαδήποτε τεχνική διαμόρφωσης χρησιμοποιεί το ίδιο υλικό. Άρα μια πιο απλή ορολογία του SDR, θα μπορούσε να είναι: “Ράδιο του οποίου κάποια ή όλα τα μέρη φυσικού στρώματος είναι λογισμικό” (στην αναφορά του ράδιο, μιλάμε για οποιαδήποτε ασύρματη επικοινωνία, μονομερή ή διμερή). Το SDR σαν ιδέα παρουσιάστηκε για πρώτη φορά στον κόσμο από τον τομέα εθνικής άμυνας στο τέλος της δεκαετίας του ‘70, τόσο στην Αμερική όσο και στην Ευρώπη, υπό το όνομα SPEAKeasy από την Αμερικάνικο στρατό του οποίου η προγραμματιζόμενη επεξεργασία ενσωματώθηκε για να εξομοιώσει περισσότερα από 10 προϋπάρχοντα στρατιωτικά ασύρματα δίκτυα που λειτουργούσαν στις συχνότητες μεταξύ των 2 MHz και 200MHz. Ο όρος Soft-Defined Radio επινοήθηκε αργότερα από τον J. Mitola το 1991.



Το SDR καθορίζει μια συλλογή τεχνολογιών υλικού και λογισμικού όπου όλες οι ραδιολειτουργίες υλοποιούνται μέσω παραμετροποιήσιμου λογισμικού ή firmware που λειτουργεί σε προγραμματιζόμενες τεχνολογίες επεξεργασίας. Αυτές οι συσκευές περιλαμβάνουν προγραμματιζόμενες διατάξεις θυρών πεδίου (FPGA), επεξεργαστές ψηφιακού σήματος (DSP), γενικής χρήσης επεξεργαστές (GPP), προγραμματιζόμενα ψηφιακά κυκλώματα συστήματος (SOC) ή άλλες εφαρμογές συγκεκριμένων προγραμματιζόμενων επεξεργαστών. Η χρήση αυτών των τεχνολογιών επιτρέπει την προσθήκη νέων ασύρματων δυνατοτήτων και ικανοτήτων στα ήδη υπάρχοντα ραδιοσυστήματα χωρίς την απαίτηση νέου υλικού.

8.7 Συστατικά μέρη του OpenBTS:

Μια πλήρη εγκατάσταση του OpenBTS περιλαμβάνει αρκετές διακριτές εφαρμογές:

- **OpenBTS** – Η πραγματική εφαρμογή, (OpenBTS) που περιλαμβάνει το μεγαλύτερο μέρος της GSM στοίβας πάνω από το ραδιοδιαμορφωτή

- **Πομποδέκτης** – Το υλικό και λογισμικό περιβάλλον του ραδιοδιαμορφωτή
- **SMQueue** - Ο RFC-3428 σέρβερ για αποθήκευση και προώθηση γραπτών μηνυμάτων.
- **Asterisk** – Το VoIP PBX.
- **SIPAuthServe** – Μια εφαρμογή για διαχείριση της βάσης των εγγεγραμμένων χρηστών
- **Άλλες υπηρεσίες** - Προαιρετικές υπηρεσίες από εξωτερικούς σέρβερ που αλληλεπιδρούν με το OpenBTS μέσω διαφόρων πρωτοκόλλων. Στο OpenBTS αυτές οι υπηρεσίες είναι:

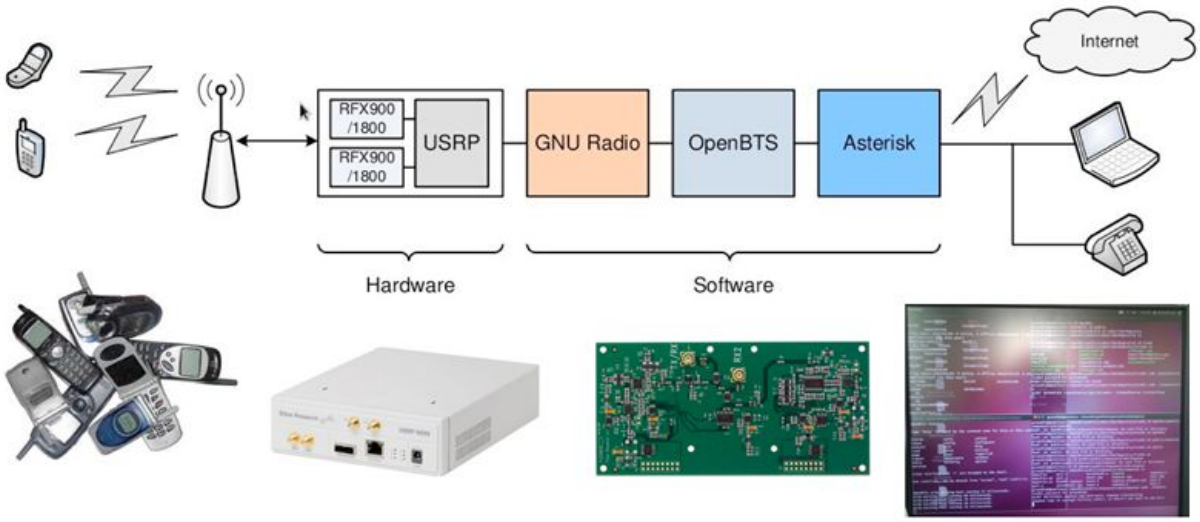
- **NodeManager**, ο JSON διαχειριστής API που επιτρέπει σε εξωτερικές εφαρμογές να διαχειριστούν βασικά δομικά στοιχεία της σουίτας του OpenBTS (OpenBTS, SMQueue και SIPAuthServe). Το “OpenRANUI” διαδικτυακή διεπαφή το οποίο παρέχεται με την επί πληρωμή έκδοση του OpenBTS, χρησιμοποιεί NodeManager.
- **SMSCB**, μια χαμηλού επιπέδου υπηρεσία δεδομένων.

Στα Range προεγκαταστημένα συστήματα, όλα τα εκτελέσιμα της πλατφόρμας εκτός του Asterisk βρίσκονται στον φάκελο “/OpenBTS” στο partition του root.

8.8 OpenBTS

Η εφαρμογή του OpenBTS περιλαμβάνει:

• **L1 TDM** λειτουργίες (GSM 05.02)
• **L1 FEC** λειτουργίες (GSM 05.03)
• **L1 Κλειστή λούπα** ελέγχου ενέργειας και ρολογίων (GSM 05.08 and 05.10)
• **L2 LAPDm** (GSM 04.06)
• **L3 Λειτουργία ελέγχου** των ραδιο-πόρων (GSM 04.08)
• **L3 GSM-SIP πύλη** για τη διαχείριση της κινητικότητας
• **L3 GSM-SIP πύλη** για τον έλεγχο των κλήσεων
• **L4 GSM-SIP πύλη** για την αποστολή μηνυμάτων κειμένου



Η γενική προσέγγιση του σχεδιασμού του OpenBTS δεν είναι να υλοποιήσει κάθε λειτουργία παραπάνω από το L3 ή L4. Έτσι στο L3 ή L4 κάθε υποπρωτόκολλο του GSM είτε τερματίζεται τοπικά είτε μεταφράζεται μέσα από μια πύλη σε κάποιο άλλο πρωτόκολλο για το χειρισμό από μια εξωτερική εφαρμογή. Ομοίως, το ίδιο το OpenBTS δεν περιέχει καμία λειτουργία αποκωδικοποίησης ομιλίας πάνω από τα FEC μέρη του L1.

8.8.1 Πομποδέκτης-Transceiver

Η εφαρμογή πομποδέκτη εκτελεί τις λειτουργίες radio modem του GSM 05.05 και διαχειρίζεται τη διεπαφή του USB στο υλικό μέρος του radio.

8.8.2 SMQueue

Το SMQueue είναι ένας RFC-3428 σέρβερ για αποθήκευση και προώθηση που χρησιμοποιείται για την αποστολή μηνυμάτων κειμένου στο σύστημα OpenBTS.
Το SMQueue απαιτείται για να σταλεί ένα μήνυμα κειμένου από το ένα κινητό στο άλλο, ή να παρέχει αξιόπιστη παράδοση των μηνυμάτων κειμένου από μία συσκευή, σε οποιαδήποτε πόρο.

8.8.3 SIP router / PBX

Το OpenBTS χρησιμοποιεί ένα δρομολογητή SIP ή PBX για να εκτελέσει τις λειτουργίες ελέγχου κλήσεων που θα έπρεπε κανονικά να εκτελεστούν από το κέντρο μεταγωγής

κλήσεων σε ένα συμβατικό δίκτυο GSM, αν και στις περισσότερες διαμορφώσεις δικτύων αυτές οι λειτουργίες μεταγωγής κατανέμονται σε πολλαπλά switches. Αυτοί οι switches παρέχουν επίσης υπηρεσίες transcoding. Από την έκδοση OpenBTS 4.0, το πρότυπο SIP router είναι το Asterisk 11. Το OpenBTS έχει χρησιμοποιηθεί με PBX VoIP και εναλλακτικές εφαρμογές, εκτός από Asterisk, ωστόσο η Range κανονικά δεν υποστηρίζει αυτές τις διαμορφώσεις.

8.8.4 SIPAuthServe

Μια εφαρμογή που περιέχει το “Μητρώου Συνδρομητών”, τη βάση δεδομένων των πληροφοριών συνδρομητή, το οποίο αντικαθιστά τόσο το μητρώο Asterisk SIP όσο και το GSM Home Location Register (HLR) το οποίο βρίσκεται σε ένα συμβατικό GSM δίκτυο. Το OpenBTS βασίζεται επίσης σε Asterisk για οποιεσδήποτε λειτουργίες transcoding.

8.9 Ασφάλεια

Στο συνέδριο DEF CON 2010, αποδείχθηκε με την χρήση OpenBTS ότι οι GSM κλήσεις μπορούν να υποκλαπούν εξαιτίας στο γεγονός ότι οι GSM συσκευές δεν αυθεντικοποιούνται από το σταθμό βάσης πριν από την πρόσβαση τους στο δίκτυο.

Το OpenBTS έχει χρησιμοποιηθεί από την κοινότητα ελέγχου ασφάλειας για να εξαπολύσουν επιθέσεις στους σταθμούς βάσης κινητών τηλεφώνων. Προηγουμένως, η έρευνα και η διεξαγωγή τέτοιων επιθέσεων θεωρούνταν ανέφικτη λόγω του υψηλού κόστους των παραδοσιακών εξοπλισμών σταθμού βάσης.

8.9.1 Field tests

Η μεγάλης κλίμακας ζωντανές δοκιμές του OpenBTS έχουν διεξαχθεί στις Ηνωμένες Πολιτείες, στη Νεβάδα και στη Βόρεια Καλιφόρνια που χρησιμοποιούν προσωρινές άδειες ραδιοσυχνοτήτων ειδικές για τις “Επεξεργασίας Σήματος Kestrel” και “Range Networks, Inc.”

8.9.2 Burning Man

Κατά τη διάρκεια του φεστιβάλ Burning Man τον Αύγουστο του 2008, ένα ζωντανό πείραμα μιας εβδομάδας διεξήχθη υπό ειδική προσωρινή άδεια. Παρά το γεγονός ότι η δοκιμή αυτή δεν προοριζόταν να είναι προσβάσιμη στο Burning Man για όλους τους συμμετέχοντες, μια σειρά από άτομα στην περιοχή κατάφεραν να κάνουν κλήσεις εκτός δικτύου. Λόγω μιας κακής εγκατάστασης του Asterisk PBX επιτρέπονταν δοκιμαστικές κλήσεις με πρόθεμα διεθνούς κώδικα κλήσης. Στο πειραματικό δίκτυο κατάφεραν να πραγματοποιηθούν 120 τηλεφωνήματα από 95 διαφορετικούς αριθμούς σε κωδικούς περιοχής από τη Βόρεια Αμερική.

Στο Burning Man φεστιβάλ του 2009, μια μεγαλύτερη πειραματική εγκατάσταση στήθηκε χρησιμοποιώντας ένα σύστημα 3-τομέων. Για το φεστιβάλ του 2010, ένα ακόμη μεγαλύτερο 2-τομέων και 3-φορέων σύστημα δοκιμάστηκε.

8.9.3 "RELIEF" Exercises

Οι RELIEF είναι μια σειρά από ασκήσεις αντιμετώπισης των καταστροφών που διαχειρίζεται η Ναυτική Μεταπτυχιακή Σχολή στην Καλιφόρνια των ΗΠΑ. Οι Range Networks που χειρίζονται τα OpenBTS δίκτυα έκαναν διάφορες δοκιμές στις ασκήσεις RELIEF το Νοέμβριο του 2011 και το Φεβρουάριο του 2012.

8.9.4 Niue

Κατά τη διάρκεια του 2010, ένα σύστημα OpenBTS εγκαταστάθηκε στο νησί του Νιούε και έγινε η πρώτη εγκατάσταση που συνδέθηκε και δοκιμάστηκε από εταιρείες τηλεπικοινωνιών. Το Νιούε είναι μια πολύ μικρή νησιωτική χώρα με πληθυσμό περίπου 1.700 - πολύ μικρό για να προσελκύσει τους παρόχους κινητής τηλεφωνίας. Η διάρθρωση του κόστους σύνδεσης των OpenBTS ταιριάζει σε περιπτώσεις σαν το Νιούε, το οποίο απαιτεί μια κινητή τηλεφωνική υπηρεσία, αλλά δεν είχε τον όγκο των πιθανών πελατών για να δικαιολογήσουν την αγορά και την υποστήριξη ενός συμβατικού συστήματος σταθμού βάσης GSM.

Η επιτυχία αυτής της εγκατάστασης και η αποδεδειγμένη ζήτηση για υπηρεσίες βοήθησε την μετέπειτα ζήτηση περισσότερων εμπορικών υπηρεσιών. Η εγκατάσταση OpenBTS αργότερα παροπλίσθηκε. Όταν το Φεβρουαρίου του 2011 η Niue Telecom, μια

εμπορική εταιρία με παροχή GSM 900 δικτύου και υποστήριξη Edge ξεκίνησε λίγους μήνες αργότερα (3x sites στο Kaimiti O2, Sekena S2 / 2/2 και Avatele S2 / 2/2) να παρέχει πλήρης κάλυψη σε όλο το νησί και γύρω από τον ύφαλο. Η εγκατάσταση περιλαμβάνει ένα σύστημα προ-πληρωμής, USSD, Int. SMS και νέα Int. πύλη.

8.9.5 Defcon 20

Από 26 Ιούλιου-29 Ιούλιου 2012, η ομάδα Ninja Δίκτυα (Ninja Networks) δημιουργήσε ένα «NinjaTel Van" στην περιοχή Vendor του Defcon 20 (στο Rio Hotel / Casino στο Λας Βέγκας). Χρησιμοποιήθηκε OpenBTS και εξυπηρετούσε ένα μικρό δίκτυο από 650 GSM τηλέφωνα με custom κάρτες SIM.

8.10 GNURadio:

Το GNURadio είναι ένα λογισμικό ανοικτού κώδικα Software Defined Radio (SDR) που άρχισε περίπου πριν από δέκα χρόνια από τον Eric Blossom, έναν ηλεκτρολόγο μηχανικό. Η κύρια ιδέα που βρίσκεται πίσω από αυτό το έργο ήταν να μετατρέψει όλα τα προβλήματα υλικού σε προβλήματα λογισμικού. Αυτή η κίνηση θα φέρει την πολυπλοκότητα ενός ραδιο-εξοπλισμού από το υλικό επίπεδο στο λογισμικό, και θα πάρει το λογισμικό όσο πιο κοντά στην κεραία είναι δυνατόν.

Ο Blossom ξεκίνησε αυτό το έργο, επειδή είχε απογοητευθεί από τα έργα SDR που ήταν διαθέσιμα εκείνη την εποχή: όλα τους είχαν μία ιδιόκτητη φύση, και ήθελε να να φέρει τη φιλοσοφία του ελεύθερου λογισμικού στον SDR κόσμο. Στον Richard Stallman, ιδρυτής του έργου GNU, άρεσε η ιδέα του Blossom και συμφώνησαν να αναλάβει το έργο στο πλαίσιο της GNU αιγίδας.

Μέχρι στιγμής, το έργο GNURadio δεν απογοήτευσε τους συνεργάτες και τους υποστηρικτές του. Ο Eric Blossom, σε συνδυασμό με την ανάπτυξη του συναδέλφου του Matt Ettus, έχουν εμπνευστεί το έργο το οποίο μπορεί να μετατρέψει ένα συνηθισμένο PC σε ένα καλής ποιότητας ραδιοφωνικό δέκτη. Το μοναδικό πρόσθετο υλικό που απαιτείται είναι ένας «χαμηλού κόστους» δέκτης RF και ένας μετατροπέας αναλογικού σήματος σε ψηφιακό για τη μετατροπή του ληφθέντος σήματος σε ψηφιακά δείγματα. Το GNURadio είναι ένα δωρεάν σύνολο εργαλείων ανάπτυξης λογισμικού το οποίο επιτρέπει την ανάπτυξη ενός προσαρμοσμένου μη εμπορικού ραδιοφωνικού δέκτη απλά συνδυάζοντας και υπερσυνδέοντας κατάλληλες ενότητες λογισμικού, σαν να ήταν λειτουργικά τμήματα (το πακέτο περιλαμβάνει περίπου 100 μονάδες, αλλά μπορούν να προστεθούν και άλλες στην αρχική βιβλιοθήκη).

Κάθε μονάδα είναι σε θέση να εκτελέσει μια συγκεκριμένη λειτουργία επεξεργασίας σήματος με μια συμπεριφορά σε πραγματικό χρόνο και με υψηλό ρυθμό διακίνησης δεδομένων. Για το λόγο αυτό, ένα πρόσφατο PC με αρκετή ικανότητα επεξεργασίας και μνήμη συνίσταται να χρησιμοποιείται. Με την προσέγγιση του GNURadio, ο σχεδιαστής είναι ένα προγραμματιστής λογισμικού που χτίζει το ραδιοπομπό με τη δημιουργία ενός γραφήματος (με παρόμοιο τρόπο με αυτό που συμβαίνει στην θεωρία γράφων), όπου οι κορυφές είναι μπλοκ επεξεργασίας σήματος και οι ακμές αντιπροσωπεύουν τη ροή δεδομένων μεταξύ τους. Τα μπλοκ επεξεργασίας σήματος είναι συνήθως υλοποιημένα σε C ++, ενώ η δομή του γράφου ορίζεται σε Python. Το GNURadio είναι ευραίως γνωστό και χρησιμοποιείται σε μεγάλο βαθμό στο ακαδημαϊκό περιβάλλον και μεταξύ “χομπιστών” και από τους ραδιοερασιτέχνες.

Χρησιμοποιείται είτε για την εφαρμογή σε πραγματικό περιβάλλον και υπό την λειτουργία ραδιο-εξοπλισμού, είτε απλά ως ένα ερευνητικό έργο στον τομέα της ασύρματης επικοινωνίας και μετάδοσης. Το GNURadio λογισμικό υποστηρίζει διάφορες διαμορφώσεις (GMSK, PSK, QAM και OFDM) κώδικες διόρθωσης σφαλμάτων (Reed-Solomon, Viterbi και Turbo Κώδικες) και παρέχει δυνατότητες επεξεργασίας σήματος (φίλτρα, FFTs, ισοσταθμιστές και ανάκτηση χρονισμού). Οι εφαρμογές GNURadio είναι γραμμένες κυρίως σε Python. Ωστόσο, οι κρίσιμοι και χαμηλού επιπέδου αλγόριθμοι και οι μονάδες επεξεργασίας σήματος είναι γραμμένοι σε C / C ++ γλώσσα προγραμματισμού, με ευρεία χρήση των ειδικών οδηγιών floating-point για τους συσχετιζόμενους επεξεργαστές. Η Python χρησιμοποιείται κυρίως για να ρυθμίσει το γράφημα ροής, αφού πρώτα το μεγαλύτερο μέρος της εργασίας γίνεται σε C / C ++. Το GNURadio είναι απλό στη χρήση και δίνει την δυνατότητα δημιουργίας ένας ραδιό-δέκτης με ένα γρήγορο και απλό τρόπο. Επιπλέον, η ανάπτυξη ενός αλγορίθμου επεξεργασίας σήματος μπορεί να πραγματοποιηθεί χρησιμοποιώντας ένα προ-καταγεγραμένο ή παράγωγο σύνολο δεδομένων, επιτρέποντας έτσι την ανάπτυξη χωρίς την ανάγκη για ένα πραγματικό υλικό RF. Ένα παράδειγμα ελάχιστης χρήσης υλικού που απαιτείται για την υλοποίηση συστήματος με το GNURadio προσφέρεται από το USRP.

8.10.1 GNURadio Companion:

Το GRC είναι μια συντομογραφία για το GNURadio Companion, η γραφική διεπαφή χρήστη που χρησιμοποιείται για συνδεθούν πολλαπλά GNURadio μπλοκ μαζί. Το GRC είναι η γραφική διεπαφή του χρήστη του GNURadio (GUI).

• Χρησιμοποιώντας τη drag and drop λειτουργία.
• Ροή μπορεί να δημιουργηθεί απλώς συνδέοντας το μπλοκ με το ποντίκι.
• Δημιουργία του πηγαίου κώδικα, σύμφωνα με τις συνδέσεις μπλοκ.

Κάθε μπλοκ στο GRC έχει ένα αντίστοιχο αρχείο XML που περιέχει τις παραμέτρους, τις IO πόρτες, και ένα πρότυπο για την παραγωγή κώδικα. Το κλειδί ID και το όνομα αρχείου του κάθε xml αρχείου ταιριάζουν ακριβώς με το όνομα του GNURadio μπλοκ για να διασφαλιστεί η μελλοντική φορητότητα. Το GRC επικυρώνει όλα τα ονόματα των μπλοκ κατά την εκτέλεση, και θα κάνει έξοδο με λάθος, εάν τυχόν κάποιο όνομα αποτύχει να περάσει την επικύρωση.

8.11 Asterisk

Το Asterisk χτίστηκε αρχικά ως PBX και σήμερα αποτελεί ένα εκπληκτικό 18% της παγκόσμιας αγοράς των επιχειρήσεων για τηλεφωνικά συστήματα. Το σύνολο των χαρακτηριστικών βάσης περιλαμβάνει πολλά από τις πιο δημοφιλείς και ισχυρές λειτουργίες των PBX. Αγγίζοντας τη δύναμη του Asterisk απαιτεί κάποια γνώση του Linux, τηλεφωνίας, τις βασικές έννοιες προγραμματισμού και των δικτύων IP.

8.11.1 Χαρακτηριστικά του Asterisk:

Το λογισμικό Asterisk περιλαμβάνει πολλά χαρακτηριστικά που είναι διαθέσιμα σε ένα ιδιόκτητο PBX συστήμα: το φωνητικό ταχυδρομείο, κλήσεις τηλεδιάσκεψης, διαδραστική φωνητική απόκριση, και αυτόματη κλήση. Οι χρήστες μπορούν να δημιουργήσουν νέες λειτουργίες με την συγγραφή script στίς δίαφορες γλώσσες που υποστηρίζει το Asterisk, προσθέτοντας προσαρμοσμένα modules γραμμένα σε C, ή με την εφαρμογή του Asterisk Gateway Interface (AGI) .Για να επισυνάψετε τα παραδοσιακά αναλογικά τηλέφωνα σε μια εγκατάσταση Asterisk, ή για να συνδεθείτε στις γραμμές κορμού PSTN, ο διακομιστής πρέπει να είναι εφοδιασμένος με ειδικό υλικό. Η Digium και ορισμένες άλλες επιχειρήσεις πωλούν κάρτες PCI για να επισυνάψετε τηλέφωνα, τηλεφωνικές γραμμές, T1 και E1 γραμμές, και άλλες αναλογικές και ψηφιακές υπηρεσίες τηλεφώνου.

Ίσως περισσότερο ενδιαφέρον για πολλούς παρόχους σήμερα είναι ότι το Asterisk υποστηρίζει επίσης ένα ευρύ φάσμα από βίντεο και Voice over IP πρωτόκολλα, συμπεριλαμβανομένων των SIP, MGCP και H.323. Το Asterisk μπορεί να διαλειτουργεί με τα περισσότερα τηλέφωνα SIP, που ενεργούν τόσο ως εγγραφείς, όσο και ως πύλες

μεταξύ τηλεφώνων IP και PSTN. Οι προγραμματιστές του Asterisk έχουν επίσης σχεδιάσει ένα νέο πρωτόκολλο, το Inter-Asterisk Exchange (IAX2), για την αποτελεσματική πραγματοποίηση των κλήσεων μεταξύ Asterisk Τηλεφωνικών Κέντρων, με τους παρόχους υπηρεσιών VoIP που το υποστηρίζουν. Μερικά τηλέφωνα υποστηρίζουν άμεσα το πρωτόκολλο IAX2. Με την υποστήριξη ενός συνδυασμού των παραδοσιακών και των VoIP τηλεφωνικών υπηρεσιών, το Asterisk επιτρέπει την εισαγωγή τους για την κατασκευή νέων τηλεφωνικών συστημάτων ή την σταδιακή μεταφορά από τα υπάρχοντα συστήματα στις νέες τεχνολογίες. Μερικά sites χρησιμοποιούν διακομιστές Asterisk για να αντικαταστήσουν ιδιόκτητα PBX αλλά και για να παρέχουν πρόσθετες λειτουργίες (όπως φωνητικό ταχυδρομείο ή φωνητική απόκριση μενού, ή καταστήματα εικονικών κλήσεων) ή για να μειώσουν το κόστος διεξαγωγής υπεραστικών κλήσεων μέσω του Διαδίκτυου.

Το Asterisk ήταν ένα από τα πρώτα πακέτα λογισμικού ανοικτού κώδικα PBX, που πλέον υπάρχουν πολλά. Εκτός από τα πρωτόκολλα VoIP, το Asterisk υποστηρίζει και πολλά παραδοσιακά πρωτόκολλα μεταγωγής κυκλώματος, όπως ISDN και SS7. Αυτό απαιτεί κατάλληλες κάρτες διασύνδεσης υλικού που υποστηρίζουν τέτοια πρωτόκολλα, οι οποίες διατίθενται στο εμπόριο από τρίτους προμηθευτές.

9 Βιβλιογραφία

http://www.iec.org/online/tutorials/gsm/topic05.asp
http://www.telecomspace.com/gsm-specifications.html
http://www.tutorialspoint.com/gsm/gsm_specification.htm
http://www.cs.ucl.ac.uk/staff/t.pagtzis/wireless/gsm/arch.html
Integration of Open-Source GSM Networks by Thomas A. Cooper
https://en.wikipedia.org/wiki/1G
https://en.wikipedia.org/wiki/2G
https://en.wikipedia.org/wiki/3G
https://en.wikipedia.org/wiki/4G
https://en.wikipedia.org/wiki/5G
https://www.timetoast.com/timelines/history-of-mobile-phones-7e561d96-e442-4495-9d71-3d0789eaaab4
http://ieeexplore.ieee.org/document/7547270
https://www.huawei.eu/sites/default/files/5G_Security_Whitepaper_en.pdf
https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf