ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αναλυτική μελέτη του φαινομένου των εσφαλμένων συγχρονισμών στα ενοποιημένα δίκτυα 3G-WLAN

Φώτιος Β. Καρζής

Επιβλέποντες: Ξενάκης Χρήστος, Καθηγητής ΠΑ.ΠΕΙ.
Χριστόφορος Νταντογιάν, Διδάκτωρ

ΠΕΙΡΑΙΑ

ΙΟΥΝΙΟΣ 2010

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αναλυτική μελέτη του φαινομένου των εσφαλμένων συγχρονισμών στα ενοποιημένα δίκτυα 3G-WLAN

Φώτιος Β. Καρζής

Μ.Ε.: 08053

ΕΠΙΒΛΕΠΟΝΤΕΣ:

Ξενάκης Χρήστος, Καθηγητής ΠΑ.ΠΕΙ.

Χριστόφορος Νταντογιάν, Διδάκτωρ

ΠΕΡΙΛΗΨΗ

Σε αυτή την διατριβή μελετούμε την λειτουργία ενοποιημένων δικτύων 3G-WLAN που χρησιμοποιούν μια πληθώρα από πρωτόκολλα για την επικοινωνία με τους χρήστες. Κάποια από τα πρωτόκολλα αυτά θα τα αναλύσουμε στην συνέχεια. Αρχικά γίνεται μια λεπτομερής αναφορά στο τι είναι και πως λειτουργούν τα μέρη ενός ενοποιημένου δικτύου. Η χρήση των δικτύων αυτών είναι πολύ μεγάλη και ολοένα αυξάνεται. Εμείς θα ασχοληθούμε κατά κύριο λόγο με την περιγραφή των UMTS και WLAN δικτύων που συναποτελούν τα δίκτυα αυτά. Τα WiMax δίκτυα αρχίζουν σιγά-σιγά να έχουν ολοένα και πιο ενεργεί συμμετοχή στα ενοποιημένα δίκτυα, λόγο της μεγάλης εξέλιξης τους, αλλά στην παρούσα διατριβή θα αρκεστούμε σε μια απλή αναφορά και λίγα λόγια. Θα περιγράψουμε επίσης το πρόβλημα που εμφανίζεται κατά την διάρκεια που κάποιος χρήστης κινείται εναλλάξ από το ένα δίκτυο στο άλλο. Το πρόβλημα των εσφαλμένων συγχρονισμών όπως αποκαλείται. Τελειώνοντας με το θεωρητικό μέρος της εργασίας, παρουσιάζεται το κύριο μέρος της εργασίας, που έχει να κάνει με την προσομοίωση ενός τέτοιου ενοποιημένου δικτύου με χρήση του προγράμματος OPNET. Αφού προγραμματίστηκε και στήθηκε ένα τέτοιο δίκτυο λοιπόν, έγιναν παρατηρήσεις για τον τρόπο λειτουργίας και τους χρόνους που μεσολαβούν για όλες τις διαδικασίες του. Βασικός σκοπός της εργασίας είναι η καταμέτρηση του αριθμού των συγχρονισμών(synchronizations) που γίνονται αλλά και την πιθανότητα που υπάρχει να συμβούν κατά την διαδικασία κίνησης ενός χρήστη από το ένα δίκτυο στο άλλο και αντίστροφα. Παρουσιάζονται γραφικές παραστάσεις που δείχνουν σε κάθε τρέξιμο του προγράμματος τα αποτελέσματα που βγήκαν, αλλά και οι τελικές γραφικές παραστάσεις που συνοψίζουν όλα τα αποτελέσματα μαζί και μας δείχνουν την λειτουργία του δικτύου αυτού και την συμπεριφορά του γενικότερα.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ασφάλεια Ενοποιημένων Δικτύων 4^{ης} γενιάς

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ : WLAN, UMTS, Synchronizations, Protocols, Authentication,

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Στην διπλωματική αυτή εργασία μελετήθηκε το πρόβλημα των εσφαλμένων συγχρονισμών που έχει τεθεί και μελετηθεί στην διατριβή[αναφορά 1], με την χρήση προσομοιώσεων. Συγκεκριμένα στην διατριβή[αναφορά 1] μέσα από μαθηματικά μοντέλα και τύπους αναδείχτηκε το πρόβλημα που δημιουργείται κατά την αυθεντικοποίηση των διαφόρων χρηστών σε κάποιο δίκτυο. Η πρακτική επαλήθευση των παραπάνω γίνεται πράξη μέσω αυτής της διπλωματικής εργασίας. Στην διπλωματική αυτή λοιπόν, με την χρήση του εργαλείου προσομοίωσης OPNET δημιουργήσαμε ένα ενοποιημένο δίκτυο, το οποίο αποτελείται από αρκετά υποδίκτυα. Με την βοήθεια του προγράμματος προσομοιώσαμε πραγματικά δεδομένα κίνησης και εγγραφής χρηστών από το ένα δίκτυο στο άλλο και αντίστροφα. Δημιουργήσαμε διάφορα σενάρια για διάφορες παραμέτρους που παίζουν ρόλο στις μετρήσεις μας. Οι παράμετροι αυτοί έχουν να κάνουν με την σωστή και ακέραια δρομολόγηση των δεδομένων μεταξύ των δικτύων. Διαπιστώσαμε το πρόβλημα με τις αυθεντικοποιήσεις των χρηστών και πρακτικά λοιπόν. Είδαμε που αυτό μεγιστοποιείται και που ελαχιστοποιείται προτείνοντας και τρόπους επίλυσης του. Όλα αυτά εξηγούνται και φαίνονται στα επόμενα κεφάλαια αναλυτικά.

Θα ήθελα σε αυτό το σημείο να ευχαριστήσω τους επιβλέποντες της διπλωματικής μου εργασίας, καθηγητή κύριο Ξενάκη Χρήστο και τον διδάκτορα Χριστόφορο Νταντογιάν, για την άμεση και πολύτιμη βοήθεια τους αλλά και για το υλικό που μου παρείχαν ώστε να πραγματοποιήσω την εργασία αυτή.

Αθήνα, Ιούνιος 2009

Φώτιος Β. Καρζής

ΚΕΦΑΛΑΙΟ 1

Ενοποιημένα δίκτυα 3G-WLAN

1.1 Εισαγωγή

Τα τελευταία χρόνια παρατηρείται μια ραγδαία ανάπτυξη των υπολογιστικών συστημάτων. Οι φορητοί υπολογιστές , οι συσκευές χειρός, τα PDA και κυρίως τα κινητά έχουν κατακλίσει την αγορά. Με το κινητό μας για παράδειγμα, μπορούμε ανά πάσα στιγμή να κάνουμε κλήση ή να συνδεθούμε στο διαδίκτυο. Μπορούμε πλέον οπουδήποτε και να είμαστε να έχουμε πρόσβαση σε υπηρεσίες και πληροφορίες απελευθερωμένοι από τα δεσμά που επιβάλλει ένα δωμάτιο ή ένας επιτραπέζιος υπολογιστής. Η ανάγκη για καλύτερες και πιο γρήγορες συνδέσεις όμως, οδηγεί στην μεταπομπή των χρηστών από δίκτυο σε δίκτυο, δημιουργώντας έτσι και διάφορα προβλήματα στις επικοινωνίες τους.

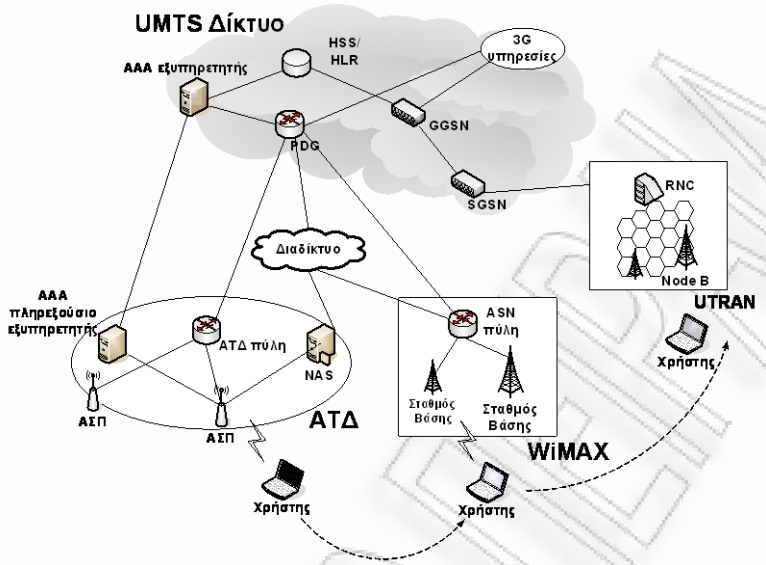
Τα ενοποιημένα δίκτυα υπόσχονται να προσφέρουν στον τελικό χρήστη υπηρεσίες πραγματικού χρόνου, όπως η μετάδοση εικόνων και φωνής με πολύ υψηλούς ρυθμούς μετάδοσης. Τα δίκτυα αυτά αποτελούνται από ετερογενή ασύρματα δίκτυα, όπως τα ασύρματα τοπικά δίκτυα, τα ασύρματα μητροπολιτικά δίκτυα WiMAX και τα κινητά συστήματα $3^{ης}$ γενιάς(3G). Ο χρήστης μπορεί να επιλέξει το κατάλληλο ασύρματο δίκτυο και να αποκτήσει πρόσβαση στις υπηρεσίες που επιθυμεί. Ωστόσο, μια βασική προϋπόθεση για την επιτυχή εδραίωση των ενοποιημένων δικτύων αποτελεί η εξασφάλιση και παροχή ενός υψηλού επιπέδου ασφάλειας και ιδιωτικότητας, που θα αποτρέπει οποιαδήποτε πιθανή επίθεση στους χρήστες ή στο δίκτυο. Για αυτό το λόγο έχουν σχεδιαστεί διάφορες αρχιτεκτονικές ασφάλειας για τα δίκτυα αυτά, που προασπίζουν την ιδιωτικότητα των χρηστών και προστατεύουν και το δίκτυο από κακόβουλες ενέργειες.

1.2 Αρχιτεκτονική Ενοποιημένων Δικτύων 3G-WLAN

Όπως αναφέρθηκε προηγουμένως, τα ενοποιημένα δίκτυα έχουν ως σκοπό την ενοποίηση ετερογενών ασύρματων δικτύων σε ένα ενιαίο δίκτυο. Μια απλοποιημένη εικόνα της αρχιτεκτονικής των ενοποιημένων δικτύων απεικονίζεται στο Σχήμα 1. Όπως φαίνεται από αυτό το σχήμα, τα δίκτυα αυτά αποτελούνται από: (1) τα ασύρματα τοπικά δίκτυα WLAN (Wireless Local Area Networks), (2) τα δίκτυα WiMAX, και (3) τα δίκτυα UMTS (Universal Mobile Telecommunications System) τα οποία αντιπροσωπεύουν τα κινητά συστήματα 3^{ης} γενιάς. Τα Ασύρματα Τοπικά Δίκτυα(ΑΤΔ) περιλαμβάνουν τα ασύρματα σημεία πρόσβασης AP (Access Point), τα οποία λειτουργούν ως πελάτες (clients) του πρωτόκολλου αυθεντικοποίησης, εξουσιοδότησης και χρέωσης AAA (Authentication, Authorization, Accounting) και προωθούν μηνύματα στον εξυπηρετητή AAA (AAA server) μέσω ενός πληρεξούσιου εξυπηρετητή AAA. Επίσης, τα ΑΤΔ περιέχουν τον εξυπηρετητή πρόσβασης δικτύου NAS (Network Access Server), το οποίο παρέχει στους χρήστες των ΑΤΔ πρόσβαση στο Διαδίκτυο.

Τα δίκτυα WiMAX, όπως φαίνεται και στο Σχήμα 1. περιλαμβάνουν χρήστες οι οποίοι συνδέονται σε σταθμούς βάσης. Επιπλέον, κάθε σταθμός βάσης είναι συνδεδεμένος με την πύλη ASN (Access Service Network).

Τέλος, τα δίκτυα UMTS αποτελούνται από τον εξυπηρετητή AAA, το PDG (Packet Data Gateway) και τις δικτυακές οντότητες του UMTS, όπως το ασύρματο δίκτυο πρόσβασης UTRAN (UMTS Terrestrial Radio Access Network), το HSS (Home Subscriber Service) το οποίο είναι μια βάση δεδομένων των χρηστών, οι κόμβοι GGSN (Gateway GPRS Support Node) και SGSN (Serving GPRS Support Node). Ο εξυπηρετητής AAA ανακτά παραμέτρους αυθεντικοποίησης από τη βάση δεδομένων του HSS και αυθεντικοποιεί τους χρήστες με βάση αυτές τις παραμέτρους. Τέλος, το PDG δρομολογεί τα δεδομένα του χρήστη στις 3G υπηρεσίες.



Σχήμα 1.2.1: Αρχιτεκτονική Ενοποιημένων Δικτύων

1.3 Αυθεντικοποίηση και Εμπιστευτικότητα Ενοποιημένων Δικτύων

Στα πλαίσια της παρούσας ενότητας θα αναπτύξουμε δυο σημαντικά ζητήματα ιδιωτικότητας (privacy) που συναντάμε στα ενοποιημένα δίκτυα(integrated networks): Την αυθεντικοποίηση (authentication) χρηστών και την εμπιστευτικότητα (confidentiality) δεδομένων. Με τον όρο αυθεντικοποίηση εννοούμε την εξακρίβωση και την επαλήθευση της ταυτότητας (identity) μιας οντότητας (φυσικό πρόσωπο, εξυπηρετητής, οργανισμός). Για να αντιληφθεί κανείς τη σπουδαιότητα της αυθεντικοποίησης αρκεί να λάβει υπόψη του ότι αν δεν υπάρχει έλεγχος στην ταυτότητα των χρηστών, τότε ένας κακόβουλος θα μπορεί να προσποιηθεί ότι είναι μια οποιαδήποτε έγκυρη οντότητα. Αν το πετύχει αυτό, τότε μπορεί να έχει πρόσβαση σε προσωπικές πληροφορίες παραβιάζοντας την ιδιωτικότητα των χρηστών. Από την άλλη πλευρά, η εμπιστευτικότητα των δεδομένων εξασφαλίζει ότι ένας κακόβουλος δεν μπορεί να «διαβάσει» τα προσωπικά δεδομένα των χρηστών καθώς αυτά μεταδίδονται μέσα σε ένα δίκτυο. Η εμπιστευτικότητα επιτυγχάνεται με την κρυπτογράφηση των δεδομένων χρησιμοποιώντας μυστικά κλειδιά, τα οποία πρέπει να είναι γνωστά μόνο στον αποστολέα και τον παραλήπτη των δεδομένων.

Μια πολύ σημαντική έννοια στα ενοποιημένα δίκτυα είναι η αμοιβαία αυθεντικοποίηση. Συγκεκριμένα, στην περίπτωση που δυο οντότητες, έστω Α και Β, θέλουν να επικοινωνήσουν μεταξύ τους, τότε αν η οντότητα Α αυθεντικοποιηθεί στην οντότητα Β, και αντίστροφα, αν η οντότητα Β αυθεντικοποιηθεί στην Α, τότε η διαδικασία αυτή ονομάζεται αμοιβαία αυθεντικοποίηση. Για παράδειγμα, αν η οντότητα Α είναι ένας χρήστης και η οντότητα Β είναι το δίκτυο με το οποίο ο χρήστης επιθυμεί να συνδεθεί, τότε με την αμοιβαία αυθεντικοποίηση εξασφαλίζεται: (1) ότι το δίκτυο γνωρίζει το χρήστη που έχει πρόσβαση σε αυτό και (2) ο χρήστης συνδέεται στο πραγματικό και σωστό δίκτυο που επιθυμεί.

Σε γενικές γραμμές τα πρωτόκολλα ασφάλειας δικτύων εφαρμόζουν δυο διαφορετικές μεθόδους αυθεντικοποίησης: (1) κώδικες HMAC (Hash Message Authentication Code) που χρησιμοποιούνται για αυθεντικοποίηση αλλά και διασφάλιση της ακεραιότητας (integrity) των μηνυμάτων και (2) χρήση ψηφιακών πιστοποιητικών (digital certificates).

Οι κώδικες HMAC παρέχουν υπηρεσίες αυθεντικοποίησης αλλά και διασφάλισης της ακεραιότητας των μηνυμάτων**.** Με τη χρήση των κωδίκων HMAC, ο αποστολέας δημιουργεί μια σύνοψη (digest) D του μηνύματος, χρησιμοποιώντας μια συνάρτηση κατακερματισμού και ένα μυστικό κλειδί, το οποίο είναι γνωστό μόνο στον αποστολέα και στον παραλήπτη. Όταν ο παραλήπτης λάβει το μήνυμα, υπολογίζει μια σύνοψη D' αυτού του μηνύματος χρησιμοποιώντας το ίδιο κλειδί που χρησιμοποίησε και ο αποστολέας και συγκρίνει τη σύνοψη D' που υπολόγισε με τη σύνοψη D του αποστολέα. Εάν υπάρχει αντιστοιχία, δηλαδή αν D=D', τότε αυτό συνεπάγεται ότι ο αποστολέας του μηνύματος είναι ο κάτοχος του μυστικού κλειδιού και επομένως έχει επαληθευθεί η ταυτότητα του, ενώ ταυτόχρονα έχει εξακριβωθεί και η ακεραιότητα του μηνύματος. Το ψηφιακό πιστοποιητικό είναι ένα ηλεκτρονικό έγγραφο (digital document) που χρησιμοποιείται για την αυθεντικοποίηση μίας οντότητας, χρησιμοποιώντας κρυπτογράφηση δημοσίου κλειδιού. Περιέχει πληροφορίες για τον κάτοχο του πιστοποιητικού, όπως για παράδειγμα το ονοματεπώνυμο του και το δημόσιο κλειδί του, καθώς επίσης και την ημερομηνία λήξης του πιστοποιητικού. Τα πιστοποιητικά πρέπει να είναι ψηφιακά υπογεγραμμένα από μια ανεξάρτητη έμπιστη αρχή, για να

εξασφαλιστεί η αυθεντικότητα του δημοσίου κλειδιού που περιέχεται στο πιστοποιητικό.

1.4 Ιδιαίτερες Απαιτήσεις Ανωνυμίας και Ιδιωτικότητας στα Ενοποιημένα Δίκτυα

Μια βασική λειτουργία των ενοποιημένων δικτύων , που όπως είπαμε αποτελούνται από ασύρματα ετερογενή δίκτυα, είναι η υποστήριξη κινητικότητας μέσω αρραγούς μεταπομπής (seamless handover) κατά την οποία ο χρήστης μετακινείται από ένα ασύρματο δίκτυο σε ένα άλλο, χωρίς την αναγκαστική διακοπή της ενεργής σύνδεσής του (βλέπε Σχήμα 1.). Για παράδειγμα, ας υποθέσουμε το εξής σενάριο: Ένας χρήστης που βρίσκεται σε ένα αυτοκίνητο πραγματοποιεί μια κλήση VoIP (Voice over IP). Ο χρήστης αναγκαστικά πρέπει να χρησιμοποιήσει το δίκτυο UMTS καθώς το τελευταίο υποστηρίζει συνεχή κινητικότητα, χωρίς όμως να προσφέρει υψηλούς ρυθμούς μετάδοσης. Όταν ο χρήστης καταφτάνει στον προορισμό του αποβιβάζεται από το αυτοκίνητο και εισέρχεται σε ένα κτίριο που διαθέτει ασύρματο δίκτυο. Ο χρήστης προκειμένου να εκμεταλλευτεί τους υψηλούς ρυθμούς μετάδοσης που προσφέρουν τα ΑΤΔ, πραγματοποιεί μια μεταπομπή (handover) μεταφέροντας την ενεργή σύνδεση του από το δίκτυο UMTS στο ΑΤΔ.

Στο παράδειγμα που μόλις αναφερθήκαμε, ο χρήστης δεν αντιλήφθηκε κάποια διακοπή στη σύνδεσή του, διότι πραγματοποιήθηκε μια μεταπομπή κατά την οποία το δίκτυο UMTS μετέφερε πληροφορίες (context transfer) σχετικές με το χρηστή και τη σύνδεσή του στο ΑΤΔ, με αποτέλεσμα η σύνδεση του χρήστη να συνεχιστεί απρόσκοπτα. Αυτές οι πληροφορίες μπορεί να είναι το είδος της εφαρμογής που ο χρήστης χρησιμοποιεί (π.χ., WWW, VoIP), τα κλειδιά κρυπτογράφησης, η ταυτότητα του χρήστη, κ.α. Παρατηρεί λοιπόν κάνεις ότι οι πληροφορίες που μεταδίδονται από το παλαιό δίκτυο στο νέο, κατά τη διάρκεια μιας μεταπομπής, περιέχουν ευαίσθητα δεδομένα που σε ενδεχόμενη υποκλοπή τους, η ιδιωτικότητα και η ανωνυμία (anonymity) του χρηστή είναι σίγουρα παραβιασμένη. Επομένως, είναι προφανές ότι η ασφαλή μετάδοση των πληροφοριών αυτών είναι απαραίτητη προϋπόθεση για την προστασία της ιδιωτικότητας και της ανωνυμίας στα ενοποιημένα δίκτυα.

Για την ασφαλή μετάδοση των πληροφοριών από το ένα δίκτυο σε ένα άλλο, κατά τη διάρκεια της μεταπομπής ακολουθείται η εξής διαδικασία: το παλαιό δίκτυο όταν αντιληφθεί ότι ο χρήστης πρόκειται να αλλάξει δίκτυο, εγκαθιστά εκ των προτέρων μια ασφαλή σήραγγα IPSec (IPsec tunnel), με το νέο δίκτυο, η οποία προστατεύει όλη την πληροφορία που μεταδίδεται από το παλαιό στο νέο δίκτυο. Σε περίπτωση που το νέο δίκτυο αρνηθεί να εγκαταστήσει τη σήραγγα IPSec, τότε διακόπτεται η σύνδεση του χρηστή και ο τελευταίος θα πρέπει να αρχικοποιήσει ξανά τη σύνδεση όταν βρεθεί στο νέο δίκτυο.

Εκτός από την ασφάλεια κατά τη διάρκεια μεταπομπών, στα ενοποιημένα δίκτυα υπάρχουν διάφορα ζητήματα που αφορούν την ιδιωτικότητα των χρηστών τα οποία πρέπει να μελετηθούν λεπτομερώς. Στις επόμενες ενότητες μελετώνται τα ζητήματα ιδιωτικότητας και ασφάλειας στα ΑΤΔ και στα δίκτυα UMTS.

ΚΕΦΑΛΑΙΟ 2

WLAN

2.1 Ιδιωτικότητα και Ασφάλεια στα Ασύρματα Τοπικά Δίκτυα

Όταν ένας χρήστης θέλει να χρησιμοποιήσει ένα ΑΤΔ για να αποκτήσει πρόσβαση στο Διαδίκτυο, τότε ο χρήστης και το δίκτυο αυθεντικοποιούνται αμοιβαία, χρησιμοποιώντας το EAP-SIM ή το EAP-AKA πρωτόκολλο Αν ο χρήστης κατέχει μια κάρτα USIM (UMTS Subscribers Identity Module), τότε εκτελείται το πρωτόκολλο EAP-AKA. Σε περίπτωση που ο χρήστης διαθέτει μια κάρτα SIM (Subscribers Identity Module), τότε εφαρμόζεται το πρωτόκολλο EAP-SIM. Ύστερα από μια επιτυχή αυθεντικοποίηση, ο χρήστης αποκτά μια διεύθυνση IP από το ΑΤΔ και έχει πρόσβαση στο Διαδίκτυο. Η προστασία της ιδιωτικότητας των προσωπικών δεδομένων των χρηστών εξασφαλίζεται από τους μηχανισμούς ασφάλειας του προτύπου IEEE 802.11i. Στις επόμενες ενότητες θα μελετήσουμε τη λειτουργικότητα των δυο πρωτόκολλων EAP-SIM και EAP-AKA καθώς και το πρότυπο (standard) IEEE 802.11i εστιάζοντας στα χαρακτηριστικά ασφάλειας που προσφέρουν.

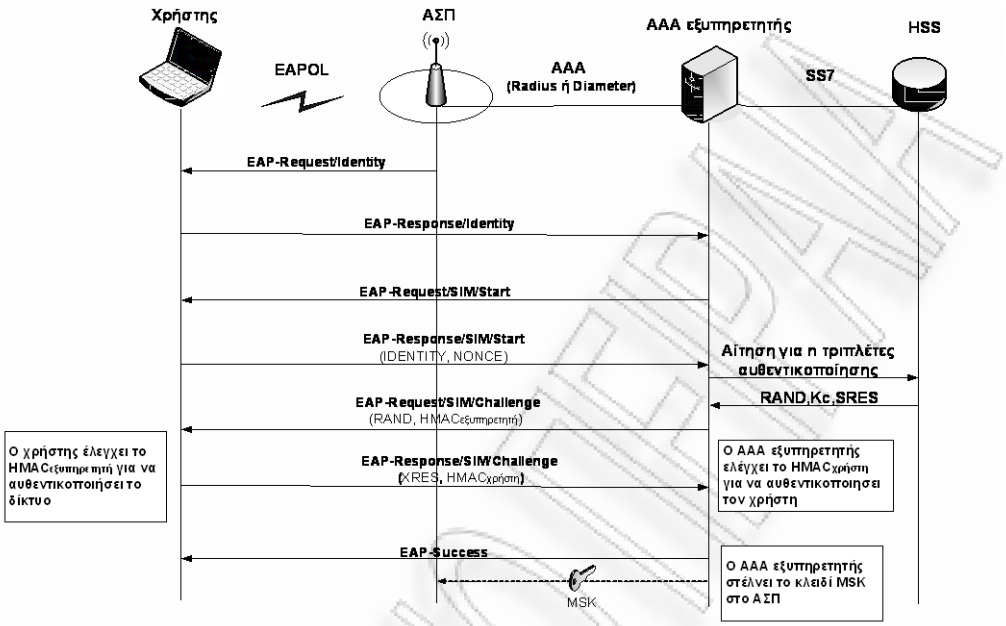
2.1.1 Το Πρωτόκολλο EAP-SIM

Το πρωτόκολλο EAP-SIM βασίζεται στη διαδικασία αυθεντικοποίησης και ανταλλαγής κλειδιού του δικτύου GSM/GPRS, χρησιμοποιώντας τις παραμέτρους ασφάλειας που είναι αποθηκευμένες στη κάρτα SIM. Το πρωτόκολλο αυτό εκτελείται μεταξύ ενός χρήστη, ενός πελάτη AAA (το οποίο ουσιαστικά είναι το AP) και ενός εξυπηρετητή AAA που ανακτά πληροφορίες αυθεντικοποίησης (δηλαδή τις τριπλέτες αυθεντικοποίησης) από τον HSS του δικτύου GSM (Global Subscriber for Mobile communications)/GPRS (General Packet Radio Service), όπου ο χρήστης είναι εγγεγραμμένος. Το EAP-SIM συνδυάζει n το πλήθος (όπου n=2 ή n=3) ξεχωριστές τιμές RAND για να παράγει n διαφορετικά κλειδιά Kc. Τα κλειδιά αυτά συνδυάζονται με έναν τυχαίο αριθμό (ο οποίος υποδηλώνεται ως NONCE), την ταυτότητα του χρήστη, και άλλα δικτυακά δεδομένα, για να παραχθεί το κλειδί MK (Master Key) του πρωτόκολλου EAP-

SIM. Στη συνέχεια, το κλειδί MK παράγει διάφορα κλειδιά, από τα οποία τα πιο σημαντικά είναι: το κλειδί MSK (Master Session Key), που χρησιμοποιείται από το πρότυπο IEEE 802.11i για να παράγει τα κλειδιά κρυπτογράφησης, και το κλειδί K_auth, το οποίο χρησιμοποιείται στο EAP-SIM για τη δημιουργία των τιμών HMAC.

Το Σχήμα 2. παρουσιάζει την ανταλλαγή μηνυμάτων EAP-SIM μεταξύ του χρήστη και του εξυπηρετητή AAA. Να σημειωθεί ότι ο χρήστης επικοινωνεί με τον Ασύρματο Σταθμό Πρόσβασης(ΑΣΠ) με τη χρήση του πρωτόκολλου EAPOL (Extensible Authentication Protocol Over LAN). Αρχικά, ο χρήστης συσχετίζεται με ένα ΑΣΠ και το τελευταίο στέλνει ένα μήνυμα EAP-Request/Identity στο χρήστη ζητώντας την ταυτότητα του. Στη συνέχεια ο χρήστης στέλνει στον εξυπηρετητή AAA μέσω του ΑΣΠ το μήνυμα EAP-Response/Identity, το οποίο περιέχει την ταυτότητα του. Αυτή η ταυτότητα μπορεί να είναι είτε η μόνιμη ταυτότητα IMSI (International Mobile Subscriber Identity) του ή μια προσωρινή ταυτότητα. Η χρήση προσωρινών ταυτοτήτων ενισχύει την ανωνυμία του χρήστη. Γνωρίζοντας την ταυτότητα του χρήστη, ο εξυπηρετητής AAA δημιουργεί ένα μήνυμα EAP-Request/SIM/Start, που στην ουσία αρχικοποιεί το πρωτόκολλο EAP-SIM. Ο χρήστης απαντά με ένα μήνυμα EAP-Response/SIM/Start που περιέχει ένα τυχαίο αριθμό NONCE. Μόλις λάβει το μήνυμα αυτό, ο εξυπηρετητής AAA επικοινωνεί με το HSS και αποκτά n το πλήθος (όπου n=2 ή n=3) τριπλέτες αυθεντικοποίησης GSM/GPRS (authentication triplets) για το συγκεκριμένο χρήστη (δηλαδή τον κάτοχο της SIM κάρτας). Μια τριπλέτα αυθεντικοποίησης GSM/GPRS περιέχει έναν τυχαίο αριθμό RAND, ένα κλειδί κρυπτογράφησης Kc, και το αναμενόμενο SRES. Η δημιουργία των τριπλετών αυθεντικοποίησης βασίζεται σε ένα μόνιμο κλειδί (permanent key) Ki, το οποίο είναι αποθηκευμένο στην κάρτα SIM και στη βάση δεδομένων του HSS. Έπειτα, ο εξυπηρετητής AAA στέλνει στο χρήστη ένα μήνυμα EAP-Request/SIM/Challenge, που περιέχει τις n το πλήθος τιμές RAND και την τιμή $HMAC_{εξυπηρετητή}$ που υπολογίζεται χρησιμοποιώντας το κλειδί K_auth πάνω στο μήνυμα EAP-Request/SIM/Challenge. Να σημειωθεί ότι πριν από τον υπολογισμό της τιμής $HMAC_{εξυπηρετητή}$, ο εξυπηρετητής AAA υπολογίζει το κλειδί MK και στη συνέχεια τα κλειδιά K_auth και MSK.

Μόλις λάβει το μήνυμα EAP-Request/SIM/Challenge, ο χρήστης εκτελεί τους αλγόριθμους αυθεντικοποίησης του GSM/GPRS n φορές (μια φορά για κάθε μια τριπλέτα αυθεντικοποίησης που έχει λάβει), για να παράγει n το πλήθος κλειδιά Kc και n τιμές XRES. Στη συνέχεια, χρησιμοποιώντας τα n κλειδιά Kc που παρήγαγε, δημιουργεί το κλειδί MK και έπειτα το κλειδί K_auth και το κλειδί MSK, όπως έκανε προηγουμένως ο εξυπηρετητής AAA. Έπειτα, ο χρήστης ελέγχει αν η τιμή $HMAC_{εξυπηρετητή}$ είναι έγκυρη, χρησιμοποιώντας το κλειδί K_auth. Αν η τιμή $HMAC_{εξυπηρετητή}$ είναι έγκυρη, τότε το δίκτυο έχει αυθεντικοποιηθεί στο χρήστη και ο τελευταίος στέλνει στον εξυπηρετητή AAA τις n το πλήθος τιμές XRES που παρήγαγε προηγουμένως, μέσα σε ένα μήνυμα EAP-Response/SIM/Challenge. Το μήνυμα αυτό περιέχει επίσης την τιμή $HMAC_{χρήστη}$, η οποία υπολογίστηκε χρησιμοποιώντας το κλειδί K_auth πάνω στο μήνυμα EAP-Response/SIM/Challenge και στις n τιμές XRES. Με το που θα λάβει αυτό το μήνυμα, ο εξυπηρετητής AAA εξετάζει αν η τιμή $HMAC_{χρήστη}$ είναι έγκυρη, χρησιμοποιώντας το κλειδί K_auth καθώς επίσης και αν οι n το πλήθος τιμές XRES αντιστοιχούν σε n το πλήθος τιμές SRES. Αν αυτοί οι έλεγχοι είναι σωστοί, τότε ο εξυπηρετητής AAA στέλνει ένα μήνυμα EAP-Success στο χρήστη που υποδηλώνει την επιτυχή αμοιβαία αυθεντικοποίηση. Επιπρόσθετα, ο εξυπηρετητής AAA στέλνει στο ΑΣΠ το κλειδί MSK. Σε αυτό το σημείο, ο χρήστης και το δίκτυο έχουν αυθεντικοποιηθεί αμοιβαία, και, επιπλέον, ο χρήστης και το ΑΣΠ μοιράζονται ένα κλειδί MSK, που θα χρησιμοποιηθεί για την κρυπτογράφηση των δεδομένων στο IEEE 802.11i.



Σχήμα 2.1.1.1: Το πρωτόκολλο EAP-SIM

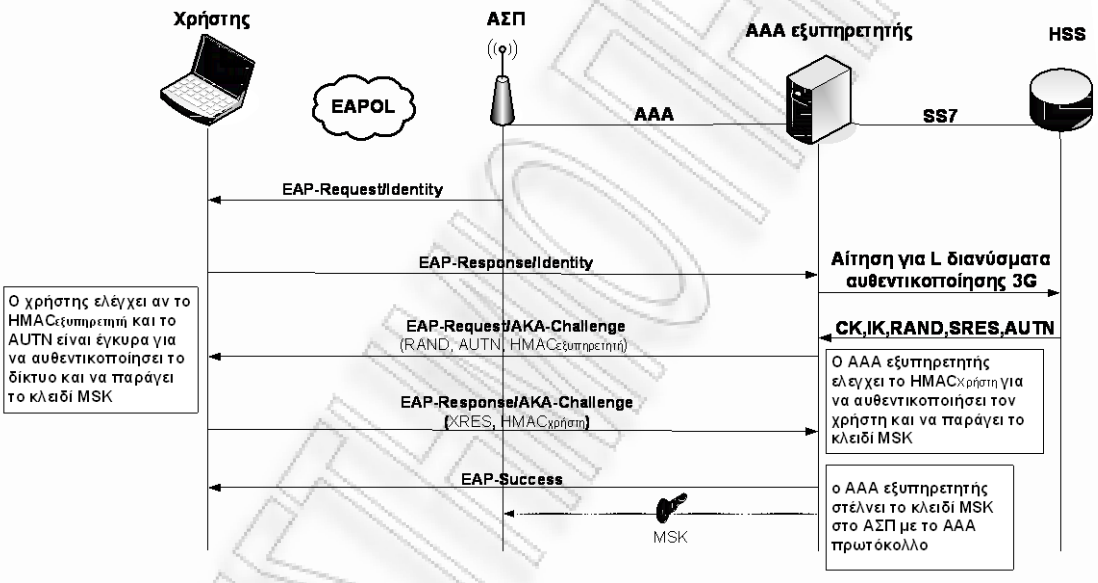
2.1.2 Το Πρωτόκολλο EAP-AKA

Το πρωτόκολλο EAP-AKA βασίζεται στη διαδικασία αυθεντικοποίησης και ανταλλαγής κλειδιών του δικτύου UTMS και χρησιμοποιεί τις παραμέτρους ασφαλείας που είναι αποθηκευμένες στις κάρτες USIM. Όπως και στο πρωτόκολλο EAP-SIM, το EAP-AKA εκτελείται μεταξύ ενός χρήστη, ενός πελάτη AAA (το οποίο στην ουσία είναι το AP) και ενός εξυπηρετητή AAA, το οποίο αντλεί πληροφορίες αυθεντικοποίησης από τον HSS του δικτύου UMTS, όπου ο χρήστης είναι εγγεγραμμένος. Επίσης χρησιμοποιεί τον εξυπηρετητή AAA και το πρωτόκολλο EAPOL για την επικοινωνία μεταξύ του χρήστη και του δικτύου.

Στο πρώτο μήνυμα του EAP-AKA, το ΑΣΠ ζητά από το χρήστη την ταυτότητά του (βλέπε Σχήμα 2.). Ο χρήστης στέλνει στον εξυπηρετητή AAA την ταυτότητά του με ένα μήνυμα EAP-Response/Identity, το οποίο περιέχει είτε την μόνιμη ταυτότητα του IMSI ή μια προσωρινή ταυτότητα. Αφού αποκτήσει την ταυτότητα του χρήστη, ο εξυπηρετητής AAA εξετάζει αν διαθέτει διανύσματα αυθεντικοποίησης 3G (3G authentication vectors), τα οποία τα έχει αποθηκεύσει από μια προηγούμενη αυθεντικοποίηση του συγκεκριμένου χρήστη με το δίκτυο.

Αν όχι, τότε ο εξυπηρετητής AAA στέλνει την ταυτότητα IMSI του χρήστη στον HSS, το οποίο με τη σειρά του χρησιμοποιώντας το μόνιμο κλειδί K του UMTS (το οποίο είναι αποθηκευμένο στη κάρτα USIM του χρήστη και στη βάση δεδομένων του HSS) δημιουργεί L το πλήθος διανύσματα αυθεντικοποίησης 3G για το συγκεκριμένο χρήστη. Να σημειώσουμε ότι ένα διάνυσμα αυθεντικοποίησης περιέχει έναν τυχαίο αριθμό RAND, το «κουπόνι» αυθεντικοποίησης AUTN, το αναμενόμενο SRES, το κλειδί κρυπτογράφησης CK και το κλειδί IK που χρησιμοποιείται για να παρέχει ακεραιότητα στα μηνύματα του χρήστη. Επίσης, να σημειωθεί ότι η διαδικασία αίτησης και παραλαβής από το HSS/AuC καινούργιων διανυσμάτων αυθεντικοποίησης ονομάζεται AVR (Authentication Vector Request). Ο εξυπηρετητής AAA διαλέγει 1 από τα L διανύσματα αυθεντικοποίησης και αποθηκεύει τα υπόλοιπα L-1 για μελλοντική χρήση. Από το επιλεγμένο διάνυσμα αυθεντικοποίησης 3G, ο εξυπηρετητής AAA θα χρησιμοποιήσει τα κλειδιά CK και IK και την ταυτότητα του χρήστη για να παράγει το κλειδί MK του EAP-AKA. Από το κλειδί MK θα παραχθεί το κλειδί MSK και το κλειδί K_auth, όπως και στο EAP-SIM. Ο εξυπηρετητής AAA υπολογίζει μια τιμή $HMAC_{εξυπηρετητής}$ και στη συνέχεια στέλνει στο χρήστη ένα μήνυμα EAP-Request/AKA-Challenge, το οποίο περιέχει ένα RAND, ένα AUTN και την τιμή $HMAC_{εξυπηρετητής}$. Να σημειωθεί ότι ο εξυπηρετητής AAA υπολόγισε το $HMAC_{εξυπηρετητής}$, χρησιμοποιώντας το κλειδί K_auth πάνω στο μήνυμα EAP-Request/AKA-Challenge, για να εξασφαλίσει την αυθεντικότητα και την ακεραιότητα του μηνύματος. Αφού λάβει ο χρήστης το μήνυμα EAP-Request/AKA-Challenge, εκτελεί τους αλγόριθμους κρυπτογράφησης UMTS-AKA και εξετάζει αν είναι έγκυρο το AUTN. Στη συνέχεια παράγει τα κλειδιά CK και IK χρησιμοποιώντας πάλι τους αλγόριθμους κρυπτογράφησης UMTS-AKA και στη συνέχεια παράγει το κλειδί MK. Έπειτα, χρησιμοποιεί το κλειδί MK, για να παράγει τα κλειδιά MSK και K_auth, όπως έκανε προηγουμένως ο εξυπηρετητής AAA, και ελέγχει την εγκυρότητα της τιμής του $HMAC_{εξυπηρετητής}$. Ύστερα, ο χρήστης υπολογίζει και στέλνει την τιμή XRES σε ένα μήνυμα EAP-Response/AKA-Challenge στον εξυπηρετητή AAA το οποίο περιέχει το XRES, καθώς επίσης την τιμή $HMAC_{χρήστη}$ που υπολογίζεται με το κλειδί K_auth. Όταν λάβει το μήνυμα EAP-Response/AKA-Challenge, ο εξυπηρετητής AAA θα εξετάσει την εγκυρότητα της τιμής $HMAC_{χρήστη}$ και θα εξετάσει αν το XRES που έλαβε από το χρήστη αντιστοιχεί στο SRES που έλαβε από το HSS. Αν όλοι οι

έλεγχοι είναι σωστοί, τότε ο εξυπηρετητής AAA θα στείλει ένα μήνυμα EAP-Success στο χρήστη μαζί με το κλειδί MSK στο ΑΣΠ (βλέπε Σχήμα 2.). Το τελευταίο θα αποθηκεύσει το κλειδί και θα προωθήσει το μήνυμα EAP-Success στο χρήστη. Ολοκληρώνοντας το πρωτόκολλο EAP-AKA, ο χρήστης και το δίκτυο έχουν αυθεντικοποιηθεί αμοιβαία, και ο χρήστης και το ΑΣΠ μοιράζονται το κλειδί MSK το οποίο θα χρησιμοποιηθεί στο πρότυπο 802.11i για να δημιουργήσει τα κλειδιά που θα παρέχουν ασφάλεια στην ασύρματη διεπαφή του ΑΤΔ.



Σχήμα 2.1.2.1 Το πρωτόκολλο EAP-AKA

2.1.3 Το Πρότυπο IEEE 802.11i

Όπως αναφέρθηκε προηγουμένως, το πρότυπο IEEE 802.11i χρησιμοποιείται για να προσφέρει εμπιστευτικότητα και ακεραιότητα στα δεδομένα των χρηστών που ανταλλάσσονται στην ασύρματη διεπαφή ενός ΑΤΔ. Το κίνητρο που οδήγησε στη σχεδίαση του IEEE 802.11i ήταν το γεγονός ότι το πρωτόκολλο WEP (Wired Equivalent Privacy) δεν μπορεί να καλύψει τις απαιτήσεις ασφάλειας που έχουν τα ΑΤΔ. Αυτή η αδυναμία του WEP οφείλεται στα πολλά κενά ασφάλειας που διαθέτει, με αποτέλεσμα να είναι τρωτό σε πολλές επιθέσεις**.** Για αυτό το λόγο σχεδιάστηκε το πρότυπο IEEE 802.11i, το οποίο ενισχύει την ασφάλεια στα ΑΤΔ.

Ο σκοπός του προτύπου IEEE 802.11i είναι διπλός: (1) να διαχειρίζεται τα κλειδιά ασφάλειας με τη χρήση της χειραψίας τεσσάρων μερών (Four way handshake) και τη χειραψία ομαδικού κλειδιού (Group key handshake) και (2) να ενισχύσει τις υπηρεσίες εμπιστευτικότητας και ακεραιότητας στα ΑΤΔ με την ενσωμάτωση δυο πρωτόκολλων ασφάλειας: (1) το πρωτόκολλο CCMP (Counter Mode/CBC MAC Protocol) που χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης (cryptography algorithm) AES (Advanced Encryption Standard) και (2) το πρωτόκολλο TKIP (Temporal Key Integrity Protocol), που χρησιμοποιεί τον ίδιο αλγόριθμο κρυπτογράφησης με το WEP, ο οποίος ονομάζεται RC4.

Μετά την εκτέλεση του πρωτόκολλου EAP-SIM ή του EAP-AKA, ο χρήστης και το ΑΣΠ εκτελούν τη χειραψία τεσσάρων μερών, καθώς επίσης και τη χειραψία ομαδικού κλειδιού του 802.11i. Κατά τη χειραψία τεσσάρων μερών, τόσο ο χρήστης όσο και το ΑΣΠ παράγουν το κλειδί PTK (Pairwise Transient Key) από το κλειδί MSK που δημιουργήθηκε κατά την εκτέλεση του EAP-SIM ή του EAP-AKA. Το κλειδί PTK χρησιμεύει για την προστασία των μηνυμάτων μονοεκπομπής (unicast). Επιπλέον, το ΑΣΠ δημιουργεί και στέλνει στο χρήστη το κλειδί GTK (Group Transient Key), το οποίο χρησιμεύει για την προστασία των μηνυμάτων ευρυεκπομπής/πολυεκπομπής (broadcast/multicast). Η ομαδική χειραψία λαμβάνει χώρα, όταν το ΑΣΠ θέλει να μοιράσει ένα καινούργιο κλειδί GTK στους συνδεδεμένους χρήστες του ΑΣΠ. Να σημειωθεί εδώ ότι όλα τα μηνύματα που ανταλλάσσονται στη χειραψία τεσσάρων μερών και στην ομαδική χειραψία χρησιμοποιούν το πρωτόκολλο EAPOL.

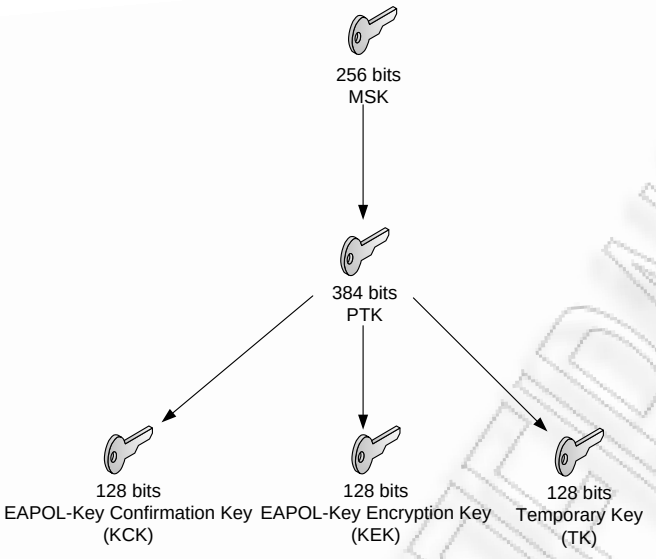
Όπως υποδηλώνει το όνομά του, η χειραψία τεσσάρων μερών αποτελείται από 4 μηνύματα. Στην αρχή της χειραψίας τεσσάρων μερών, το ΑΣΠ στέλνει στο χρήστη ένα μήνυμα EAPOL που περιέχει το Anonce, το οποίο είναι ένας τυχαίος αριθμός και χρησιμοποιείται για τη δημιουργία του κλειδιού PTK, όπως θα αναλυθεί παρακάτω. Όταν λάβει το πρώτο μήνυμα EAPOL, ο χρήστης παράγει με τη σειρά του έναν τυχαίο αριθμό Snonce. Μετά, υπολογίζει το κλειδί PTK χρησιμοποιώντας το κλειδί MSK, τη διεύθυνση του χρήστη, τη διεύθυνση του ΑΣΠ, το Anonce, και τέλος, το Snonce, όπως φαίνεται στην παρακάτω εξίσωση:

PTK= prf [1](MSK, Min(διεύθυνση ΑΣΠ, διεύθυνση χρήστη) | Max(διεύθυνση ΑΣΠ, διεύθυνση χρήστη) | Min(Anonce, Snonce) | Max(Anonce, Snonce))[2]

Όπου Min και Max ορίζονται ως συναρτήσεις οι οποίες επιστέφουν το ελάχιστο και το μέγιστο μεταξύ δυο τιμών αντίστοιχα. Στη συνέχεια, το παραγόμενο κλειδί PTK διασπάται σε τρία άλλα κλειδιά: (1) στο κλειδί KCK (Key Confirmation Key) το οποίο προσφέρει υπηρεσίες ακεραιότητας δεδομένων στα υπόλοιπα μηνύματα EAPOL της χειραψίας τεσσάρων μερών, (2) στο κλειδί KEK (Key Encryption Key) που χρησιμοποιείται για να κρυπτογραφήσει το κλειδί GTK, όπως θα αναλυθεί παρακάτω, και (3) στο κλειδί TK (Temporal Key) που θα παρέχει ασφάλεια στα δεδομένα του χρήστη που θα μεταφέρονται στην ασύρματη διεπαφή του ΑΤΔ (βλέπε Σχήμα 2.1.). Μετά τον υπολογισμό αυτών των κλειδιών, ο χρήστης προωθεί στο ΑΣΠ το δεύτερο μήνυμα EAPOL, που περιέχει το Snonce, το RSN IE (Robust Security Network Information Element) το οποίο περιλαμβάνει το σύνολο των κρυπτογραφικών αλγόριθμων που η συσκευή του χρήστη υποστηρίζει, και το MIC (Message Integrity Code) το οποίο είναι μια τιμή HMAC που υπολογίζεται με το κλειδί KCK και μια συνάρτηση κατακερματισμού πάνω στο μήνυμα EAPOL.

1. Το συμβολό *prf* αντιπροσωπεύει μια ψευδοτυχαία συνάρτηση. Οι ψευδοτυχαίες συναρτήσεις χαρακτηρίζονται από το ψευδοτυχαίο των εξόδων τους, δηλαδή, κάθε bit στην έξοδο της συνάρτησης είναι απρόβλεπτο. Στην πράξη, η prf είναι υλοποιημένη χρησιμοποιώντας μονόδρομες συναρτήσεις κατακερματισμού.

2. Το σύμβολο | δηλώνει συνένωση



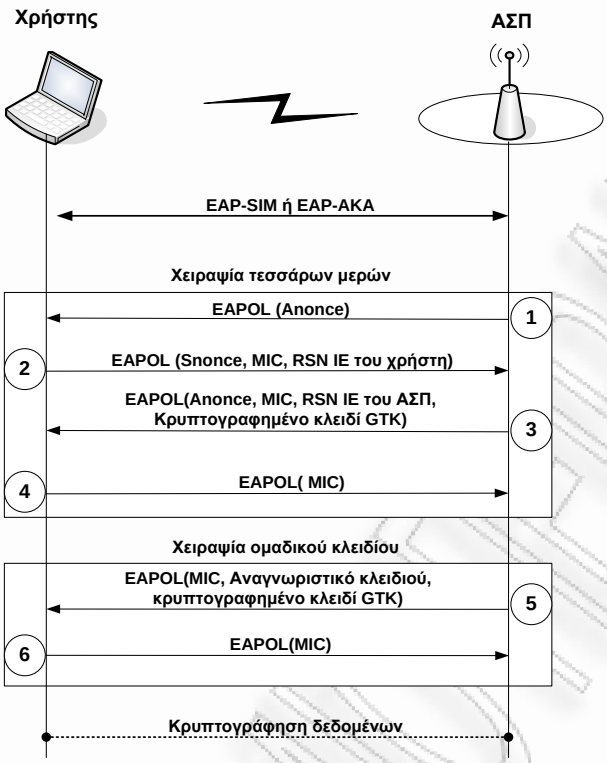
Σχήμα 2.1.3.1: Ιεραρχία κλειδιών στο IEEE 802.11i

Αφού λάβει αυτό το μήνυμα, το ΑΣΠ υπολογίζει το κλειδί PTK και τα σχετικά κλειδιά (δηλαδή τα κλειδιά KCK, KEK και TK) όπως έκανε προηγουμένως ο χρήστης και μετά επαληθεύει την ακεραιότητα του μηνύματος ελέγχοντας την εγκυρότητα του MIC. Στη συνέχεια, το ΑΣΠ απαντάει με το τρίτο μήνυμα EAPOL, το οποίο περιέχει το Anonce (το οποίο έχει την ίδια τιμή με το πρώτο μήνυμα EAPOL), ένα MIC στο τρίτο μήνυμα EAPOL, το RSN IE του ΑΣΠ και τέλος, το κλειδί GTK, το οποίο χρησιμοποιείται για να προστατεύσει τα μηνύματα ευρυεκπομπής/πολυεκπομπής. Να σημειωθεί ότι το κλειδί GTK μεταφέρεται κρυπτογραφημένο χρησιμοποιώντας το κλειδί KEK.

Όταν λάβει αυτό το μήνυμα, ο χρήστης ελέγχει αν το MIC είναι έγκυρο και συγκρίνει το δικό του RSN IE με το RSN IE που έλαβε από το ΑΣΠ για να εξασφαλιστεί ότι και τα δυο μέρη υποστηρίζουν τους ίδιους αλγόριθμους κρυπτογράφησης. Τέλος, αν όλοι οι έλεγχοι είναι σωστοί, τότε ο χρήστης αποκτά το κλειδί GTK αποκρυπτογραφώντας το με το κλειδί KEK, και στέλνει στο ΑΣΠ το τελευταίο μήνυμα της χειραψίας τεσσάρων μερών, το οποίο περιέχει ένα MIC για το τέταρτο μήνυμα EAPOL. Το μήνυμα αυτό στέλνεται για να ενημερώσει ο χρήστης το ΑΣΠ ότι έχει στην κατοχή του το κλειδί PTK και τα σχετικά κλειδιά KEK, KCK και TK καθώς επίσης και το κλειδί GTK. Το ΑΣΠ, όταν λάβει το τέταρτο μήνυμα EAPOL, ελέγχει την εγκυρότητα του MIC. Αν

αυτός ο τελευταίος έλεγχος είναι σωστός, τότε η χειραψία τεσσάρων μερών έχει ολοκληρωθεί με επιτυχία και τόσο ο χρήστης όσο και το ΑΣΠ μοιράζονται το κλειδί TK και GTK τα οποία προστατεύουν τα μηνύματα μονοεκπομπής και ευρυεκπομπής/πολυεκπομπής αντίστοιχα.

Σε περίπτωση που το ΑΣΠ επιθυμεί να μοιράσει ένα καινούργιο κλειδί GTK στους χρήστες του ΑΤΔ, τότε εκτελείται η χειραψία ομαδικού κλειδιού. Όπως φαίνεται στο Σχήμα 2.1., το ΑΣΠ πρώτα στέλνει ένα μήνυμα EAPOL, το οποίο περιέχει ένα MIC που υπολογίζεται από το μήνυμα EAPOL χρησιμοποιώντας το κλειδί KCK και το αναγνωριστικό (identifier) του κλειδιού GTK. Επίσης, περιέχει και το νέο κλειδί GTK, το οποίο είναι κρυπτογραφημένο χρησιμοποιώντας το κλειδί KEK. Υπενθυμίζουμε ότι τόσο ο χρήστης όσο και το ΑΣΠ έχουν στην κατοχή τους τα κλειδιά KEK και KCK τα οποία δημιουργήθηκαν στη χειραψία τεσσάρων μερών. Ο χρήστης όταν λάβει το προηγούμενο μήνυμα, εφαρμόζει το κλειδί KCK για να εξακριβώσει την εγκυρότητα του MIC και έπειτα αποκρυπτογραφεί το κλειδί GTK χρησιμοποιώντας το κλειδί KEK. Τέλος, ο χρήστης απαντάει στο ΑΣΠ με ένα μήνυμα EAPOL, το οποίο περιέχει ένα MIC με το οποίο γνωστοποιεί το ΑΣΠ ότι έχει στην κατοχή του το καινούργιο κλειδί GTK. Όταν το ΑΣΠ λάβει το μήνυμα αυτό θα ελέγξει κατά τα γνωστά την εγκυρότητα της τιμής MIC. Αν αυτός ο τελευταίος έλεγχος είναι σωστός, τότε η χειραψία ομαδικού κλειδιού έχει ολοκληρωθεί με επιτυχία και ο χρήστης κρυπτογραφεί τα μηνύματα ευρυεκπομπής/πολυεκπομπής, χρησιμοποιώντας το καινούργιο κλειδί GTK.



Σχήμα 2.1.3.2: Χειραψία τεσσάρων μερών και χειραψία ομαδικού κλειδιού

ΚΕΦΑΛΑΙΟ 3

UMTS

3.1 Ιδιωτικότητα και Ασφάλεια στα δίκτυα UMTS

Η αυθεντικοποίηση στα δίκτυα UMTS είναι μια διαδικασία αίτησης – απόκρισης κατά την όποια η κάρτα USIM του MS ζήτα από το οικείο δίκτυο του να παράγει και να του αποστείλει διαπιστευτήρια αυθεντικοποίησης, τα οποία ονομάζονται 3G διανύσματα αυθεντικοποίησης. Για την αποφυγή επιθέσεων επανάληψης, η 3GPP έχει υιοθετήσει έναν ειδικό μηχανισμό, ο οποίος εξασφαλίζει ότι κάθε διάνυσμα αυθεντικοποίησης μπορεί να χρησιμοποιηθεί μόνο μια φορά. Για να επιτευχτεί αυτό, το οικείο δίκτυο διατηρεί ένα μετρητή SQN_{HE} με το οποίο παράγεται ένας αύξων αριθμός ακολουθίας SEQ, το οποίο είναι μοναδικό ανά διάνυσμα αυθεντικοποίησης. Ο αριθμός ακολουθίας SEQ αποστέλλεται μαζί με το διάνυσμα αυθεντικοποίησης στον κινητό σταθμό(MS). Από την άλλη πλευρά, η κάρτα USIM διατηρεί το μεγαλύτερο αριθμό ακολουθίας που έχει λάβει από το οικείο δίκτυο.

Όταν η κάρτα USIM λάβει ένα διάνυσμα αυθεντικοποίησης, ελέγχει αν το ληφθέν SEQ είναι μεγαλύτερο από το αντίστοιχο αποθηκευμένο στην κάρτα USIM. Αν είναι μεγαλύτερο, τότε αυτό σημαίνει ότι το διάνυσμα αυθεντικοποίησης δεν έχει ξαναχρησιμοποιηθεί στο παρελθόν. Έτσι, η κάρτα USIM δέχεται το διάνυσμα αυθεντικοποίησης και αποθηκεύει τον αριθμό ακολουθίας SEQ που έλαβε, το οποίο θα χρησιμοποιηθεί για τον επόμενο έλεγχο που θα γίνει. Σε αντίθετη περίπτωση, η κάρτα USIM απορρίπτει το διάνυσμα αυθεντικοποίησης, καθώς θεώρει ότι έχει ξαναχρησιμοποιηθεί στο παρελθόν και αρχικοποιεί μια διαδικασία επανα-συγχρονισμού. Στη διαδικασία αυτή, το οικείο δίκτυο παράγει καινούργια διανύσματα αυθεντικοποίησης, αφού πρώτα γίνει ένας έλεγχος της τιμής του μετρητή του οικείου δικτύου. Είναι φανερό ότι η διαδικασία επανα-συγχρονισμού προκαλεί σημαντικές καθυστερήσεις στη διαδικασία αυθεντικοποίησης του MS. Ιδιαίτερα στην περίπτωση που το MS έχει μια ενεργή σύνδεση πραγματικού χρόνου (VoIP, video conference), η εκτέλεση της διαδικασίας επανα-

συγχρονισμού μπορεί να προκαλέσει τον πρόωρο τερματισμό της σύνδεσης του MS.

Αν και ο παραπάνω μηχανισμός προσφέρει σημαντική προστασία από επιθέσεις επανάληψης, η 3GPP έχει αναγνωρίσει περιπτώσεις, στις οποίες το διάνυσμα αυθεντικοποίησης που θα λάβει το MS μπορεί να περιέχει ένα αριθμό ακολουθίας SEQ, το οποίο να είναι μικρότερο από το αποθηκευμένο αριθμό ακολουθίας στην κάρτα USIM του MS, χωρίς ωστόσο το συγκεκριμένο διάνυσμα αυθεντικοποίησης να έχει χρησιμοποιηθεί στο παρελθόν. Η περίπτωση αυτή ονομάζεται εσφαλμένος συγχρονισμός (false synchronization). Δυστυχώς, και στην περίπτωση αυτή η κάρτα USIM απορρίπτει το διάνυσμα αυθεντικοποίησης και εκτελεί τη χρονοβόρα διαδικασία επανα-συγχρονισμού. Για την αντιμετώπιση των εσφαλμένων συγχρονισμών, η 3GPP προτείνει η κάρτα USIM να αποθηκεύει α το πλήθος προηγούμενους αριθμούς ακολουθίας SEQ που έχει λάβει από το οικείο δίκτυο για να δέχεται τιμές του SEQ που είναι εκτός εμβέλειας έως α μονάδες. Η παράμετρος α την οποία ονομάζουμε offset έχει μια προεπιλεγμένη σταθερή τιμή και αποτελεί ένα «παράθυρο» ανοχής στους εσφαλμένους συγχρονισμούς.

Ωστόσο, όπως θα μελετήσουμε σε αυτό το κεφάλαιο, η χρήση μιας σταθερής τιμής του offset α δεν αποτελεί τη βέλτιστη λύση για την αποτελεσματική μείωση των εσφαλμένων συγχρονισμών στα ενοποιημένα δίκτυα 3G-WLAN. Σε αυτά τα δίκτυα το MS έχει τη δυνατότητα να περιάγει από το δίκτυο 3G στο WLAN και αντίστροφα για να έχει την καλύτερη δυνατή σύνδεση στο διαδίκτυο ή στις 3G υπηρεσίες. Η συχνή περιαγωγή μεταξύ των δικτύων έχει ως αποτέλεσμα να μεγαλώνει η απόκλιση των αριθμών ακολουθιών SEQ τα οποία αποστέλλονται στο MS από την κανονική τους διάταξη με άμεση συνέπεια την αύξηση των εσφαλμένων συγχρονισμών. Αν και η προφανή λύση θα ήταν η τιμή του offset α να ήταν αρκετά μεγάλη για να έχουμε μεγάλο περιθώριο ανοχής στα σφάλματα συγχρονισμού, θα αποδείξουμε σε επόμενο κεφάλαιο πως η παράμετρος offset α συνδέεται με την πιθανότητα εκδήλωσης μιας συγκεκριμένης επίθεσης στα

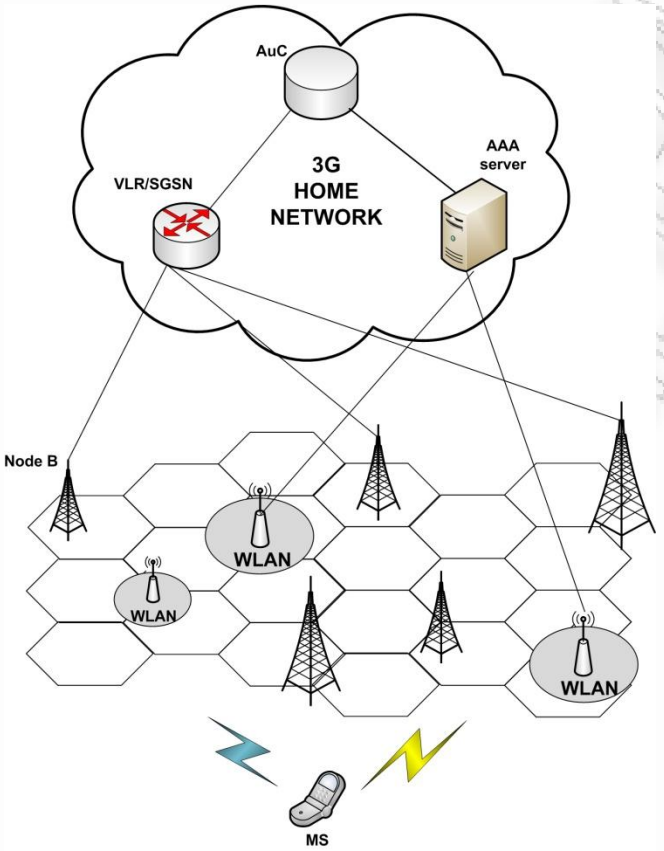
ενοποιημένα δίκτυα 3G-WLAN, η οποία ονομάζεται επίθεση ψεύτικου σημείου πρόσβασης.

3.2 Αρχιτεκτονική ενοποιημένων δικτύων 3G-WLAN

Το Σχήμα 3. παρουσιάζει μια απλοποιημένη αρχιτεκτονική ενοποιημένων δικτύων 3G-WLAN. Να σημειωθεί ότι το σχήμα αυτό είναι παρόμοιο με το Σχήμα 1. που αναλύθηκε στο Κεφάλαιο 1. Ωστόσο, για λόγους πληρότητας κρίνεται σκόπιμη η ανάλυση των πιο σημαντικών στοιχείων του, η κατανόηση των οποίων είναι απαραίτητη για τη συνέχιση του κεφαλαίου. Η ενοποιημένη αρχιτεκτονική δικτύων 3G-WLAN αποτελείται από τρία μέρη (βλ. Σχήμα 3.): (1) το MS (Mobile Station), (2) το ασύρματο δίκτυο πρόσβασης, και, 3) το δίκτυο κορμού 3G. Το MS αποτελείται από την συσκευή του χρήστη (π.χ. φορητός υπολογιστής, PDA) και την κάρτα USIM. Η συσκευή του MS διαθέτει δυο ξεχωριστές διεπαφές: μια διεπαφή UMTS και μια διεπαφή WLAN. Από την άλλη πλευρά, το ασύρματο δίκτυο πρόσβασης προσφέρει την ασύρματη σύνδεση του MS με το δίκτυο κορμού 3G. Αποτελείται από πολλαπλά Node B τα οποία συνδέονται με τον κόμβο RNC (Radio Network Controller). Επίσης, το ασύρματο δίκτυο πρόσβασης περιέχει και τα ασύρματα σημεία πρόσβασης AP των δικτύων WLAN. Τέλος, το δίκτυο κορμού 3G περιέχει τον κόμβο SGSN, το οποίο υποστηρίζει την κινητικότητα και τις ενεργές συνδέσεις του MS, και το AAA server, το οποίο προσφέρει υπηρεσίες αυθεντικοποίησης, εξουσιοδότησης και λογιστικής. Όπως φαίνεται στο Σχήμα 3., ένα SGSN συνδέεται με πολλαπλά RNC, ενώ ένα AAA server συνδέεται με πολλαπλά AP. Τόσο το SGSN όσο και το AAA server συνδέονται με τη βάση δεδομένων Home Subscriber Server/Authentication Center (HSS/AuC), η οποία περιέχει τα διαπιστευτήρια αυθεντικοποίησης του MS. Να σημειωθεί ότι η περιοχή κάλυψης των κόμβων Node B τα οποία είναι συνδεμένα στο ίδιο SGSN (μέσω των RNC) ονομάζεται περιοχή κάλυψης SGSN.

Όταν το MS θέλει να πραγματοποιήσει μια σύνδεση είτε με το δίκτυο 3G είτε με το δίκτυο WLAN, θα πρέπει πρώτα να εκτελέσει μια διαδικασία αυθεντικοποίησης. Πιο συγκεκριμένα, όταν το MS θέλει να συνδεθεί με το δίκτυο 3G, θα πρέπει να εκτελέσει τη διαδικασία αυθεντικοποίησης UMTS-AKA. Από

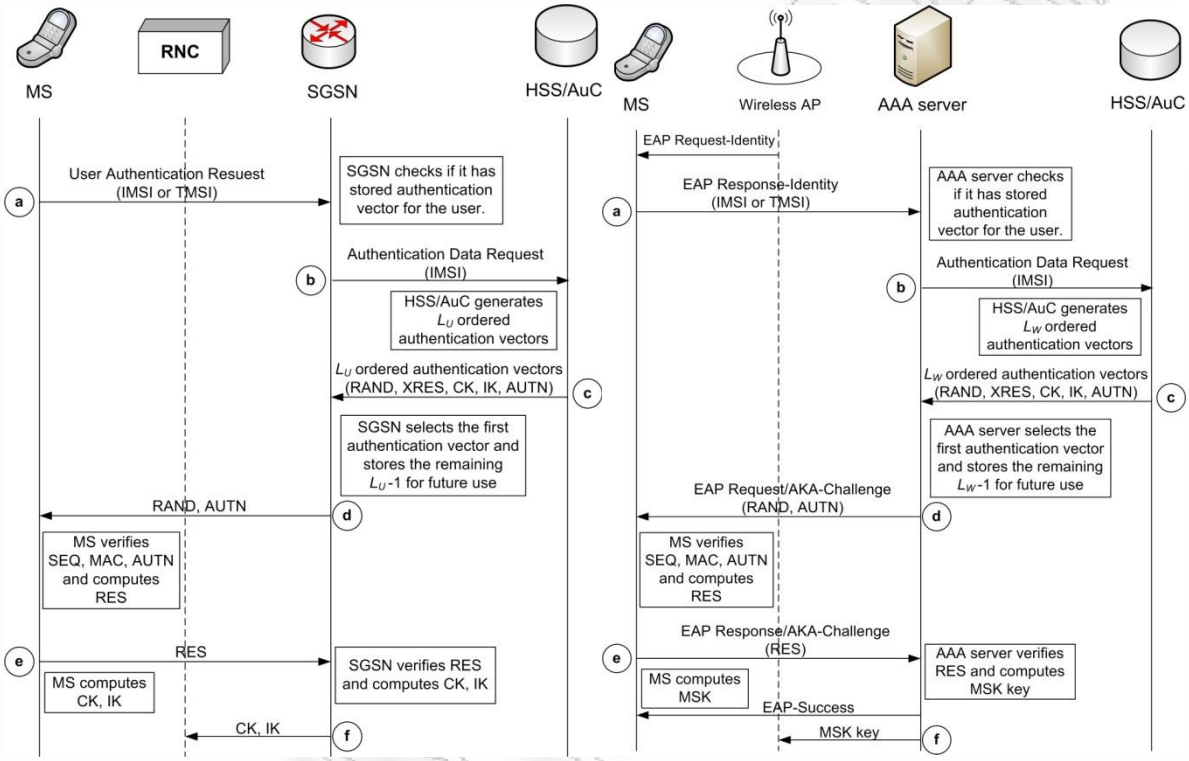
την άλλη πλευρά, αν το MS βρεθεί σε μια περιοχή κάλυψης WLAN, θα πρέπει να εκτελέσει τη διαδικασία αυθεντικοποίησης EAP-AKA. Στη συνέχεια αναλύουμε αυτές τις δυο διαδικασίες αυθεντικοποίησης.



Σχήμα 3.2.1: Απλοποιημένη αρχιτεκτονική ενοποιημένων δικτύων 3G-WLAN

3.2.1 Διαδικασία αυθεντικοποίησης UMTS-AKA

Η διαδικασία UMTS-AKA παρέχει αμοιβαία αυθεντικοποίηση μεταξύ του MS και του δικτύου UMTS, βασιζόμενη στην κοινή γνώση ενός μυστικού κλειδιού K, το οποίο είναι αποθηκευμένο στην κάρτα USIM του MS και στη βάση δεδομένων HSS/AuC.



(α) (β)

Σχήμα 3.2.1.1: (α) Η διαδικασία αυθεντικοποίησης UMTS-AKA και (β) Η διαδικασία αυθεντικοποίησης EAP-AKA

Η διαδικασία αυθεντικοποίησης UMTS-AKA λαμβάνει χώρα ως εξής: αρχικά το MS αρχικοποιεί ένα αίτημα αυθεντικοποίησης UAR (User Authentication Request) κατά την οποία στέλνει τη μόνιμη ταυτότητα IMSI ή μια προσωρινή ταυτότητα TMSI στο κόμβο SGSN (βλ. Σχήμα 3.2.(α) – βήμα 1). Ο τελευταίος εξετάζει αν έχει αποθηκευμένα διανύσματα αυθεντικοποίησης για το συγκεκριμένο MS. Αν έχει τότε στέλνει το διάνυσμα αυθεντικοποίησης πίσω στο MS για να συνεχιστεί η διαδικασία αυθεντικοποίησης. Ωστόσο, αν το SGSN/VLR δεν έχει αποθηκευμένο κάποιο διάνυσμα αυθεντικοποίησης, τότε

αυτό εκτελεί ένα αίτημα αυθεντικοποίησης διανυσμάτων AVR (Authentication Vector Request) με το HSS/AuC. Στη διαδικασία αυτή, το SGSN στέλνει τη μόνιμη ταυτότητα IMSI του MS στο HSS/AuC. Το τελευταίο χρησιμοποιώντας τη μόνιμη ταυτότητα IMSI του MS ανακτά το μόνιμο κλειδί K και παράγει L_U το πλήθος διαφορετικά διανύσματα αυθεντικοποίησης σε διαταγμένη σειρά. Κάθε διάνυσμα αυθεντικοποίησης αποτελείται από έναν τυχαίο αριθμό RAND, μια αναμενόμενη απάντηση XRES (eXpected RESponse), το κλειδί κρυπτογράφησης CK, το κλειδί ακεραιότητας IK και το κουπόνι αυθεντικοποίησης AUTN (Authentication Token).

Για την υποστήριξη του μηχανισμού προστασίας από επιθέσεις επανάληψης, κάθε διάνυσμα αυθεντικοποίησης που παράγεται περιέχει έναν αύξων αριθμό ακολουθίας SEQ, ο οποίος είναι μοναδικός ανά διάνυσμα αυθεντικοποίησης. Η 3GPP έχει προτείνει δύο διαφορετικές μεθόδους παραγωγής αριθμών ακολουθίας SEQ με την προαναφερθέν ιδιότητα: (α) χρήση χρονοσφραγίδων (timestamps) και (β) χρήση μετρητών (counters). Για την υλοποίηση της πρώτης μεθόδου απαιτείται η κάρτα USIM και το HSS/AuC να διατηρούν συγχρονισμένα ρολόγια, γεγονός το οποίο αυξάνει σημαντικά την πολυπλοκότητα της μεθόδου**.** Σε αυτό το κεφάλαιο μελετάται μόνο η δεύτερη μέθοδος (δηλ. χρήση μετρητών). Στη μέθοδο αυτή, οι αριθμοί ακολουθίας SEQ παίρνουν τιμές από έναν μετρητή SQN_{HE}, ο οποίος διατηρείται από το HSS/AuC και αυξάνεται κατά 1 μονάδα για κάθε ένα διάνυσμα αυθεντικοποίησης που παράγεται.

Επίσης, η κάρτα USIM δέχεται τιμές του SEQ που είναι εκτός εμβέλειας έως α μονάδες. Για την υλοποίηση αυτού του μηχανισμού, η 3GPP προτείνει τη χρήση πινάκων στη κάρτα USIM (array mechanism). Πιο συγκεκριμένα, η κάρτα USIM διατηρεί έναν πίνακα SEQ_{MS} για την αποθήκευση α τιμών αριθμών ακολουθίας SEQ που έχουν γίνει αποδεκτά από προηγούμενες αυθεντικοποιήσεις. Η παράμετρος α ονομάζεται offset. Χρησιμοποιούμε το συμβολισμό $SEQ_{MS}(i)$, για να υποδηλώσουμε τη τιμή του πίνακα SEQ_{MS} στη θέση i ($0 \leq i \leq \alpha - 1$). Επίσης, το HSS/AuC παρακολουθεί το μετρητή IND_{HE}, ο

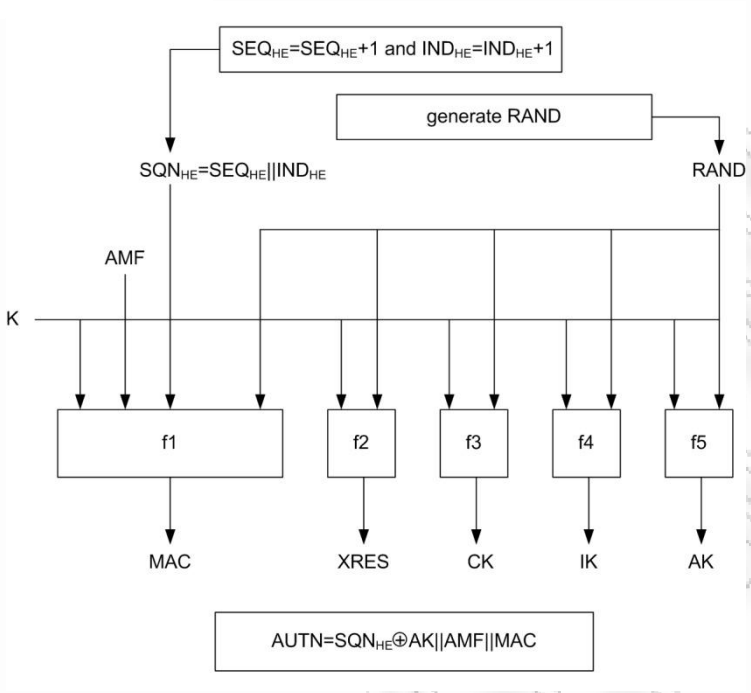
οποίος αυξάνεται κατά μια μονάδα για κάθε διάνυσμα αυθεντικοποίησης που παράγεται και παίρνει τιμές από 0 έως α-1.

Η διαδικασία που ακολουθεί το HSS/AuC για την παραγωγή ενός διανύσματος αυθεντικοποίησης είναι η εξής (βλ. Σχήμα 3.2.1.2): Αρχικά, το HSS/AuC αυξάνει κατά μια μονάδα τους μετρητές SEQ_{HE} και IND_{HE}. Έστω SEQ και IND οι καινούργιες τιμές των μετρητών SEQ_{HE} και IND_{HE}. Στη συνέχεια, το HSS/AuC υπολογίζει την παράμετρο SQN ως εξής:

$$SQN = SEQ \;||\; IND$$

Το HSS/AuC παράγει επίσης έναν τυχαίο αριθμό RAND και χρησιμοποιώντας το μυστικό κλειδί K και τις μονόδρομες συναρτήσεις κατακερματισμού f_1, f_2, f_3, f_4, f_5 υπολογίζει τις εξής παραμέτρους:

1. Τον κώδικα αυθεντικοποίησης μηνυμάτων $MAC = f_1(SQN||RAND||AMF)$, όπου το πεδίο AMF (Authentication and key Management Field) χρησιμοποιείται για να γνωστοποιήσει στην κάρτα USIM την τιμή κάποιας παραμέτρου η οποία αλλάζει δυναμικά.
2. Την αναμενόμενη απάντηση $XRES = f_2(RAND)$ Το κλειδί κρυπτογράφησης $CK = f_3(RAND)$
3. Το κλειδί ακεραιότητας $IK = f_4(RAND)$
4. Το κλειδί ανωνυμίας $AK = f_5(RAND)$.
5. Το κουπόνι αυθεντικοποίησης, $AUTN = SQN\ (XOR)\ AK||AMF||MAC$



Σχήμα 3.2.1.2: Διαδικασία παραγωγής διανυσμάτων αυθεντικοποίησης

Η διαδικασία αυτή επαναλαμβάνεται L_U φόρες για την αντίστοιχη παραγωγή L_U διαφορετικών διανυσμάτων αυθεντικοποίησης. Έπειτα το HSS/AuC προωθεί στο SGSN τα L_U διανύσματα αυθεντικοποίησης σε διατεταγμένη σειρά με βάση τον αριθμό ακολουθίας SEQ που περιέχουν. Όταν το SGSN λάβει τα L_U διανύσματα αυθεντικοποίησης, επιλέγει το πρώτο διάνυσμα αυθεντικοποίησης από τη διαταγμένη σειρά και διαβιβάζει τις παραμέτρους RAND και AUTN στο MS, ενώ αποθηκεύει τα υπόλοιπα $L_U - 1$ για μελλοντική χρήση.

Το MS όταν λάβει το ζεύγος (RAND, AUTN), τις προωθεί στην κάρτα USIM, η οποία, χρησιμοποιώντας το μυστικό κλειδί K υπολογίζει αρχικά το κλειδί AK καθώς $AK = f_5(RAND)$, και στη συνέχεια ανακτά από το κουπόνι αυθεντικοποίησης AUTN την παράμετρο $SQN = (SQN\ (XOR)\ AK)\ (\mathrm{XOR})\ AK$. Από το SQN η κάρτα USIM ανακτά τον αριθμό ακολουθίας SEQ που παρήχθη από το HSS/AuC για το συγκεκριμένο διάνυσμα αυθεντικοποίησης καθώς και

την παράμετρο IND. Όπως αναφέρθηκε προηγουμένως, η κάρτα USIM διατηρεί τον πίνακα SEQ_{MS} το οποίο περιέχει α προηγούμενες τιμές αριθμών ακολουθίας SEQ, που έχουν γίνει αποδεκτά. Η κάρτα USIM χρησιμοποιώντας το IND ελέγχει αν SEQ_{MS} (IND) < SEQ. Αν ναι, τότε η κάρτα USIM δέχεται το διάνυσμα αυθεντικοποίησης, καθώς θεωρεί ότι δεν έχει ξαναχρησιμοποιηθεί και αποθηκεύει το ληφθέν αριθμό ακολουθίας στη θέση i=IND του πίνακα SEQ_{MS} (δηλ. $SEQ_{MS}(i)=SEQ$). Σε διαφορετική περίπτωση (δηλ. SEQ_{MS} (i) > SEQ), η κάρτα USIM απορρίπτει το διάνυσμα αυθεντικοποίησης και αρχικοποιεί τη διαδικασία επανα-συγχρονισμού. Στη διαδικασία αυτή, το SGSN διαγράφει τα αποθηκευμένα διανύσματα αυθεντικοποίησης για τον συγκεκριμένο MS (εφόσον διαθέτει) και εκτελεί μια διαδικασία AVR, για να παραλάβει καινούργια διανύσματα αυθεντικοποίησης από το HSS/AuC.

Στην περίπτωση που η κάρτα USIM δεχτεί το διάνυσμα αυθεντικοποίησης, τότε συνεχίζει τη διαδικασία αυθεντικοποίησης υπολογίζοντας το $XMAC = f_1(SQN||RAND||AMF)$ και το *AUTN'*. Αν *AUTN'=AUTN*, τότε η κάρτα USIM θεωρεί ότι το δίκτυο UMTS κατέχει το μόνιμο κλειδί K και επομένως είναι αυθεντικό. Έπειτα, η κάρτα USIM υπολογίζει την τιμή $XRES = f_2(RAND)$ και το προωθεί στο MS για να το αποστείλει στο SGSN. Παράλληλα, η κάρτα USIM υπολογίζει τα κλειδιά $CK = f_3(RAND)$ και $IK = f_4(RAND)$. Μόλις το SGSN λάβει το *RES*, εξετάζει αν RES=XRES. Εάν ισχύει ο τελευταίος αυτός έλεγχος, τότε η αυθεντικοποίηση του MS ολοκληρώνεται με επιτυχία, καθώς το δίκτυο θεωρεί ότι το MS κατέχει το μόνιμο κλειδί K. Στην τελική φάση του UMTS-AKA, η κάρτα USIM και το SGSN μεταφέρουν στο MS και στον κόμβο RNC αντίστοιχα τα συμφωνημένα κλειδιά CK και IK. Τα κλειδιά αυτά παρέχουν υπηρεσίες εμπιστευτικότητας και ακεραιότητας στην ασύρματη διεπαφή του δικτύου UMTS.

3.2.2 Διαδικασία αυθεντικοποίησης EAP- AKA

Όπως αναφέρθηκε πριν, όταν το MS επιθυμεί να χρησιμοποιήσει το δίκτυο WLAN, πρέπει να εκτελέσει τη διαδικασία αυθεντικοποίησης EAP-AKA με την ίδια κάρτα USIM που χρησιμοποιείται για τη διαδικασία αυθεντικοποίησης UMTS-AKA. Όπως φαίνεται από το Σχήμα 3.2.(β), οι οντότητες που συμμετέχουν στο EAP-AKA είναι: (α) το MS, (β) το AP, (γ) το AAA server, και (δ) το HSS/AuC. Η διαδικασία αυθεντικοποίησης EAP-AKA έχει ήδη αναλυθεί στο ΚΕΦΑΛΑΙΟ 2 και δεν θα μιλήσουμε περεταίρω για αυτήν. Επισημαίνουμε μόνο το γεγονός ότι όταν το AAA server εκτελέσει μια διαδικασία AVR, τότε το HSS/AuC θα παράγει και θα στείλει πίσω στο AAA server L_W διατεταγμένα διανύσματα αυθεντικοποίησης. Να σημειωθεί ότι το L_W δεν είναι υποχρεωτικά ίσο με το L_U της διαδικασίας UMTS-AKA.

ΚΕΦΑΛΑΙΟ 4
Το Πρόβλημα των Εσφαλμένων Συγχρονισμών

4.1 Εισαγωγή

Ο σκοπός αυτού του κεφαλαίου είναι να προσφέρει μια ολοκληρωμένη μελέτη για το φαινόμενο των εσφαλμένων συγχρονισμών στα ενοποιημένα δίκτυα 3G-WLAN. Αφού μελετήσαμε τα πρωτόκολλα και τις διαδικασίες που απαιτούνται είμαστε σε θέση πιο συγκεκριμένα, να προτείνουμε και αναπτύξουμε ένα μοντέλο προσομοίωσης που περιγράφει τη δυναμική συμπεριφορά ενός κινητού κόμβου(MS) που περιάγετε στα ενοποιημένα δίκτυα 3G-WLAN. Το μοντέλο προσομοίωσης, μας επιτρέπει να υπολογίσουμε την πιθανότητα εσφαλμένων συγχρονισμών καθώς και τη μέση τιμή συγχρονισμών σε σχέση με το ρυθμό αυθεντικοποίησης και την κινητικότητα του MS. Επίσης, στο κεφάλαιο αυτό θα τεκμηριώσουμε ότι η αύξηση της τιμής του α ενδέχεται να έχει αρνητική επίδραση στο επίπεδο ασφάλειας των ενοποιημένων δικτύων 3G-WLAN καθώς αυξάνει την πιθανότητα εκδήλωσης επίθεσης ψεύτικου σημείου πρόσβασης (AP).

Το κεφάλαιο αυτό ολοκληρώνεται με την ανάλυση της βέλτιστης στρατηγικής για το MS το οποίο θα βασίζεται στη δυναμική προσαρμογή της τιμής του offset α για να επιτευχτεί μια χρυσή τομή μεταξύ ασφάλειας και απόδοσης. Συνολικά, οι συνεισφορές αυτού του κεφαλαίου είναι οι εξής:

- Περιγραφή και ανάλυση του φαινομένου των εσφαλμένων συγχρονισμών στα ενοποιημένα δίκτυα 3G-WLAN.
- Ανάπτυξη ενός μοντέλου προσομοίωσης για τον υπολογισμό της πιθανότητας εσφαλμένου συγχρονισμού και της μέσης τιμής εσφαλμένων συγχρονισμών.
- Ανάλυση της επίθεσης ψεύτικου σημείου πρόσβασης AP και μελέτη της επιρροής του offset α σε αυτήν.
- Βέλτιστη στρατηγική για την επιλογή της τιμής του α στα ενοποιημένα δίκτυα 3G-WLAN.

4.2 Εσφαλμένοι Συγχρονισμοί

Σε αυτήν την ενότητα περιγράφουμε το πρόβλημα των εσφαλμένων συγχρονισμών με τη χρήση ενός αριθμητικού παραδείγματος για την καλύτερη κατανόηση του. Υποθέτουμε πως ένα συγκεκριμένο MS περιάγετε μεταξύ των δικτύων UMTS και WLAN στην ευρύτερη περιοχή κάλυψης ενός SGSN, εκτελώντας διαδικασίες αυθεντικοποίησης UMTS-AKA ή EAP-AKA αντίστοιχα. Θεωρούμε ότι το πλήθος L_U και L_W των διανυσμάτων αυθεντικοποίησης UMTS και WLAN είναι 6 και 4 αντίστοιχα, ενώ η τιμή του offset α είναι 7 (δηλ. $L_U = 6,\ L_W = 4,\ \alpha = 7$). Αρχικά, το SGSN και το AAA server δεν έχουν κανένα αποθηκευμένο διάνυσμα αυθεντικοποίησης για το συγκεκριμένο MS, ενώ ο πίνακας SEQ_{MS} είναι κενός. Επίσης, η τιμή του μετρητή SEQ_{HE} είναι ίση με 1 (δηλ. SEQ_{HE}=1), ενώ η τιμή του μετρητή IND_{HE} είναι ίση με 0 (δηλ. IND_{HE}=0). Όπως αναλύθηκε στην ενότητα 3.2.1, κάθε διάνυσμα αυθεντικοποίησης που παράγεται από το HSS/AuC περιέχει την παράμετρο SQN, το οποίο αποτελείται από το SEQ_{HE} και IND_{HE}. Για αυτό το λόγο, χρησιμοποιούμε το συμβολισμό SQN=α||β, για να υποδηλώσουμε ότι η παράμετρος SQN αποτελείται από το SEQ_{HE} =α και IND_{HE}=β.

Υποθέτουμε ότι αρχικά το MS βρίσκεται στο δίκτυο 3G και τη χρονική στιγμή t_0, αρχικοποιεί μια διαδικασία αυθεντικοποίησης UMTS-AKA. Καθώς το SGSN δεν έχει κανένα διάνυσμα αυθεντικοποίησης εκτελεί ένα AVR με το AuC. Το τελευταίο παράγει $L_U = 6$ διανύσματα αυθεντικοποίησης. Καθώς ισχύει αρχικά ότι SEQ_{HE}=0 και IND_{HE}=0, τα παραγόμενα διανύσματα αυθεντικοποίησης περιέχουν τους αριθμούς ακολουθίας SQN=1||0, SQN=2||1, SQN=3||2, SQN=4||3, SQN=5||4, SQN=6||5. Να σημειωθεί ότι μετά την παραγωγή αυτών των διανυσμάτων αυθεντικοποίησης ισχύει ότι SEQ_{HE}=7 και IND_{HE}=6. Στη συνέχεια, το HSS/AuC αποστέλλει στο SGSN τα $L_U = 6$ διανύσματα αυθεντικοποίησης. Το SGSN διαλέγει το πρώτο από τα L_U διατεταγμένα διανύσματα αυθεντικοποίησης (δηλ. το διάνυσμα αυθεντικοποίησης με

SQN=1||0) και αποστέλλει το (RAND,AUTN) στο MS, ενώ αποθηκεύει τα υπόλοιπα 5 διανύσματα για μελλοντική χρήση. Η κάρτα USIM δέχεται το ληφθέν (RAND, AUTN) και αποθηκεύει στη θέση 0 του πίνακα των αριθμών ακολουθίας που διατηρεί το SEQ=1 (δηλ. $SEQ_{MS}(0)=1$). Το MS τη χρονική στιγμή t_1 εκτελεί ξανά μια διαδικασία αυθεντικοποίησης UMTS-AKA. Το SGSN δε χρειάζεται να εκτελέσει διαδικασία AVR, καθώς διαθέτει πλέον αποθηκευμένα διανύσματα αυθεντικοποίησης και αποστέλλει στο MS το (RAND, AUTN) με SQN=2||1. Η κάρτα USIM δέχεται το ληφθέν (RAND, AUTN) και αποθηκεύει στη θέση 1 του πίνακα των αριθμών ακολουθίας που διατηρεί το SEQ=2 (δηλ. $SEQ_{MS}(1)=2$). Υποθέτουμε ότι στη συνέχεια το MS πραγματοποιεί 4 διαδοχικές διαδικασίες UMTS-AKA και το SGSN αποστέλλει στο MS 4 (RAND, AUTN) με SQN=3||2, SQN=4||3, SQN=5||4, SQN=6||5 αντίστοιχα. Το MS θα δεχτεί όλα τα ληφθέν (RAND, AUTN) και θα αποθηκεύσει τους αντίστοιχους αριθμούς ακολουθίας στο πίνακα SEQ_{MS}. Έστω τώρα ότι το MS τη χρονική στιγμή t_2 εκτελεί ξανά το UMTS-AKA. Καθώς το SGSN δεν έχει πλέον αποθηκευμένα διανύσματα αυθεντικοποίησης, εκτελεί ένα AVR με το AuC. Το τελευταίο παράγει $L_U = 6$ διανύσματα αυθεντικοποίησης με αριθμούς ακολουθίας SQN=7||6, SQN=8||0, SQN=9||1, SQN=10||2, SQN=11||3, SQN=12||4. Μετά την παραγωγή των διανυσμάτων αυθεντικοποίησης ισχύει ότι $SEQ_{HE}=13$ και $IND_{HE}=5$. Κατά τα γνωστά, το SGSN θα στείλει στο MS το (RAND, AUTN) με SQN=7||6. Το MS θα δεχτεί το (RAND, AUTN) και θα αποθηκεύσει τον αριθμό ακολουθίας SEQ=7 (βλ. Πίνακας 4.2.- t_2). Στη συνέχεια, θεωρούμε ότι το MS εκτελεί 3 διαδοχικές διαδικασίες UMTS-AKA και το SGSN απαντά με 3 διαδοχικά (RAND,AUTN) τα οποία περιέχουν τα SQN=8||0, SQN=9||1, SQN=10||2. Το MS κατά τα γνωστά θα δεχτεί όλα τα ληφθέν (RAND, AUTN) και θα αποθηκεύσει τους αντίστοιχους αριθμούς ακολουθίας στο πίνακα SEQ_{MS}. Τη χρονική στιγμή t_3, το MS εκτελεί ξανά το UMTS-AKA και το SGSN αποστέλλει πίσω στο MS το (RAND, AUTN), το οποίο περιέχει το SQN=11||3. Το MS θα δεχτεί το (RAND, AUTN), καθώς ισχύει ότι $SEQ_{MS}(3)=4<SEQ=11$ και θα αποθηκεύσει το SEQ=11 (βλ. Πίνακας 4.2.- t_3).

Μέτα τη χρονική στιγμή t_3, το MS μεταπηδά από το UMTS στο WLAN και στη χρονική στιγμή t_4 εκκινεί το πρωτόκολλο EAP-AKA. Το AAA server

πραγματοποιεί μια διαδικασία AVR με το HSS/AuC, καθώς δε διαθέτει κάποιο διάνυσμα αυθεντικοποίησης για το συγκεκριμένο MS. Με τη σειρά του, το HSS/AuC παράγει $L_W = 4$ διανύσματα αυθεντικοποίησης με αριθμούς ακολουθίας SQN=13||5, SQN=14||6, SQN=15||0, SQN=16||1 και τα παραδίδει πίσω στον AAA server. Μετά την παραγωγή αυτών των διανυσμάτων αυθεντικοποίησης ισχύει ότι SEQ_{HE} =17 και IND_{HE}=2. Στη συνέχεια, το AAA sever αποστέλλει στο MS το (RAND, AUTN) με SQN=13||5. Η κάρτα USIM δέχεται το (RAND, AUTN) καθώς ισχύει ότι $SEQ_{MS}(5)=6<SEQ=13$ (βλ. Πίνακας 4.2.- t_4). Τη χρονική στιγμή t_5 το MS εκτελεί ξανά το EAP-AKA, και το AAA server παραδίδει στο MS το (RAND, AUTN) με SQN=14||6. Κατά τα γνωστά το MS δέχεται το (RAND, AUTN) και αποθηκεύει τον αριθμό ακολουθίας SEQ=14 στη θέση 6 του πίνακα (βλ. Πίνακας 4.2.- t_5).

Μετά τη χρονική στιγμή t_5, το MS επιστρέφει στο δίκτυο UMTS και τη χρονική στιγμή t_6 εκτελεί μια διαδικασία αυθεντικοποίησης UMTS-AKA. Το SGSN διαθέτει αποθηκευμένο ένα διάνυσμα αυθεντικοποίησης με SQN=12||4. Η κάρτα USIM δέχεται το ληφθέν (RAND, AUTN), καθώς ισχύει ότι $SQN_{MS}(4)=5<SEQ=12$ και αποθηκεύει το καινούργιο αριθμό ακολουθίας (βλ. Πίνακας 4.2.- t_6). Τη χρονική στιγμή t_7 το MS εκτελεί ξανά το UMTS-AKA. Το SGSN καθώς δε διαθέτει πλέον αποθηκευμένα διανύσματα αυθεντικοποίησης θα πραγματοποιήσει μια διαδικασία AVR με το AuC. Το τελευταίο θα παράγει $L_U = 6$ διανύσματα αυθεντικοποίησης με αριθμούς ακολουθίας SQN=17||2, SQN=18||3, SQN=19||4, SQN=20||5, SQN=21||6, SQN=22||0 και τα αποστέλλει στον SGSN. Μετά την παραγωγή αυτών των διανυσμάτων αυθεντικοποίησης ισχύει ότι SEQ_{HE} =23 και IND_{HE}=1. Το SGSN θα επιλέξει το πρώτο διάνυσμα αυθεντικοποίησης και θα αποστείλει το (RAND, AUTN) με SQN=17||2 στο MS. Το τελευταίο θα δεχτεί το (RAND, AUTN) καθώς $SQN_{MS}(2)=10<SEQ=17$ (βλ. Πίνακας 4.2.- t_7). Στη συνέχεια, θεωρούμε ότι το MS εκτελεί 4 διαδοχικές διαδικασίες UMTS-AKA, ενώ το SGSN αποστέλλει 4 διαδοχικά (RAND, AUTN) με SQN=18||3, SQN=19||4, SQN=20||5, SQN=21||6 αντίστοιχα. Το MS θα δεχτεί όλα τα ληφθέν (RAND, AUTN) και θα αποθηκεύσει τους αντίστοιχους αριθμούς ακολουθίας στο πίνακα SEQ_{MS}. Έστω ότι τη χρονική στιγμή t_8 το MS εκτελεί άλλη μια φορά το UMTS-AKA και

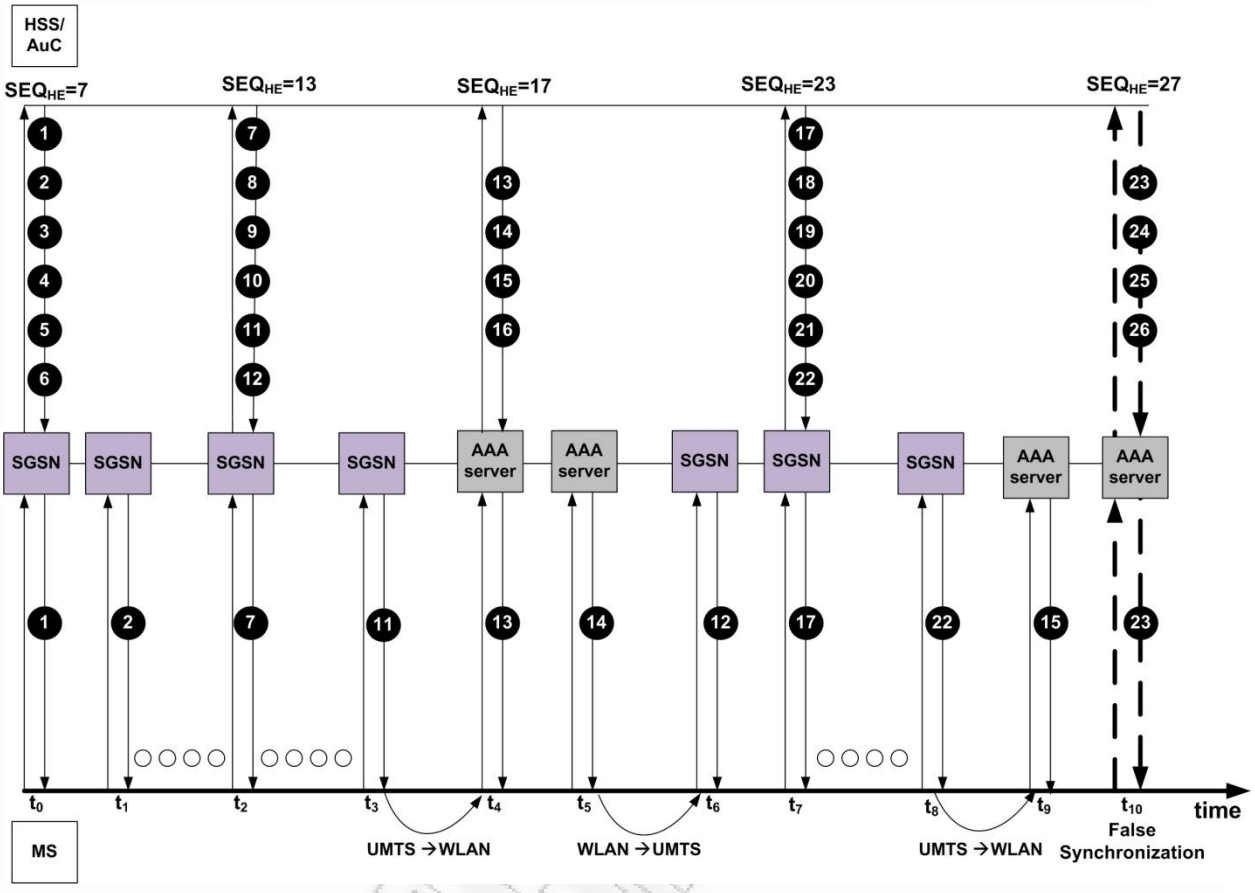
το SGSN αποστέλλει πίσω στο MS το (RAND, AUTN) με SQN=22||0. Το τελευταίο θα δεχτεί το (RAND, AUTN), καθώς ισχύει ότι $SQN_{MS}(0)=8<SEQ=22$ (βλ. Πίνακας 4.2.- t_9).

Μετά τη χρονική στιγμή t_8, το MS μεταπηδά στο WLAN και τη χρονική στιγμή t_9 εκτελεί το πρωτόκολλο EAP-AKA με το AAA server. Το τελευταίο διαθέτει αποθηκευμένο διάνυσμα αυθεντικοποίησης με αριθμό ακολουθίας SQN=15||0. Έτσι, αποστέλλει στο MS το (RAND, AUTN) με SQN=15||0. Σε αυτήν την περίπτωση η κάρτα USIM απορρίπτει το ληφθέν (RAND, AUTN), καθώς ισχύει ότι $SQN_{MS}(0)=22>SEQ=15$. Παρατηρούμε επομένως ότι η κάρτα USIM απορρίπτει το διάνυσμα αυθεντικοποίησης, παρόλο που δεν υπήρχε καμία επίθεση επανάληψης. Το φαινόμενο αυτό ονομάζεται εσφαλμένος συγχρονισμός (false synchronization). Στη συνέχεια, το MS εκτελεί τη διαδικασία επανα-συγχρονισμού, κατά την οποία το SGSN διαγράφει όλα τα αποθηκευμένα διανύσματα αυθεντικοποίησης για το συγκεκριμένο MS και εκκινεί μια διαδικασία AVR με το HSS/AuC. Το τελευταίο κατά τα γνωστά παράγει $L_U = 6$ διανύσματα αυθεντικοποίησης και τα αποστέλλει πίσω στο SGSN και η διαδικασία αυθεντικοποίησης συνεχίζεται κανονικά. Είναι φανερό ότι η διαδικασία επανα-συγχρονισμού προκαλεί σημαντικές καθυστερήσεις στη διαδικασία αυθεντικοποίησης και μπορεί να προκαλέσει τον πρόωρο τερματισμό της τρέχουσας σύνδεσης του MS.

Από την προηγούμενη ανάλυση, είναι φανερό ότι η χρήση μιας σταθερής τιμής του offset α δεν αποτελεί τη βέλτιστη στρατηγική για τη μείωση των εσφαλμένων συγχρονισμών στην περίπτωση των ενοποιημένων δικτύων 3G-WLAN. Η παρατήρηση αυτή απορρέει από το γεγονός ότι στα δίκτυα αυτά το MS έχει τη δυνατότητα να περιάγει από το δίκτυο 3G στο WLAN και αντίστροφα για να έχει την καλύτερη δυνατή σύνδεση στο διαδίκτυο ή στις 3G υπηρεσίες. Η συχνή περιαγωγή μεταξύ των δικτύων έχει ως αποτέλεσμα να μεγαλώνει η απόκλιση των αριθμών ακολουθιών SEQ τα οποία στέλνονται στο MS από την κανονική τους διάταξη, με άμεση συνέπεια την αύξηση των εσφαλμένων συγχρονισμών. Θα πρέπει επίσης να επισημανθεί το γεγονός ότι η ενσωμάτωση των δικτύων WiMAX με τα δίκτυα 3G, ενδέχεται να επιφέρει επιδείνωση του φαινομένου. Η αυθεντικοποίηση στα δίκτυα WiMAX μπορεί να

πραγματοποιηθεί με τις εξής μεθόδους: (α) χρήση του PKM, το οποίο ορίζεται στις προδιαγραφές του WiMAX, (β) χρήση του πρωτοκόλλου EAP-TLS ή EAP-AKA. Στην τελευταία περίπτωση (δηλ. αυθεντικοποίηση με χρήση του EAP-AKA), οι εσφαλμένοι συγχρονισμοί μπορεί να αυξηθούν σημαντικά, καθώς το MS θα περιάγετε μεταξύ τριών διαφορετικών δικτύων (δηλ., UMTS, WiMAX, WLAN), προκαλώντας μεγαλύτερη αναδιοργάνωση των αριθμών ακολουθίας.

Για αυτό το λόγο, η τιμή του offset α θα πρέπει να είναι αρκετά μεγάλη, για να έχουμε μεγάλο περιθώριο ανοχής στα σφάλματα συγχρονισμού των ενοποιημένων δικτύων 3G-WLAN. Ωστόσο, όταν η τιμή του offset α είναι πολύ μεγάλη, τότε αυξάνεται σημαντικά το ρίσκο να πραγματοποιηθεί μια συγκεκριμένη επίθεση στα ενοποιημένα δίκτυα 3G-WLAN, η οποία ονομάζεται επίθεση ψεύτικου σημείου πρόσβασης. Εδώ έγκειται το πρόβλημα να σταλεί από τον επιτιθέμενο, διάνυσμα αυθεντικοποίησης με αριθμό ακολουθίας που δεν θα ακολουθεί την σειρά των πραγματικών διανυσμάτων και όμως να γίνει δεκτό αφού θα είναι μέσα στο περιθώριο(offset α) που έχουμε θέσει για να μην έχουμε επανα-συγχρονισμό. Επομένως, κρίνεται απαραίτητη η δυναμική προσαρμογή της τιμής του offset α στα ενοποιημένα δίκτυα 3G-WLAN, για να επιτευχτεί μια χρυσή τομή μεταξύ ασφάλειας και απόδοσης.



Σχήμα 4.2.1: Χρονικό διάγραμμα

Πίνακας 4.2.2: Αποθηκευμένοι αριθμοί ακολουθίας στην κάρτα USIM

	array SEQ_{MS}						
	0	1	2	3	4	5	6
t_0	1	-	-	-	-	-	-
t_1	1	2	-	-	-	-	-
t_2	1	2	3	4	5	6	7
t_3	8	9	10	11	5	6	7
t_4	8	9	10	11	5	13	7
t_5	8	9	10	11	5	13	14
t_6	8	9	10	11	12	13	14
t_7	8	9	17	11	12	13	14
t_8	22	9	17	18	19	20	21
t_9	**X**	9	17	18	19	20	21
t_{10}	23	9	17	18	19	20	21

ΚΕΦΑΛΑΙΟ 5

ΜΟΝΤΕΛΟΠΟΙΗΣΗ ΔΙΚΤΥΟΥ UMTS-WLAN

5.1 Εισαγωγή

Μέχρι τώρα έχουμε εξηγήσει και περιγράψει κάποιες βασικές έννοιες με τις οποίες ασχολήθηκε η εργασία αυτή. Το κύριο μέρος όμως αφορά στην προσομοίωση με την βοήθεια του OPNET ενός δικτύου που χρησιμοποιεί τα δίκτυα UMTS και WLAN για την λειτουργία του. Το OPNET είναι πρόγραμμα που παρέχει ένα εικονικό περιβάλλον και μοντελοποιεί τη συμπεριφορά ενός ολόκληρου δικτύου, συμπεριλαμβανομένων των δρομολογητών, των διακοπτών, των πρωτοκόλλων, των εξυπηρετητών και των υπηρεσιών του. Δουλεύοντας σε ένα εικονικό περιβάλλον όπως αυτό, είναι δυνατή η εύκολη και έγκαιρη διάγνωση των σχεδιαστικών προβλημάτων και η διόρθωση τους πριν την υλοποίηση του δικτύου στην πραγματικότητα.

Συγκεκριμένα, ασχοληθήκαμε με τον προγραμματισμό και γενικότερα την μοντελοποίηση της λειτουργίας ενός δικτύου, κατά το οποίο διάφοροι χρήστες συνδέονται εναλλάξ με ένα UMTS και ένα WLAN δίκτυο. Σε κάθε σύνδεση χρειάζεται να γίνει αυθεντικοποίηση του χρήστη για την απρόσκοπτη εξυπηρέτηση του από το εκάστοτε δίκτυο. Για τις αυθεντικοποιήσεις αυτές χρειάζεται η επικοινωνία του κάθε δικτύου με το Authentication Center, το οποίο είναι αρμόδιο για την παροχή μοναδικών κωδικών αναγνώρισης για τον κάθε χρήστη. Κάθε κωδικός δεν χρησιμοποιείται δεύτερη φορά. Με αυτόν λοιπόν τον τρόπο μπορούμε να καταλάβουμε αν κάποιος έχει υποκλέψει τον κωδικό που χρησιμοποιήσαμε για να συνδεθεί σε κάποιο από τα δίκτυα. Βγάλαμε λοιπόν συμπεράσματα για τον αριθμό αυτών των υποκλοπών(synchronizations) όταν υπάρχει εναλλαγή κάποιου χρήστη ανάμεσα στα δύο αυτά δίκτυα. Μπορέσαμε να βγάλουμε γραφικές

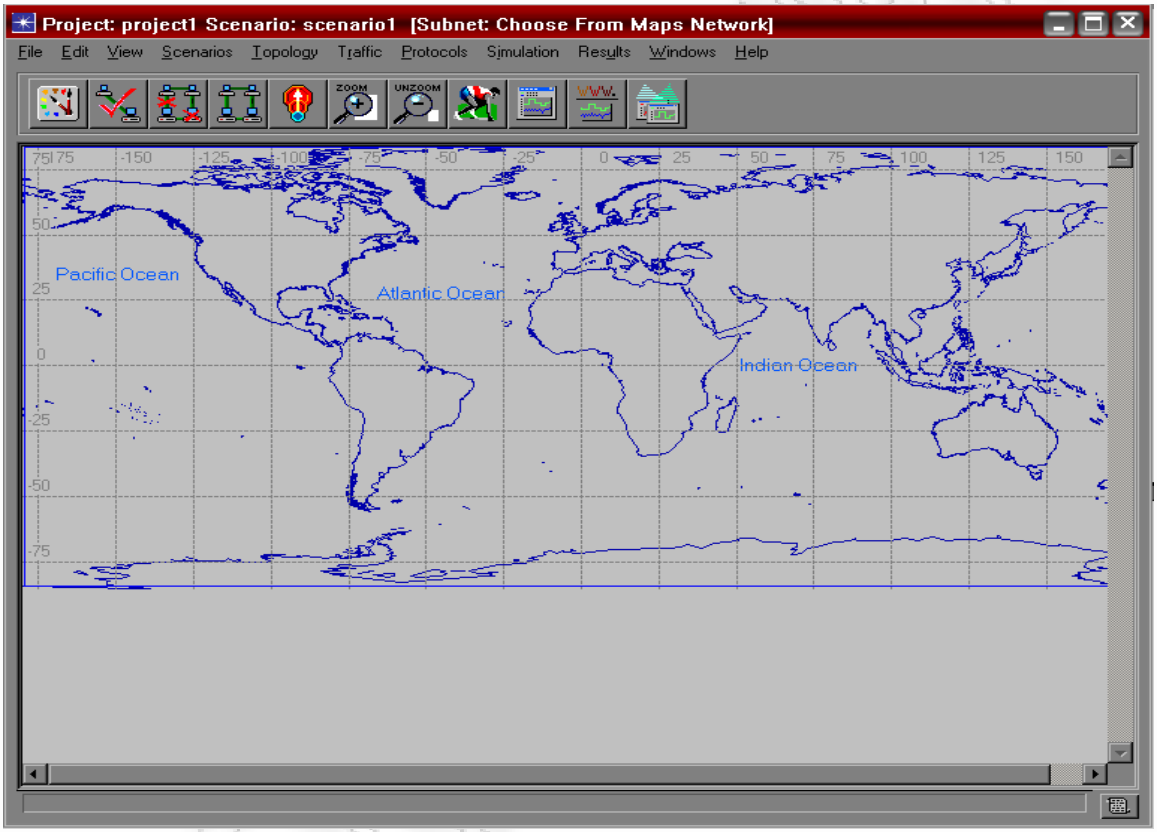
απεικονίσεις που μας βοηθούμε την περεταίρω κατανόηση του προβλήματος ώστε να μπορέσουμε να το επιλύσουμε.

5.2 Περιγραφή OPNET

Πριν ξεκινήσουμε με την αναλυτική περιγραφή του σχεδιασμού της προσομοίωσης θα αναφερθούμε με λίγα λόγια για το OPNET και τις λειτουργίες του. Έχει μια πληθώρα εφαρμογών, οι οποίες στην πλειοψηφία τους δεν θα μας απασχολήσουν. Θα σταθούμε στις σημαντικότερες και ξεκινάμε με τον Project Editor, ο οποίος είναι η κύρια περιοχή στην οποία θα στηθεί το δίκτυο μας. Το εργαλείο από το οποίο μπορούμε να παίρνουμε στατιστικά, να τρέχουμε την προσομοίωση και να βλέπουμε αποτελέσματα για την λειτουργία του δικτύου μας. Στην συνέχεια θα χρησιμοποιήσουμε τον Node Editor για καθορίσουμε την συμπεριφορά και τα χαρακτηριστικά της κάθε οντότητας που παίρνει μέρος στο δίκτυο μας. Επιπλέον έχουμε τον Process Model Editor, ο οποίος καθορίζει την λειτουργία των κόμβων-οντοτήτων που έχουν δημιουργηθεί, με χρήση της γλώσσα προγραμματισμού C. Τέλος ο Link Model Editor που χρησιμεύει στην δημιουργία των συνδέσεων για την επικοινωνία των κόμβων μεταξύ τους και ο Packet Format Editor που καθορίζει την μορφή των δεδομένων που θα στέλνονται από τους κόμβους.

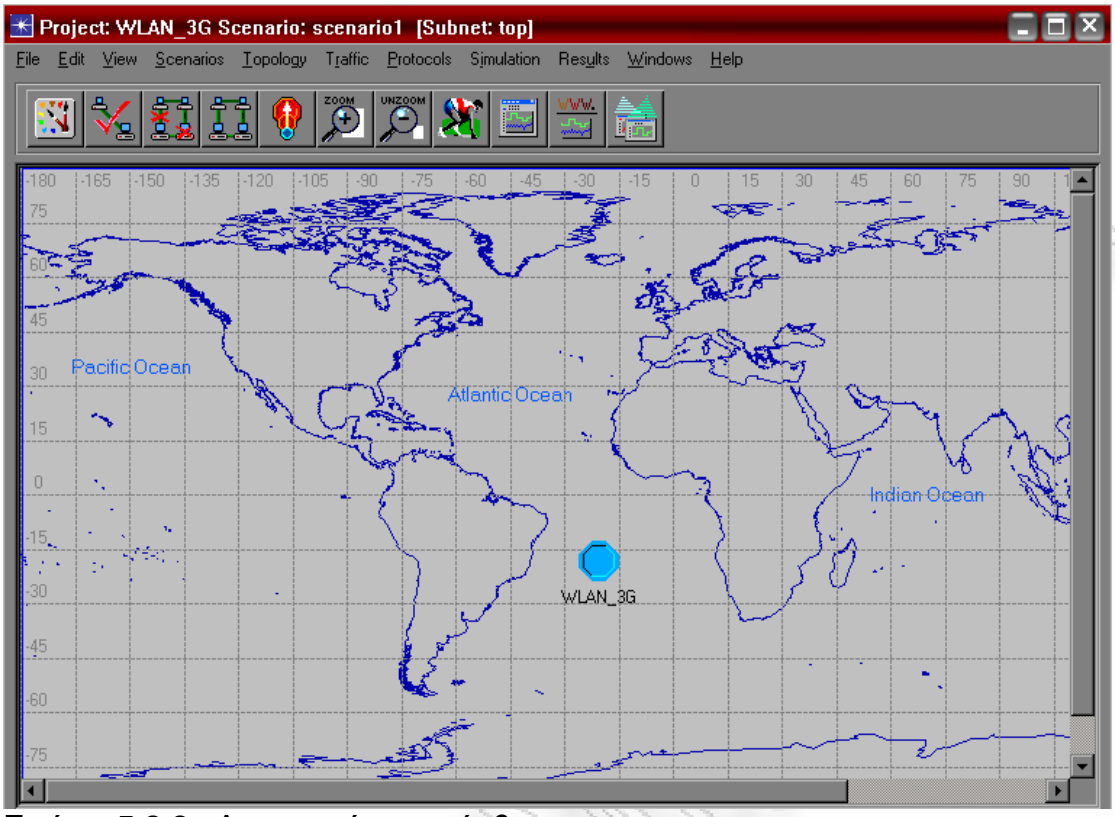
5.3 Αναλυτική περιγραφή σχεδιασμού του δικτύου

Τρέχουμε την εφαρμογή του OPNET, από το FILE στο menu επιλέγουμε NEW και έπειτα Project, για δημιουργήσουμε τον χώρο όπου θα στηθεί το δίκτυο μας. Επιλέγουμε σε κάθε βήμα το επιθυμητό και προχωράμε. Αυτό που θα πρέπει να προκύψει είναι κάτι τέτοιο.



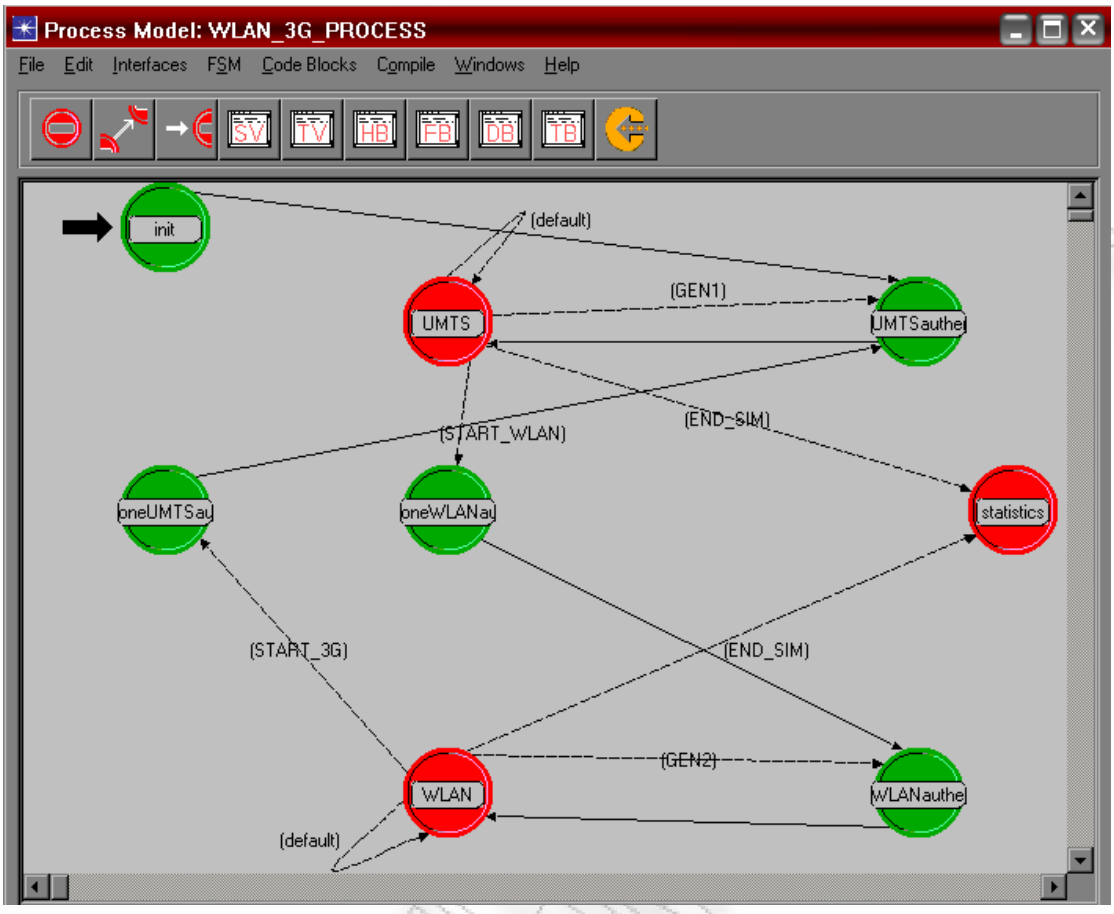
Εικόνα 5.3.1 : Βασικό περιβάλλον OPNET

Αφού δημιουργήσαμε το χώρο που θα στήσουμε το δίκτυο μας, επιλέγουμε από το παραπάνω FILE->NEW->Node Model. Εδώ θα αρχίσουμε να δημιουργούμε τους κόμβους-οντότητες που θα πάρουν μέρος στο δίκτυο μας. Εμείς θα ασχοληθούμε με ένα κυρίως κόμβο που θα προσομοιώσει καλύτερα την λειτουργία που θέλουμε να κάνει. Δημιουργούμε λοιπόν τον WLAN-3G.



Εικόνα 5.3.2 : Δημιουργία του κόμβου

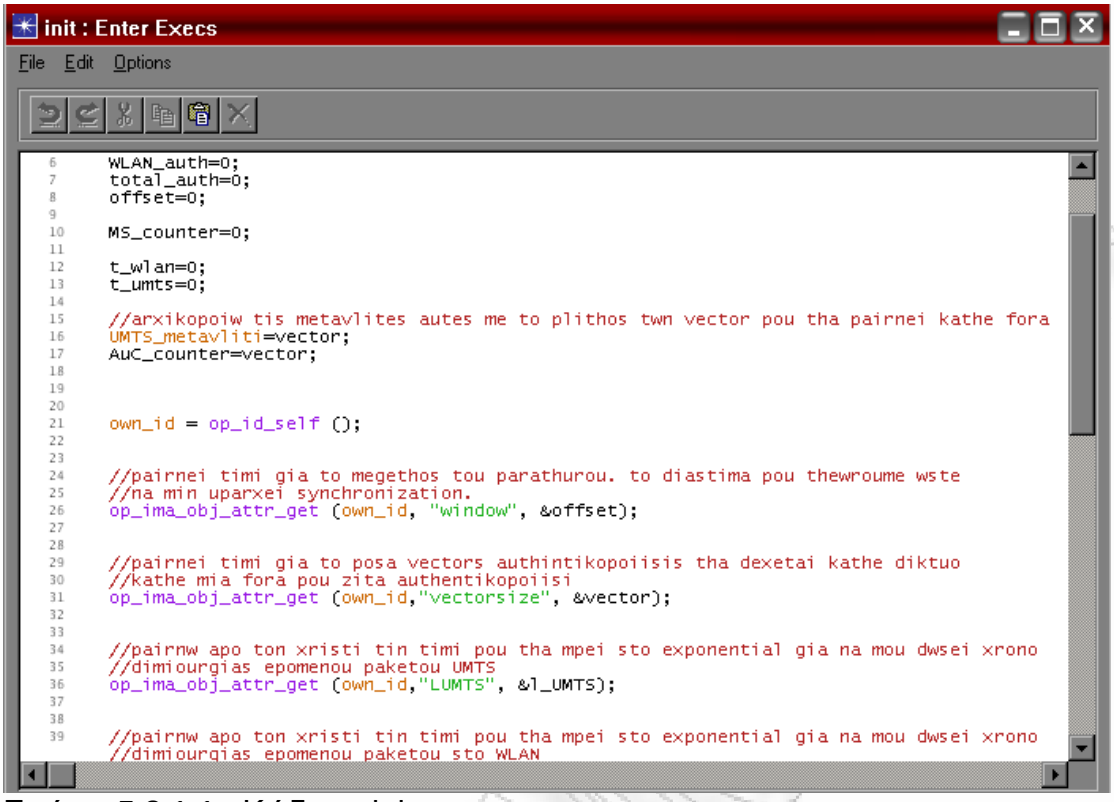
Επιλέγοντας τώρα FILE->NEW->Process Model θα δημιουργήσουμε τις διαδικασίες που θα αποτελείται ο κόμβος μας. Παρουσιάζω αμέσως λοιπόν τι πρέπει να φτιάξουμε και θα εξηγήσω σιγά-σιγά την λειτουργία κάθε διαδικασίας.



Εικόνα 5.3.3 : Processes που αποτελείται ο κόμβος.

5.3.1 Init

Στην οντότητα init έχουμε αρχικοποιήσει όλες τις μεταβλητές που θα χρειαστούμε στους υπολογισμούς μας. Πέραν από τις αρχικοποιήσεις όμως έχουμε χρησιμοποιήσει και την εντολή op_ima_obj_attr_get, η οποία παίρνει τιμή που θα δώσει ο χρήστης και την χρησιμοποιεί για συγκεκριμένες πράξεις. Εδώ έχουμε ορίσει 6 μεταβλητές να δίνει ο χρήστης. Κατά σειρά δίνει ,τον ρυθμό παραγωγής κλήσεων του χρήστη στο UMTS (l_umts), τον ρυθμό παραγωγής κλήσεων στο WLAN(l_wlan), τον ρυθμό παραμονής του στο UMTS (m_umts), τον ρυθμό παραμονής του στο WLAN(l_wlan), τον αριθμό των διανυσμάτων αυθεντικοποίησης(vectorsize) θα έχουμε και τέλος το offset που είναι ένα παράθυρο ανοχής για το πότε έχουμε υποκλοπή (synchronization).

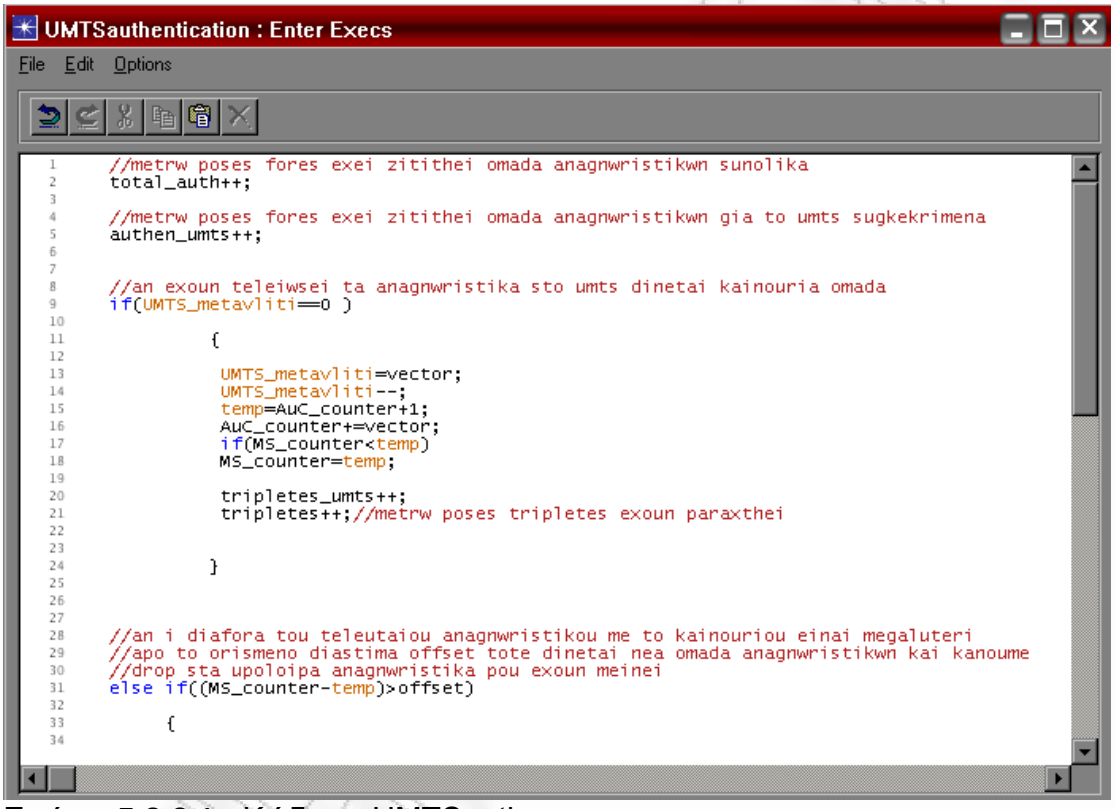


Εικόνα 5.3.1.1 : Κώδικας init.

5.3.2 UMTS και UMTSauthe

Μετά την init μεταφέρεται ο έλεγχος που προγράμματος στην UMTSauthe οντότητα. Αυτή η process προσομοιώνει το authentication center ενός πραγματικού δικτύου όπως το έχουμε περιγράψει στα προηγούμενα κεφάλαια. Την πρώτη φορά που γίνεται κλήση στο δίκτυο UMTS ζητάτε να γίνει αυθεντικοποίηση της κλήσης αυτής με κάποιο αναγνωριστικό. Αυτά τα αναγνωριστικά στην πραγματικότητα τα δίνει το authentication center κατά ομάδες για καλύτερη και πιο γρήγορη επικοινωνία του δικτύου μας. Το authentication center εδώ είναι η οντότητα UMTSauthe. Στην πρώτη κλήση λοιπόν θα δοθεί μια ομάδα αναγνωριστικών στο UMTS. Αν τώρα δεν είναι η πρώτη μας κλήση, η αυθεντικοποίηση γίνεται με αναγνωριστικά από την ομάδα που είχε ληφθεί τελευταία, μειώνοντας τον αριθμό τους κατά ένα κάθε φορά. Όταν μας τελειώσουν τα αναγνωριστικά, τότε ζητά το δίκτυο μας νέα ομάδα από το UMTSauthe. Ταυτόχρονα γίνεται και ο έλεγχος της τιμής του αναγνωριστικού που παίρνει η κλήση μας με την τιμή του αναγνωριστικού που δόθηκε από το δίκτυο τελευταία. Αν η διαφορά τους είναι μεγαλύτερη από την αρχική τιμή offset

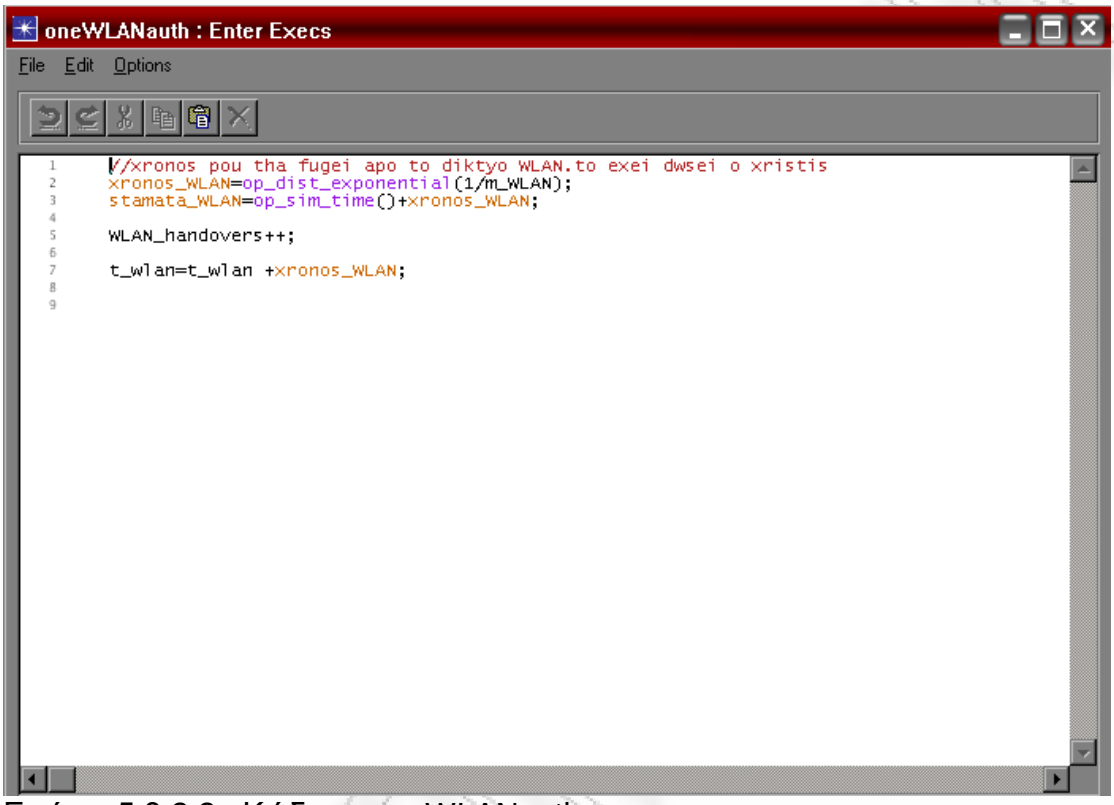
που θέσαμε τότε έχουμε synchronization. Synchronization, έχουμε όταν το αναγνωριστικό μιας κλήσης βρεθεί να χρησιμοποιείται ξανά. Τα αναγνωριστικά είναι μοναδικά και δεν μπορούν να ξαναχρησιμοποιηθούν. Αν συμβεί κάτι τέτοιο όμως , μετρούμε τις φορές που συνέβη και ακυρώνουμε όλα τα υπόλοιπα αναγνωριστικά που έχει το δίκτυο ζητώντας καινούρια ομάδα από το UMTSauthe. Διαφορετικά συνεχίζουμε με την ίδια ομάδα αναγνωριστικών.



Εικόνα 5.3.2.1 : Κώδικας UMTSauthe.

Αφού λάβουμε το αναγνωριστικό από το UMTSauthe ο έλεγχος του προγράμματος μεταφέρεται στο UMTS process. Εκεί μόλις εκπληρωθεί ο χρόνος τις κλήσης πραγματοποιείται μια νέα κλήση και μεταφέρεται πάλι στο UMTSauthe ο έλεγχος. Η παραπάνω διαδικασία που περιγράψαμε συνεχίζεται μέχρι να φτάσει η χρονική στιγμή εκείνη που έχουμε αρχικά ορίσει ως χρόνο παραμονής στο δίκτυο UMTS. Όταν φτάσει αυτός ο χρόνος εκπληρώνεται μια συνθήκη μέσα στην οντότητα UMTS και , με την χρήση της

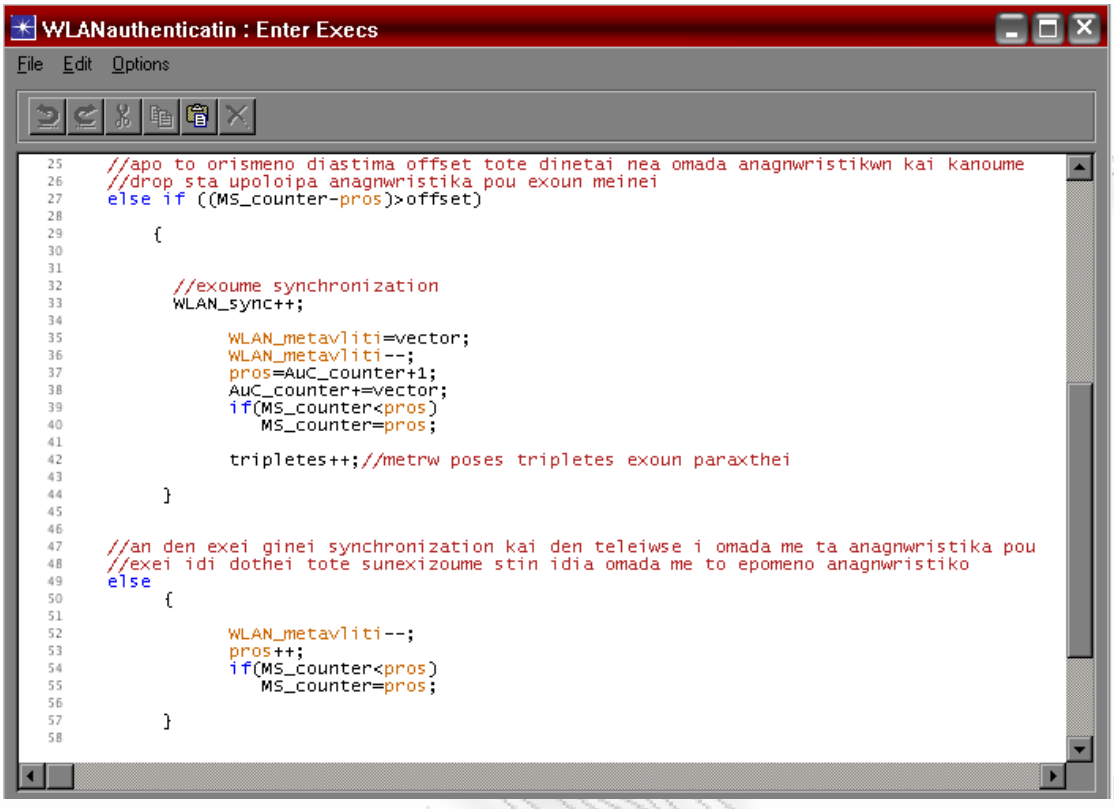
op_intrpt_schedule_self δίνει τον έλεγχο στην οντότητα oneWLANauthe. Εδώ ορίζεται ο χρόνος που θα φύγει ο έλεγχος από την οντότητα WLAN και θα επιστρέψει στο UMTS.



Εικόνα 5.3.2.2 : Κώδικας oneWLANauth.

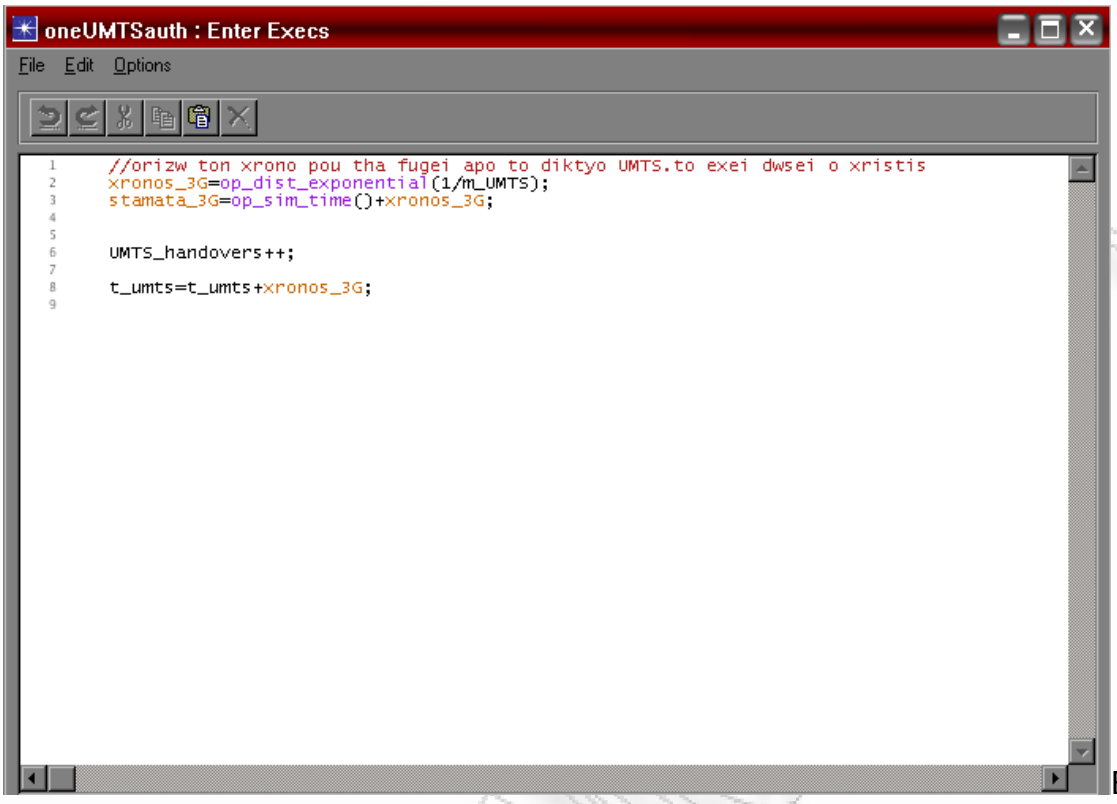
5.3.3 WLAN και WLANauthe

Μετά την οντότητα oneWLANauthe ο έλεγχος μεταφέρεται στην WLANauthe. Εδώ θα δημιουργηθούν τα αναγνωριστικά που θα χρειαστούν στις αυθεντικοποιήσεις των κλήσεων. Τα αναγνωριστικά δίνονται με τον ίδιο τρόπο όπως και προηγουμένως. Δίνονται σε ομάδες με τον αριθμό τους να μειώνεται σε κάθε κλήση για να δοθεί νέα ομάδα όταν τελειώσουν. Πότε θα γίνει κάθε κλήση ορίζεται από την WLAN οντότητα περίπτωση synchronization ακολουθείται η ίδια διαδικασία με πριν, ακυρώνοντας όλα τα αναγνωριστικά και ζητώντας νέα ομάδα. Η λειτουργία της οντότητας WLAN είναι ίδια με την λειτουργία της UMTS. Κάθε φορά μεταφέρεται ο έλεγχος στην WLANauthe μέσω της op_intrpt_schedule_self που έχει η WLAN για να δοθούν τα αναγνωριστικά.



Εικόνα 5.3.3.1 : Κώδικας WLANauthe.

Όταν τώρα εκπληρωθεί ο χρόνος που έχουμε ορίσει αρχικά για την παραμονή στο δίκτυο WLAN φεύγει ο έλεγχος του προγράμματος μας από εδώ και επιστρέφει ξανά στο δίκτυο UMTS και στην οντότητα oneUMTSauthe.



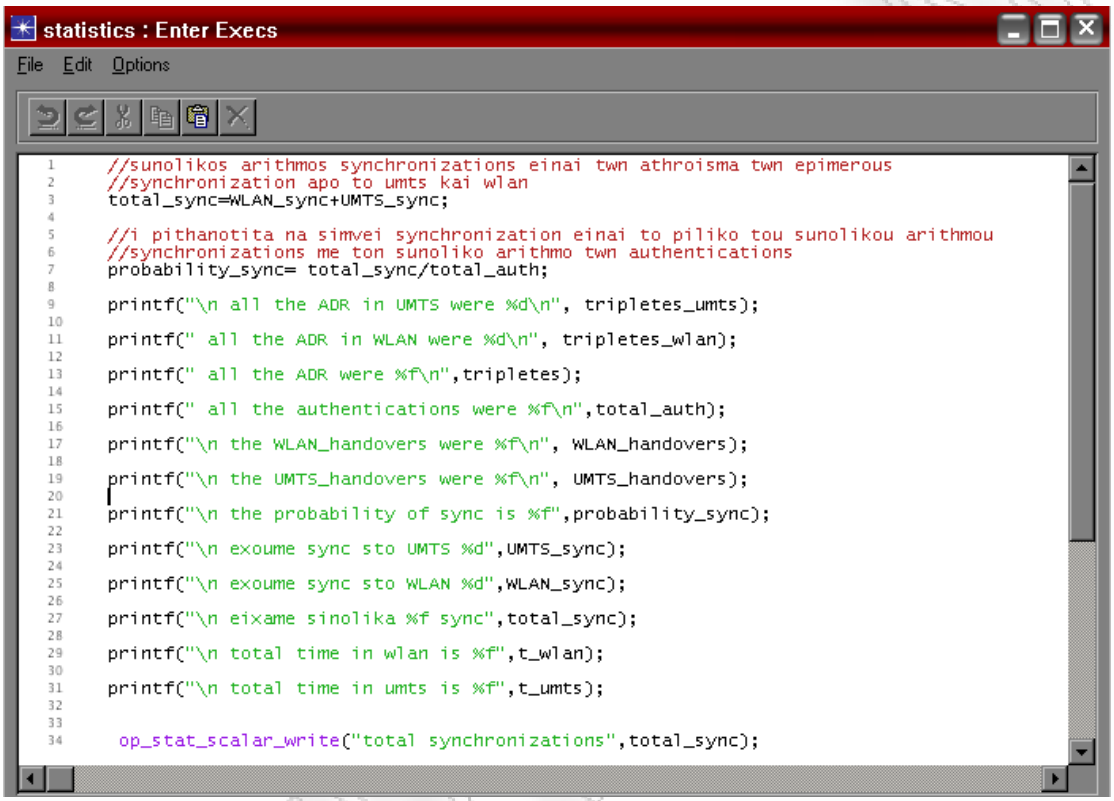
Εικόνα 5.3.3.2 : Κώδικας oneUMTSauth.

Το UMTS τώρα είναι αυτό που λαμβάνει πλέον τις κλήσεις που θέλουμε να κάνουμε συνεχίζοντας με τα αναγνωριστικά από εκεί που είχε μείνει την τελευταία φορά που ήμασταν σε αυτό. Το ίδιο θα συμβεί και με το WLAN την επόμενη φορά που θα δρομολογηθούν οι κλήσεις μέσω αυτού. Εξαίρεση αποτελεί η περίπτωση κατά την οποία έχει γίνει synchronization από το ένα δίκτυο ή το άλλο όπου πρέπει να ληφθεί νέα ομάδα αναγνωριστικών.

5.3.4 Statistics

Οι κλήσεις που πραγματοποιούμε εμείς στην πραγματικότητα γίνονται εναλλάξ μέσω του ενός ή του άλλου δικτύου. Στο πρόγραμμα που έχουμε δημιουργήσει προσομοιώνουμε αυτή την διαδικασία με το να μεταφέρεται ο έλεγχος του προγράμματος από την μια οντότητα στην άλλη, όπως είδαμε παραπάνω. Αυτό γίνεται συνεχώς μέχρι να τελειώσει ο χρόνος προσομοίωσης του προγράμματος

μας. Όταν γίνει αυτό ο έλεγχος μεταφέρεται στην οντότητα statistics. Εκεί υπολογίζουμε όλες τις πληροφορίες που χρειαζόμαστε για να βγάλουμε συμπεράσματα για την προσομοίωση μας.



Εικόνα 5.3.4.1 : Κώδικας Statistics

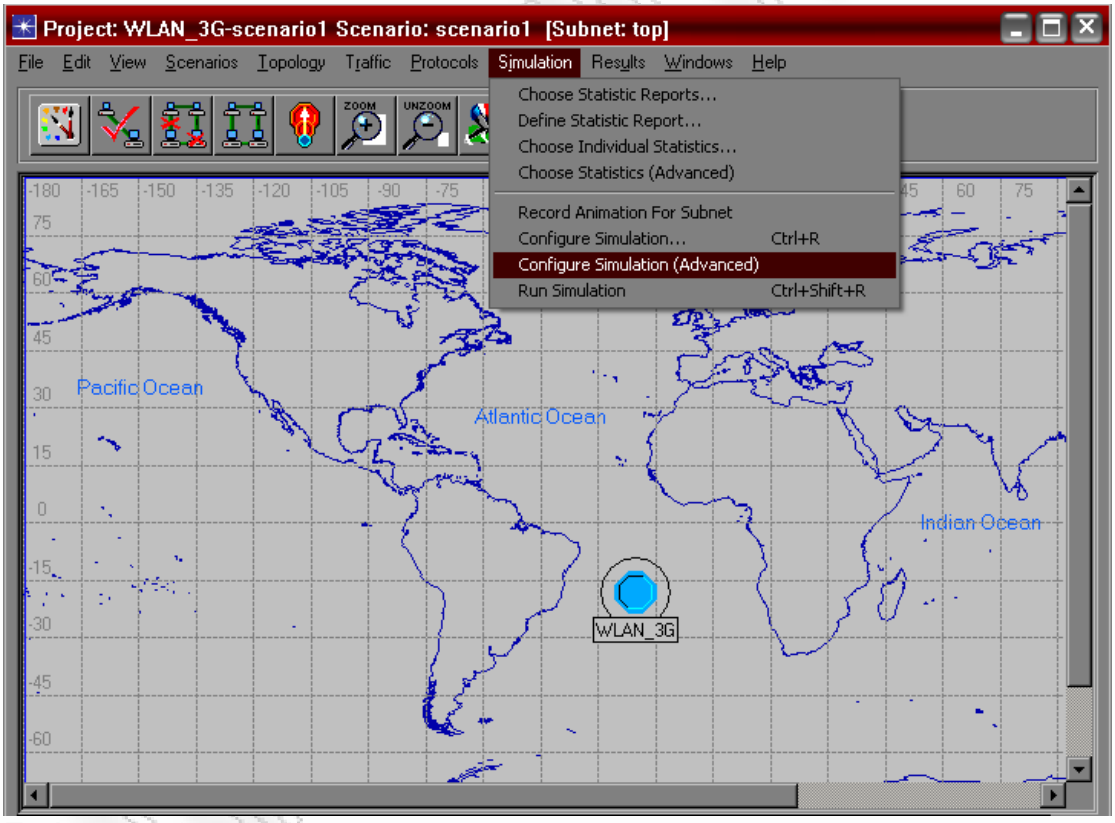
Σε αυτό το process υπολογίζουμε την πιθανότητα να έχουμε synchronization αλλά και το σύνολο των synchronizations που έγιναν καθ' όλη την διάρκεια της προσομοίωσης. Μετράμε επίσης ξεχωριστά για κάθε δίκτυο διάφορες παραμέτρους, όπως τον χρόνο που έμεινε στο κάθε δίκτυο ο χρήστης ή τον αριθμό των μεταπομπών που έκανε κάθε φορά ή πόσα synchronizations έγιναν από κάθε δίκτυο. Αυτές τις τιμές θα τις χρησιμοποιήσουμε για την δημιουργία παρακάτω γραφικών παραστάσεων που θα μας βοηθήσουν στην καλύτερη κατανόηση των πλεονεκτημάτων και των μειονεκτημάτων των ενοποιημένων δικτύων 3G-WLAN.

ΚΕΦΑΛΑΙΟ 6
ΑΠΟΤΕΛΕΣΜΑΤΑ ΠΡΟΣΟΜΟΙΩΣΗΣ

6.1 Εκτέλεση Προγράμματος

Έχοντας ολοκληρώσει το πρόγραμμα μας σε αυτό το σημείο ξεκινούμε την εκτέλεση του. Θα περιγράψουμε αναλυτικά κάθε βήμα που ακολουθείται για να είναι πιο κατανοητό.

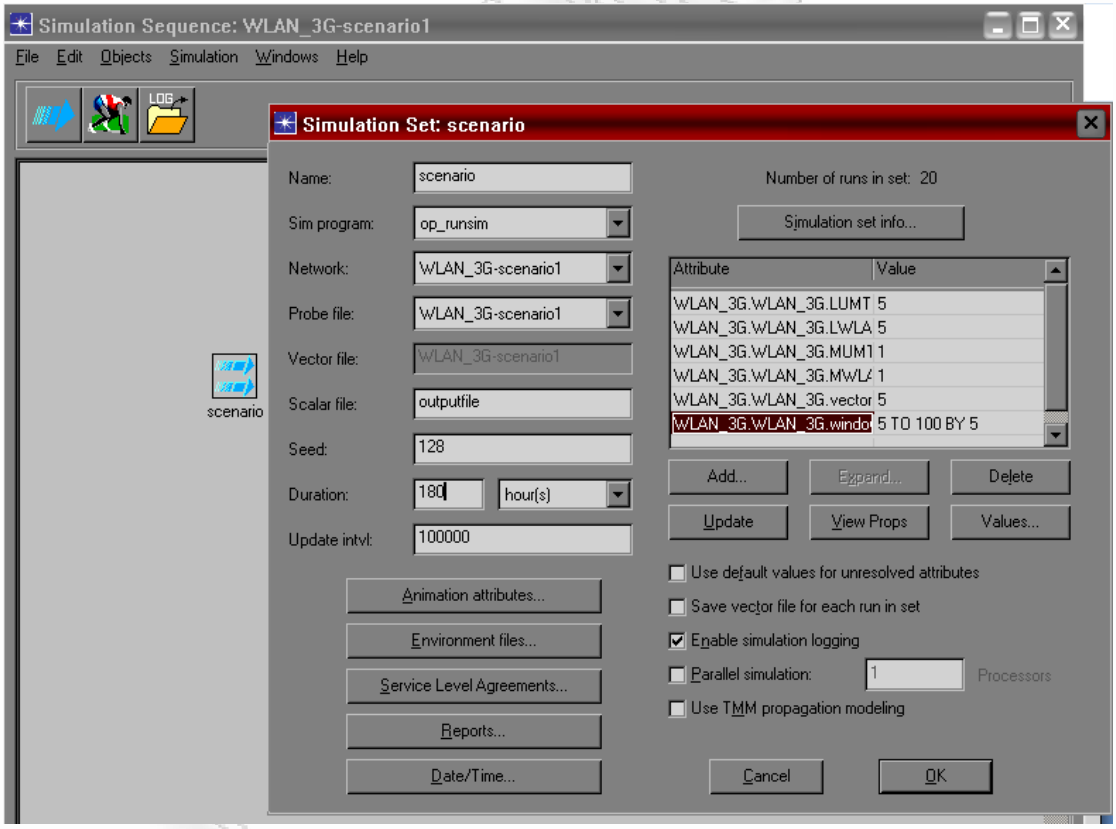
Από το menu επιλέγουμε την επιλογή simulation και στην συνέχεια το configure Simulation(advanced) όπου θα ορίσουμε τις παραμέτρους του προγράμματος.



Εικόνα 6.1.1

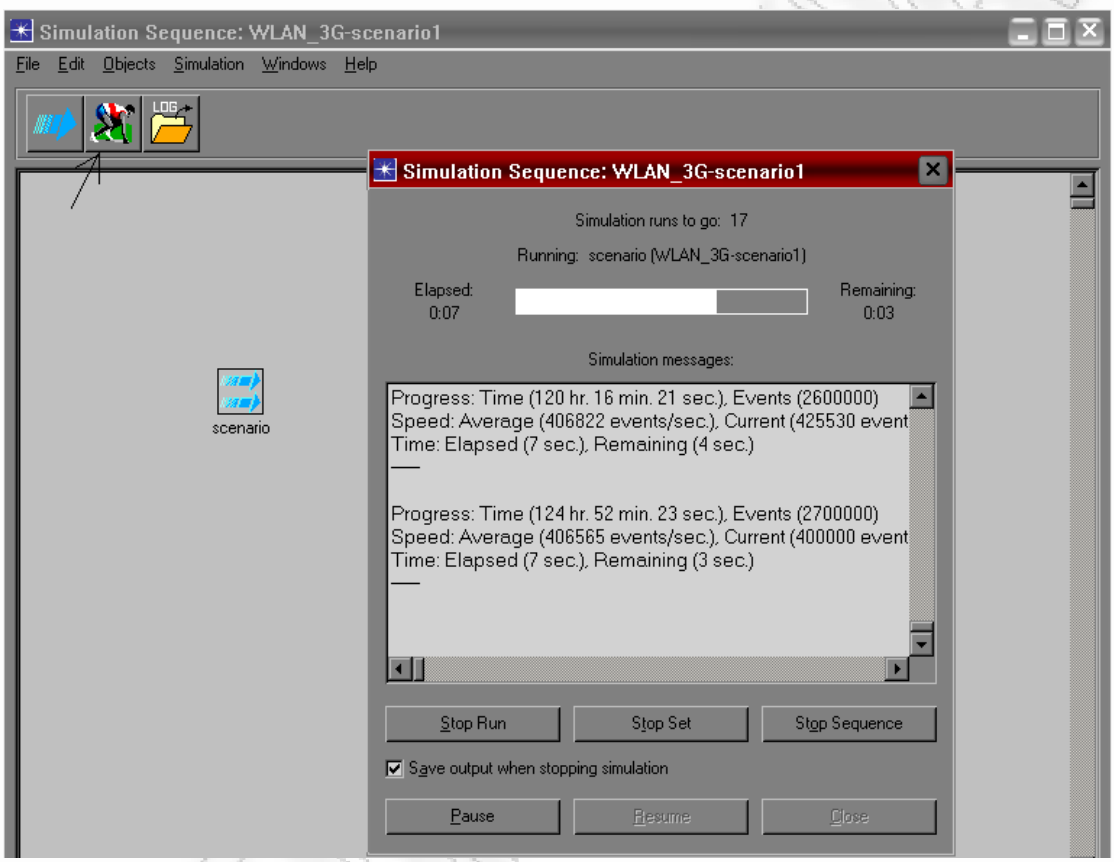
Επιλέγοντας την επιλογή αυτή θα οδηγηθούμε στο παρακάτω παράθυρο που περιέχει το σενάριο που θα εκτελέσουμε. Πατώντας δεξί κλίκ πάνω στο σενάριο μας δίνεται η επιλογή edit attributes που οδηγεί στο άνοιγμα του παρακάτω παραθύρου.

Σε αυτό το σημείο θέτουμε το αρχείο που θα αποθηκευτούν τα αποτελέσματα της εκτέλεσης. Εκεί που αναφέρει scalar file γράφουμε το όνομα του αρχείου αυτού. Στην περίπτωση μας το outputfile. Στην συνέχεια ορίζουμε την διάρκεια της προσομοίωσης. Εδώ έχουμε βάλει 180 ώρες έτσι ώστε να έχει έρθει σε ισορροπία το δίκτυο που προσομοιώνουμε για να μας δώσει καλύτερα αποτελέσματα-καλό είναι να βάζουμε μεγάλο χρόνο προσομοίωσης. Δεξιά επιλέγουμε add και προσθέτουμε όλες τις μεταβλητές εκείνες που πρέπει να δώσει ο χρήστης. Στην περίπτωση μας θα προστεθούν οι 6 μεταβλητές για τις οποίες μιλήσαμε στο κεφάλαιο 5.3.1.



Εικόνα 6.1.2

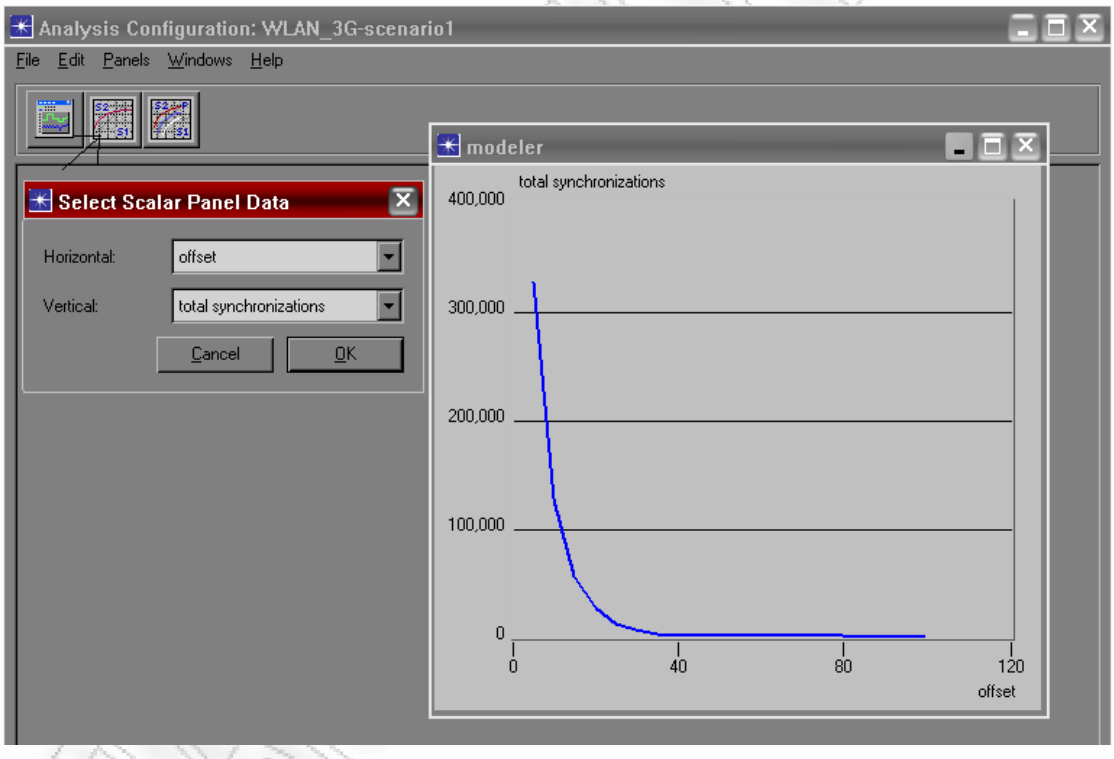
Στην συνέχεια πατάμε οκ και συνεχίζουμε με την εκτέλεση. Πατάμε το εικονίδιο που δείχνει το βελάκι στην παρακάτω εικόνα και περιμένουμε να ολοκληρωθεί η προσομοίωση.



Εικόνα 6.1.3

6.2 Εμφάνιση Αποτελεσμάτων

Με την ολοκλήρωση της προσομοίωσης, από το αρχικό menu επιλέγουμε Results->View Results(Advanced). Από το νέο παράθυρο που θα ανοίξει επιλέγουμε FILE->Load Output Scalar File και δίνουμε το όνομα του αρχείου που έχουμε αποθηκεύσει τα αποτελέσματα μας(outputfile). Στην συνέχεια επιλέγουμε το δεύτερο από τα τρία εικονίδια που βλέπουμε(βλ. Εικόνα 6.2.1)για να δημιουργήσουμε γράφημα με ορισμένο οριζόντιο και κάθετο άξονα από εμάς. Επιλέγουμε ποια μεταβλητή θα βάλουμε στον οριζόντιο άξονα(offset)και ποια στον κάθετο(total synchronizations) και παίρνουμε τις γραφικές απεικονίσεις όπως φαίνεται παρακάτω.

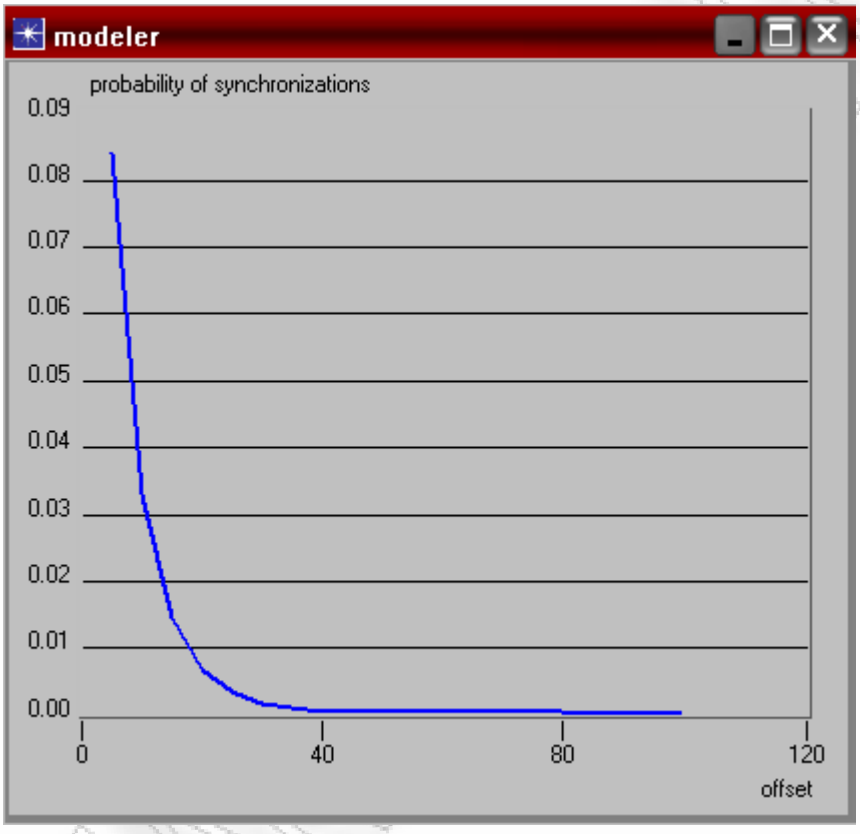


Εικόνα 6.2.1

Συνολικά για τα δεδομένα εισόδου:

LUMTS=5 (ρυθμός παραγωγής κλήσεων στο UMTS)
LWLAB=5 (ρυθμός παραγωγής κλήσεων στο WLAN)
MUMTS=1 (ρυθμός παραμονής στο UMTS)
MWLAN=1 (ρυθμός παραμονής στο WLAN)
Vectorsize=5 (αριθμός διανυσμάτων αυθεντικοποίησης)
Window=5 to 100 step 5 (offset, παίρνει ένα διάστημα τιμών)

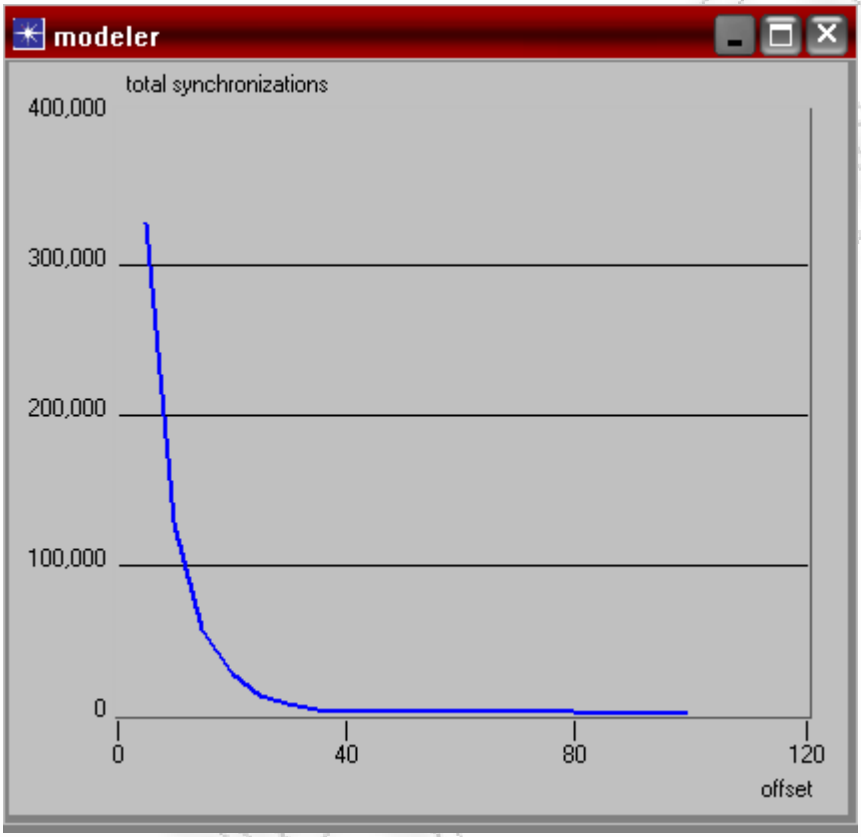
Έχουμε τα παρακάτω αποτελέσματα:



Εικόνα 6.2.2: Γραφική παράσταση probability of synchronization/offset, (LUMTS/MUMTS)=5

Σε αυτή την γραφική βλέπουμε μια φθίνουσα καμπύλη. Όσο το offset μεγαλώνει η πιθανότητα να έχουμε synchronization μειώνεται ανάλογα. Με μικρό offset η πιθανότητα είναι κοντά στην μονάδα, όντας πολύ πιθανό να έχουμε synchronization. Καθώς το offset μεγαλώνει όμως η πιθανότητα αυτή

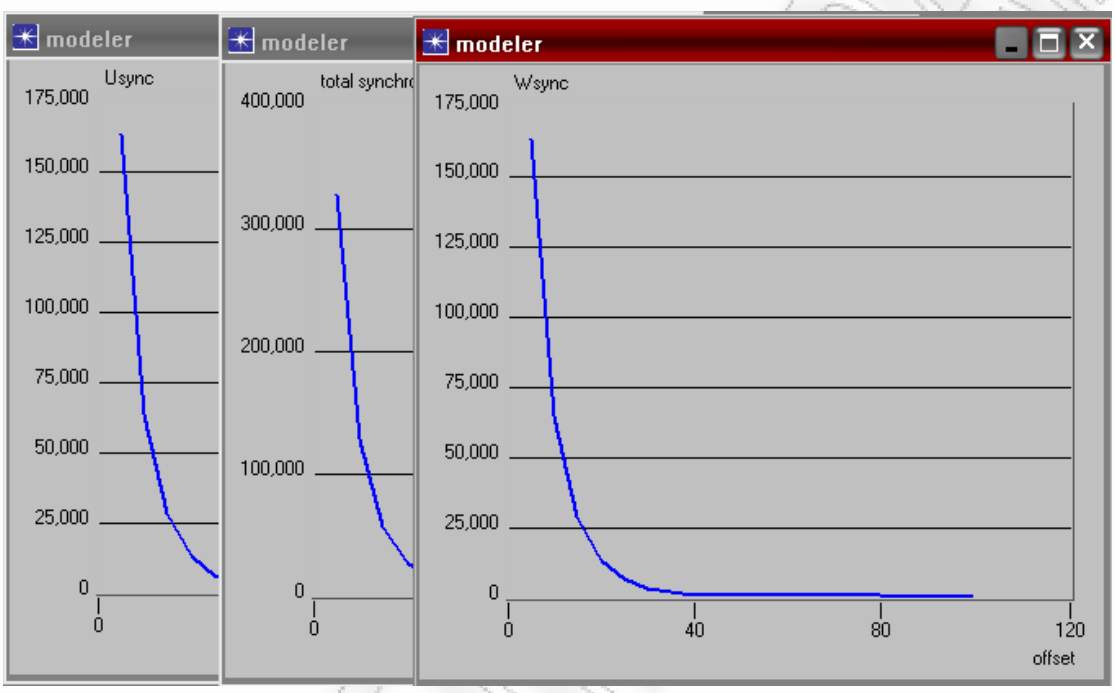
τείνει στο μηδέν. Το offset να θυμίσουμε ότι αναφέρεται σε ένα παράθυρο ανοχής των λαμβανόμενων διανυσμάτων αυθεντικοποίησης που λαμβάνει κάθε δίκτυο. Αν λάβει δηλαδή το δίκτυο μικρότερο αριθμό στο διάνυσμα αυθεντικοποίησης από το διάστημα αυτό κάθε φορά έχουμε synchronization. Ο ρυθμός παραμονής και παραγωγής κλήσεων και για τα δύο δίκτυα είναι ο ίδιος.



Εικόνα 6.2.3: Γραφική παράσταση total synchronizations/offset, (LUMTS/MUMTS)=5

Μια φθίνουσα καμπύλη περιμέναμε και για την γραφική Εικόνα 6.2.3, αφού όσο μικρότερη είναι η τιμή της μεταβλητής offset τόσο περισσότερα synchronization έχουμε. Ο αριθμός τους μειώνεται για μεγάλη τιμή του offset. Η τιμή του total synchronizations είναι το άθροισμα των επιμέρους synchronizations που γίνονται στο UMTS(Usync) και WLAN (Wsync)

δίκτυο. Αυτό φαίνεται και από το Εικόνα 6.2.4 που βρίσκουμε τις γραφικές για κάθε δίκτυο και τις συγκρίνουμε με την γραφική Εικόνα 6.2.3.

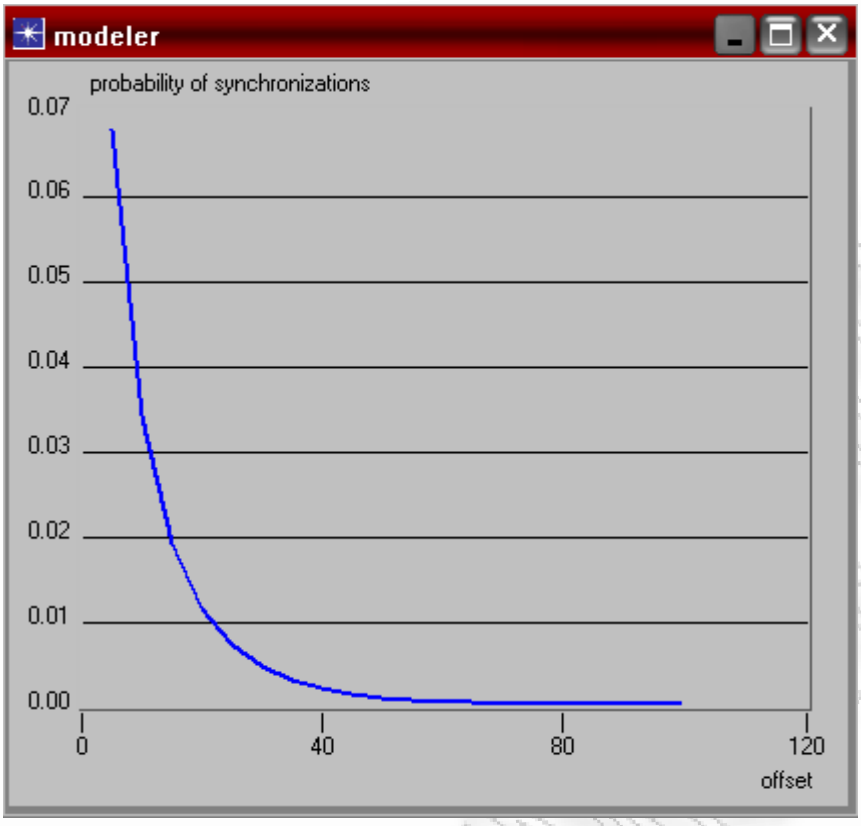


Εικόνα 6.2.4: Γραφική παράσταση total synchronizations/offset και για τα επιμέρους δίκτυα WLAN και UMTS, (LUMTS/MUMTS)=5

Αλλάζουμε τα δεδομένα εισόδου:

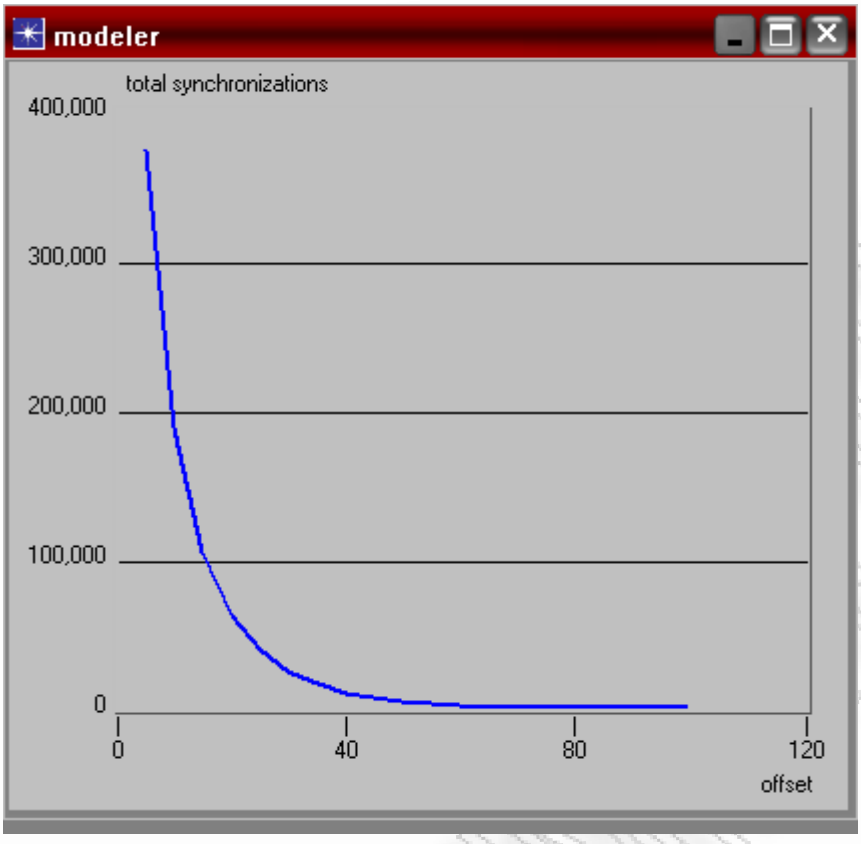
LUMTS=10 (ρυθμός παραγωγής κλήσεων στο UMTS)
LWLAB=5 (ρυθμός παραγωγής κλήσεων στο WLAN)
MUMTS=1 (ρυθμός παραμονής στο UMTS)
MWLAN=1 (ρυθμός παραμονής στο WLAN)
Vectorsize=5 (αριθμός διανυσμάτων αυθεντικοποίησης)
Window=5 to 100 step 5 (offset, το οποίο αλλάζει κάθε φορά)

Έχουμε τα παρακάτω αποτελέσματα:



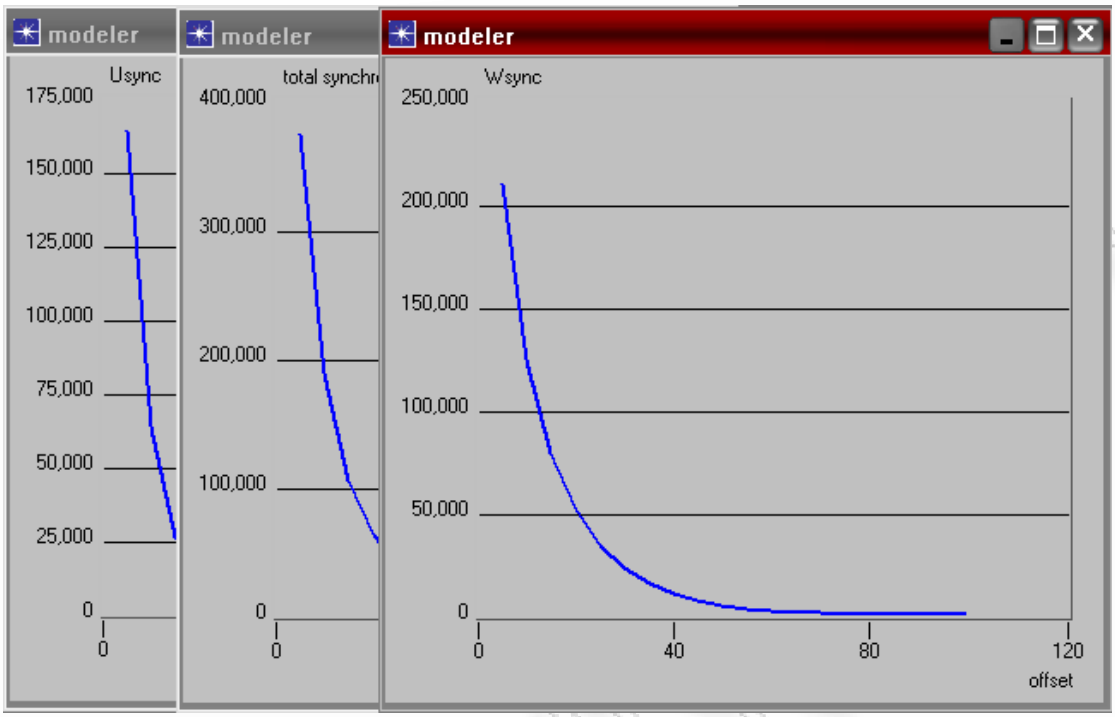
Εικόνα 6.2.5: Γραφική παράσταση probability of synchronization/offset, (LUMTS/MUMTS)=10

Αλλάζοντας τον λόγο (LUMTS/MUMTS)=10, παρατηρούμε πάλι την ίδια φθίνουσα καμπύλη όπως αναμέναμε. Αυτό που διαφέρει σε σχέση με πριν όμως(βλ. Εικόνα 6.2.2) είναι ότι για τις ίδιες τιμές του offset η πιθανότητα αρχικά να συμβεί synchronization είναι κοντά στο 0.68 ενώ πριν κοντά στο 0.84. Έχουμε δηλαδή μικρότερη πιθανότητα και την καμπύλη να τείνει στο μηδέν πιο αργά σε σχέση με πριν. Για offset=40 στο Σχήμα 6.2.2 έχει σχεδόν μηδενιστεί η πιθανότητα ενώ στο Σχήμα 6.2.5 αυτό γίνεται με offset=65.



Εικόνα 6.2.6: Γραφική παράσταση total synchronizations/offset, (LUMTS/MUMTS)=10

Ο αριθμός των συνολικών synchronizations σε αυτή την περίπτωση σε σχέση με πριν(βλ. Εικόνα 6.2.3) είναι μεγαλύτερος. Η καμπύλη φθίνει με μικρότερο ρυθμό και μηδενίζεται σε μεγαλύτερο offset από ότι πριν.



Εικόνα 6.2.7: Γραφική παράσταση total synchronizations/offset και για τα επιμέρους δίκτυα WLAN και UMTS, (LUMTS/MUMTS)=10

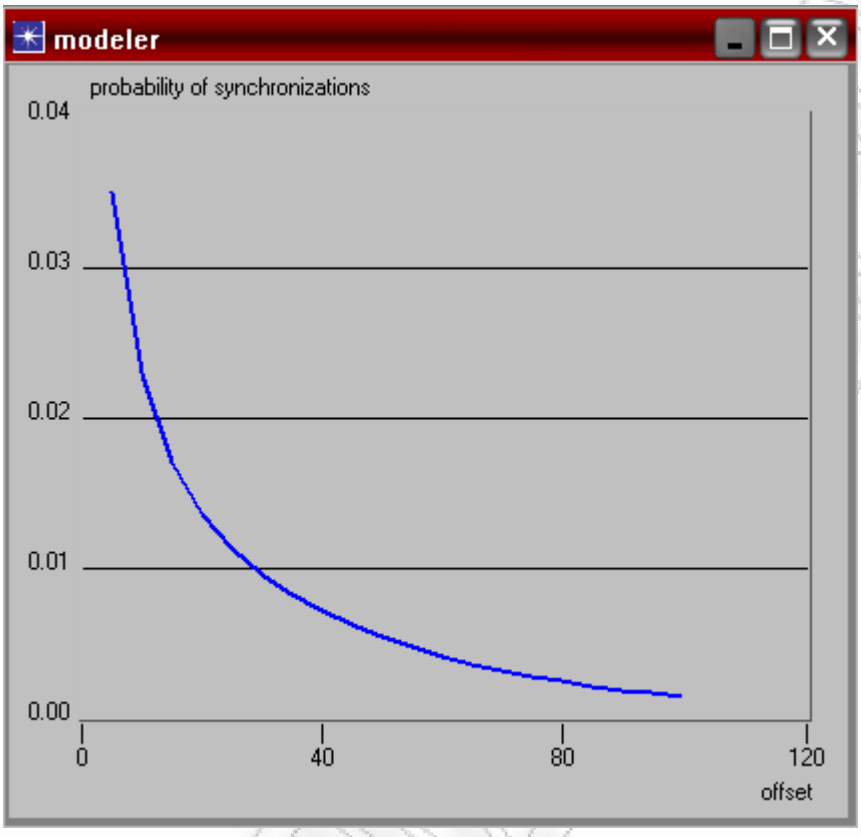
Εδώ φαίνεται ξεκάθαρα ότι από την στιγμή που μεγαλώσαμε τον λόγο LUMTS/MUMTS για το UMTS ο αριθμός των synchronizations που συνέβαιναν στο άλλο δίκτυο WLAN έχουν συνολικά αυξηθεί. Σε σχέση με πριν πλέον γίνονται πιο πολλά synchronizations στο WLAN και τείνουν στο μηδέν σε μεγαλύτερα offset. Για μεγαλύτερο εύρος τιμών του offset δηλαδή, το WLAN έχει περισσότερα synchronizations.

Αλλάζουμε τα δεδομένα εισόδου για μια τρίτη φορά:

LUMTS=30 (ρυθμός παραγωγής κλήσεων στο UMTS)
LWLAN=5 (ρυθμός παραγωγής κλήσεων στο WLAN)
MUMTS=1 (ρυθμός παραμονής στο UMTS)
MWLAN=1 (ρυθμός παραμονής στο WLAN)
Vectorsize=5 (αριθμός διανυσμάτων αυθεντικοποίησης)

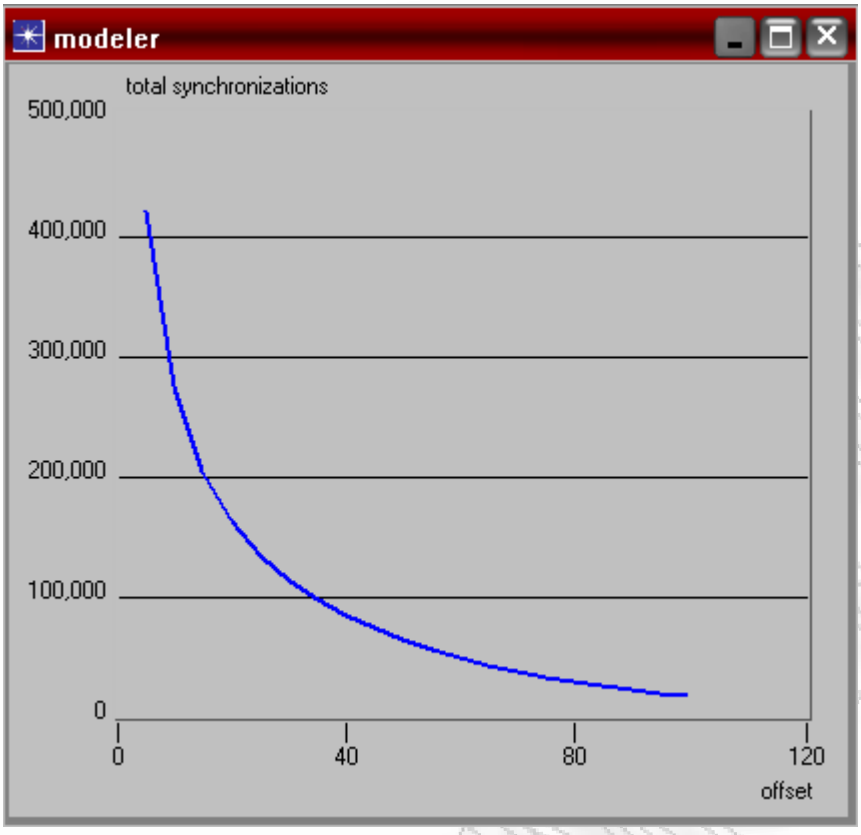
Window=5 to 100 step 5 (offset, το οποίο αλλάζει κάθε φορά)

Έχουμε τα παρακάτω αποτελέσματα:



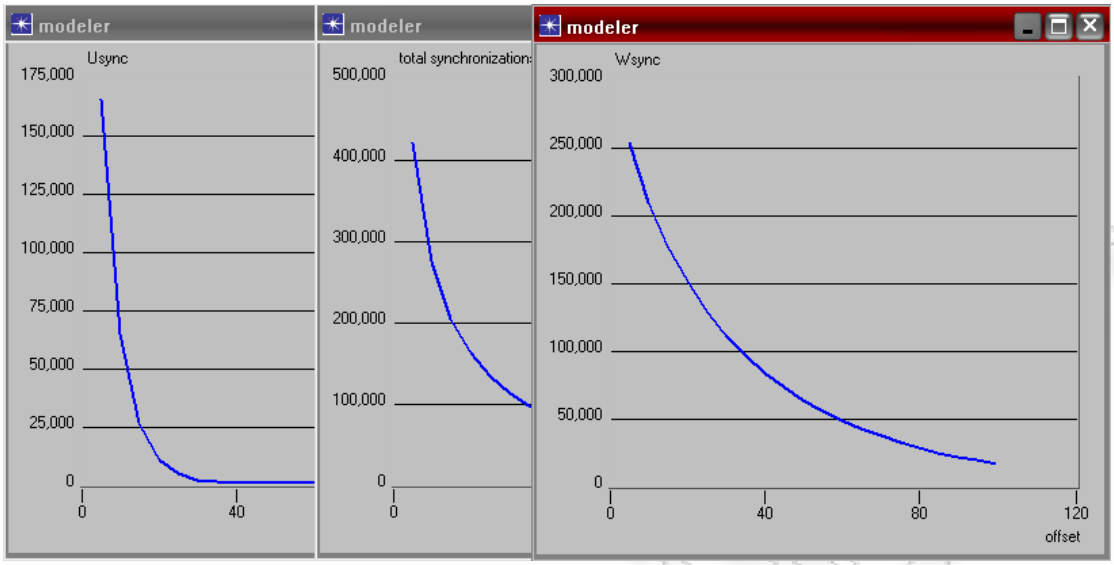
Εικόνα 6.2.8: Γραφική παράσταση probability of synchronization/offset, (LUMTS/MUMTS)=30

Δίνοντας ακόμα μεγαλύτερη τιμή στον λόγο (LUMTS/MUMTS) φαίνεται ακόμα πιο έντονα ότι η καμπύλη αργεί να μηδενίσει. Αν και ξεκινά αρχικά με μικρή πιθανότητα να συμβεί κάποιο synchronization, διατηρεί για όλο και πιο μεγάλες τιμές του offset μεγαλύτερη πιθανότητα σε σχέση τις προηγούμενες φορές.



Εικόνα 6.2.9: Γραφική παράσταση total synchronizations/offset, (LUMTS/MUMTS)=30

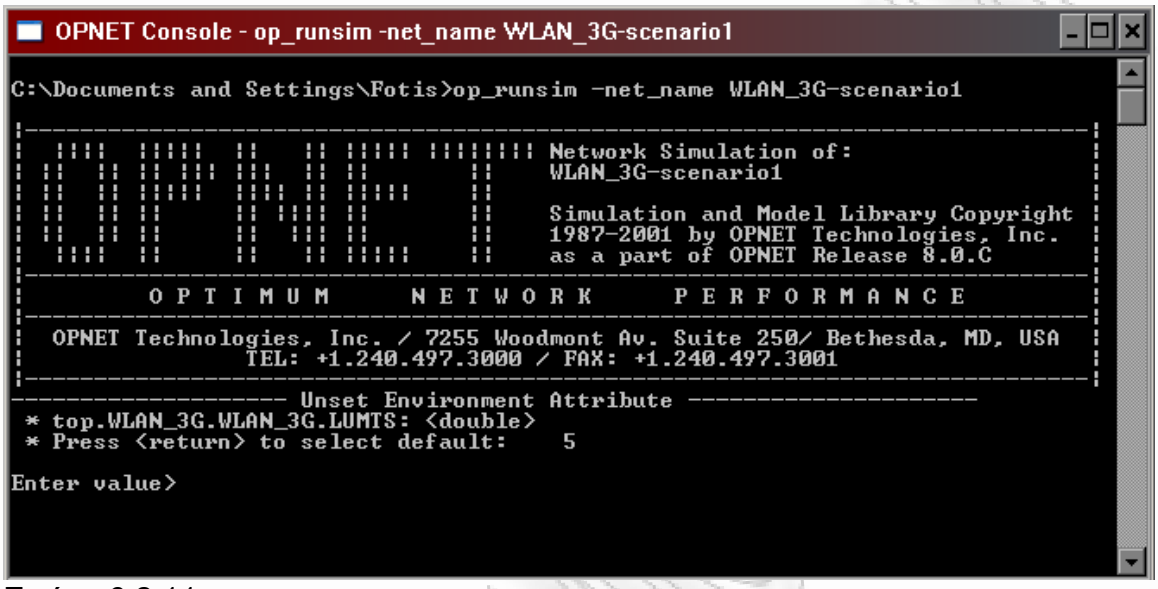
Σε αυτή την περίπτωση έχουμε αρχικά περισσότερα synchronization, τα οποία και μειώνονται με αργό ρυθμό. Για όλο και μεγαλύτερες τιμές του offset τόσο περισσότερα synchronization έχουμε για κάθε τιμή.



Εικόνα 6.2.10: Γραφική παράσταση total synchronizations/offset και για τα επιμέρους δίκτυα WLAN και UMTS, (LUMTS/MUMTS)=30

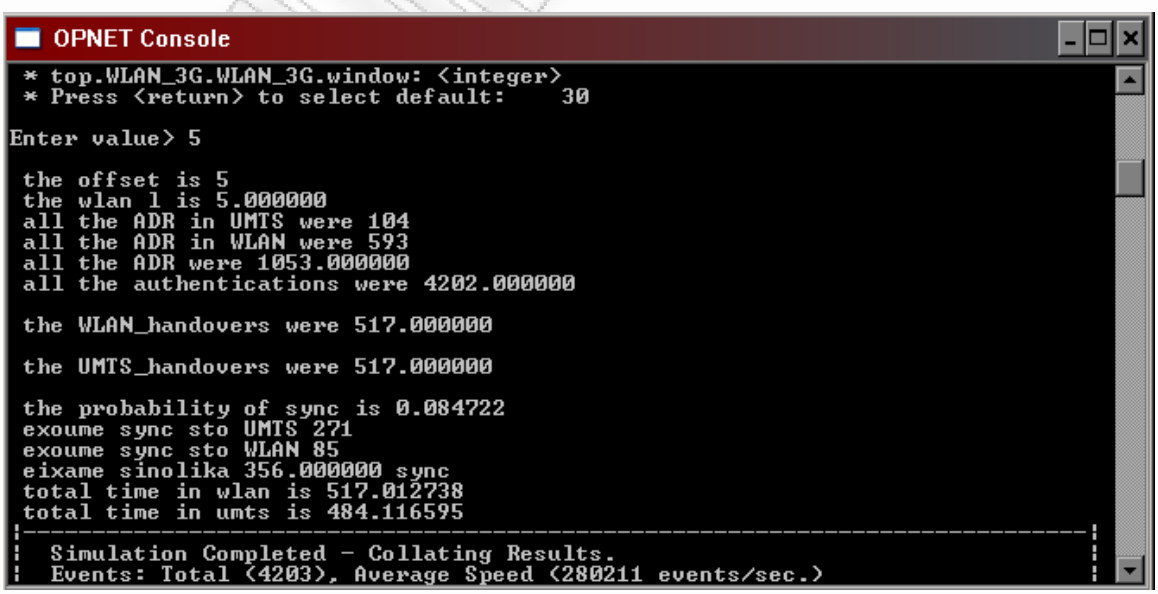
Εδώ φαίνεται πολύ καθαρά το πόσο γρήγορα φθίνει η καμπύλη των synchronization που συμβαίνουν στο UMTS στο οποίο ο λόγος (LUMTS/MUMTS)=30 και πόσο αργά φθίνει η καμπύλη για το WLAN για το οποίο ισχύει (LWLAN/MWLAN)=10. Αυξάνοντας τον λόγο του ενός δικτύου επηρεάζονται τα synchronizations του άλλου όπως φαίνεται από τη παραπάνω εικόνα.

Χρησιμοποιώντας επίσης την console για να τρέξουμε το πρόγραμμα, μπορούμε να πατήσουμε την εντολή op_runsim –net_name WLAN_3G-scenario1. Θα έχουμε δηλαδή το παρακάτω.



Εικόνα 6.2.11

Τώρα θα χρειαστεί να δώσουμε τις 5 παραμέτρους που ορίζουμε εμείς στο πρόγραμμα μας. Τον χρόνο παραμονής σε κάθε δίκτυο του χρήστη, τον ρυθμό παραγωγής κλήσεων, το offset και τον παραγόμενο αριθμό διανυσμάτων κάθε φορά. Για συγκεκριμένες παραμέτρους λοιπόν θα πάρουμε και τα παρακάτω αποτελέσματα.



Εικόνα 6.2.12

ΚΕΦΑΛΑΙΟ 7

ΣΥΜΠΕΡΑΣΜΑΤΑ

Συνοψίζοντας, στην εργασία αυτή έγινε προσομοίωση με την χρήση του OPNET, ενός ενοποιημένου δικτύου 3G-WLAN. Πραγματοποιήσαμε τρία σενάρια εκτέλεσης στα οποία κάθε φορά αλλάξαμε τα δεδομένα εισόδου. Παρατηρήσαμε λοιπόν ότι όσο αυξάνεται ο λόγος LUMTS/MUMTS για το UMTS έχουμε όλο και πιο πολλά synchronizations στο δίκτυο WLAN και αντίστροφα. Σε σχέση και με την αλλαγή τιμών στο παράθυρο ανοχής offset, παρατηρούμε ότι όσο μεγαλώνει το offset τόσο λιγότερα synchronizations συμβαίνουν στο ενοποιημένο δίκτυο και τόσο πιο μικρή είναι η πιθανότητα να συμβούν αυτά. Επίσης για όσο μεγαλύτερες τιμές στον λόγο LUMTS/MUMTS τόσο πιο πολλά synchronizations έχουμε για κάθε τιμή του offset. Τελικά, βλέπουμε ότι οι τιμές που παίρνουν οι παράμετροι LUMTS/MUMTS και offset προκαλούν αντίστροφα αποτελέσματα στην πιθανότητα και στον αριθμό των synchronizations του δικτύου. Σε πραγματικά δεδομένα επομένως θα πρέπει να οριστεί ένας μέσος αριθμός παραθύρου ανοχής και ταυτόχρονα να έχουμε μικρό ρυθμό παραγωγής κλήσεων στα δίκτυα UMTS ή WLAN με σταθερό ρυθμό παραμονής στα δίκτυα αυτά για να έχουμε μικρό αριθμό synchronizations και μικρή πιθανότητα να συμβεί κάτι τέτοιο.

ΟΡΟΛΟΓΙΑ

Εδώ θα εξηγήσουμε κάποιους όρους που θα μας χρειαστούν για να κατανοήσουμε καλύτερα τα παραπάνω

Κινητός κόμβος(MN): Μπορεί να είναι κάποια συσκευή-τερματικό ή κάποιος χρήστης. Μπορεί να αλλάζει δίκτυα ή υποδίκτυα αλλά κρατά την ίδια IP διεύθυνση.

Οικιακός πράκτορας(HA): Η οντότητα που βρίσκεται στο οικιακό δίκτυο του κινητού κόμβου και κρατά πληροφορία αλλά και δρομολογεί τα δεδομένα στον κόμβο αυτό.

Ξένος πράκτορας(FA): Η οντότητα που βρίσκεται στο ξένο δίκτυο που πάει ο κινητός κόμβος και βοηθά στην αποστολή των δεδομένων στον κόμβο αυτό.

Ανταποκριτής(CN): Η οντότητα που επικοινωνεί και στέλνει δεδομένα στον κινητό κόμβο.

Διεύθυνση επιμέλειας(COA): Η διεύθυνση IP που δίνεται στον κινητό κόμβο μέσα στο ξένο δίκτυο για να συνδεθεί με αυτό και να λαμβάνει τα πακέτα δεδομένων.

Ξένο δίκτυο(FN): Οποιοδήποτε δίκτυο πέραν του οικιακού δικτύου του κόμβου.

Οικιακό δίκτυο(HN): Είναι το δίκτυο που αρχικά συνδέθηκε ο κόμβος πριν φύγει και θεωρείται το «σπίτι» του.

Μόνιμη διεύθυνση(HA): Η διεύθυνση IP που δίνεται στον κόμβο από το οικιακό δίκτυο και παραμένει σταθερή όπου και αν βρίσκεται ο κόμβος.

Κινητή IP: Πρωτόκολλο που χρησιμοποιείται για την κινητικότητα των κόμβων.

IETF: Επιτροπή που σχεδίασε το MIP.

Πρωτόκολλο Ελέγχου Μεταφοράς(*TCP):* Οι κύριοι στόχοι του πρωτοκόλλου TCP είναι να επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων.

Πρωτόκολλο User Datagram(UDP***): Γ***ρήγορο και αποτελεσματικό, αφού δεν παρέχει μηχανισμούς ασφάλειας δεδομένων.

ICMP: Το πρωτόκολλο ICMP διαφέρει από τα πρωτόκολλα TCP και UDP διότι συνήθως δεν χρησιμοποιείται από τις εφαρμογές που εκτελούνται σε κάποιον υπολογιστή, αλλά από το λειτουργικό του σύστημα. για την ανταλλαγή μηνυμάτων λάθους.

Δρομολογητής(Router): λαμβάνει και εκπέμπει πακέτα δεδομένων στους κόμβους ενός δικτύου.

Τοπικό δίκτυο(LAN): Ενσύρματο δίκτυο που καλύπτει μικρό εύρος γεωγραφικής περιοχής.

Ευρείας περιοχής δίκτυο(WAN): Ενσύρματο δίκτυο ευρείας περιοχής.

Ασύρματο δίκτυο(WLAN): Ασύρματο δίκτυο τοπικής περιοχής.

Τρίτης γενιάς δίκτυο(3G): Δίκτυο που χρησιμοποιείται κυρίως για την επικοινωνία με τα κινητά.

Αυθεντικοποίηση(AH): αυθεντικοποιεί την προέλευση των πακέτων δεδομένων.

SPD: Ορίζει κανόνες (rules) για τον τρόπο που το IPsec πρέπει να μεταχειριστεί τα διάφορα IP πακέτα (datagrams).

Έλεγχος ακεραιότητας (ICV): Είναι η τιμή με την οποία γίνεται η πιστοποίηση της ταυτότητας του χρήστη, δηλ. η «καρδιά» του πρωτοκόλλου AH.

ΑΚΡΩΝΥΜΙΑ

ESP	Encapsulating Security Payload
AH	Authentication Header
SPI	Security Parameter Index
COA	Care of Address
IP	Internet Protocol
MIP	Mobile IP
IETF	Internet Engineering Task Force
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
WAN	Wide Area Network
WLAN	Wireless Local Area Network
SPD	Security Policy Database
UMTS	Universal Mobile Telecommunications System
AAA	Authentication, Authorization, Accounting
ICV	Integrity Check Value
LAN	Local Area Network

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] Χριστόφορος Νταντογιάν, "Μελέτη και σχεδιασμός μηχανισμού δρομολόγησης για δίκτυα αισθητήρων", Διδακτορική διατριβή, Δεκ. 2009.

[2] R. Thayer, R. Glenn, IP Security Document Roadmap, November 1998, http://www.faqs.org/rfcs/rfc2411.html

[3] W. Stallings, *"Network Security Essentials: Applications and Standards",* 3rd edition, Prentice Hall, 2007

[4] 3GPP TS 23.234 (v8.0.0), "*3GPP System to WLAN Interworking; System description*", Release 8, 2008.

[5] J. Arkko, H. Haverinen, "*EAP-AKA Authentication*", RFC 4187, Jan. 2006.

[6] Tom Sheldon and Big Sur Multimedia, IPSec (IP Security), 2001, http://www.linktionary.com/i/ipsec.html

[7] 3GPP TS 22.100 (v3.7.0), "*UMTS Phase 1 Release '99*", Oct. 2001.

[8] M. Lee, G. Kim, S. Park, S. Jun, J. Nah, O. Song, "Efficient 3G/WLAN Interworking Techniques for Seamless Roaming Services with Location-Aware Authentication", *NETWORKING 2005*, Waterloo Ontario, Canada, May 2005

[9] S. Kent, R. Atkinson, "*Security Architecture for Internet Protocol*", RFC 2401, Nov. 1998.

[10] S. Kent, R. Atkinson, "*IP Authentication Header (AH)*", RFC 2402, Nov. 1998.

[11] S.Kent, R.Atkinson, "*IP Encapsulating Security Payload (ESP)*", RFC 2406, Nov. 1998.

[12] 3GPP TS 33.234 (v8.1.0), "*3G security; WLAN interworking security; System description*", Release 8, Mar. 2008.

[13] H. Haverinen, J. Saloway "*EAP-SIM Authentication*", RFC 4186, Jan. 2006.

[14] C. Xenakis, L. Merakos, “Security in third Generation Mobile Networks”, *Computer Communications*, Elsevier Science, Vol.27, No. 7, pp 638-650, May 2004.

[15] C. Laat, G .Gross, L.Gommans, J.Vollbrecht, D. Spence, “*Generic AAA Architecture*”, RFC 2903, Aug. 2000.

[16] IEEE 802.16e-2005, “*IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1*,” 2005

[17] B.Aboba, L.Blunk, J.Vollbrecht, J.Carlson, H.Levkowetz, “*The Extensible Authentication Protocol (EAP)*”, RFC 3748, Jun. 2004.

[18] B. Aboba, D. Simon, “*EAP TLS Authentication Protocol*”, RFC2716, Oct. 1999.

[19] ETSI TS 33.902, “Formal Analysis of 3G Authentication Protocol”, 2002.

[20] C. Kaufman, “The Internet Key Exchange (IKEv2) Protocol”, RFC 4306, Dec. 2005.

[21] Y. Zhang, M. Fujise, “*An Improvement for Authentication Protocol in Third Generation Wireless Networks*”, IEEE Transactions on Wireless Communications”, Vol.5, No. 9, pp 2348-2352, Sep.2006.

[22] N. Asokan, V. Niemi, K. Nyberg. “*Man-in-the-Middle in Tunneled Authentication Protocols*”. Lecture Notes in Computer Science, Vol. 3364, pp. 28-41, Springer 2005.

[23] C.C. Yang, Y.W. Yang, W.T. Liu, “*A Robust Authentication Protocol with Non-Repudiation Service for Integrating WLAN and 3G Network*”, Wireless Personal Communications, Springer, Vol. 39, No 2, pp 229-251, Oct 2006.

[24] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, S. Miller, “*Efficient Authentication and Key Distribution in Wireless IP Networks*”, IEEE Wireless Communications, Vol 10, No 6, pp 52–61, Dec 2003.

[25] P. Prasithsangaree, P. Krishnamurthy, "*A new authentication mechanism for loosely coupled 3G-WLAN integrated networks*" in IEEE 59th Vehicular Technology Conference, (VTC), Vol. 5, pp. 2998–3003, May 2004.

[26] Y.B. Lin, Y.K. Chen, *"Reducing Authentication Signalling Traffic in Third-Generation Mobile Network",* IEEE Transactions on Wireless Communications", Vol.2, No. 3, pp 493-501, May 2003.

[27] W. Liang, W. Wang, "*A Local Authentication Control Scheme Based on AAA Architecture in Wireless Networks*", in IEEE 60th Vehicular Technology Conference (VTC), Vol. 7, pp. 5276-5280, Sep. 2004.

[28] J.A. Saraireh, S. Yousef, "*A New Authentication Protocol for UMTS Mobile Networks***",** EURASIP Journal on Wireless Communications and Networking, 2006.

[29] C.C. Chang, J.S. Lee, Y.F. Chang, "*Efficient Authentication Protocols of GSM*", Computer Communication, Elsevier Science, Vol. 28, No 8, pp. 921-928, Feb. 2005.

[30] 3GPP TS 33.203 (v8.5.0), "3G security; Access security for IP based services", Release 8, 2008.

[31] 3GPP TS 33.102 (v.8.1.0), "*3G Security; Security architecture*", Release 8, 2008.

[32] H. Krawczyk, M. Bellare, R. Canetti, "*HMAC: Keyed-Hashing for Message Authentication",* RFC 2104, Feb 1997.

[33] H. Haverinen, J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC 4186, Jan 2006.

[34] J. Rosenberg, "*SIP: Session Initiation Protocol*", RFC 3261, Jun 2002

[35] P. Funk, S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLSv0)", RFC 5281, Aug 2008

[36] C.M. Huang, J.W. Li, "*One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem for UMTS*", IEEE 21st International Conference on Advanced Networking and Applications (AINA'07), Niagara Falls, Canada, May 2007

[37] C. Ntantogian, C. Xenakis, "*Reducing Authentication Traffic in 3G-WLAN Integrated Networks*", IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC), Athens, Greece, Sep 2007.

[38] WiMAX Forum Network Architecture Stages 2 and 3 - Release 1, http://www.wimaxforum.org

[39] Christoforos Ntantogian, Christos Xenakis, Lazaros Merakos, *"An Enhanced EAP-SIM Authentication Scheme for Securing WLAN"*, 15th IST Mobile & Wireless Communications, Mykonos, Greece, June 2006.

[40] Christoforos Ntantogian, Christos Xenakis, "*A Security Binding for Efficient Authentication in 3G-WLAN Heterogeneous Networks*", PhD poster presented in the 6th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2007), Corfu, Greece, June 2007.

[41] Christoforos Ntantogian, Christos Xenakis, Ioannis Stavrakakis, "*Efficient Authentication for Users Autonomy in Next Generation All-IP Networks*", In Proc. In Proc. 2nd International Conference on Bio-Inspired Models of Network, Information, and Computing Systems (BIONETICS 2007), Budapest, Hungary, Dec 2007.

[42] Christoforos Ntantogian, Christos Xenakis,*"One pass EAP-AKA Authentication in 3G-WLAN Integrated Networks"*,Wireless Personal Communications, Springer, (accepted for publication).

[43] Lin-Yi Wu and Yi-Bing Lin, "Authentication Vector Management for UMTS", IEEE Transactions on Wireless Communications, Vol. 6 No 11, Nov. 2007.