Ατομική Διπλωματική Εργασία

ΑΣΦΑΛΕΙΑ ΣΕ ΠΡΩΤΟΚΟΛΛΑ ΚΙΝΗΤΙΚΟΤΗΤΑΣ ΒΑΣΙΣΜΕΝΑ ΣΤΟ IPv6: ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΣΥΣΤΑΣΕΙΣ.

Ευτύχιος Τσιχλάκης

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάης 2009

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ασφάλεια σε πρωτόκολλα κινητικότητας βασισμένα στο IPv6: αξιολόγηση και συστάσεις.

Ευτύχιος Τσιχλάκης

Επιβλέπων Καθηγητής

Βάσος Βασιλείου

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάης 2009

Ευχαριστίες

Αρχικά θέλω να ευχαριστήσω τους γονείς μου που έκαναν τα πάντα για εμένα και μου στάθηκαν σε όλες τις φάσεις της ζωής μου. Έπειτα τους φίλους μου και εδώ και στην Ελλάδα που με στήριξαν, καθώς και τον επιβλέπων καθηγητή μου κύριο Βασιλείου που έκανε πολύ υπομονή με εμένα. Τέλος ένα ιδιαίτερο ευχαριστώ στην κυρία Ειρήνη Πασπαράκη η οποία με την υπομονή της κατάφερε να με μάθει πολλά πράγματα.

Ειδικά ευχαριστώ την Άννα-Τσαμπίκα-Σαρρή για την εξέταση αυτής της διατριβής για την ορθογραφική αρτιότητα της.

Περίληψη

Η διπλωματική αυτή εργασία έχει ως στόχο να αναλύσει το πόσο ασφαλής είναι τα πρωτοκόλλα που έχουν προταθεί και είναι βασισμένα στο Mobile IPv6. Τα πρωτόκολλα αυτά είναι: MIPv6, FMIPv6, HMIP, FHMIPv6, S-MIP, F-FHMIPv6, TIMIP, eTIMIP, SIGMA, P-SIGMA και MIFA. Αφού τα εξετάσαμε, είδαμε το πώς μπορεί ένα πρωτόκολλο να πέσει θύμα κακόβουλης ενέργειας. Περιγράψαμε και ομαδοποιήσαμε αυτές τις επιθέσεις. Έπειτα αναλύσαμε το IPSec, ένα ευρέως διαδεδομένο πρωτόκολλο για να ασφαλίζει το IP, το οποίο προσαρμόζεται ανάλογα με τις ανάγκες. Εξετάσαμε τα πρωτόκολλα σχετικά με τις επιθέσεις, είδαμε ποιες αρχές ασφάλειες προσφέρουν, και όπου κρίθηκε αναγκαίο εφαρμόσαμε χαρακτηριστικά του IPSec. Τέλος συνοψίσαμε τα συμπεράσματα για την ασφάλεια πρωτοκόλλων κινητικότητας.

Περιεχόμενα

1. Εισαγωγή

1.1 *Στόχος εργασίας και μεθοδολογία*

Ήδη ζούμε σε μια εποχή όπου σε όποιο σημείο και αν βρισκόμαστε, πάντα υπάρχει ένα δίκτυο στο οποίο μπορούμε να έχουμε πρόσβαση και να μας παρέχει υπηρεσίες. Όσο εξελίσσεται αυτή η τεχνολογία, τόσο μεγαλύτερες ανάγκες δημιουργούνται και τόσο οι απαιτήσεις μας μεγαλώνουν. Ήδη μιλάμε για κινητά δίκτυα επικοινωνίας που συνδέουν τον καθένα μας και είναι συνδεδεμένα εικοσιτέσσερις ώρες και επτά μέρες την εβδομάδα. Για το άμεσα ορατό μέλλον βλέπουμε συσκευές να επικοινωνούν αυτόματα και ασύρματα και να ανταλλάσουν πληροφορίες.

Μέσα σε όλο αυτό το πολύπλοκο μέλλον των κινητών δικτύων υπάρχει η έννοια της ασφάλειας των ευαίσθητων πληροφοριών οι οποίες είναι δυνατόν να <<ακουστούν>> από τον καθένα. Στόχος λοιπόν αυτής τις διπλωματικής είναι να εξετάσει ποιες παραμέτρους και ποιά μεθοδολογία θα πρέπει να ακολουθεί ένα ασφαλές πρωτόκολλο κινητής επικοινωνίας, βασισμένο στο IPv6, καθώς και να αξιολογήσει ήδη υπάρχοντα πρωτόκολλα.

Ειδικότερα, θα εξεταστούν τρόποι ασφαλούς επικοινωνίας. Η εξέταση, θα γίνει υπό την παρατήρηση του πώς λειτουργούν ήδη εγκεκριμένα πρωτοκολλά ασφαλείας. Έπειτα, θα εξετάσουμε εάν αυτά εφαρμόζονται σε άλλα πρωτόκολλα, τα οποία είναι παρεμφερή με αυτά που είναι καθορισμένα από τον IETF (Internet Engineer Task Force).

Το συμπέρασμα, αυτής της διπλωματικής εργασίας είναι να κριθούν κάποια πρωτόκολλα σαν ασφαλή ή μη και να βγει μια μεθοδολογία όπου θα εκφράζει το τί πρέπει να πληροί ένα πρωτόκολλο για να είναι ασφαλές.

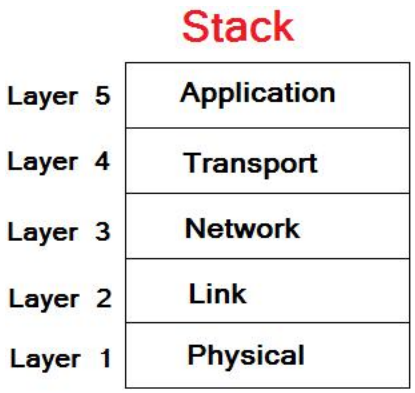
Για να διερευνήσουμε το αντικείμενο αφενός πρέπει να γνωρίζουμε το πώς λειτουργούν τα πρωτοκολλά και αφετέρου να εξετάσουμε τις απειλές που διατρέχουν από τις κακόβουλες ενέργειες.

2. Δίκτυα και ασφάλεια

2.1 *Internet protocol stack*

Κάθε πακέτο το όποιο δρομολογείται μέσα στο διαδίκτυο κουβαλάει ένα header το οποίο είναι υπεύθυνο για την πλοήγηση του πακέτου προς το σωστό προορισμό και με ορθό τρόπο. Κάθε επίπεδο από αυτά είναι υπεύθυνο για ορισμένες λειτουργίες κατά τη δρομολόγηση, οι οποίες αρχίζουν από τη διαχείριση του πακέτου στο φυσικό επίπεδο ως και το επίπεδο της εφαρμογής.

Γενικά υπάρχουν πέντε στρώματα στα οποία έχουν διακριτά διαμοιραστεί οι λειτουργίες δρομολόγησης. Τα στρώματα αυτά είναι:



Σχήμα 2.1 Στοίβα δικτύων

Το σύνολο αυτής της διαστρωμάτωσης ονομάζεται Internet Protocol stack.

Application layer

Το στρώμα αυτό είναι στην ουσία η διεπαφή με την οποία συνεργάζονται τα προγράμματα για να πραγματοποιούν τις διεργασίες που κάνουν χρήση του δικτύου.

Transport layer

Το στρώμα αυτό είναι υπεύθυνο για την ορθή μεταφορά και των πακέτων ανάμεσα στους τερματικούς κόμβους.

Network layer

Το στρώμα δικτύου είναι αυτό το όποιο μας απασχολεί σε αυτή τη διπλωματική εργασία. Είναι το layer, το όποιο τρέχει το Internet Protocol (IP). Το στρώμα αυτό

είναι υπεύθυνο για τη δρομολόγηση των πακέτων μέσα στο διαδίκτυο μέχρι να φτάσουν στον τελικό προορισμό τους. Ακόμα το στρώμα αυτό είναι που διαχειρίζονται οι ενδιάμεσοι router για να δρομολογήσουν και να ταυτοποιήσουν το πακέτο. Το IP παρέχει και τη διεύθυνση του εκάστοτε πακέτου. Από αυτό απορρέουν πολλά ζητήματα ασφάλειας των επικοινωνιών τα οποία θα δούμε εκτενεστέρα.

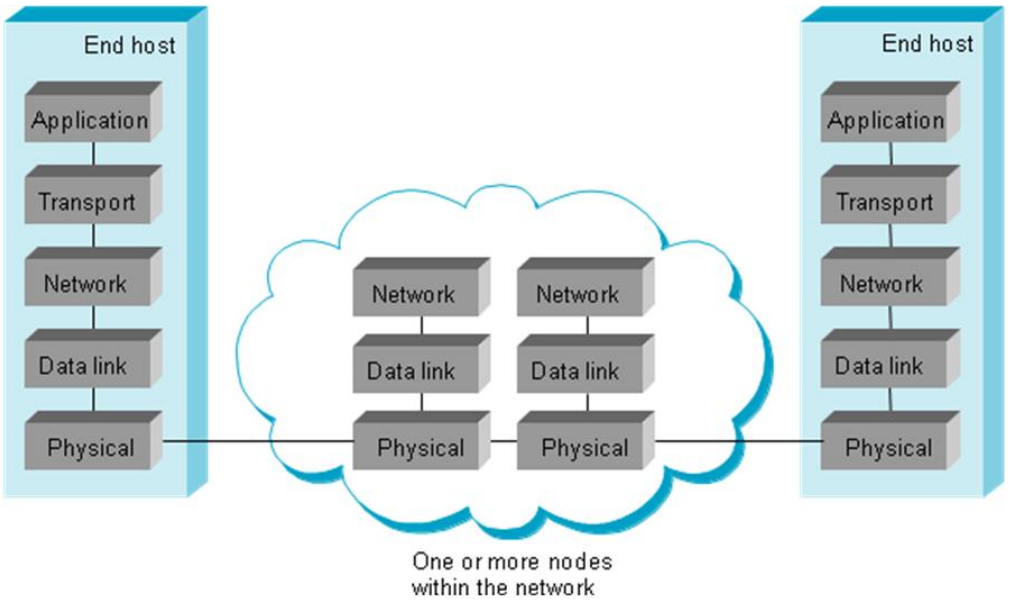
Link layer

Το στρώμα αυτό είναι υπεύθυνο αφού πάρει τη τοπική διεύθυνση του πακέτου να το δρομολογήσει προς τη σωστή κατεύθυνση.

Physical layer

Το στρώμα αυτό έρχεται σε άμεση επαφή με το φυσικό μέσο μεταφοράς του πακέτου και την προώθηση του από αυτό.

Παρακάτω βλέπουμε από ποια σταδία πέρνα ένα πακέτο από τον αρχικό μέχρι τον τελικό κόμβο.



Σχήμα 2.2 Διαπλεκόμενα στρώματα στην επικοινωνία

2.2 *Η έννοια της ασφάλειας δικτύων*

Όπως καταλαβαίνουμε και από τον τίτλο του έγγραφου θα αναλύσουμε πρωτόκολλα για κινητά δίκτυα. Τα κινητά δίκτυα είναι μια υποομάδα των δικτύων και κληρονομούν χαρακτηριστικά από αυτά. Αυτό σημαίνει ότι θα εξετάσουμε τα προβλήματα ασφάλειας που απορρέουν από το ότι τα δίκτυα που μελετάμε είναι για κινητικότητα και παράλληλα θα δούμε και τα προβλήματα που έχουν τα δίκτυα σαν γενική έννοια. Βλέποντας το θέμα της ασφαλείας δικτύων από μια θεωρητική σκοπιά μπορούμε να πούμε ότι οι αρχές που το διέπουν είναι οι έξης [ΓΒ2]:

1. **Authentication** (Πιστοποίηση)

   Με αυτή την αρχή εννοούμε ότι όταν ένας χρήστης ισχυρίζεται ότι είναι κάποιος πρέπει να μπορεί να πιστοποιήσει ότι είναι αυτός που ισχυρίζεται ότι είναι.

2. **Integrity** (Ακεραιότητα)

   Με τον όρο ακεραιότητα αναφερόμαστε στην έννοια κατά την οποία γίνεται η διασφάλιση του ότι τα δεδομένα από τον αποστολέα μέχρι να φτάσουν στον παραλήπτη δεν θα έχουν υποστεί αλλοιώσεις.

3. **Confidentiality** (Εμπιστευτικότητα)

   Με τον όρο εμπιστευτικότητα εννοούμε ότι τα δεδομένα που διακινούνται μέσα στο δίκτυο είναι δυνατόν να διαβαστούν από τον παραλήπτη τους και μόνο από αυτόν.

4. **Encryption** (κρυπτογράφηση)

   Είναι ο μηχανισμός που εγγυάται την εμπιστευτικότητα.

5. **Non – repudiation** (μη αποκήρυξη)

   Με τον όρο αυτό εννοούμε ότι, ο παραλήπτης δεδομένων από κάποιον αποστολέα μπορεί να αποδείξει ότι τα δεδομένα στάλθηκαν πράγματι από τον αποστολέα, δηλαδή ο αποστολέας δεν μπορεί να αρνηθεί ότι πράγματι τα έστειλε. Αν κάποιο δίκτυο αδυνατεί να διασφαλίσει τα παραπάνω αυτομάτως είναι μη ασφαλές.

2.3 *Δίκτυα και συναλλαγές*

Στα τέλη της δεκαετίας του 1990 οι συνδιαλλαγές που γίνονται μέσω κάποιου δικτύου ή του διαδικτύου έγιναν ευρύτερα γνωστές σε όλο το κόσμο. Ακόμα και σήμερα όμως οι συνδιαλλαγές μέσω δικτύων δεν έχουν κερδίσει πλήρως την εμπιστοσύνη του κόσμου, λόγω του ότι ο πελάτης πρέπει να <<εκθέσει>> προσωπικά δεδομένα για να ολοκληρωθεί η συνδιαλλαγή και σε συνδυασμό με τις κακόβουλες ενέργειες που ακούγονται κατά καιρούς να γίνονται, έχοντας ως στόχο αυτές τις συνδιαλλαγές. Όσοι ασχολούνται με το σχεδιασμό των δικτύων έχουν λάβει σοβαρά υπόψη τους την παράμετρο της ασφάλειας δικτύων και προσπαθούν να δώσουν στα δίκτυα τα χαρακτηριστικά εκείνα τα οποία θα τα καταστήσουν ασφαλή.

Όταν εφαρμόσουμε ένα πρωτόκολλο να τρέχει σε ένα δίκτυο, αυτό από μόνο του δεν μας παρέχει τα χαρακτηριστικά εκείνα τα οποία προσδίδουν ασφάλεια στο δίκτυο. Για να γίνει αυτό πρέπει να διαμορφώσουμε κατάλληλα τη λειτουργία του πρωτοκόλλου μας έτσι ώστε να τροποποιήσουμε κατάλληλα λειτουργίες οι οποίες είναι κρίσιμες για την ασφαλή λειτουργία του πρωτοκόλλου. Αυτό προϋποθέτει ότι πρέπει να έχουμε επίγνωση των απειλών που είναι δυνατόν να αντιμετωπίσει το δίκτυο σε επίπεδο πρωτοκόλλου σε όλο τον κύκλο ζωής του. Ειδικότερα για κάθε απειλή πρέπει να γνωρίζουμε, υπό ποιες προϋποθέσεις ένα πρωτόκολλο είναι εκτεθειμένο σε μια απειλή, με ποιο τρόπο προκαλεί τη ζημία, ποιες είναι η συνέπειες του κίνδυνου και πως προστατευόμαστε από αυτή την απειλή. Βεβαία το πρόβλημα μιας απειλής δεν είναι τόσο εύκολο να αντιμετωπιστεί όπως ίσως κάποιος να φαντάζεται αρχικά. Για παράδειγμα όταν έχουμε διαμορφώσει τις ενέργειες του πρωτοκόλλου μας έτσι ώστε να αντιμετωπίζει μια συγκεκριμένη απειλή, είναι δυνατόν το πρωτόκολλο να είναι ευάλωτο σε μια απειλή στην οποία δεν ήταν πριν τη διαμόρφωση ασφάλειας.

Μπορούμε να καταλήξουμε στο συμπέρασμα ότι δεν υπάρχουν άψογες λύσεις που να μας διασφαλίζουν απόλυτα την ασφάλεια σε ένα πρωτόκολλο. Για αυτό το λόγο πρέπει να γίνεται προσεκτικός σχεδιασμός ασφάλειας για τα πρωτόκολλα, ιδιαιτέρως για αυτά του διαχειρίζονται πακέτα με ευαίσθητες πληροφορίες. Βέβαια για να είμαστε ακριβείς πρέπει να πούμε ότι αν και η ασφάλεια σε ένα πρωτόκολλο δεν είναι απόλυτη, παρόλα αυτά πρακτικά η επικοινωνία είναι απόλυτα ασφαλής με την έννοια

του ότι σε ένα καλά σχεδιασμένο πρωτόκολλο από πλευράς ασφάλειας δεν κινδυνεύουν τα δεδομένα να κλαπούν, διότι η κωδικοποίηση είναι τέτοια που χρειάζεται πάρα πολλά χρόνια έτσι ώστε ο ταχύτερος υπολογιστής να τα αποκωδικοποιήσει.

3. Πρωτόκολλα βασισμένα στο Mobile IPv6

3.1 *Mobile IPv6 (MIPv6)*

Το MIPv6 [1] είναι η mobile έκδοση του πρωτοκόλλου IPv6. Λόγω του ότι οι κόμβοι που έχουν την ιδιότητα να κινούνται από μέρος σε μέρος και από δίκτυο σε δίκτυο, έχουν επιπρόσθετες ανάγκες. Για αυτό το λόγο σχεδιάστηκε το MIPv6 για να καλύψει αυτές τις ανάγκες. Τα επιπρόσθετα αυτά χαρακτηριστικά καλύπτουν τις ανάγκες για προσδιορισμό νέας τοποθεσίας του κινητού κόμβου καθώς και τη δρομολόγηση της πληροφορίας που το αφόρα, αυτόματα χωρίς νέες ρυθμίσεις από πλευράς χρήστη.

Στόχοι του MIPv6:

- Αδιάκοπη σύνδεση στο δίκτυο
- Σταθερή διεύθυνση
- Απρόσκοπτη μετακίνηση μεταξύ διάφορων αρχιτεκτονικών πρόσβασης στο δίκτυο (πχ WLAN, WiMAX, GSRP)
- Αδιάκοπη εκτέλεση εφαρμογών
- Mobile Node (MN) δρουν και ως server

3.1.1 Ορολογία για το Mobile IPv6

Παρακάτω παρατίθενται οι βασικοί οροί που χρησιμοποιούντα από το MIPv6.

- **Mobile Node (MN)**

Είναι ο κινητός κόμβος που κάνει χρήση του MIPv6 για να έχει πρόσβαση στο δίκτυο. Ο MN είναι εγγεγραμμένος σε ένα δίκτυο που ονομάζεται οικιακό δίκτυο. Ο MN έχει τη δυνατότητα να περιηγείται από δίκτυο σε δίκτυο και να επικοινωνεί απρόσκοπτα με τους άλλους κόμβους.

- **Correspondent Node (CN)**

Είναι ο κόμβος που δέχεται και στέλνει πληροφορίες στον MN. Ο CN μπορεί να είναι είτε κινητός είτε σταθερός κόμβος, μέσα και έξω από το δίκτυο.

- **Home Agent (HA)**

Είναι ο κόμβος – δρομολογητής που βρίσκεται στο οικείο δίκτυο. Οποιοδήποτε πακέτο σχετίζεται με τον MN δρομολογείται μέσο του HA. Όταν κάποιος CN γενικά θέλει να επικοινωνήσει με τον MN στέλνει τα πακέτα στο HA και αυτό με τη σειρά του τα δρομολογεί προς τον MN.

- **Home Address (HADD)**

Η διεύθυνση του MN στο Home Network.

- **Care of Address (CoA)**

Είναι μια προσωρινή IP διεύθυνση που δίδεται σε ένα MN όταν επισκέπτεται ένα άλλο δίκτυο και παρέχει πληροφορίες για το τρέχον σημείο σύνδεσης του κόμβου. Επίσης ο HA του κόμβου γνωρίζει αυτήν την διεύθυνση και στέλνει τα δεδομένα που προορίζονται για τον MN σε αυτήν μέσω tunneling.

- **Foreign Agent (FA):**

Ο δρομολογητής που βρίσκεται στο δίκτυο που έχει επισκεφθεί ο MN. Ο FA επικοινωνεί με τον HA για να τον ενημερώσει για την CoA του MN. Επίσης παραλαμβάνει και παραδίδει στον MN τα πακέτα που προορίζονται γι' αυτόν.

3.1.2 Μηνύματα MIPv6

- **Binding Refresh Request**

Το binding refresh request στέλνεται από το home agent ή τον correspondent node στον κινητό κόμβο όταν η εγγραφή τους στο binding cache για τον κινητό κόμβο είναι κοντά στο τέλος της ισχύος της. Η απόκριση από τον κινητό κόμβο που θέλει να συνεχίσει την επικοινωνία του είναι ένα binding update.

- **Binding Update (BU)**

Είναι το μήνυμα που στέλνει ο MN στο HA ή στο CNγια να τον ενημερώσει για την αλλαγή της CoA του.

- **Binding Acknowledgement (BA)**

Είναι το μήνυμα που στέλνει είτε ο HA είτε ο CN ως ένδειξη ότι έλαβαν το BU.

- **Home Test Init (HoTI)**

Το HoTI στέλνεται κατά την εκτέλεση της Return Routability procedure από τον κινητό κόμβο για να δοκιμάσει αν είναι εφικτή η έμμεση επικοινωνία με τον correspondent node μέσο του home agent.

- **Care-of Test Init (CoTI)**

Το CoTI στέλνεται κατά την εκτέλεση της Return Routability procedure από τον κινητό κόμβο για να δοκιμάσει αν είναι εφικτή η άμεση επικοινωνία με τον correspondent node μέσο του home agent.

- **Home Test (HoT)**

Στέλνεται σαν απόκριση στο HoTI

- **Care-of Test (CoT)**

Στέλνεται σαν απόκριση στο CoTI

3.1.3 Επικοινωνία CN με MN (έμμεση)

Όταν κάποιος CN, δεν είναι συμβατός με MIPv6 ή δεν έχει ολοκληρωθεί ακόμη η εγγραφή του binding του MN, μπορεί να επικοινωνήσει έμμεσα με τον MN. Για να γίνει αυτό πρέπει να γίνουν τα έξης βήματα:

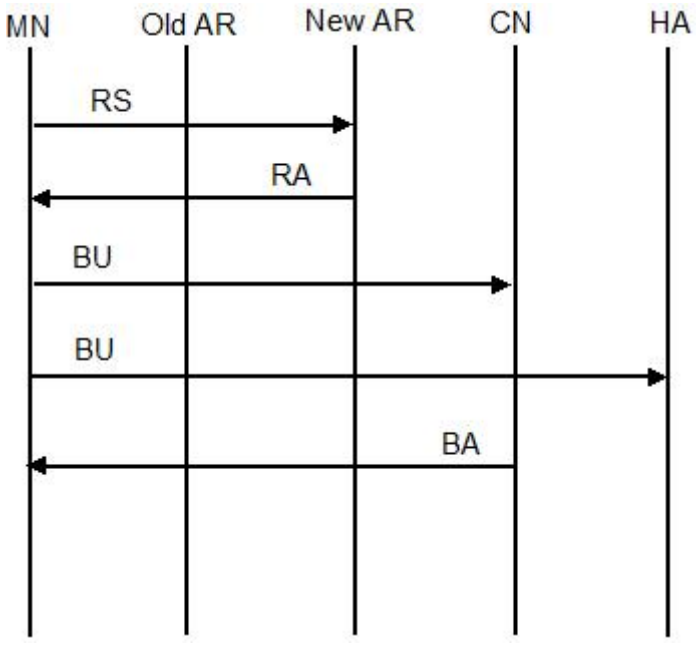
1. Πρώτα ο CN στέλνει το πακέτο με destination address τη διεύθυνση του MN στο Home Network (HADD). Για να γίνει ο διαχωρισμός σε ποιον MN αναφερόμαστε, ο κάθε MN αντιστοιχεί σε κάποιο port του HA.
2. Στην περίπτωση όπου ο MN είναι άμεσα προσβάσιμος από τον HA (είναι δηλαδή στην εμβέλεια του HA) τότε του στέλνει απευθείας το πακέτο, αλλιώς συνεχίζουμε με τα παρακάτω.
3. Ο HA εσωκλείει το πακέτο του CN σε ένα νέο πακέτο με destination address την CoA του MN και το αποστέλλει.
4. Όταν ο πακέτο έχει σαν CoA τη διεύθυνση του FA τότε αυτός με τη σειρά του βγάζει το περίβλημα του πακέτου, αλλάζει τη διεύθυνση του πακέτου με την διεύθυνση του MN στο ξένο δίκτυο και το παραδίδει.

3.1.4 Επικοινωνία CN με MN (άμεση)

Αν ο CN είναι συμβατός με το MIPv6 τότε μπορούν να ανταλλάσουν άμεσα μηνύματα σα δυο κομβόι του κινητού δικτύου.

3.1.5 Handoff

Ονομάζεται η διαδικασία κατά την οποία ο MN αποφασίζει πότε θα αλλάξει το παρόν δίκτυο με ένα καινούριο. Όταν το σήμα του Access Router (AR) γίνει αδύναμο τότε στέλνει Router Solicitation (RS) μηνύματα και οι AR αποκρίνονται με Router Advertisement (RA) μηνύματα. Όταν ο MN αποκτήσει τη νέα CoA, πρέπει να ενημερώσει τον HA και τους CN για την διεύθυνση αυτή. Για αυτό τον σκοπό ο MN στέλνει ένα Binding Update που περιέχει τη νέα του διεύθυνση. Για επιβεβαίωση ότι ο παραλήπτης πράγματι παρέλαβε το Binding Update, ο κινητός κόμβος στέλνει το Binding Acknowledgment. Μέχρι να λάβει επιβεβαίωση ο φορητός κόμβος συνεχίζει να μεταδίδει περιοδικά το πακέτο του Binding Update. Πριν τη λήξη μιας καταχώρησης στην Binding Cache για ένα κινητό κόμβο, ο CN μπορεί να ανανεώσει την καταχώρηση στέλνοντας ένα Binding Request στον κινητό κόμβο και αυτός του απαντά με ένα Binding Update.

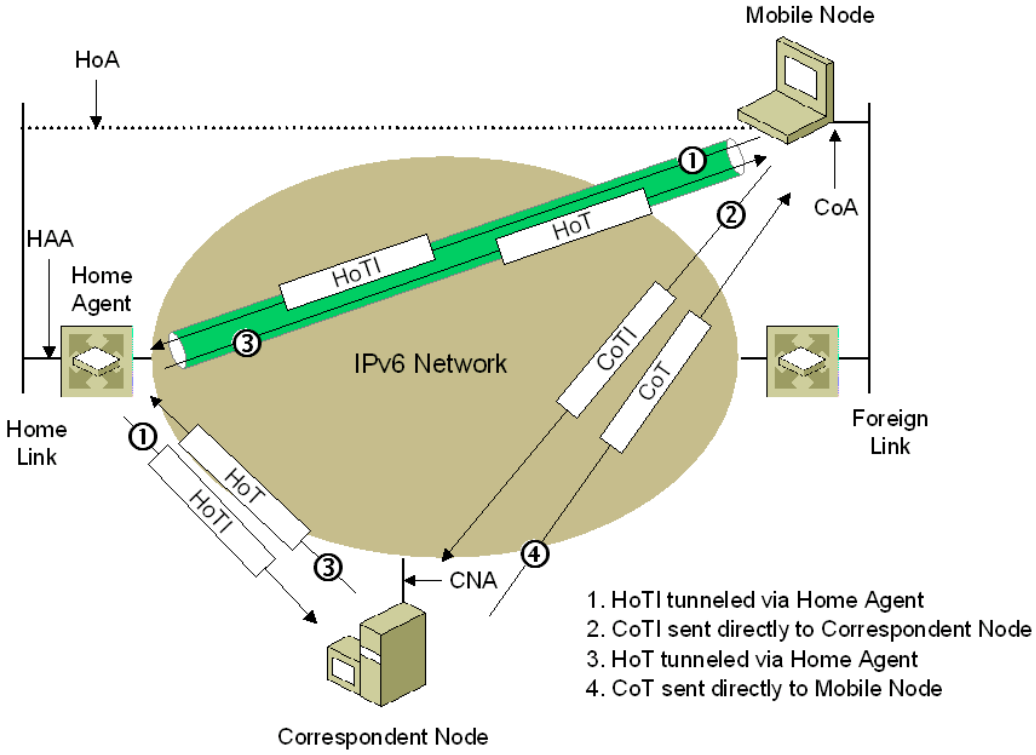


Σχήμα 3.1 MIPv6 handoff

3.1.6 Return Routability procedure

Το return routability είναι μια διαδικασία η οποία εξασφαλίζει στον CN ότι ο MN μπορεί να βρεθεί στη διεύθυνση στην οποία ισχυρίζεται ότι βρίσκεται. Μόνο με αυτή τη διαβεβαίωση ο CN μπορεί να κάνει δεκτά τα BU από τον MN. Είναι η διαδικασία κατά την οποία ελέγχεται αν η επικοινωνία του correspondent node και του κινητού κόμβου είναι μέσω του home agent. Η διαδικασία του return Routability είναι:

1. Ο MN στέλνει ένα μήνυμα HoTI έμμεσα στο CN, μέσω του HA.
2. Ο MN στέλνει το CoTI άμεσα στον CN.
3. Ο CN στέλνει ένα HoT ως απάντηση στο μήνυμα HoTI
4. Ο CN στέλνει το CoT ως απάντηση στο μήνυμα CoTI



Σχήμα 3.2 Return routability

3.1.7 Mobile Prefix Solicitation

Η διαδικασία κατά την οποία ο MN όταν βρίσκετε εκτός HA στέλνει ένα μήνυμα για να εξακριβώσει σε ποιο δίκτυο υπάγεται. Η απόκριση σε αυτό το μήνυμα είναι ένα Mobile prefix advertisement.

3.1.8 Mobile Prefix Advertisement

Η διαδικασία κατά την οποία ένας HA στέλνει μηνύματα ανά τακτά χρονικά διαστήματα ώστε να πληροφορήσει τους MN για το πρόθεμα του δικτύου. Με άλλα λόγια για να καταλάβουν οι MN σε ποιο οικείο δίκτυο υπάγονται.

3.1.9 Home Agent Address Discovery Request

Μια από τις βασικές διαδικασίες το MIPv6 είναι η διαδικασία όπου ο κάθε MN πρέπει να αποφασίσει σε ποιό δίκτυο υπάγεται κάθε στιγμή. Όταν ένας MN μετακινείται και αλλάζει δίκτυο, τότε ενεργοποιεί το μηχανισμό handoff ο όποιος εκτελείται στο physical στρώμα. Για να ολοκληρωθεί η διαδικασία και ο MN να καταλάβει ότι έχει αλλάξει δίκτυο ο κάθε agent κάθε δικτύου στέλνει ανά τακτά χρονικά διαστήματα ICMP με ένα Mobile Prefix Advertisement. Αυτά τα μηνύματα περιέχουν τις πληροφορίες διεύθυνσης (το πρόθεμα του δικτύου) του agent του δικτυού. Ο MN συγκρίνει την CoA με την καινούρια διεύθυνση που λαμβάνει και αποφασίζει αν άλλαξε δίκτυο η όχι.
Σε περίπτωση που κάποιος MN θέλει να πάρει πληροφορίες για τον agent άμεσα, στέλνει ένα ICMP router solicitation message, και ο agent αποκρίνεται.

3.1.10 Διαδικασία εγγραφής (Registration)

Όταν ο MN έχει αλλάξει και βρίσκεται σε ξένο δίκτυο και έχοντας πάρει την CoA, πρέπει να ενημερώσει ο HA για τη νέα θέση του. Αυτή η διαδικασία ονομάζεται registration. Η διαδικασία που ακολουθείται είναι:

1. Ο MN στέλνει registration request στον FA που θέλει να χρησιμοποιήσει
2. Ο FA συσχετίζει αυτήν την αίτηση με τον HA του κόμβου
3. Ο HA αποδέχεται ή απορρίπτει αυτήν την αίτηση και στέλνει registration replay στον FA.
4. Ο FA συσχετίζει αυτήν την απάντηση στον κινούμενο κόμβο.

3.1.11 Δομές δεδομένων του MIPv6

Binding Cache

Το binding cache είναι μια δομή με τη μορφή πινάκα η οποία διατηρείται από τους HA και τους CN και η οποία περιέχει τα τελευταία BA του MN. Η δομή αυτή περιέχει τα έξης στοιχεία σε κάθε εγγραφή:

- Το Home Address
- Το Care-of-Address
- Το Lifetime της έγγραφης
- Το χρόνο της τελευταίας έγγραφης

3.1.12 Binding Update list

Το binding cache είναι μια δομή με τη μορφή πίνακα η οποία διατηρείται από τον κινητό κόμβο με τα πρόσφατα binding update τα οποία έστειλε στους correspondent node και στους home agent. Η δομή αυτή περιέχει τα έξης στοιχεία σε κάθε εγγραφή:

- Τη διεύθυνση στην οποία στάλθηκε το binding update
- Την care-of-address που στάλθηκε
- Το χρόνο στον όποιο στάλθηκε
- Το χρόνο ζωής της έγγραφης
- Τη μεγίστη τιμή του sequence number από τα προηγούμενα binding update
- Το χρόνο στον όποιο το προηγούμενο binding updates στάλθηκε

3.1.13 Home Agents list

Το home agent list είναι μια δομή με τη μορφή πινάκα η οποία διατηρείται από τον home agent και περιέχει τους router από τους οποίους έλαβε ένα router advertisement message στον όποιο ο mobile node δήλωσε ότι είναι ο home agent του. Οι home agent διατηρούν αυτή τη λίστα ώστε να μπορούν να την στείλουν σε κάποιο κινητό κόμβο ο όποιος είναι μακριά από το home agent του και στέλνει μήνυμα home agent discovery. Η δομή αυτή περιέχει τα έξης στοιχεία σε κάθε εγγραφή:

- Την τοπική διεύθυνση του router η οποία αποκτήθηκε από την πηγαία διεύθυνση του Router Advertisement message
- Την διεύθυνση\εις του home agent
- Το χρόνο στον όποιο παραλήφθηκε
- Το lifetime την έγγραφης

3.2 *Hierarchical Mobile IPv6 (HMIPv6)*

Το HMIPv6 [2] είναι μια παραλλαγή του MIPv6 και έχει σαν στόχο την μείωση των μηνυμάτων Binding Updates και ως επέκταση την επιτάχυνση της επικοινωνίας των κινητών κόμβων του δικτύου. Αυτό επιτυγχάνεται με τη χρήση ενός νέου κόμβου που συντονίζει τη διαδικασία. Ο κόμβος αυτός ονομάζεται Mobility Anchor Point (MAP) και είναι ο κόμβος με τον οποίο επικοινωνεί άμεσα ο MN.

3.2.1 Ορολογία για το Hierarchical Mobile IPv6

❖ **Regional Care-of Address (RCoA)**

Είναι η διεύθυνση που παίρνει ο MN σε ένα ξένο δίκτυο. Αποτελεί διεύθυνση του υποδικτύου του Mobility Anchor Point (MAP) και γίνεται auto-configured από τον MN όταν αντιλαμβάνεται την δυνατότητα για να χρησιμοποιήσει MAP.

❖ **On-link Care-of Address (LCoA)**

Είναι η διεύθυνση που σχηματίζεται στην διεπιφάνεια του MN και βασίζεται στο πρόθεμα που διαφημίζει ο δρομολογητής.

❖ **Mobility Anchor Point (MAP)**

Ο MAP κόμβος είναι μια οντότητα που εισάγεται για να λειτουργήσει το HMIPv6. Είναι ο δρομολογητής που βρίσκεται στο δίκτυο που επισκέπτεται ο κόμβος. Ο MAP χρησιμοποιείται από τον MN σαν τοπικός HA. Η λειτουργία των HA και των CN παραμένει η ίδια, ενώ ο νέος τύπος κόμβου MAP λειτουργεί HA που κρατά ένα binding της RCoA με την LCoA του MN.

Το HMIPv6 αποτελεί μία επέκταση του MIPv6. Έτσι ένας MN που υποστηρίζει HMIPv6 επιλέγει να κάνει χρήση του MAP, αν ανακαλύψει ότι υπάρχει αυτή η δυνατότητα στην αρχιτεκτονική του δικτύου που επισκέπτεται αλλιώς λειτουργεί βάσει του MIPv6 πρωτοκόλλου. Αυτό μπορεί να γίνει και σε περιπτώσεις που ο MN επισκέπτεται ένα δίκτυο το οποίο βρίσκεται κοντά στο οικείο του δίκτυο. Σε αυτή τη περίπτωση ο MN μπορεί να χρησιμοποιήσει τον HA αντί τον MAP.

Πιο συγκεκριμένα ο MAP δίνει λύση με τον ακόλουθο τρόπο:

1. Ο MN στέλνει τα BU στον MAP αντί να τα στέλνει στο HA και σε όλους τους CN, όπως προβλέπει το MIPv6 για κάθε φορά που ο MN αλλάζει υποδίκτυο.
2. Μόνο ένα BU χρειάζεται να σταλεί στο MAP για να επαναδρομολογηθεί όλος ο όγκος δεδομένων στον καινούριο προορισμό (το νέο υποδίκτυο). Μόνο ένα χρειάζεται ανεξάρτητα από το πόσοι CN έχουν επικοινωνία με τον MN.

- **HMIPv6-Aware Mobile Node**

Ο HMIPv6-Aware MN είναι ουσιαστικά ο κόμβος ο οποίος είναι συμβατός με το HMIPv6. Αυτός ο κόμβος έχει την ιδιότητα να λαμβάνει και να προωθεί μηνύματα στον MAP.

- **Access Router (AR)**

Είναι ο προκαθορισμένος router του MN, ο οποίος παραλαμβάνει την εξωτερική κυκλοφορία των κινητών του κόμβων.

- **Local Binding Update (LBU)**

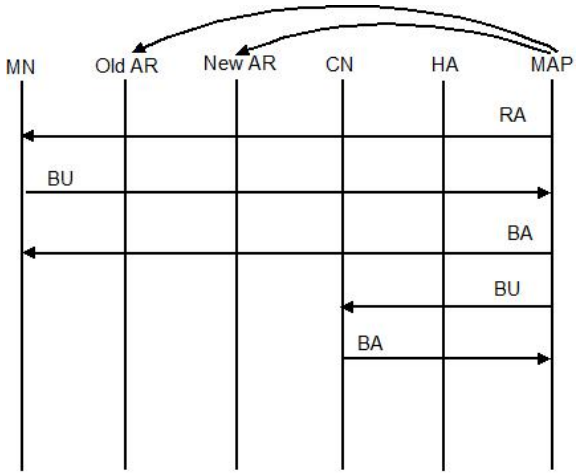
Μήνυμα που στέλνεται από τον MAP για εγκαθίδρυση της δέσμευσης μεταξύ RCoA και LCoA.

3.2.2 Εισαγωγή κινητού κόμβου σε εμβέλεια του MAP

Όταν ένας MN εισέρχεται στην περιοχή ενός καινούριου MAP θα λάβει Router Advertisements που περιέχουν πληροφορίες για έναν ή περισσότερους τοπικούς MAP. Ο MN μπορεί να δεσμεύσει την τρέχουσα θέση του (*on-link CoA*) με μία διεύθυνση στο υποδίκτυο του MAP (*RCoA*).

3.2.3 Προώθηση πακέτων προς κινητό κόμβο

Ο MAP λειτουργεί σαν HA για τον MN. Ο MAP θα λάβει όλα τα πακέτα εκ μέρους του MN που εξυπηρετεί, θα τα ενθυλακώσει και θα τα προωθήσει απευθείας στην LCoA του MN. Όταν ο MN αλλάζει τη διεύθυνση εντός της περιοχής ενός MAP πρέπει μόνο να εγγράψει την LCoA με τον MAP. Η RCoA δε χρειάζεται να εγγραφεί με τον HA και τους CN, αφού δεν αλλάζει εντός της περιοχής του MAP. Με τον τρόπο αυτό οι κινήσεις του MN είναι αόρατες στους CN με τους οποίους επικοινωνεί ο MN.

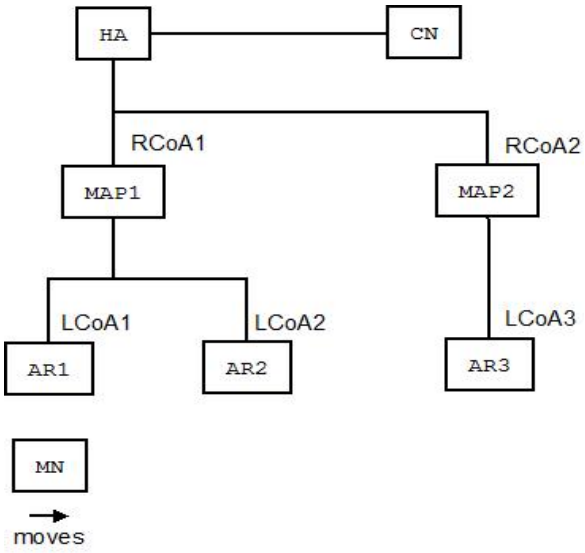


Σχήμα 3.3.1 HMIPv6 handoff

3.2.4 Περιήγηση κινητού κόμβου ανάμεσα στους MAP

Όταν ο MN περιηγείται μέσα στο δίκτυο, ελέγχει μέσω router advertisment message αν βρίσκεται ακόμη στην ίδια MAP περιοχή. Σε περίπτωση που ανακαλύψει ότι βρίσκεται σε άλλη περιοχή στέλνει Binding Update στον HA και στους CN και θα αρχίσει τη διαδικασία ανεύρεσης νέου MAP. Εφόσον βρει νέο MAP ο MN στέλνει ένα BU που περιέχει την RCoA και την LCoA, για να εγγράφει με το MAP. Στην συνέχεια χρησιμοποιεί αυτές τις πληροφορίες για να είναι σε θέση να προωθεί τα πακέτα, που λαμβάνει από τον HA ή τους CN, στον προορισμό τους.

Εάν δε βρεθεί υποψήφιος MAP τότε ο MN χρησιμοποίει το MIPv6, αφού έχουμε αναφέρει ότι το HMIPv6 είναι συμβατό με το MIPv6.

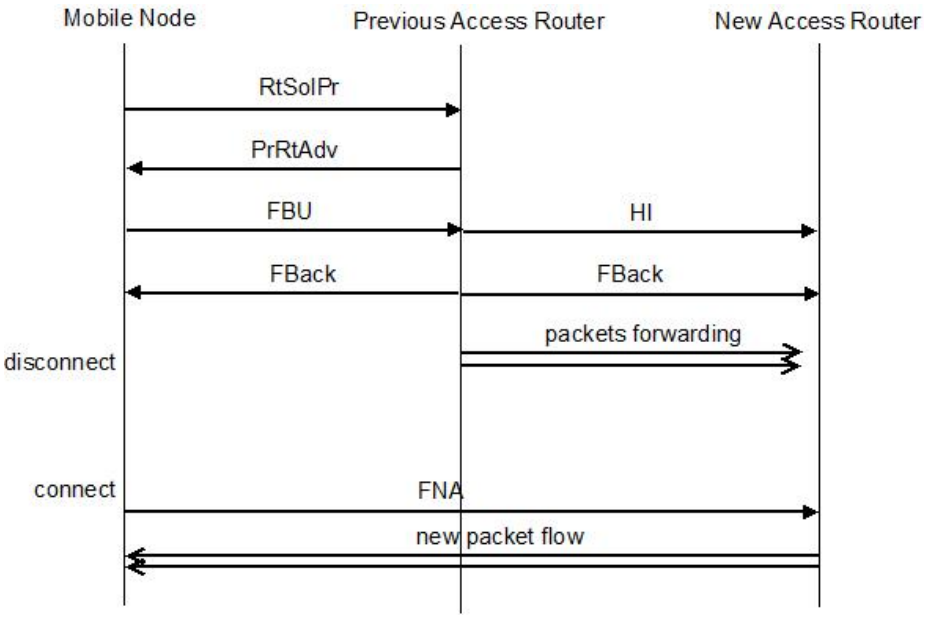


Σχήμα 3.3.2 HMIPv6 schema

3.3 *Fast Handoff Mobile IPv6 (FMIPv6)*

Το FMIPv6 [3] έρχεται να αντιμετωπίσει το πρόβλημα του πώς θα επιτραπεί σε έναν MN να στέλνει πακέτα αμέσως μόλις ανακαλύψει μία νέα σύνδεση και πώς θα λαμβάνει πακέτα μόλις η παρουσία του γίνει φανερή στον νέο AR. Το πρόβλημα αυτό συχνά επηρεάζει τις real time εφαρμογές, όπου η καθυστέρηση μέχρι να ολοκληρωθεί το handoff μπορεί να επηρεάσει την εφαρμογή αισθητά.

Η λύση επιτρέπει σε έναν MN να συνεχίζει να χρησιμοποιεί την παλιά CoA μέχρι να κάνει τον εαυτό του ένα MIPv6 end-point κόμβο και να λάβει από μακριά μία νέα CoA. Η βασική ιδέα πίσω από την λειτουργία του πρωτοκόλλου είναι να παίρνει πληροφορίες από το link στρώμα (με χρήση ενός trigger) είτε για να προβλέψει, είτε για να αντιδράσει γρήγορα σε περίπτωση handoff. Το πρωτόκολλο επιτρέπει σε ένα MN να εντοπίσει τη μετακίνηση του σε ένα υποδίκτυο και να του παρέχει όλες τις απαραίτητες πληροφορίες για το νέο σημείο σύνδεσης ενώ αυτός είναι ακόμη συνδεδεμένος στο παλιό.



Σχήμα 3.4 FMIP signals flow

3.3.1 Ορολογία για το Fast Handoff Mobile IPv6

- **Mobile Node (MN)**

FMIPv6 συμβατός κόμβος.

- **Access Point (AP)**

Μια Στρώμα 2 συσκευή που συνδέεται σε ένα υποδίκτυο IP η οποία προσφέρει ασύρματη συνδεσιμότητα σε MN.

- **Access Router (AR)**

Ο router που βρίσκεται ο MN.

- **Previous Access Router (PAR)**

Ο router που ήταν ο MN πριν το handoff.

- **New Access Router (NAR)**

Ο router που ήταν ο MN μετά το handoff.

- **Previous CoA (PCoA)**

Η CoA που είχε ο MN όταν ήταν στην εμβέλεια του PAR

- **New CoA (NCoA)**

Η CoA που έχει ο MN όταν θα είναι στην εμβέλεια του NAR

- **Handoff**

Μια διαδικασία κατά την οποία ο MN αλλάζει από τον πρώτο AR στον επόμενο και σηματοδοτεί την αλλαγή υποδίκτυου.

- **Router Solicitation for Proxy Advertisement (RtSolPr)**

Ένα μήνυμα από τον MN στην PAR ζητώντας πληροφορίες για το ενδεχόμενο handoff.

- **Proxy Router Advertisement (PrRtAdv)**

Ένα μήνυμα από τον PAR στον MN το οποίο παρέχει πληροφορίες σχετικά με τα γειτονικά links. Το μήνυμα επίσης σηματοδοτεί το network-initiated handoff.

- **(AP-ID, AR-Info) tuple**

Περιέχει τους access routers και τις IP διευθύνσεις, καθώς και την πρόθεμα που ισχύει για την διασύνδεση με το οποίο επισυνάπτεται.

- **Assigned Addressing**

Ένα ιδιαίτερο είδος NCoA configuration κατά την οποία ο NAR αναθέτει μία IPv6 διεύθυνση στον MN.

- **Fast Binding Update (FBU)**

Μήνυμα από τον MN που αναθέτει στο PAR να αναπροσανατολίσουν τη ροή των δεδομένων (προς NAR).

- **Fast Binding Acknowledgment (FBack)**

Η απόκριση από το PAR για το FBU

- **Fast Neighbor Advertisement (FNA)**

Ένα μήνυμα από τον MN προς τον NAR για να ανακοινώσει την σύνδεση και για να επιβεβαιώσει την χρήση NCoA όταν ο MN δεν έχει λάβει FBACK.

- **Handoff Initiate (HI)**

Ένα μήνυμα από τον PAR στην NAR MN σχετικά με το handoff.

- **Handoff Acknowledge (HAck)**

Ένα μήνυμα από το NAR στην PAR ως απάντηση στην HI.

- **Trigger**

Για τις ανάγκες του πρωτοκόλλου χρειάζεται να το link στρώμα να παρέχει κάποιες πληροφορίες οι οποίες εκμεταλλεύονται για το σκοπό του fast handoff. Ένας trigger λοιπόν ειδοποιεί από το link στρώμα το πρωτόκολλο (network στρώμα) βάσει του σήματος που δέχεται από τον router.

3.3.2 Λειτουργία του Fast Handoff

Μόλις ο MN ανακαλύψει ένα ή περισσότερα νέα AR στέλνει RtSolPr για να πάρει πληροφορίες από τον AR. Σαν απάντηση στο RtSolPr, ο AR στέλνει το PrRtAdv, στο οποίο μπορεί να περιέχονται ένα από τα παρακάτω γεγονότα:

1. Αν ο AR δεν έχει καταχώρηση για το νέο/α AR, τότε θα απαντήσει ότι το νέο AR είναι άγνωστο. Έτσι ο MN πρέπει να σταματήσει τη διαδικασία fast handoff που γίνονται στο τρέχων link και να στείλει FBU σε νέο link αν υπάρχει. Αν το NAP είναι συνδεδεμένο στο τρέχον AR, ο παλιός AR πρέπει να απαντήσει δίνοντας μια τιμή που δηλώνει ότι το NAR είναι συνδεδεμένο με τον AR (PAR) και δεν είναι απαραίτητο να στείλει πληροφορίες για prefix.
2. Αν το νέο AR είναι γνωστό, ο AR απαντά ενημερώνοντας με την πλειάδα [AP-ID, AR-Info].
3. Εάν παρέχεται η δυνατότητα από τον νέο AR να παρέχει πληροφορίες για νέα AR αποκρίνεται με πλειάδες [AP-ID, AR-Info] και ο MN τις επεξεργάζεται ανάλογα.

Αφότου πάρει το PrRtAdv, ο MN στέλνει FBU μήνυμα το οποίο περιέχει την NCoA. Ο MN στέλνει FBU από το link του PAR όταν υπάρχει δυνατότητα για πρόβλεψη του NAR. Αν δεν υπάρχει δυνατότητα για πρόβλεψη ή αν δεν φτάσει FBack, ο MN θα στείλει το FBU μόλις συνδεθεί στο NAR. Το FBU θα ήταν καλό να ενθυλακώνεται

σε ένα FNA μήνυμα. Αυτό επιτρέπει στο NAR να απορρίψει το FBU σε περίπτωση που η διεύθυνση συγκρούεται με το εξωτερικό FNA πακέτο.

Σαν απόκριση FBU, ο PAR εγκαθιδρύει μια σύνδεση με τον PCoA και στέλνει το σήμα FBack στον MN. Προτού γίνει αυτό, ο PAR στέλνει ένα HI μήνυμα στο NAR και λαμβάνει ως απάντηση ένα σήμα Hack. Για να καθορίσει την NCoA, ο PAR εφαρμόζει το longest prefix της NCoA με τα prefix των γειτονικών router. Αν η διεύθυνση προέλευσης στο FBU είναι PCoA, αυτό σημαίνει ότι στάλθηκε από το link του PAR. Με το HI αρχίζει ένα tunnel μεταξύ του NAR και του PAR, για να μπορεί ο MN να έχει την PCoA για τις συνδέσεις που διατηρεί. Σαν απόκριση του HI, ο NAR στέλνει ένα HACK σήμα. Σε περίπτωση που η NCoA μπορεί να χρησιμοποιηθεί τότε:

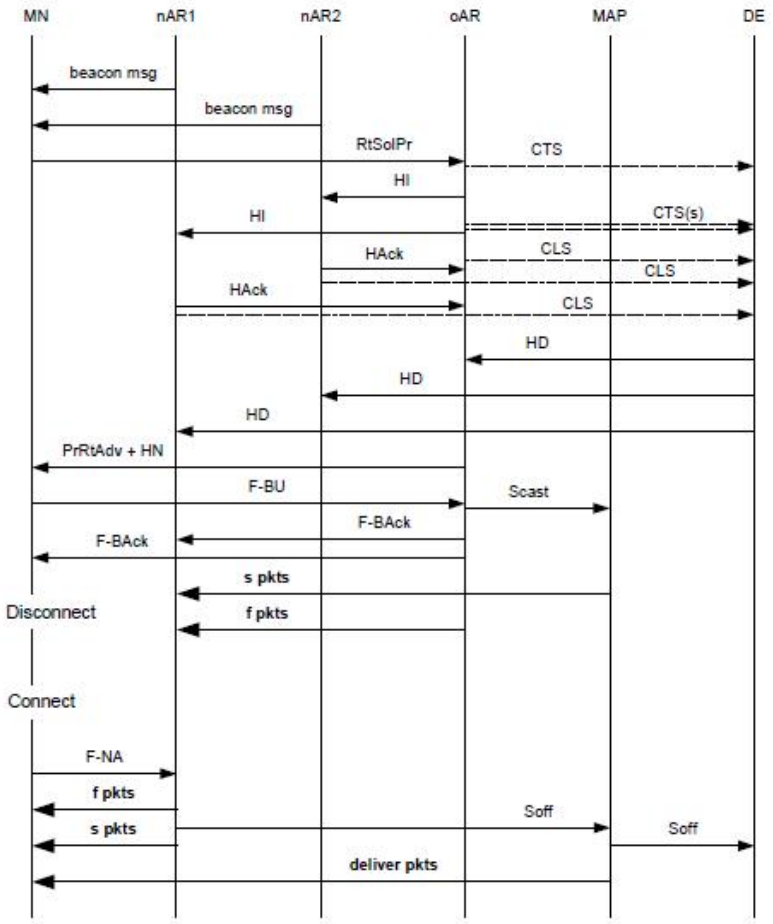
1. Η NCoA λειτουργεί ως proxy διεύθυνση για ένα χρονικό διάστημα στο οποίο αναμένεται να ολοκληρωθεί το handoff.
2. Έπειτα από το χρόνο αυτό η NCoA δεσμεύεται για τον MN
3. Τέλος στέλνεται ένα HACK σήμα.

Μετά τη λήψη του HACK μηνύματος, ο PAR στέλνει ένα Fast Binding Acknowledgement (FBACK) μήνυμα στον MN, για να επιβεβαιώσει τη δυνατότητα χρήσης της NCoA. Μόνο μετά από αυτό το μήνυμα ο MN μπορεί να χρησιμοποιήσει την NCoA.

Αμέσως μετά την σύνδεση με τον NAR, ο MN στέλνει ένα Fast Neighbor Advertisement (FNA) μήνυμα. Το μήνυμα αυτό περιλαμβάνει την PCoA και τη διεύθυνση του στρώματος σύνδεσης του MN, εξυπηρετώντας στην επιβεβαίωση της NCoA όταν το FBACK δεν είχε ληφθεί και σε κάθε περίπτωση ανακοινώνει την παρουσία του MN στον NAR. Ως απάντηση, ο NAR στέλνει ένα Router Advertisement με μία Neighbor Advertisement Acknowledgement (NAACK) επιλογή η οποία υποδεικνύει αν επιτρέπεται η χρήση της NCoA. Αν δεν επιτρέπεται η χρήση της ο MN πρέπει να σχηματίσει άλλη νέα CoA. Μόλις ο MN κρίνει έγκυρη την νέα CoA στέλνει Neighbor Advertisement μήνυμα. Αυτό το μήνυμα επιτρέπει στους γείτονες του MN να ανανεώσουν τα cache entries τους με την νέα διεύθυνση του MN.

3.4 *Seamless Mobile IPv6 (S-MIP)*

Το S-MIP [4] δημιουργήθηκε για να καλύψει την ανάγκη για μια ομαλότερη επικοινωνία κατά τις μετακινήσεις ενός MN μέσα στο δίκτυο. Υπάρχει το πρόβλημα ότι όταν γίνεται το handoff διακόπτονται όλες οι συνδέσεις και επανεγκαθιδρύονται όταν έχει τελειώσει το handoff για την κύρια έκδοση του MIPv6. Ο κύριος στόχος του S-MIP είναι να μειώσει το χρόνο που γίνονται τα handoff. Το S-MIP κάνει εισαγωγή ενός νέου κόμβου, του Decision Engine (DE), όπου ο σκοπός του DE είναι να παρακολουθεί την κίνηση των κινητών κόμβων και να παίρνει αποφάσεις για τυχόν handoff τους. Γενικά το S-MIP έχει στοιχεία και από το FMIPv6 και το HMIPv6.



Σχήμα 3.6 Signals flow για το seamless Mobile IPv6

3.4.1 Ορολογία για το Seamless Mobile IPv6

- **Current Tracking Status (CTS)**

Στέλνεται από τον oAR στον DE και περιέχει πληροφορίες για την θέση του MN.

- **Carrying Load Status (CLS)**

Στέλνεται από τους AR στο DE και περιέχει πληροφορίες για το πόσες κινητές συσκευές διαχειρίζεται ο AR.

- **Handoff Decision (HD)**

Στέλνεται από τον DE στους AR και περιέχει την απάντηση για το ποιός AR θα κάνει handoff.

- **Handoff Notification (HN)**

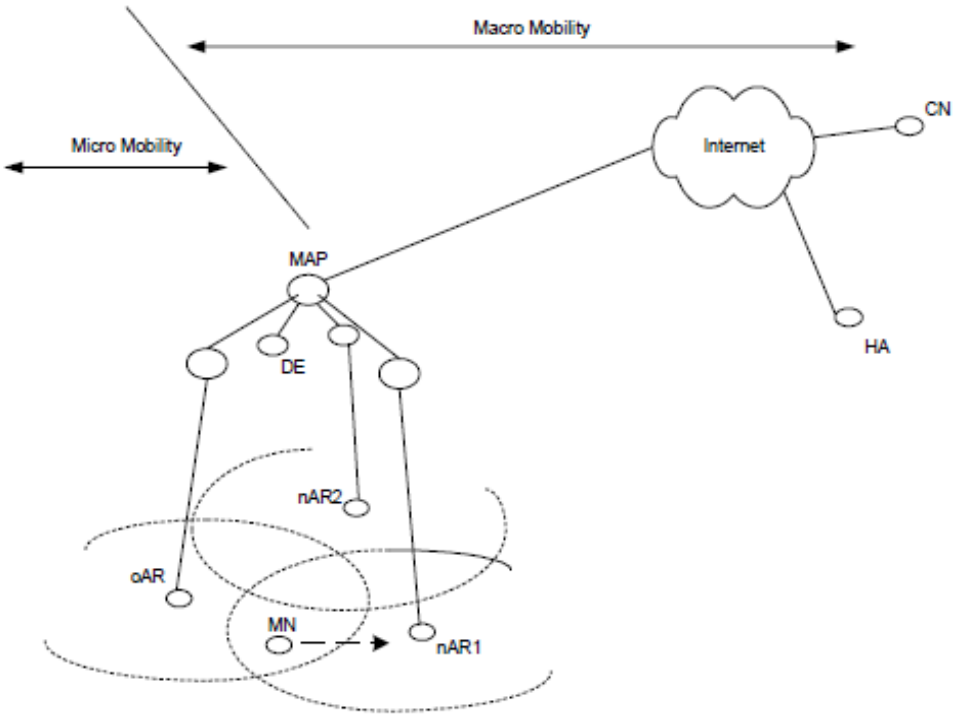
Στέλνεται από τον παλιό AR στον MN. Περιέχει την ένδειξη για τον νέο AR που θα ενωθεί ο MN.

- **Simulcast (Scast)**

Στέλνεται από τον νέο AR στον MAP για εκκίνηση του simulcast.

- **Simulcast Off (*Soff*)**

Στέλνεται από τον νέο AR στον MAP για τερματισμό του simulcast.



Σχήμα3.5 S-MIP schema

3.4.2 Λειτουργία του handoff στο Seamless Mobile IPv6

Η διαδικασία ξεκίνα μόλις ο MN λάβει ένα beacon (advertisement) message από τους νέους AR που ανακαλύφθηκαν. Ο MN, στέλνει RtSolPr μήνυμα στον oAR. Ο oAR στέλνει με την σειρά του HI σε όλους τους υποψήφιους nAR. Το HI μήνυμα περιέχει την ζητούμενη CoA του nAR και την τρέχουσα διεύθυνση που χρησιμοποιείται από τον oAR. Όλοι οι nAR θα απαντήσουν στο HI μήνυμα με Hack μήνυμα δηλώνοντας εάν αποδέχονται ή όχι την νέα CoA. Εάν η νέα CoA γίνει αποδεχτή από τον nAR, ο oAR στήνει ένα προσωρινό tunnel με την νέα CoA, αλλιώς ο oAR προωθεί τα πακέτα που προορίζονται για τον MN στον nAR. Ως απάντηση στο RtSolPr, ο MN λαμβάνει PrRtAdv από τον oAR. Οι nAR στέλνουν περιοδικά CLS μηνύματα στον DE. Το CLS δηλώνει πόσοι κινητοί κόμβοι συνδέονται με ένα συγκεκριμένο AR καθώς και τις IP διευθύνσεις αυτών των κόμβων. Το CTS μήνυμα δημιουργείται από τον MN κάθε φορά που λαμβάνει ένα L2 beacon advertisement μήνυμα από τους nAR. Κάθε CTS περιέχει την ισχύ σήματος του AR που εντοπίστηκε και την ID του αντίστοιχου AR. Αυτά τα στοιχεία χρησιμοποιούνται για εντοπισμό της θέσης του nAR. Ο τρέχων AR προωθεί αυτές τις πληροφορίες σε κάθε δευτερόλεπτο μέχρι να λάβει HD μήνυμα από τον DE. Ο DE, αφού αναλύσει τα CTS και CLS, στέλνει HD μηνύματα σε όλους

τους συμμετέχοντες AR ζητώντας seamless handoff. Έπειτα ο παλιός AR στέλνει HN μήνυμα μαζί με PrPtAdv στον MN δηλώνοντας του σε ποιό AR θα ενωθεί . Ο MN αρχικοποιεί το L3 handoff στέλνοντας FBU μήνυμα στον oAR. Αυτό το FBU δεσμεύει την τρέχουσα link address του MN με την νέα CoA. Όταν ο παλιός AR λάβει το FBU στέλνει Scast στον MAP που τον ειδοποιεί να ξεκινήσει να θέτει το S bit στα πακέτα που προορίζονται για τον MN και να τα μεταδώσει στον oAR και στον nAR. Επιπλέον, σαν απάντηση στο FBU του MN, ο παλιός AR στέλνει ένα FBack μήνυμα και στο παλιό και στο νέο δίκτυο. Αυτό γίνεται για να είναι σίγουρο ότι ο MN έλαβε το FBack, γιατί η στιγμή που ο MN αλλάζει δίκτυο δεν είναι προβλέψιμη. Ο nAR διατηρεί 2 ξεχωριστά buffers. Το f-buffer και το s-buffer. Το πρώτο, περιέχει πακέτα που προωθούνται από τον παλιό AR, ενώ το δεύτερο περιέχει πακέτα που μαρκάρονται με το S bit. Ο nAR ξεκινά να στέλνει τα πακέτα αφού λάβει το FNA μήνυμα από τον MN, τον οποίο ενημερώνει ότι ο έχει φθάσει στο δίκτυο του. Ο νέος AR στέλνει πρώτα όλα τα πακέτα από το f-buffer και έπειτα από το s-buffer. Όταν αδειάσει το f-buffer ο nAR στέλνει Soff μήνυμα στον MAP ενημερώνοντας τον να σταματήσει το casting και να συνεχίζει την κανονική παράδοση στον τρέχων AR του MN. Μόλις λάβει το Soff διεξάγει binding update για συσχετισμό της νέας on-link address με την regional CoA του MN. Το Soff στέλνεται και στον DE από τον MAP. Ο DE δεν επιτρέπει την διεξαγωγή νέου seamless handoff πριν την ολοκλήρωση του τρέχοντος.

3.5 *Fast Handover for Hierarchical MIPv6 (F-HMIPv6)*

Το F-HMIPv6 [5] είναι ένα πάντρεμα των πρωτόκολλων του FMIPv6 και HMIPv6. Κάθε ένα από αυτά έχει σχεδιαστεί με διαφορετικό τρόπο για βελτίωση της απόδοσης του handover του MIPv6. Το HMIPv6 αναπτύχθηκε για να μειώσει το φόρτο σηματοδοσίας και την καθυστέρηση στο binding update. Το FMIPv6 σχεδιάστηκε έτσι ώστε να προβλέπει το handover και να δημιουργεί διπλότυπα πακέτων, στον παλιό και νέο access point.

4.2.1 Ορολογία για το F-HMIPv6

- **New Access Router (NAR)**

Ο router που ήταν ο MN μετά το handoff.

- **Previous Access Router (PAR)**

Ο router που ήταν ο MN πριν το handoff.

- **New Access Router (NAR)**

Ο router που ήταν ο MN μετά το handoff.

- **Proxy Router Advertisement (PrRtAdv)**

Ένα μήνυμα από τον PAR στην MN το οποίο παρέχει πληροφορίες σχετικά με τα γειτονικά links.

- **Fast Binding Update (FBU)**

Μήνυμα από τον MN που αναθέτει στο PAR να αναπροσανατολίσουν τη ροή των δεδομένων (προς NAR).

- **Fast Binding Acknowledgment (FBack)**

Η απόκριση από το PAR για το FBU

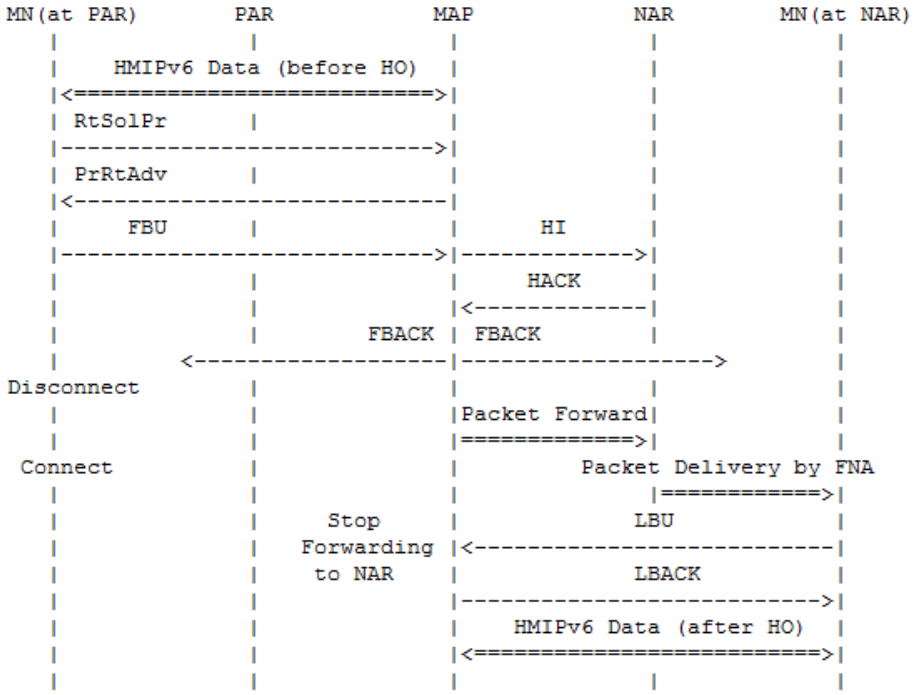
- **Handover Initiate (HI)**

Το HI περιέχει αίτημα για επικύρωση της νέας LCoA και για εγκαθίδρυση ενός διπλοκατευθυνόμενου tunnel, μεταξύ του MAP και NAR.

3.5.1 Mobile-Initiated Handover

Όταν ο L2 trigger του MN εντοπίσει κίνηση προς τον NAR, τότε στέλνει RtSolPr μήνυμα στον MAP για να ζητήσει πληροφορίες για τον NAR και μια νέα on-link CoA. Ο MAP αποκρίνεται στο μήνυμα του MN με ένα PrRtAdv, το οποίο περιέχει πληροφορίες για την νέα coA διεύθυνση του MN. Ο MN σχηματίζει την νέα CoA και στέλνει FBU μήνυμα στον MAP, το οποίο περιέχει την νέα LCoA. Μόλις ο MAP λάβει το FBU ξεκινά την διαδικασία του fast handover, στέλνοντας ένα HI μήνυμα στον NAR. Ως απάντηση στο HI, είναι το Hack αφού πρώτα γίνει duplicated address

detection (DAD) από τον NAR. Αφού λάβει το Hack, ο MAP στέλνει Fast Binding Acknowledgement (FBack) στον MN. Ο MAP θα ξεκινήσει να προωθεί τα πακέτα που προορίζονται για τον MN στον NAR, χρησιμοποιώντας το tunnel. Όταν ο MN ολοκληρώσει τη μεταφορά του στο NAR του στέλνει FNA μήνυμα για να τον ενημερώσει ότι ολοκλήρωσε. Έπειτα ο NAR στέλνει στον MN τα πακέτα που προορίζονται γι' αυτόν. Όταν ο MAP λάβει το νέο LBU με την νέα LcoA από τον MN, σταματά την προώθηση πακέτων στον NAR και τερματίζει το tunnel που εγκαθιδρύθηκε για fast handover. Για να απαντήσει στο LBU, ο MAP στέλνει Local Binding Acknowledgement (LBack) στον MN. Στην συνέχεια οι λειτουργίες που ακολουθούν είναι ίδιες με το HMIPv6.



Σχήμα 3.7 F-HMIP signal flow

3.5.2 Network-Initiated Handover

Σε αυτή τη περίπτωση υποθέτουμε ότι ο παλιός και ο νέος AR, εντοπίζουν την κίνηση του MN. Όταν ο AR λάβει trigger, στέλνει handover indication σήμα στον MAP. Το σήμα περιέχει πληροφορίες για την link-στρώμα address ή αναγνωριστικό για το συσχετιζόμενο NAR. Όταν υπάρχει ένδειξη για network initiated handover, ο MAP στέλνει PrPtAdv μήνυμα στο MN. Το PrRtAdv μήνυμα , πρέπει να περιέχει πληροφορίες για την νέα CoA που θα χρησιμοποιήσει ο MN στην περιοχή του NAR.

Οι υπόλοιπες διαδικασίες που ακολουθούνται είναι πανομοιότυπες με αυτές που γίνονται στο Mobile -initiated handover.

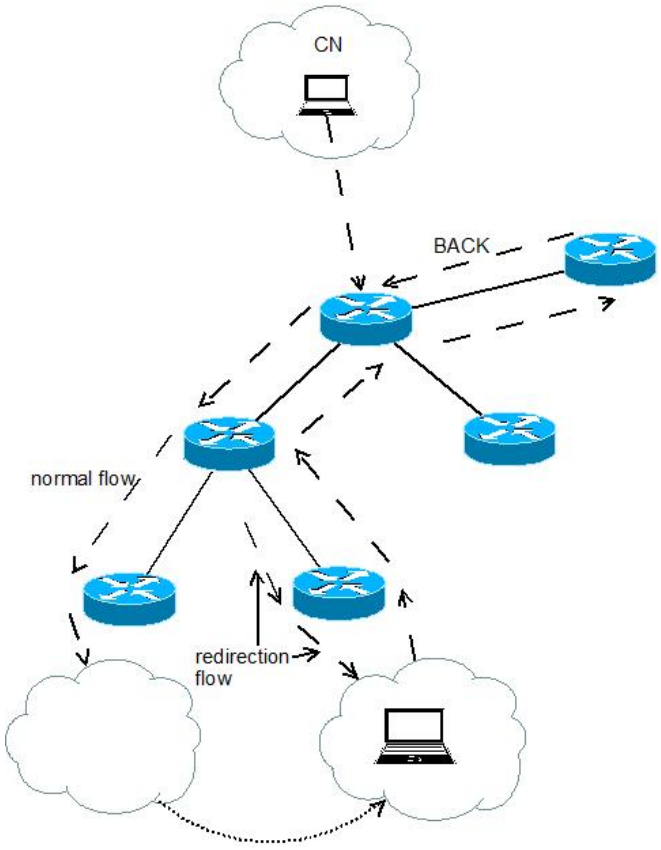
3.6 *Flow-based Fast Handover for MIPv6 (FFHMIPv6)*

Βασισμένο στη ροή (Flow-based) γρήγορο handover για κινητό IPv6 (FFHMIPv6) [6] είναι μια νέα μέθοδος παράδοσης που σχεδιάστηκε για Κινητά δίκτυα IP. Το FFHMIPv6 χρησιμοποιεί τις flow-state πληροφορίες και την ενθυλάκωση πακέτων που επιτρέπουν υποδοχή των πακέτων ταυτόχρονα με τη διαδικασία εγγραφής διευθύνσεων του MIPv6. Η ανάλυση και η αξιολόγηση απόδοσης του FFHMIPv6 παρουσιάζει ότι χειρίζεται τη καθυστέρηση του handover αποτελεσματικότερα από το βασικό MIPv6, το ιεραρχικό MIPv6, καθώς επίσης και γρήγορα handovers για τους μηχανισμούς handover MIPv6.

3.6.1 Flow-based Fast Handover Μηχανισμός για MIPv6

Η μέθοδος Flow-based Fast Handover για κινητό IPv6 (FFHMIPv6) χρησιμοποιεί τα χαρακτηριστικά γνωρίσματα IPv6 πρωτοκόλλου και οφέλη από το IPv6 έλεγχο της κυκλοφορίας. Το FFHMIPv6 παίρνει το ρόλο του μηχανισμού handover μέσα στο MIPv6 δίκτυο όταν ανιχνεύεται η αλλαγή της Care-of-Address (CoA) από το MN, για παράδειγμα όταν αλλάζει το αρχικό CoA. Το CoA είναι μια διεύθυνση που ορίζεται στο MN όταν τοποθετείται σε ένα ξένο δίκτυο. Οι διαδικασίες του γίνονται κυρίως στο MN και τους δρομολογητές. Σε λειτουργία το FFHMIPv6, χρησιμοποιεί και το παλαιό και το νέο CoA μαζί με τις flow state πληροφορίες των δρομολογητών για να εντοπίσει (να προσδιορίσει) το flows που κατευθύνονται στο παλαιό CoA και να τους επαναδρομολογήσει στο νέο CoA. Η κυκλοφοριακή ροή καθορίζεται από την IPv6 ετικέτα ροής, και τις διευθύνσεις πηγής και προορισμού. Η λειτουργία της μεθόδου FFHMIPv6 παρουσιάζεται στο σχήμα 3.8. Όταν συμβαίνει handover, ο MN εκτελεί αρχικά L2 handover. Μετά από τις ειδοποιήσεις εκείνου του MN ότι έχει αλλάξει το L3 σημείο σύνδεσής του και δημιουργείται ένα νέο CoA (φάση 3). Σε FFHMIPv6, ένα πλαίσιο Hop-by-Hop προστίθεται στο κανονικό FBU μήνυμα αναπροσαρμογής θέσης στον HA, διαμορφώνοντας κατά συνέπεια μια FFHMIPv6 Binding Update (FFHBU) (φάση 4). Αυτό το πλαίσιο Hop-by-Hop περιλαμβάνει την παλαιά CoA και όλες τις CN's διευθύνσεις. Σε κάθε δρομολογητή μεταξύ του MN και του HA, εάν ο

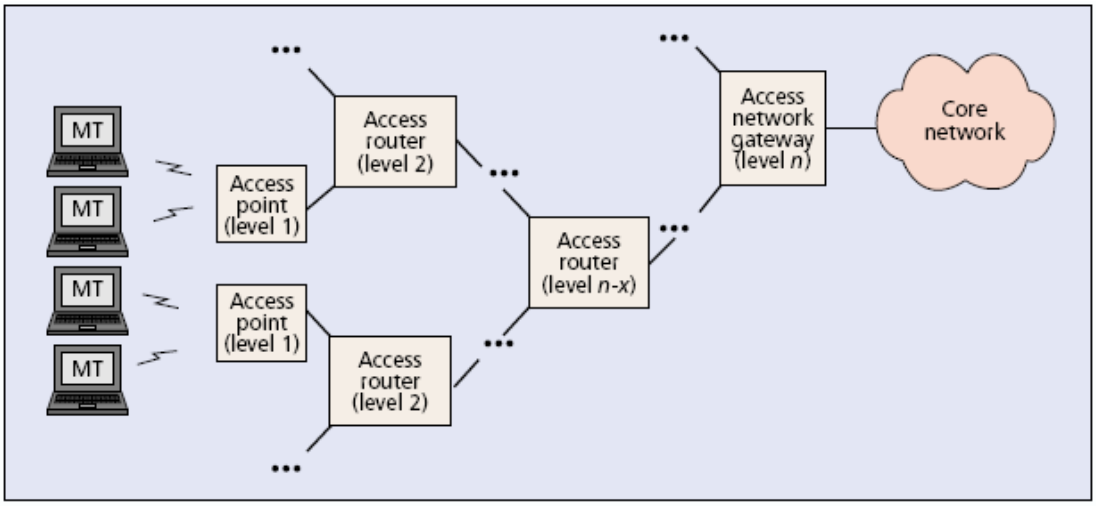
FFHMIPv6 καθορισμός προσδιορίζεται, η τρέχουσα flow state πληροφορία (δηλ. flow cache) συγκρίνεται ενάντια στην παλαιά flow state πληροφορία από το hop-by-hop header. Εάν βρεθεί κυκλοφοριακή ροή, μια IPv6 σήραγγα καθιερώνεται μεταξύ του δρομολογητή διασταυρώσεων (Crossover Router) και της νέας CoA του MN βάσει αυτής της αναπροσαρμογής FFHBU. Η κυκλοφοριακή ροή από τον HA και τον CN ανοίγεται στη νέα CoA. Κατά συνέπεια, το FFHMIPv6 επιτρέπει την υποδοχή των ενεργών ροών του ακόμη και προτού να τελειώσουν τη BU διαδικασία. Με MIPv6 το MN θα ήταν σε θέση να λάβει τα στοιχεία μόνο μετά από την παραλαβή του BACK μηνύματος από τον HA (και ο CN σε περίπτωση βελτιστοποίησης διαδρομών).



Σχήμα 3.8 FFHMIPv6 signals Flow

3.7 *Terminal Independent Mobility for IPv6 (TIMIP)*

Το πρωτόκολλο TIMIP [7] έρχεται να δώσει λύση σε ένα πρόβλημα το οποίο αποτρέπει την περιπλάνηση μεταξύ διαφόρων δικτύων, περιορίζοντας έτσι την κινητικότητα τους μόνο εντός ενός δικτύου, που αντιμετωπίζουν ορισμένοι κινητοί τερματικοί κόμβοι σε ένα δίκτυο. Η αιτία αυτού του προβλήματος είναι ότι τα περισσότερα τερματικά χρησιμοποιούν legacy IP stacks αντί του mobility-aware stacks που προβλέπει ο IETF. Για να αντικατασταθούν όλα τα legacy IP stacks, υπάρχει μεγάλη δυσκολία αν λάβουμε υπόψη, την ποικιλία που υπάρχει σε λειτουργικά συστήματα κινητών κόμβων. Το TIMIP χρησιμοποιεί μια ιεραρχία από access points (στη βάση του) και routers σε σχήμα πυραμίδας.



Σχήμα 3.9 Timip schema

3.7.1 Ορολογία για το Seamless Mobile TIMIP

- **Access Router (AR)**

Router ο οποίος υποστηρίζει λειτουργίες διαχείρισης κινητικότητας και παρέχει συνδεσιμότητα στους MN.

- **Access Point (AP)**

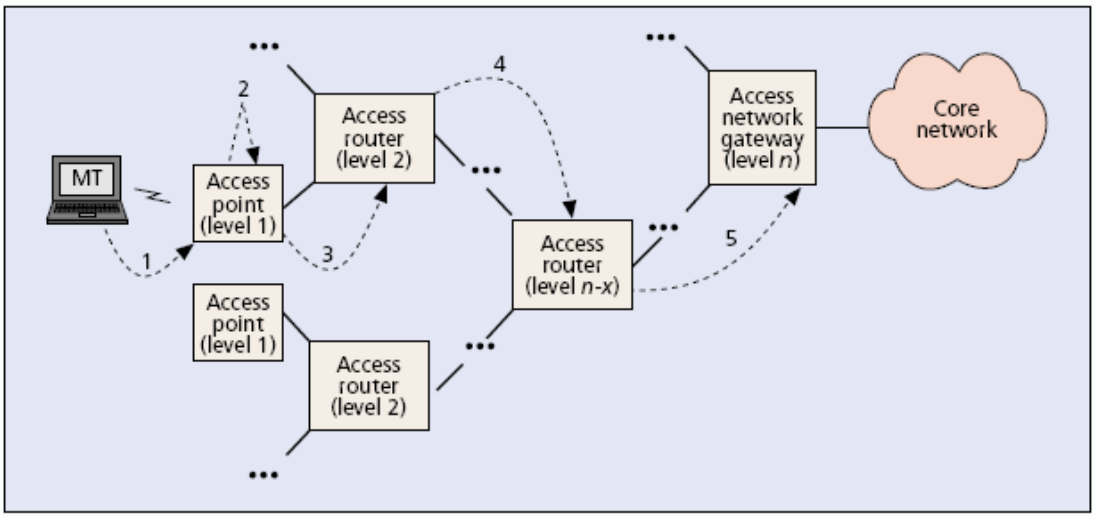
Access Router που προσφέρει στρώμα-2 connectivity στους MN, επικοινωνεί κατευθείαν μαζί τους μέσω της διεπιφάνειας ασύρματης εκπομπής. Ο AP στέλνει και λαμβάνει πακέτα από τους MN, είναι υπεύθυνος για εντοπισμό Handoff και για την ενεργοποίηση για χάρη του MN, διαδικασιών διαχείρισης κινητικότητας.

- **Access Network Gateway (ANG)**

Ο ANG αποτελεί την ρίζα στην δενδρική τοπολογία του δικτύου και συνδέεται άμεσα με ένα ξένο δίκτυο. Υποστηρίζει λειτουργίας διαχείρισης κινητικότητας που βασίζονται σε MIP μακρό-κινητικότητα.

3.7.2 Power-up

Είναι η διαδικασία κατά την οποία δημιουργείται το μονοπάτι επικοινωνίας από τον MN στον access point έως και τον ANG.



Σχήμα 3.10 Timip power up schema

1. Ο MN συσχετίζεται με ένα AP που ανήκει στο TIMIP δίκτυο.

2. Ενόσω βρισκόμαστε στον AP, η στρώμα-2 στέλνει την MAC διεύθυνση του MN στην IP στρώμα, ενημερώνοντας την για την παρουσία του MN . Η MAC διεύθυνση συσχετίζεται με τις πληροφορίες εγγραφής, που λαμβάνονται από τον ANG, και ανακαλύπτεται η αντίστοιχη IP διεύθυνση. Ανανεώνεται ο πίνακας δρομολόγησης του AP με πληροφορίες για τον νέο MN.

3. Ο AP στέλνει Routing Update μήνυμα στον AR που βρίσκεται στο δεύτερο ιεραρχικό επίπεδο. Ο AR απάντα με Routing Update Acknowledgement και ενημερώνει τον πίνακα δρομολόγησης του με νέα καταχώρηση που σχετίζεται με τον MN.

4. Τα ίδια μηνύματα ανταλλάσσονται ανεβαίνοντας την ιεραρχία των ARs. Σε κάθε επίπεδο έχουμε ανανέωση του πίνακα δρομολόγησης, με νέα καταχώρηση για τον MN. Κάθε καταχώρηση δείχνει πάντοτε στον AR πού έστειλε το Routing Update, έτσι ώστε να καθορίζεται το μονοπάτι με το οποίο μπορούμε να φθάσουμε στον MN.

5. Ανεβαίνοντας την ιεραρχία μέσω της ανταλλαγής τέτοιων μηνυμάτων, φθάνουμε στο ANG, όπου και ολοκληρώνεται η δημιουργία του νέου μονοπατιού δρομολόγησης.

Όλα τα πακέτα που φθάνουν σε έναν AR, στον οποίο υπάρχει η αντίστοιχη καταχώρηση στον πίνακα δρομολόγησης για τον προορισμό τους , προωθούνται κάτω στην ιεραρχία των δρομολογητών μέχρι να φθάσουν στην διεπιφάνεια ασύρματης εκπομπής που βρίσκεται ο MN. Σε περίπτωση που δεν υπάρχει καταχώρηση σε κάποιο AR, τα πακέτα που φθάνουν σε αυτόν προωθούνται πάνω στην ιεραρχία των AR.

3.7.3 Handoff σε Micro επίπεδο

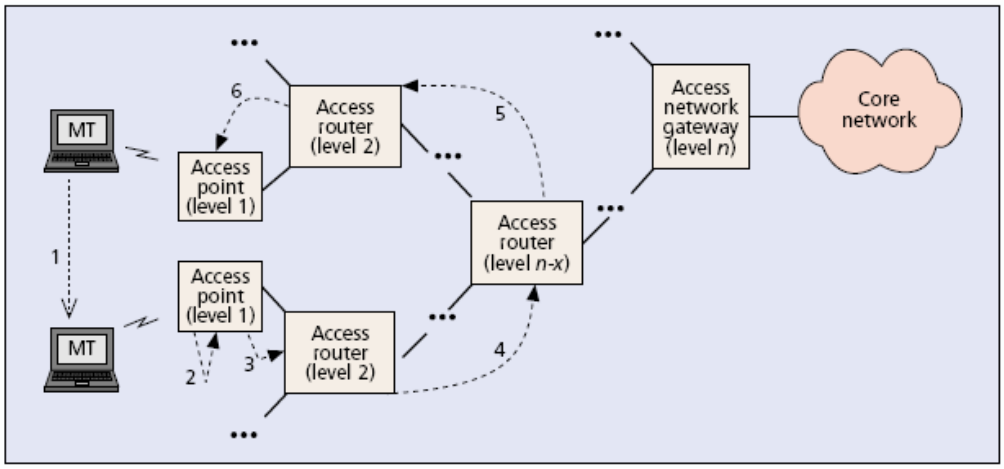
Είναι διαδικασία κατά την οποία εκτελείται το handoff από έναν AP του TIMIP δικτύου σε έναν άλλο του ίδιου δικτύου.

Τα πρώτα 4 βήματα είναι τα ίδια με αυτά στην power-up διαδικασία.

5 Μέσω ανταλλαγής RU / RUAck μηνυμάτων, ανεβαίνουμε την ιεραρχία και φθάνουμε μέχρι τον πρώτο AR που ανήκει την ίδια στιγμή και στο παλιό και στο νέο μονοπάτι δρομολόγησης. Με την ολοκλήρωση του νέου μονοπατιού το παλιό πρέπει να διαγραφεί. Ο AR που λαμβάνει το μήνυμα αντιλαμβάνεται ότι ο MN δεν είναι πλέον προσβάσιμος μέσω αυτού και διαγράφει από τον πίνακα δρομολόγησης του την αντίστοιχη καταχώρηση του MN και στέλνει πίσω Routing Update Acknowledgement.

6 Μέσω ανταλλαγής RU / RUAck μηνυμάτων κατεβαίνουμε την ιεραρχία ακολουθώντας το παλιό μονοπάτι, μέχρι να φθάσουμε στο παλιό AP. Σε κάθε

επίπεδο διαγράφεται η καταχώρηση για τον MN από τον πίνακα δρομολόγησης κάθε AR.



Σχήμα 3.11 Timip micro handoff

3.7.4 Macro επίπεδο

Για παροχή μακρο-κινητικότητας το TIMIP βασίζεται στο πρωτόκολλο MIP. Ο ANG λειτουργεί σαν οικείος πράκτορας για MNs που το οικείο δίκτυο τους είναι το TIMIP. Για legacy MN, ο ANG υλοποιεί όλες τις απαραίτητες λειτουργίες για χάρη του. Σε περίπτωση επισκέπτη MN, ο ANG λειτουργεί σαν ξένος πράκτορας.

3.7.5 Macro-κινητικότητα για MN me legacy stack

Όταν ένας MN εισέλθει σε ένα άλλο TIMIP δίκτυο δημιουργείται ένα μονοπάτι δρομολόγησης μεταξύ αυτού και του ANG (power-up). Έτσι τα πακέτα στέλνονται ή λαμβάνονται από τον ANG. Σε περίπτωση που το οικείο δίκτυο του MN είναι ένα διαφορετικό δίκτυο, τότε ο οικείος πράκτορας ενημερώνεται και εγκαθιδρύεται μια σήραγγα για να στέλνονται μεταξύ του οικείου και του ξένου πράκτορα που βρίσκεται στον ANG.

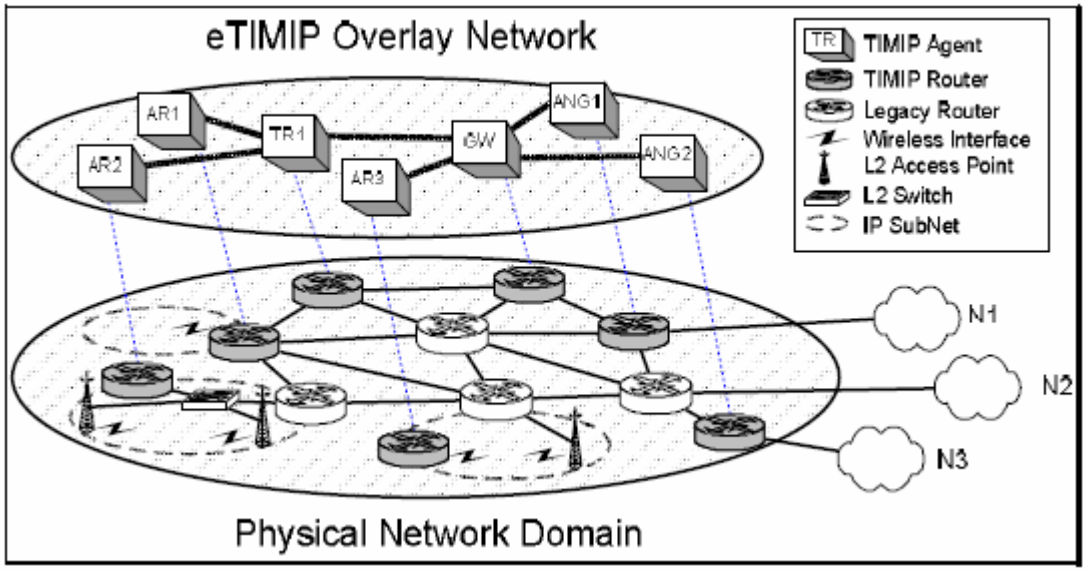
3.8 *Enhanced TIMIP*

Όλες οι προηγούμενες λύσεις που έχουν προταθεί, απαιτούν την χρήση ειδικών ιεραρχικών δικτύων που πρέπει να επεκταθούν για να παρέχουν κινητικότητα, πράγμα το όποιο έχει αρκετά μεγάλο οικονομικό κόστος. Αυτό το κόστος μπορεί να αποφευχθεί, αν η κινητικότητα υλοποιείται χρησιμοποιώντας της legacy δομές που

ήδη υπάρχουν. Το πρωτόκολλο αυτό παρουσιάζει μια νέα λύση για κινητικότητα, παρέχοντας ανεξάρτητες αρχιτεκτονικές και για δίκτυα και για τερματικά. Βασίζεται στην χρήση ενός overlay δικτύου, το οποίο του παρέχει κινητικότητα.

3.8.1 Αρχιτεκτονική eTIMIP

Το eTIMIP [8] παρουσιάζει μια νέα αρχιτεκτονική που στηρίζεται στις αρχές του overlay δικτύου και στόχος του είναι να υποστηρίζει την κινητικότητα αποδοτικά και με διαφάνεια. Η δομή της αρχιτεκτονικής παρουσιάζεται πιο κάτω:



Σχήμα 3.12 Etimip schema

Κάθε eTIMIP δίκτυο είναι οργανωμένο σε δύο επίπεδα το physical επίπεδο δικτύου και το overlay επίπεδο.

3.8.2 Physical Επίπεδο Δικτύου

Σε αυτό το επίπεδο δίκτυο μπορεί να έχει οποιαδήποτε τοπολογία. Η δρομολόγηση στο intra – domain γίνεται με πρωτόκολλα όπως είναι ο OSPF και ο RIP. Μερικοί δρομολογητές που βρίσκονται στα όρια μπορούν να συμμετέχουν και στη δρομολόγηση του inter-domain , μέσω του BGP πρωτοκόλλου. Τα προαναφερθέντα πρωτόκολλα κατατάσσονται στην κατηγορία fixed routing, ενώ το eTIMIP στο mobile routing. Η ασύρματη πρόσβασή γίνεται μέσω των AP.

3.8.3 Overlay επίπεδο δικτύου

Βρίσκεται πάνω από το Physical Επίπεδο και φτιάχτηκε για να παρέχει αποδοτικές υπηρεσίες κινητικότητας. Αποτελείται από etimip πράκτορες που σχηματίζουν ένα λογικό δένδρο μεταξύ τους. Το βασικό στοιχείο του δικτύου αυτού είναι ο eTIMIP router (TR). Ο έλεγχος και τα δεδομένα εναλλάσσονται μεταξύ των TR για να παρέχεται κινητικότητα. Τα πακέτα ελέγχου, χρησιμοποιούνται για κατανομή πληροφοριών δρομολόγησης των MN. Αυτές οι πληροφορίες χρησιμοποιούνται για προώθηση των δεδομένων στο MN. Ανάλογα με την θέση τους, οι TR έχουν διαφορετικούς ρόλους. Στην κορυφή του δένδρου βρίσκεται ο gateway (GW), ο οποίος χρησιμοποιείται για να συγκεντρώνει τις λειτουργίες διαχείρισης και είναι μοναδικός σε κάθε τέτοιο δίκτυο.

Οι Access Network Gateways (ANG), χρησιμοποιούνται για σύνδεση με δίκτυα εκτός της περιοχής. Παρόμοιο του είναι ο AR που είναι TR και προσφέρει συνδεσιμότητα στο MN. Οι πιο σημαντικές του λειτουργίες είναι ο εντοπισμός κίνησης και η παραγωγή των αντίστοιχων μηνυμάτων. Τέλος, υπάρχουν οι legacy MN, που ενώνονται στο δίκτυο χρησιμοποιώντας wireless interface.

Στα όρια του δικτύου, υπάρχουν τοποθετημένοι eTIMIP πράκτορες που παραλαμβάνουν όλη την εισερχόμενη ροή. Το eTIMIP καθορίζει ένα κινητό δίκτυο, που δημιουργείται και διαχειρίζεται με fixed routing και το οποίο σχετίζεται με τον GW, τους AR και όλους τους legacy MN του δικτύου. Κάθε πακέτο που φθάνει από κάποιο legacy οριακό δρομολογητή, στέλνεται κατευθείαν στο GW με fixed routing και από το σημείο αυτό μπορεί να επωφεληθεί από την παροχή κινητικότητας και να αρχίσει να χρησιμοποιεί mobile routing.

Για βελτίωση της απόδοσης και της επεκτασιμότητας του δικτύου, οι legacy MN μπορούν να χαρακτηριστούν ως active ή idle, ανάλογα με την χρήση τους στο δίκτυο. Active είναι αυτοί, που κατά την παρούσα στιγμή, στέλνουν ή λαμβάνουν πακέτα και η λειτουργία τους παρακολουθείται από το δίκτυο για γρήγορη και άμεση υπηρεσία. Όσον αφορά τους Idle κόμβους, το δίκτυο θα διεξάγει λιγότερο ακριβές προσπάθειες εντοπισμού τους. Τέτοιοι κόμβοι εξυπηρετούνται κατόπιν αιτήματος, όποτε έχουν δεδομένα να παραδώσουν.

3.8.4 Διαδικασία Εντοπισμού και Εγγραφής

Όταν ο MN φθάσει σε ένα eTIMIP δίκτυο, διεξάγει Power-up. Το eTIMIP εντοπίζει την άφιξη του και προσθέτει νέα καταχώρηση στους πίνακες δρομολόγησης των πρακτόρων που πρέπει να γνωρίζουν την ύπαρξη του. Σε περίπτωση που ο MN περιπλανιέται μεταξύ δύο AP στην περιοχή , διεξάγεται λειτουργία handover. Στις δύο αυτές περιπτώσεις, ο εντοπισμός του MN εκτελείται συνεχώς από τα AR που ενώνονται στο δίκτυο. Μόλις ένας MN ενωθεί με ένα AR, εντοπίζεται το γεγονός και συλλέγονται όλες οι απαραίτητες πληροφορίες. Ο AR που εντόπισε τον MN, είναι υπεύθυνος να ξεκινήσει την διαδικασία εγγραφής, ενημερώνοντας τους ενδιαφερόμενους πράκτορες για την νέα θέση του MN. Αυτοί οι πράκτορες, είναι αυτοί που βρίσκονται μεταξύ του AR και του GW. Κάθε ένας από αυτούς, ανανεώνει το πίνακα δρομολόγησης του και μεταδίδει TIMIP μηνύματα, πάνω στην ιεραρχία προς τον GW σε περίπτωση power-up ή στον διασταυρωμένο AR, σε περίπτωση handover.

3.8.5 Μεταφορά δεδομένων

Όταν ο eTIMIP πράκτορας λάβει πακέτα δεδομένων, ελέγχει για τον προορισμό τους στο πίνακα δρομολόγησης του. Αν βρει αντίστοιχη είσοδο, προωθεί τα πακέτα στον επόμενο eTIMIP πράκτορα, χρησιμοποιώντας downlink διαδικασία. Σε αντίθετη περίπτωση, τα πακέτα προωθούνται στο καθορισμένο upstream πράκτορα, προς τον GW, μέσω uplink routing. Για intra-domain ροή μεταφέρεται μέσω του λογικού δένδρου που ενώνει τον MN με τον CN. Η inter-domain ροή, πρέπει να περάσει μέσα από τον GW του δικτύου.

3.9 *SIGMA*

Το SIGMA [9] έρχεται και αυτό να αντιμετωπίσει ένα πρόβλημα το οποίο δεν αντιμετωπίζεται αποτελεσματικά από ανάλογες προτάσεις πάνω στο MIPv6. Το πρόβλημα αυτό είναι το μεγάλο latency κατά τη διαδικασία του handoff. Αυτό το πρόβλημα με τη σειρά του έχει ως αποτέλεσμα να χάνονται τα πακέτα. Το SIGMA εργάζεται με τα ήδη υπάρχοντα συστατικά του δικτύου. Το SIGMA ενεργεί με

seamless τρόπο για να πετύχει το χαμηλό latency και ως επέκταση μικρό ποσοστό χαμένων πακέτων κατά τη διαδικασία του handoff.

3.9.1 Ορολογία

- **Mobile Node (MN)**

Είναι ο κινητός κόμβος που κάνει χρήση του MIPv6 για να έχει πρόσβαση στο δίκτυο. Ο MN είναι εγγεγραμμένος σε ένα δίκτυο που ονομάζεται οικιακό δίκτυο. Ο MN έχει τη δυνατότητα να περιηγείται από δίκτυο σε δίκτυο και να επικοινωνεί απρόσκοπτα με τους άλλους κόμβους.

- **Correspondent Node (CN)**

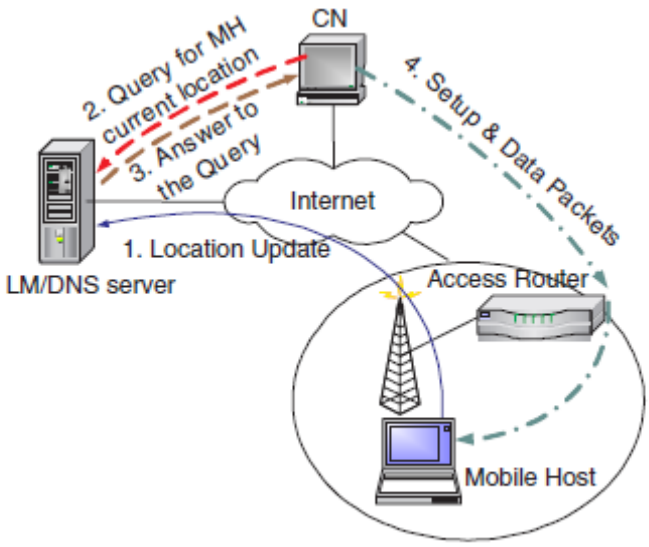
Είναι ο κόμβος που δέχεται και στέλνει πληροφορίες στον MN. Ο CN μπορεί να είναι είτε κινητός είτε σταθερός κόμβος, μέσα και έξω από το δίκτυο.

- **Domain Name System (DNS)**

Το DNS είναι ένα ιεραρχικό σύστημα ονοματοθεσίας για τους υπολογιστές, τις υπηρεσίες, ή οποιοδήποτε άλλο πόρο που συμμετέχει στο Διαδίκτυο. Συνδέει τις διάφορες πληροφορίες με τα ονόματα περιοχών που ορίζονται.

3.9.2 Location Manager

Είναι μια θεμελιώδης έννοια για το SIGMA. Ο LM είναι αυτός που ενημερώνεται για το πού βρίσκεται κάποιος κόμβος σε κάποιο δίκτυο. Ειδικότερα ο location manager διατηρεί μια βάση με τα ID των MH καθώς και την τωρινή τους (κύρια) IP. Με αυτόν συνεννοείται και ο εκάστοτε correspondent node για να βρει κάποιον μέσα σε ένα δίκτυο. Τον ρόλο αυτό τον έχει ο domain name server (DNS). Εν αντιθέσει με το MIP στο SIGMA αυτός που έχει το ρόλο του LM πρέπει να είναι αναγκαστικά στο ίδιο υποδίκτυο με τον MH. Στο SIGMA ο LM αντικαθιστά τις έννοιες-λειτουργίες του home agent και foreign agent που υπάρχουν στο MIPv6.



Σχήμα 3.13 Η λειτουργία του location manager για τους correspondence και το mobile host

3.9.3 SIGMA Handoff

Ο μηχανισμός του handoff στο SIGMA όπως μας παρουσιάζετε είναι διαχωρισμένος σε πέντε διακριτά βήματα. Τα οποία είναι τα έξεις:

ΒΗΜΑ 1: Λήψη της νέας διεύθυνσης IP

Η διαδικασία προετοιμασίας του handoff αρχίζει όταν ο MH κινείται στον τομέα επικάλυψης των δύο υποδικτύων. Μόλις λάβει ο MH route advertisement message από το νέο AR (AR2), πρέπει να αρχίσει να κάνει ενέργειες για να αποκτήσει μια νέα διεύθυνση IP στο νέο υποδίκτυο. Αυτό μπορεί να ολοκληρωθεί μέσω διάφορων μηχανισμών-τρόπων (DHCP, DHCPv6, ή IPv6 stateless address auto-conΣχήμαuration).

ΒΗΜΑ 2: Πρόσθεση της διεύθυνσης IP στην ένωση

Αφότου λάβει ο MH τη διεύθυνση IP IP2 από το βήμα 1, ο MH πρέπει να δηλώσει στο CN για τη διαθεσιμότητα της νέας διεύθυνσης IP μέσω του Address Dynamic Reconfiguration. Αυτή η επιλογή καθορίζει δύο νέους τύπους σημάτων για τη γνωστοποίηση της νέας IP στον CN, το ASCONF και ASCONF-ACK, καθώς και διάφορους τύπους παραμέτρου (Add IP Address, Delete IP address and Set Primary Address).

ΒΗΜΑ 3: Αναπροσαρμογή των πακέτων προς τη νέα IP

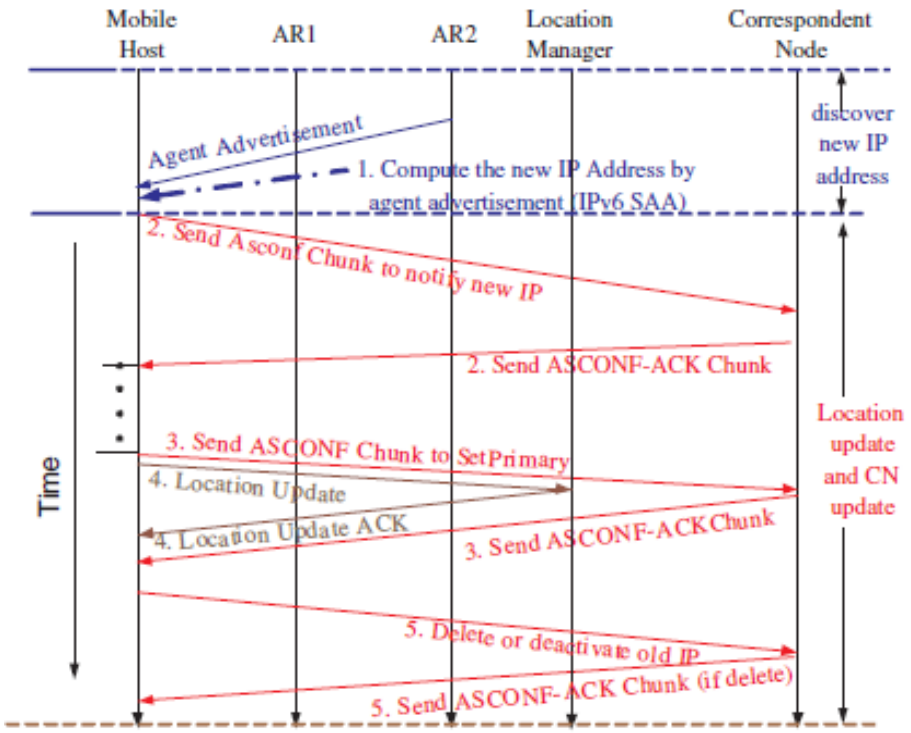
Όταν ο MH έχει προχωρήσει αρκετά μέσα στη κάλυψη του καινούριου δικτύου τότε μπορεί να ενημερώσει τον CN να αναπροσαρμόσει τη διαδρομή των πακέτων προς τη νέα IP. Αυτό γίνεται με σκοπό να έχουν τα πακέτα μεγαλύτερη πιθανότητα να φτάσουν στον MH και αυτό είναι λογικό διότι έχει όπως προανέφερα προχωρήσει αρκετά μέσα στη κάλυψη του καινούριου δικτύου. Και αυτή η διαδικασία εκτελείται με ASCONF και ASCONF-ACK.

ΒΗΜΑ 4: ενημέρωση του location manager

Στέλνεται ένα σήμα προς τον LM από τον MH ότι η διεύθυνση IP του έχει αλλάξει.

ΒΗΜΑ 5: Αποδέσμευση της παλιάς IP

Αυτό το βήμα έχει δυο τρόπους για να πραγματοποιηθεί, ο κάθε ένας από αυτούς με τα δικά του πλεονεκτήματα. Ο προφανής τρόπος είναι να σταλεί ένα ASCONF μήνυμα από τον MH στο CN και να διαγραφεί η παλιά διεύθυνση. Ο δεύτερος τρόπος είναι να στείλει ο MH ένα μήνυμα διαφήμισης “zero receiver window”. Αυτό προκαλεί ένα πάγωμα της παλιάς IP του MH, αφού δεν την αποδεσμεύει, αλλά απλώς ενημερώνει να μη του στέλνονται πακέτα σε αυτή. Αυτό αντιμετωπίζει καλύτερα τα προβλήματα του «ζικ-ζακ» από το ένα AR στο άλλο, αφού μπορεί πολύ γρήγορα να χρησιμοποιηθεί άμεσα η παλιά IP αν ξαναπεράσει ο MH από αυτό τον AR. Βέβαια αυτός ο τρόπος γεννά ερωτηματικά γύρω από θέματα ασφάλειας.



Σχήμα 3.14 Handoff με τα 5 βήματα του SIGMA

3.10 *P-SIGMA*

Το P-SIGMA [10] έρχεται και αυτό να αντιμετωπίσει ένα πρόβλημα το οποίο δεν αντιμετωπίζεται αποτελεσματικά από ανάλογες προτάσεις πάνω στο MIPv6. Το πρόβλημα αυτό είναι το μεγάλο latency κατά τη διαδικασία του handoff. Αυτό το πρόβλημα με τη σειρά έχει ως αποτέλεσμα να χάνονται τα πακέτα. Το P-SIGMA εργάζεται με τα ήδη υπάρχοντα συστατικά του δικτύου και αντιμετωπίζει το πρόβλημα του υψηλού latency με την εισαγωγή της τεχνικής paging. Paging είναι μια ευρέως διαδεδομένη τεχνική για να εντοπίσει και να επικοινωνήσει με τις idle devices στα cellular networks. Το Paging μπορεί να ενσωματωθεί με ένα δίκτυο IP για να μειώσει το φορτίο του signaling στο δίκτυο.

3.10.1 Ορολογία

- **Mobile Host (MH)**

Είναι ο mobile node

- **Paging Aria (PA)**

Είναι καθορισμένα υποδίκτυα των οποίων ο AP ελέγχεται από μια gateway.

- **Paging Gateway (PGW)**

Όταν ένας PA ελέγχεται από μια gateway, αποκαλούμενη paging gateway (PGW).

- **Domain Name System (DNS)**

Το DNS είναι ένα ιεραρχικό σύστημα ονοματοθεσίας για τους υπολογιστές, τις υπηρεσίες, ή οποιοδήποτε άλλο πόρο που συμμετέχει στο Διαδίκτυο. Συνδέει τις διάφορες πληροφορίες με τα ονόματα περιοχών που ορίζονται.

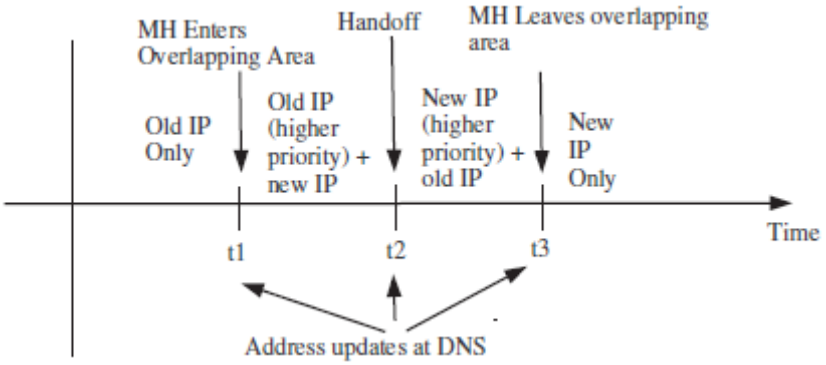
3.10.2 P-SIGMA Handoff

Όταν ο MH κινείται στην κάλυψη ενός νέου υποδικτύου μέσα στο ίδιο PA, λαμβάνει μια νέα διεύθυνση IP διατηρώντας την παλαιά στη περιοχή όπου τα δυο υποδίκτυα επικαλύπτονται. Ο MH επικοινωνεί μέσω της παλαιάς διεύθυνσης IP ενώ καθιέρωνει μια νέα σύνδεση μέσω της καινούριας IP address. Όταν η δύναμη σημάτος του παλιού AP είναι κάτω από ένα ορισμένο κατώτατο όριο, η σύνδεση παραδίδεται στο νέο υποδίκτυο και η νέα διεύθυνση IP γίνεται η κύρια διεύθυνση του MH. Όταν MH αφήνει την περιοχή επικάλυψης, αποδεσμεύει την παλαιά διεύθυνση IP και επικοινωνεί μόνο με τη νέα διεύθυνση IP. Κάθε φορά που ο MH εκτελεί το handoff σε ένα νέο υποδίκτυο, ενημερώνει DNS με τη νέα διεύθυνση IP του.

3.10.3 P-SIGMA Location Management (LM)

Το P-*SIGMA* επεκτείνει τις αρμοδιότητες του DNS server του δικτύου από έναν server ονοματοθεσίας σε έναν server που επιπλέον κάνει και Location management. Δηλαδή, προσδιορίζει-γνωρίζει τις θέσεις των κόμβων που είναι στο δίκτυο. Όποτε ένας MH αλλάζει το σημείο σύνδεσής του, καταχωρεί τη νέα διεύθυνση IP Authoritative Name Server (ANS) μέσω της dynamic secure update. Ο authoritative name server είναι ένας name server ο οποίος δίνει authoritative απαντήσεις σε ένα DNS ερώτημα. Ο DNS είναι αυτός που δημιουργεί τις συνδέσεις, όταν ο MH αλλάζει τη διεύθυνση IP του και διαχειρίζεται τις διευθύνσεις σε όλη τη διάρκεια του handoff.

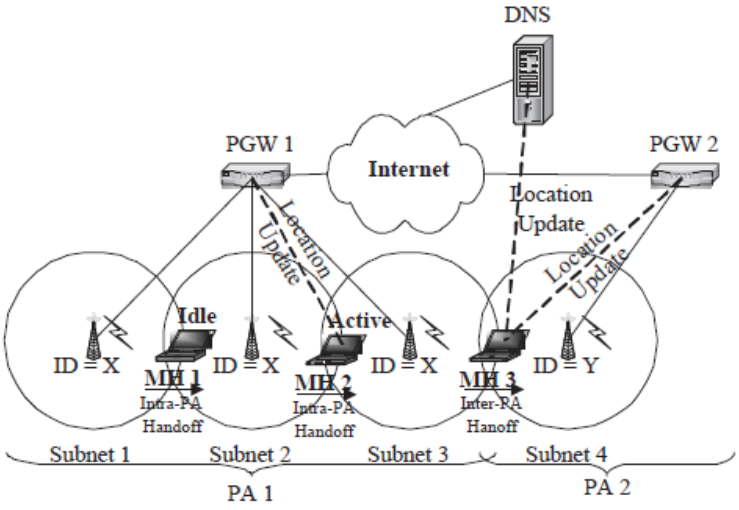
Κατά περιόδους το t1, το t2 και t3, ο MH λαμβάνει τη νέα διεύθυνση, προχωρώντας στο νέο υποδίκτυο και απελευθερώνοντας την παλαιά διεύθυνση IP, αντίστοιχα. Σε κάθε περίοδο η παλιά και η νέα διεύθυνση έχει διαφορετική βαρύτητα. Σε κάθε σημείο του handoff, το DNS ενημερώνεται για να εξασφαλίσει ότι ο CN παίρνει πάντα την ενημερωμένη διεύθυνση IP.



Σχήμα 3.15 Προτεραιότητα των IP στο P-SIGMA κατά τη διάρκεια του handoff

3.10.4 Λειτουργία του P-SIGMA

Το paging εισάγει μια ιεραρχική διαχείριση της θέσης ενός MH. Το βασικό συστατικό για το paging είναι το paging area. Μια απόφαση που πρέπει να πάρει οποιοδήποτε σχεδίου paging είναι να προσδιορίζει ένα idle MH. Εάν ένας MH δεν λάβει οποιοδήποτε πακέτο για μια ορισμένη χρονική περίοδο T, πηγαίνει στο idle mode. Όταν λάβει ένα πακέτο, γίνεται ξανά ενεργός και ξαναξεκινά ο χρόνος από το μηδέν. Τα idle MH δεν χρειάζεται να ανανεώνουν τη θέση τους όποτε κινούνται τοπικά σε από ένα AP σε ένα άλλο AP που ανήκουν στο ίδιο PGW. Το PGW πρέπει να ξέρει AP που ελέγχει. Αυτό επιτυγχάνεται με το να αποδώσουμε ένα προκαθορισμένο ID στα AP που είναι κάτω από ένα ενιαίο PA. Όποτε ένας MH κινείται από το υποδίκτυο του σε ένα άλλο υποδίκτυο μέσα στο ίδιο PA και είναι σε μη idle state, εκτελεί το P-SIGMA handoff. Όταν ένας MH εξέρχεται από ένα PA και μπαίνει σε ένα άλλο PA, εκτελεί το P-SIGMA handoff και ενημερώνει και το LM και το PGW με τη νέα διεύθυνση.



Σχήμα 3.16 P-SIGMA schema

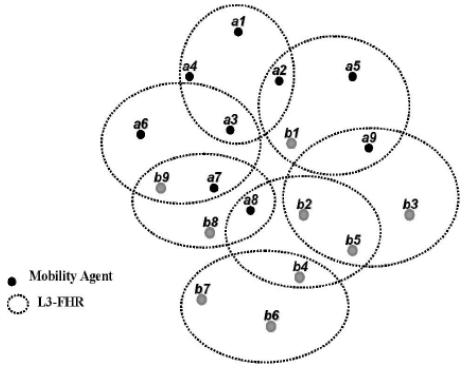
3.11 *Mobile IP Fast Authentication MIFA*

Το MIFA [11] όπως μπορούμε να καταλάβουμε και από το όνομα του προσπαθεί να πετύχει fast authentication όταν ένας κόμβος προχωρεί από ένα υποδίκτυο σε ένα άλλο. Κύριο χαρακτηριστικό του MIFA είναι το γεγονός ότι όταν μετακινείται ο MN από τον παλιό FA στο νέο, δε χρειάζεται να κάνει authentication στο Home Agent αλλά στον καινούριο FA.

3.11.1 Ορολογία για το Mobile IP Fast Authentication

- **Στρώμα3 Frequent Handoff Region (L3-FHR)**

Το L3-FHR είναι ένα σύνολο από γειτονικούς FA. Πάνω σε αυτές τις ομάδες από FA στηρίζεται το authentication, το οποίο μπορεί να χαρακτηριστεί και ως τοπικό authentication. Συνήθως σε ένα δίκτυο υπάρχουν παραπάνω από μία τέτοιες ομάδες. Οι FA που ανήκουν στο ίδιο L3-FHR έχουν ένα security association. Όταν κάποιος MN εισέλθει στη δικαιοδοσία κάποιου FA τότε αυτός ενημερώνει όλους τους FA που ανήκουν στο ίδιο L3-FHR. Αυτές οι ενημερώσεις περιλαμβάνουν τις authentication values μεταξύ του MN και του HA.



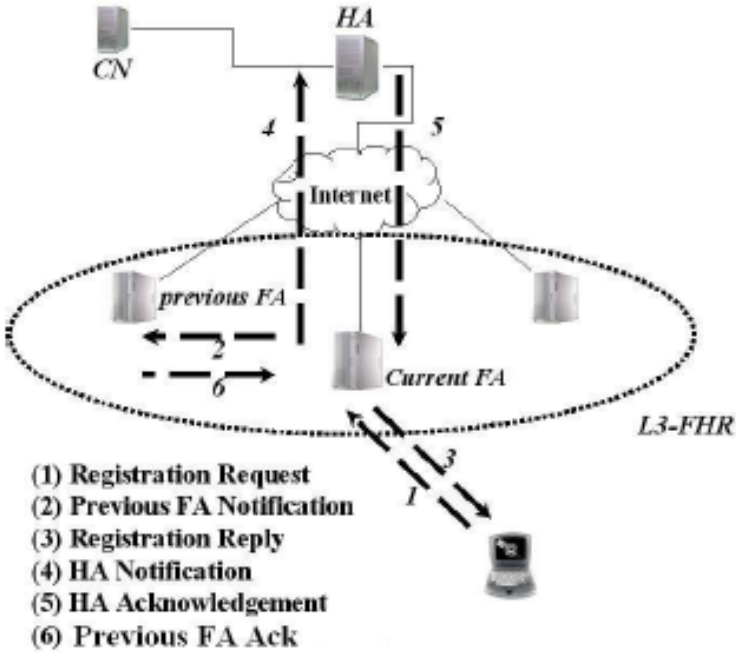
Σχήμα 3.17 L3-FHR schema

3.11.2 Handoff στο Mobile IP Fast Authentication

Η βασική ιδέα του MIFA είναι ότι μεταφέρεται η αρμοδιότητα για authentication από τον HA στο FA. Ειδικότερα ο FA πιστοποιεί τον MN σε συνεργασία με τον HA, αλλά η διεργασία αυτή λαμβάνει χώρα στο FA.

Αρχικά ο MN στέλνει ένα RegReq (registration request) στον FA και αυτός αποκρίνεται με ένα RegRply (registration replay). Αφότου λάβει το RegRply, ο MN μπορεί να επαναλάβει τη μετάδοση uplink. Για τα εισερχόμενα πακέτα προβλέπεται η εγκαθίδρυση ενός tunnel από τον παλιό FA προς τον νέο, μέχρι ο HA ενημερωθεί για τη μετακίνηση και αναδιαμορφωθεί το ρεύμα των εισερχομένων πακέτων προς το νέο FA. Επιπλέον ο χρόνος που απαιτείται για να χτίσει μια σήραγγα IPSec, εάν είναι απαραίτητο, αποφεύγεται. Όταν ο MN κινείται προς ένα FA από L3-FHR, στο οποίο ο προηγούμενος FA ανήκει, τότε ο MN στέλνει ένα μήνυμα RegRqst σε αυτόν τον FA. Αυτός ο νέος FA κάνει τον MN. Το authentication ελέγχεται από το security association που στέλνεται στον προηγούμενο FA. Στη συνέχεια, ο νέος FA ελέγχει τις πληροφορίες στο MIFA, οι οποίες επικυρώνονται σε σχέση με τις πληροφορίες που υπάρχουν από η πιστοποίηση του MN και του HA. Το νέο FA ελέγχει έπειτα εάν οι απαιτήσεις που ζητούνται από το HA μπορούν να ικανοποιηθούν. Εάν η πιστοποίηση είναι επιτυχές, το νέο FA στέλνει ένα notification στο προηγούμενο FA για να ενημερώσει ότι πρέπει να διαβιβάσει τα πακέτα που στέλνονται στο MN στο νέο FA. Μετά από αυτόν το νέο FA στέλνει την απάντηση εγγραφής στο MN. Επιπλέον το νέο FA στέλνει ένα μήνυμα στον HA για να ενημερώσει για τη μετακίνηση. Στη

συνέχεια ο HA καθιερώνει μια νέα σήραγγα προς στο νέο FA. Μετά από αυτό, ο HA προωθεί τα πακέτα στο νέο FA.



Σχήμα 3.18 MIFA schema

4. Επιθέσεις

4.1 *Επιθέσεις στα δίκτυα γενικά*

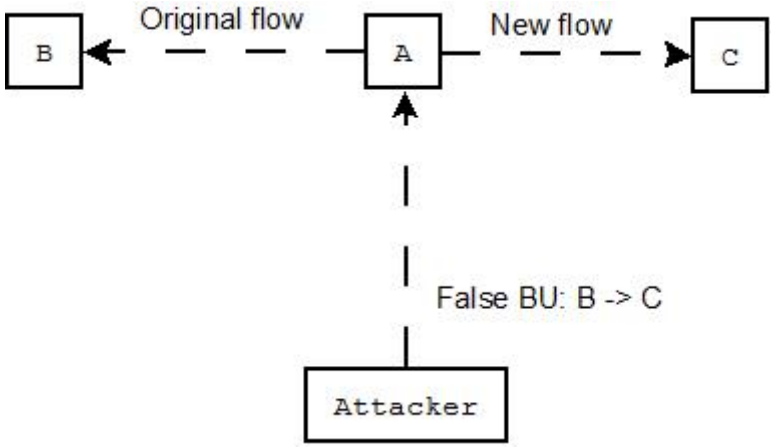
Οι επιθέσεις στα κινητά δίκτυα χωρίζονται σε τρεις κατηγορίες [12]. *Επιθέσεις κατά της διεύθυνσης*: αυτές οι επιθέσεις στοχεύουν στο να υποκλέψει ή να προσποιηθεί μια διεύθυνση ένας κακόβουλος κόμβος, *επιθέσεις κατά άλλων κόμβων* του δικτύου. Αυτές οι επιθέσεις στοχεύουν στο να υπερφορτώσουν κάποιο κόμβο του δικτύου έτσι ώστε να μη μπορεί να διαχειριστεί το φόρτο και ως αποτέλεσμα να τον καταστήσει άχρηστο. *Επιθέσεις κατά Binding Update:* Αυτές οι επιθέσεις στοχεύουν στις πηγές των κόμβων που επικοινωνούν με τον κόμβο θύμα ή και τον ίδιο τον κόμβο θύμα. Οι επιθέσεις γενικά έχουν ως σκοπό είτε να υποκλέψουν πληροφορία (attack to confidentiality), είτε να την αλλάξουν(attack to message integrity), ακόμη και να παρεμποδίσουν την επικοινωνία.

4.2 *Επιθέσεις κατά της διεύθυνσης*

4.2.1 Κλοπή διεύθυνσης κινητού κόμβου (address stealing of mobile node)

Ο πιο προφανής κίνδυνος για ένα δίκτυο είναι η προσποίηση ενός επιτιθέμενου ο οποίος είναι ένας κόμβος εγγεγραμμένος στο δίκτυο. Αυτό γίνεται με το να εμφανίσει τη διεύθυνση του άλλου ως δική του και να κλέψει την ροή των δεδομένων που προορίζονταν για τον άλλον. Αυτό γενικά είναι εφικτό με πλαστό binding update για την αλλαγή του “care of address” του κινητού κόμβου. Με απλά λόγια αλλαγή της διεύθυνσης αποστολής των πακέτων στον home agent και ως επέκταση της ροής τους.

Στη πιο απλή του μορφή δηλαδή, χωρίς να υπάρχει κάποιου είδους πιστοποίηση των binding updates αρκεί να γίνει από οποιονδήποτε ένα binding update με πλαστά στοιχεία και αυτομάτως αλλάζει η ροή της πληροφορίας προς τον επιτιθέμενο.



Σχήμα 4.1 address stealing of mobile node

4.2.2 Κλοπή διεύθυνσης μόνιμου κόμβου κινητού δικτυού (Stealing Addresses of Stationary Nodes)

Σε αυτό τον τύπο ο επιτιθέμενος πρέπει να ξέρει ή να υποθέσει τις διευθύνσεις IP και τις πηγές των πακέτων που εκτρέπονται και του προορισμού των πακέτων. Αυτό σημαίνει ότι είναι δύσκολο να επαναπροσανατολιστούν όλα τα πακέτα σε ή από έναν συγκεκριμένο κόμβο επειδή ο επιτιθέμενος θα πρέπει να ξέρει τις διευθύνσεις IP όλων των κόμβων με τους οποίους επικοινωνεί.

Οι κόμβοι με τις γνωστές διευθύνσεις, όπως οι server και εκείνοι που χρησιμοποιούν stateful configuration, είναι περισσότερο τρωτοί. Κόμβοι που είναι μέρος της υποδομής δικτύου, όπως DNS, είναι ιδιαίτερα ενδιαφέροντες στόχοι για τους επιτιθεμένους και ιδιαίτερα εύκολο να προσδιοριστούν. Οι κόμβοι που αλλάζουν συχνά τις διευθύνσεις τους είναι σχετικά ασφαλείς. Εντούτοις, εάν καταχωρούν την IP τους στο DNS, είναι και αυτοί εκτεθειμένοι. Το IPv6 εξετάζοντας τα χαρακτηριστικά γνωρίσματα της επίθεσης μετριάζει αυτούς τους κινδύνους.

Γενικά είναι δυνατόν να κλαπεί η διεύθυνση ενός stationary node του δικτύου εάν αρχικά μπορέσουμε να απομονώσουμε τον stationary node με κάποια επίθεση denial-of-service και στη συνεχεία προσποιηθεί ο επιτιθέμενος ότι είναι ο απομονωμένος stationary node.

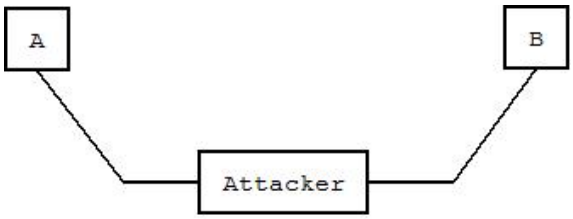
4.2.3 Κλοπή μελλοντικής διεύθυνσης κινητού κόμβου (Future Stealing Addresses)

Όπως καταλαβαίνουμε και από τον τίτλο, η επίθεση αυτή στοχεύει τις μελλοντικές διευθύνσεις που μπορεί να πάρει ένας κόμβος ο όποιος αποτελεί το στόχο αυτής της επίθεσης. Ένας επιτιθέμενος μπορεί να έχει τη δυνατότητα να μαντέψει ή να γνωρίζει ποια διεύθυνση θα υιοθετήσει ο κόμβος-στόχος. Είναι εφικτό να γίνει αυτού του είδους η επίθεση εάν ο home agent του δικτύου επιτρέπει τη δυναμική δέσμευση διευθύνσεων από τους κινητούς κόμβους. Με τη διεύθυνση της πρόβλεψης ο επιτιθέμενος δημιουργεί μια εγγραφή στο Binding Cache με αυτή τη διεύθυνση στο home address του επιτιθέμενου. Η εγγραφή της διεύθυνσης στο Binding Cache ενόσω είναι σε ισχύ, ο επιτιθέμενος και ο κόμβος στόχος θα έχουν την ιδία διεύθυνση. Αυτό δίνει τη δυνατότητα στον επιτιθέμενο να διαπράξει τις επιθέσεις man in the middle και denial of service.

4.2.4 Man in the middle (Επίθεση του ενδιάμεσου κόμβου)

Η επίθεση αυτή έχει ως στόχο να την κλοπή ή και την αλλαγή πληροφοριών μεταξύ της επικοινωνίας ενός κινητού κόμβου με κάποιον Home Agent. Επιτυγχάνεται με το να στείλει ο επιτιθέμενος δυο binding updates, ένα στον κινητό κόμβο-στόχο και ένα στον agent με τον όποιο επικοινωνεί. Αυτό πρέπει να γίνει με τέτοιο τρόπο ώστε να αλλάξει τη ροή της πληροφορία που ανταλλάσουν μεταξύ τους με τέτοιο τρόπο ώστε να γίνει ένας αναμεταδότης τους. Με αυτό τον τρόπο θα έχει πρόσβαση στο περιεχόμενο των μηνυμάτων τους.

4.2 Original data path, before man-in-the-middle attack



4.3 Modified data path, after the falsified binding updates

4.2.5 Denial of service (Άρνηση παροχής υπηρεσίας)

Ως αποτέλεσμα αυτού του τύπου της επίθεσης είναι η διακοπή της επικοινωνία μεταξύ του κινητού κόμβου και του Agent. Αυτό είναι εφικτό με το να στείλει ο επιτιθέμενος ένα Binding Update στον κινητό κόμβο – στόχο ή στον Agent ή και στους δυο, και να τους αλλάξει τη ροή αποστολής των μηνυμάτων τους προς μια τυχαία διεύθυνση.

4.2.6 Επανάληψη και παρεμπόδιση των Binding Updates (Replaying and Blocking Binding Updates)

Στόχος αυτής της επίθεσης είναι τα δίκτυα που χρησιμοποιούν σύστημα πιστοποίησης για τα binding update. Ο επιτιθέμενος είναι σε θέση να καταγράψει τα πιστοποιημένα binding update. Εφόσον ο κινητός κόμβος – στόχος αλλάξει Agent, ο επιτιθέμενος επαναλαμβάνει τη διαδικασία με τα κλεμμένα και πιστοποιημένα binding update. Έτσι, με αυτόν τον τρόπο, παίρνει τη προηγούμενη θέση του κινητού κόμβου – στόχου και αναπροσαρμόζει τη ροή της πληροφορία προς αυτή. Με αυτό τον τρόπο μπορεί να προκαλέσει τις επιθέσεις denial of service και κλοπής πακέτων ακόμα και να προσποιηθεί ο επιτιθέμενος ότι είναι ο κινητός κόμβος.

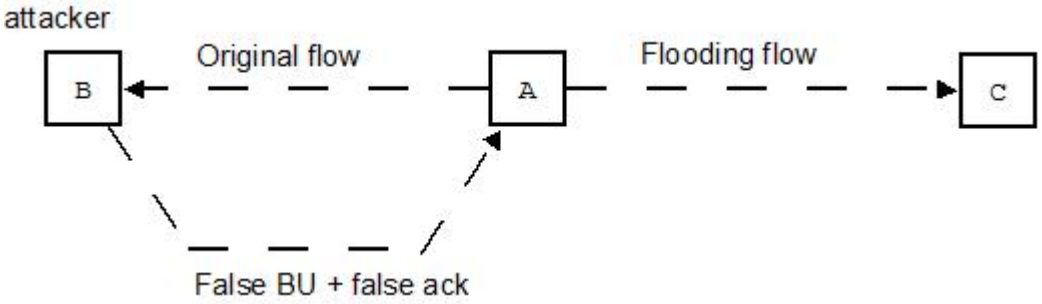
Μια παραλλαγή της επίθεσης αυτής είναι το ότι ο επιτιθέμενος παρεμποδίζει τα binding update του κινητού κόμβου από την καινούρια του θέση. Αυτό είναι εφικτό με το να δημιουργήσει φόρτο από άχρηστη πληροφορία στη συχνότητα ή με το να υιοθετήσει το flooding attack προς τον κινητό κόμβο.

Για τις δυο πιο πάνω παραλλαγές τη επίθεσης ο επιτιθέμενος πρέπει να βρίσκεται στο ίδιο τοπικό δίκτυο με τον κινητό κόμβο – θύμα, για να μπορεί να εποπτεύει τα πακέτα και να τα παρεμποδίζει εάν χρειαστεί. Γι’ αυτό το λόγο οι επιθέσεις αυτού του τύπου θεωρούνται ελάσσονος σημασίας.

4.3 *Επιθέσεις κατά άλλων κόμβων του δικτυού*

4.3.1 Flooding

Όπως καταλαβαίνουμε και από το όνομα της επίθεσης flooding (κατακλυσμός), η επίθεση αυτή στηρίζεται στο να κατακλειστεί με (άχρηστες) πληροφορίες ο στόχος. Σε μια απλή μορφή αυτής της επίθεσης ο επιτιθέμενος καλεί ένα μεγάλο όγκο πληροφορίας προς το μέρος του και έπειτα τον ανακατευθύνει προς το στόχο με ένα binding update. Για να συνεχιστεί η ροή της πληροφορίας προς το στόχο και να μη διακοπεί λόγω μη αποστολής acknowledgments (εφόσον τα πακέτα δε του έρχονται από δική του κλήση), ο επιτιθέμενος στέλνει πλαστά acknowledgments.



Σχήμα 4.4 Basic Flooding Attack

Return-to-Home Flooding

Μια παραλλαγή του παραπάνω είναι ο στόχος της επίθεσης να είναι ο home agent ή το οικείο δίκτυο (ή κάποιο δίκτυο το όποιο επισκέφθηκε ο στόχος) αντί ο στόχο να είναι ο κινητός κόμβος. Θα μπορούσε απλά να ανακατευθύνει τη δεδομένα προς τη διεύθυνση του δικτύου και να στέλνει acknowledgments. Αλλιώς, ο επιτιθέμενος θα μπορούσε να ισχυριστεί ότι είναι ένα κόμβος με διεύθυνση ίδια με τη διεύθυνση του δικτύου-στόχου. Ενόσω ο επιτιθέμενος στέλνει πλαστά μηνύματα ότι είναι εκτός οικείου δικτύου, θα άρχιζε να καλεί μεγάλα stream δεδομένων με στόχο το δίκτυο. Τέλος θα μπορούσε να κατακλείσει τον agent με πλαστά binding updates.

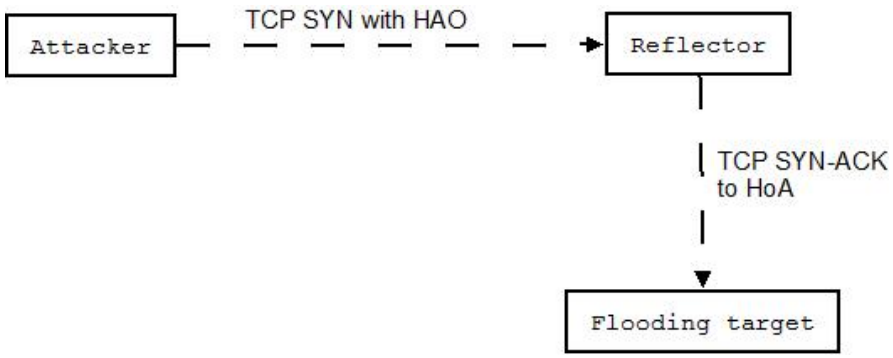
4.4 *Επιθέσεις κατά Binding Update*

4.4.1 Unnecessary Binding Updates

Όταν ένας κινητός κόμβος λαμβάνει ένα πακέτο από ένα νέο correspondent node μέσω του home agent, τότε μπορεί να κάνει ένα binding update. Ένας επιτιθέμενος μπορεί να το εκμεταλλευτεί αυτό και να στέλνει πλαστά πακέτα που να φαίνεται ότι προέρχονται από ένα νέο correspondent node. Έτσι, ο home agent μπορεί να ξεκινήσει να κάνει binding updates για κάθε νέο (πλαστό) correspondent node. Η λήψη απόφασης για την εγγράφη των binding updates μπορεί να εξαρτάται από πολλούς παράγοντες. Η μη καταγραφή των binding update μπορεί να μετριάσει τις επιθέσεις αυτές, αλλά δεν θα τις σταματήσει εντελώς. Με αυτόν τον τρόπο, ο επιτιθέμενος μπορεί να προκαλέσει την κατασπατάληση των πόρων.

4.4.2 Reflection attack

Είναι μια παραλλαγή του flooding attack αλλά αντί ο επιτιθέμενος να στέλνει τη ροή πληροφοριών απευθείας στον στόχο και να τον κατακλίσει από το φόρτο προκαλώντας denial of service, ξεγελά και αναγκάζει ένα τρίτο κόμβο να στείλει τη ροή στο κόμβο. Με αυτό τον τρόπο δεν είναι εύκολα εφικτό στο να ανακαλύψει κάποιος τον πραγματικά επιτιθέμενο αφού κάνει την επίθεση έμμεσα. Η επίθεση αυτή είναι πιο επικίνδυνη αν με ένα σήμα του επιτιθέμενου προς τον τρίτο κόμβο, τον αναγκάζει να στείλει πολλαπλά πακέτα. Σε αυτή την επίθεση εύκολα μπορούν να γίνουν στόχοι οι agent του συστήματος, διότι μπορεί ο επιτιθέμενος να αναγκάσει τον τρίτο κόμβο να στείλει τα πακέτα σε ένα κόμβο όπου για να γίνει εφικτό αυτό θα πρέπει τα πακέτα να περάσουν έναν agent. Έτσι μπορεί να προκαλέσει μεγαλύτερης κλίμακας προβλήματα. Γενικά θεωρείται πολύ επικίνδυνος τύπος επίθεσης.



4.5 Reflection Attack

5. Ασφαλίζοντας ένα Πρωτόκολλο κινητικότητας IPv6

5.1 *Γενικά σχόλια περί ασφάλειας*

Έχοντας αναλύσει τα πρωτόκολλα και τις επιθέσεις πάνω σε αυτά στα προηγούμενα κεφάλαια μπορούμε να αρχίσουμε να σκεφτόμαστε το τι θέλουμε από ένα πρωτόκολλο έτσι ώστε να το θεωρήσουμε ασφαλές; αφού αναγνωρίσουμε αυτό, τι είναι αυτό που πρέπει να κάνουμε ώστε να γίνει ασφαλές;

Μια αρχική σκέψη είναι να μη μπορεί κάποιος να διαβάσει εύκολα την πληροφορία από τα πακέτα που στέλνουμε και λαμβάνουμε. Αυτό είναι η μία παράμετρος αλλά όχι μια ολική λύση στο πρόβλημα της ασφάλειας. Σύμφωνα με τη θεωρία ένα ασφαλές δίκτυο παρέχει τα εξής χαρακτηριστικά:

1. Πιστοποίηση (Authentication)
2. Ακεραιότητα (Integrity)
3. Εμπιστευτικότητα (Confidentiality)
4. Κρυπτογράφηση (Encryption)
5. Μη αποκήρυξης (Non – repudiation)

Τα οποία έχουμε αναλύσει αρχικά.

Η ακεραιότητα, η εμπιστευτικότητα, η κρυπτογράφηση και σε ορισμένες περιπτώσεις η πιστοποίηση, μπορούν να διασφαλιστούν με τη διαδικασία της κρυπτογράφησης στα πακέτα και τα σήματα που ανταλλάσσονται στο δίκτυο. Υπάρχουν και ιδικές τεχνικές που προσφέρουν πιστοποίηση.

Υπάρχουν δυο κατηγορίες αλγόριθμων κρυπτογράφησης, οι συμμετρικοί και οι ασύμμετροι αλγόριθμοι. Οι συμμετρικοί εκτελούν την κρυπτογράφηση και την αποκρυπτογράφηση με το ίδιο κλειδί, ενώ οι ασύμμετροι παράγουν το κρυπτόγαμμα (το αποτέλεσμα μετά την κρυπτογράφηση) με ένα κλειδί που είναι συνήθως δημόσιο και αποκρυπτογραφούν με ένα άλλο που κρατιέται κρυφό. Το πρόβλημα με τους συμμετρικούς αλγορίθμους είναι το πώς δυο κόμβοι που θέλουν να επικοινωνήσουν θα ανταλλάξουν το κλειδί τους.

Όπως μπορούμε να καταλάβουμε τεράστιας σημασίας για τους αλγορίθμους κρυπτογράφησης είναι το κλειδί, όσον αφόρα το μέγεθος του και το πώς αυτό θα (μυστικά) διανεμηθεί. Γενικά ένα άλλο συστατικό είναι πολύ σημαντικό για την ασφάλεια ενός πρωτοκόλλου και αυτό είναι το IKE.

Το πρόβλημα τις μη αποκήρυξης λύνεται με traffic analysis τεχνικές. Είναι ιδιαίτερα σημαντικό πρόβλημα καθώς αν καταφέρει κάποιος να αποκλίσει ένα κόμβο κλειδί για τη λειτουργία του δικτύου (λχ home agent) τότε θα έχει παραλύσει όλο το δίκτυο.

Τα πρωτόκολλα τα οποία έχουν φτάσει σε επίπεδο να έχουν RFC προβλέπουν μέτρα προστασίας για μερικούς ή όλους του τύπους απειλών. Άρα, από τα πρωτόκολλα πρέπει να δούμε για ποιές απειλές μεριμνούν και αν αφήνουν κενά πώς αυτά καλύπτονται.

5.2 *Authentication header (AH)*

Το Authentication Header [13] είναι ένας μηχανισμός για να παρέχει ακεραιότητα και πιστοποίηση για τα πακέτα του IP. Επίσης παρέχει μη αποκήρυξη, ανάλογα με το οποίο ο κρυπτογραφικός αλγόριθμος χρησιμοποιείται. Παραδείγματος χάριν, η χρήση ενός ασύμμετρου αλγορίθμου, όπως ο RSA, θα μπορούσε να παρέχει προστασία κατά τις μη αποκήρυξης.

5.3 *Encapsulate Secure Payload (ESP)*

Το Encapsulate Secure Payload (ESP) [14] παρέχει εμπιστευτικότητα και ακεραιότητα με την κρυπτογράφηση των στοιχείων και τοποθέτηση των κρυπτογραφημένων στοιχείων στο IP. Η χρήση του ESP θα αυξήσει το κόστος επεξεργασίας πρωτοκόλλου IP στα συμμετέχοντα συστήματα καθώς και την καθυστέρηση στην επικοινωνίας.

5.4 *Αλγόριθμοι για το Authentication Header και το Encapsulate Secure Payload*

Ενδεικτικά παραθέτουμε δύο αλγόριθμους που μπορούν να υιοθετηθούν από το ESP και το AH για να τους παρέχουν διάφορες ιδιότητες ο κάθε ένας. Ο HMAC-SHA-1-96 που παρέχει ακεραιότητα και πιστοποίηση καθώς και ο Triple-DES-CBC που παρέχει εμπιστευτικότητα. Εδώ πρέπει να πούμε ότι η ισχυροτήτα των αλγορίθμων αυτών μειώνεται σε σχέση με το χρόνο. Αυτό γιατί βασίζονται σε σκληρά προβλήματα που είναι δύσκολο-χρονοβόρο για να λυθούν με τα σημερινά δεδομένα. Όμως αν λάβουμε υπόψη ότι η υπολογιστική ισχύς αυξάνεται τότε καταλαβαίνουμε ότι σε μερικά χρόνια αυτοί οι αλγόριθμοι θα είναι ανεπαρκείς.

5.5 *IP security (IPsec)*

Το IPsec [15] παρέχει υπηρεσίες ασφάλειας στο IP για τη διευκόλυνση ενός συστήματος για να επιλέξει τα απαραίτητα πρωτόκολλα ασφάλειας, να καθορίσει τους αλγόριθμους που χρησιμοποιούνται και να βάζει σε ισχύ οποιαδήποτε κρυπτογραφικά κλειδιά που απαιτούνται για να παρέχουν τις ζητούμενες υπηρεσίες. Το IPsec μπορεί να χρησιμοποιηθεί για να προστατεύσει ένα ή περισσότερα μονοπάτια μεταξύ ενός ζευγαριού κόμβων, μεταξύ ενός ζευγαριού security gateways ή μεταξύ μιας security gateways και ενός host.

Το IPsec χρησιμοποιεί δύο πρωτόκολλα για να παρέχει την ασφάλεια κυκλοφορίας Authentication Header (AH) και το Encapsulating secure payload (ESP). Το AH παρέχει ακεραιότητα, πιστοποίηση και μια προαιρετικά υπηρεσία anti-replay attack. Το ESP μπορεί να παρέχει την εμπιστευτικότητα και με περιορισμένες δυνατότητες πιστοποίησης, ακεραιότητας και μια προαιρετική υπηρεσία anti-replay attack.
Κάθε πρωτόκολλο υποστηρίζει δύο μεθόδους χρήσης:

1. Transport mode: τα πρωτόκολλα παρέχουν την προστασία για τα πρωτόκολλα σε ανώτερα στρώμα.
2. Tunnel mode, τα πρωτόκολλα εφαρμόζονται στα ανοιγμένα IP πακέτα.

5.5.1 Εφαρμογή του IPsec σε IP πρωτόκολλα

Υπάρχουν διάφοροι τρόποι με τους οποίους το IPsec μπορεί να εφαρμοστεί σε έναν host ή από κοινού με έναν router ή ένα firewall

1. Ένταξη του IPsec μέσα στο IP. Αυτό απαιτεί την πρόσβαση στον πηγαίο κώδικα του IP και ισχύει και στους host και σε secure gateways.

2. "Bump-in-the-stack" (BITS), όπου IPsec εφαρμόζεται κάτω από το υπάρχον IP πρωτόκολλο, μεταξύ του εγγενούς IP και των local network drivers. Η πρόσβαση στο πηγαίο κώδικα του IP δεν απαιτείται. Αυτή η προσέγγιση υιοθετείται συνήθως στους host.

3. Με τη χρήση ενός εξωτερικού crypto-επεξεργαστή. Ο crypto-επεξεργαστής είναι ένα χαρακτηριστικό σχεδιασμού των συστημάτων ασφαλείας δικτύων που χρησιμοποιείται από στρατιωτικές και μερικές εμπορικές εφαρμογές. Ο crypto-επεξεργαστής είναι optimized για κρυπτογραφικές πράξεις.

5.5.2 Security Association

Ένα Security Association (SA) είναι η καθιέρωση των κοινών πληροφοριών ασφάλειας μεταξύ δύο οντοτήτων ενός δικτύου για να υποστηρίξει την ασφαλή επικοινωνία. Ένα SA μπορεί να περιλαμβάνει τα κλειδιά κρυπτογράφησης, τα initialization vectors ή τα digital certificates. Ένα SA είναι ένα μονής κατεύθυνσης κανάλι και λογική σύνδεση που παρέχει μια ασφαλή σύνδεση στοιχείων μεταξύ των συσκευών του δικτύου.

Ένα SA είναι απαραίτητο για να εφαρμόσουμε πάνω στο IP το AH, ESP ή και τα δύο. Οι υπηρεσίες ασφάλειας που διατίθενται σε ένα SA είναι με την χρήση του AH, ή του ESP, αλλά όχι των δύο. Εάν θέλουμε να εφαρμόσουμε και το AH και το ESP σε μια επικοινωνία τότε πρέπει να δημιουργηθούν δύο SA. Για να εξασφαλιστεί η αμφίδρομη επικοινωνία μεταξύ δύο host ή μεταξύ δύο secure gateway, δύο SA απαιτούνται (μια από τον A προς το B και μια από το B προς τον A).Ένα SA προσδιορίζεται με τρία χαρακτηριστικά:

1. Security Parameter Index (SPI)

2. IP Destination Address (είτε unicast, είτε multicast,είτε broadcast)
3. security protocol (AH or ESP) identifier

Όπως αναφέρθηκε πιο πάνω, υπάρχουν δύο τύποι-mode για το SA, το transport mode και το tunnel mode. Το transport mode είναι για την ασφαλή επικοινωνία μεταξύ δύο host. Στην περίπτωση του ESP σε SA transport mode παρέχει τις υπηρεσίες ασφάλειας μόνο για τα πρωτόκολλα σε υψηλότερα στρώμα. Στην περίπτωση AH σε SA transport mode, η προστασία επεκτείνεται επίσης σε επιλεγμένα σημεία του IP header.

Το SA σε tunnel mode είναι ουσιαστικά ένα SA που εφαρμόζεται σε ένα tunnel του IP.

Ένας τρόπος SA σηράγγων είναι ουσιαστικά ένα SA που εφαρμόζεται σε μια σήραγγα IP. Όποτε το τέλος ενός SA είναι ένα secure gateway, το SA πρέπει να είναι tunnel. Κατά συνέπεια, ένα SA μεταξύ δύο secure gateway είναι πάντα tunnel SA, όπως είναι ένα SA μεταξύ ενός host και ενός secure gateway.

Για το SA σε tunnel mode, υπάρχει ένα εξωτερικό IP header που διευκρινίζει τον προορισμό επεξεργασίας IPsec και ένα εσωτερικό IP header που διευκρινίζει το τελικό προορισμό για το πακέτο. Εάν το AH υιοθετηθεί στον tunnel mode, τότε μέρη του εξωτερικού IP header θα είναι προστατευμένα, καθώς επίσης και όλο το εσωτερικό IP header και επίσης όλα τα πρωτόκολλα σε υψηλότερα στρώμα. Εάν το ESP υιοθετείται, η προστασία διατίθεται μόνο στο ανοιγμένο πακέτο, όχι στην εξωτερική header.

Εν κατακλείδι, ένας host πρέπει να υποστηρίξει και το transport mode και το tunnel mode. Ενώ ένα secure gateway απαιτείται να υποστηρίζει μόνο το tunnel mode. Εάν υποστηρίζει το transport mode, αυτός πρέπει να χρησιμοποιηθεί μόνο όταν το secure gateway ενεργεί ως host.

5.5.3 Λειτουργικότητα του Security Association

Το σύνολο υπηρεσιών ασφάλειας που προσφέρονται από ένα SA εξαρτάται από το πρωτόκολλο ασφάλειας (AH ή ESP) που επιλέγονται, τον SA τρόπο (transport mode

ή tunnel mode), τα end point σημεία SA και από την εκλογή των προαιρετικών υπηρεσιών μέσα στο πρωτόκολλο. Παραδείγματος χάριν, το AH παρέχει την authentication του αποστολέα των πακέτων και όχι connectionless για τα διαγράμματα IP δεδομένων.

Το AH επίσης προσφέρει προστασία από το replay attack εάν το θέλει ο δέκτης host, για να βοηθήσει με αυτό τον τρόπο στην αντιμετώπιση του denial-of-service attack. Το AH είναι ένα κατάλληλο πρωτόκολλο για να υιοθετηθεί όταν το εμπιστευτικότητα δεν απαιτείται. Το AH επίσης παρέχει πιστοποίηση για τα επιλεγμένα κομμάτια του IP header. Παραδείγματος χάριν, εάν η ακεραιότητα ενός extension του IPv6 header πρέπει να προστατευθεί καθοδόν μεταξύ του αποστολέα και του δέκτη, το AH μπορεί να παρέχει αυτήν την υπηρεσία.

Το ESP προαιρετικά παρέχει την εμπιστευτικότητα για την κυκλοφορία, η δύναμη της υπηρεσίας του εμπιστευτικότητα εξαρτάται εν μέρει από τον αλγόριθμο κρυπτογράφησης που υιοθετείται. Το ESP επίσης μπορεί προαιρετικά να παρέχει την πιστοποίηση. Εάν η πιστοποίηση συζητιέται για ένα ESP SA, ο δέκτης μπορεί επίσης να εκλέξει να επιβάλει προστασία από το replay attack με τα ίδια χαρακτηριστικά γνωρίσματα όπως στο AH.

Εάν την εμπιστευτικότητα επιλέγεται, κατόπιν ένα SA σε tunnel mode με ESP μεταξύ δύο secure gateway μπορεί να προσφέρει εμπιστευτικότητα σε μερικό του traffic flow. Η χρήση του tunnel mode επιτρέπει στις εσωτερικές IP header για να κρυπτογραφηθούν, κρύβοντας τις ταυτότητες της πηγής και του προορισμού του traffic.

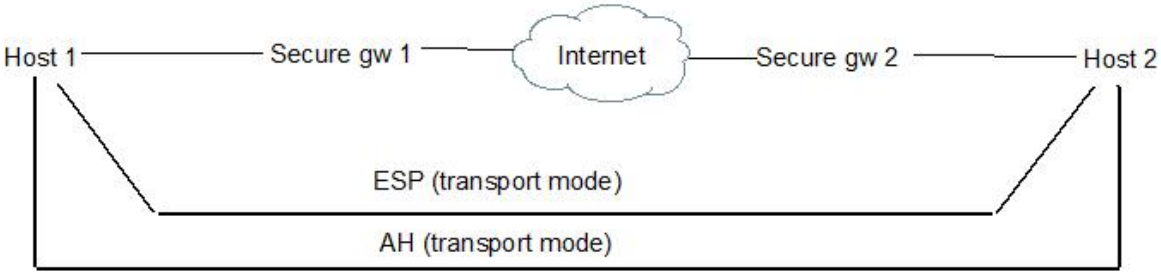
5.5.3.1 Συνδυασμοί με Security Association

Τα διαγράμματα δεδομένων IP που διαβιβάζονται μέσω κάποιου SA προστατεύονται από ακριβώς ένα πρωτόκολλο ασφάλειας, είτε AH είτε ESP, αλλά όχι και τα δύο μαζί. Μερικές φορές μια πολιτική ασφαλείας μπορεί να απαιτεί έναν συνδυασμό υπηρεσιών ασφαλείας για ένα ιδιαίτερο traffic flow που δεν μπορεί να επιτευχθεί με ένα SA. Σε τέτοιες περιπτώσεις θα είναι απαραίτητο να χρησιμοποιηθούν πολλαπλά

SA για να εφαρμοστεί η απαραίτητη πολιτική ασφαλείας στην επικοινωνία. Το "Security association bundle"είναι αυτό που εφαρμόζεται σε μια ακολουθία SA μέσω της οποίας η κυκλοφορία πρέπει να υποβληθεί σε επεξεργασία για να ικανοποιήσει την απαιτούμενη πολιτική ασφαλείας. Η σειρά της ακολουθίας καθορίζεται από την πολιτική. (Σημειώστε ότι το SA που περιλαμβάνει μια δέσμη μπορεί να ολοκληρώσει σε διαφορετικά σημεία κατάληξης. Παραδείγματος χάριν, ένα SA μπορεί να επεκταθεί μεταξύ ενός MN και ενός secure gateway και ένα δεύτερο ενθυλακωμένο SA μπορεί να επεκταθεί σε έναν host από το secure gateway).

Τα SA μπορούν να συνδυαστούν σε bundle με δύο τρόπους, transport adjacency και iterated tunneling.

- Το transport adjacency αναφέρεται στην εφαρμογή περισσότερων από ενός πρωτοκόλλων ασφάλειας στο ίδιο IP datagram, χωρίς να χρειάζεται να υλοποίηση tunnel. Αυτή η προσέγγιση στο συνδυασμό με το AH και το ESP επιτρέπει μόνο ένα επίπεδο συνδυασμού. Περαιτέρω ενσωμάτωση κάποιου SA δεν θα έχει κανένα επιπλέον όφελος δεδομένου ότι η επεξεργασία εκτελείται σε ένα instance του IPsec.

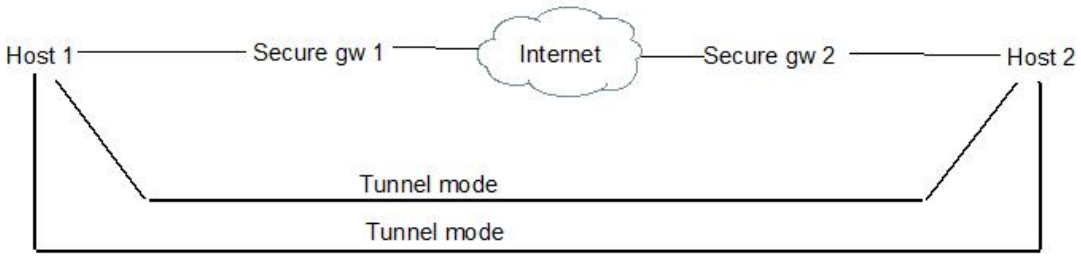


Σχήμα 5.1 ESP + AH σε host to host

Τα διαδοχικά tunnel εφαρμόζονται σε εφαρμογές με πολλαπλά στρώματα πρωτοκόλλων ασφάλειας που επηρεάζονται από το IP tunnel. Αυτή η προσέγγιση επιτρέπει τα πολλαπλάσια επίπεδα ενθυλάκωσης πρωτοκόλλων ασφάλειας, δεδομένου ότι το κάθε tunnel μπορεί να αρχίζει ή τερματίζει σε ένα διαφορετικό IPsec κατά μήκος του μονοπατιού του.

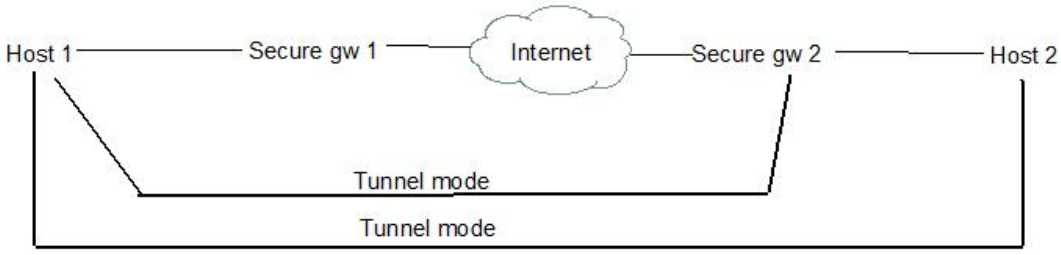
Υπάρχουν τρεις βασικές περιπτώσεις με διαδοχικά tunnel:

1. Σε αυτή τη περίπτωση και τα δύο σημεία τέλους για τη SA είναι τα ίδια. Τα εσωτερικά και εξωτερικά tunnel μπορούν το καθένα να είναι είτε σε AH είτε σε ESP πρωτόκολλο ασφαλείας, ή ακόμα και σε απίθανο σενάριο τα δύο tunnel μπορεί να εφαρμόζουν και το ίδιο πρωτόκολλο ασφαλείας.



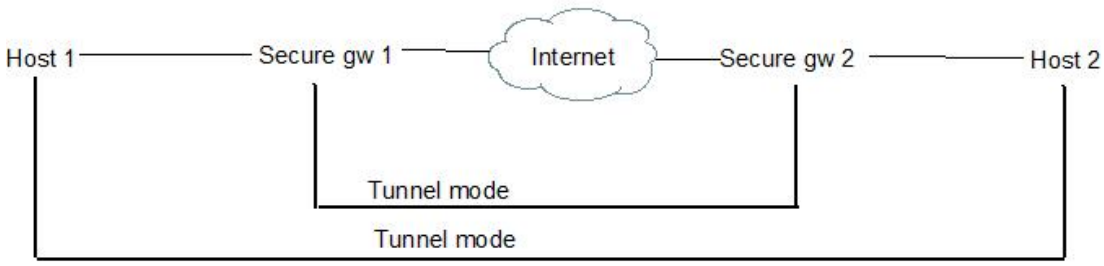
Σχήμα 5.2 Host to host tunnels

2. Το ένα σημείο τέλους της SA είναι το ίδιο. Το εσωτερικό και εξωτερικό tunnel θα μπορούσε να είναι είτε AH είτε ESP πρωτόκολλο ασφαλείας.



Σχήμα 5.3 Host to host and gateway tunnels

3. Κανένα από τα σημεία τέλους δεν είναι το ίδιο. Το εσωτερικό και εξωτερικό tunnel θα μπορούσε να είναι είτε AH είτε ESP πρωτόκολλο ασφαλείας.



Σχήμα 5.4 Gateway to gateway and host to host tunnels

Αυτές οι δύο προσεγγίσεις μπορούν επίσης να συνδυαστούν, π.χ., το SA bundle θα μπορούσε να κατασκευαστεί με tunnel mode και έναν ή δύο SA transport mode, που να εφαρμόζεται διάταξη σειράς. Σημειώνουμε ότι το ενθυλακωμένο tunnel δεν είναι ούτε στην πηγή, ούτε στον προορισμό ταυτόχρονα. Σε αυτή την περίπτωση, δεν θα υπήρχε host ή secure gateway με bundle που αντιστοιχεί στο ενθυλακωμένο tunnel. Για transport mode SA, η σειρά των πρωτοκόλλων ασφάλειας φαίνεται κάνει τη διαφορά. Το AH εφαρμόζεται και στα ανώτερα στρώμα του πρωτοκόλλου και σε κομμάτια IP header. Κατά συνέπεια εάν το AH χρησιμοποιείται σε transport mode, από κοινού με ESP, AH πρέπει να εμφανιστεί ως πρώτη επιγραφή μετά από το IP και πριν από την εμφάνιση του ESP. Σε αυτή την περίπτωση, το AH εφαρμόζεται στην παραγωγή κρυπτογραφημάτων από την παραγόμενη έξοδο του ESP. Αντίθετα, για SA με tunnel mode, μπορεί να κάνει χρήση του AH και του ESP με οποιαδήποτε σειρά. Η προϋπόθεση για να δημιουργηθεί ένα SA bundle είναι ότι το IPσsec πρέπει να είναι ρυθμισμένο να δέχεται αυτή τη διάταξη.

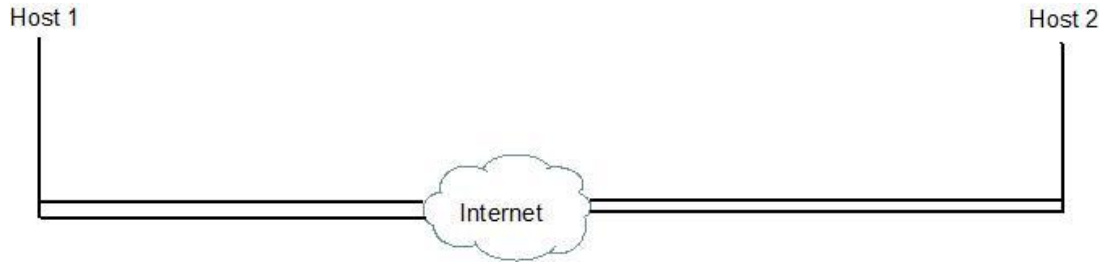
5.5.4 Βασικοί συνδυασμοί των Security Associations

Αυτό το τμήμα περιγράφει τα τέσσερα παραδείγματα των συνδυασμών SA που πρέπει να υποστηρίζονται από τους IPsec host ή τα secure gateway. Πρόσθετοι συνδυασμοί του AH ή/και του ESP με tunnel mode ή/και transport mode μπορούν να υλοποιηθούν κατά την κρίση του administrator του δικτύου.

==== = ένα ή περισσότερα SA (AH ή ESP, transport ή tunnel)
---- = connectivity
Hx = host x
SGx = security gateway x
X* = X supports IPsec

Σημείωση: Τα SA μπορούν να είναι είτε AH είτε ESP. Το mode (tunnel ή transport) καθορίζεται από τη φύση των σημείων τέλους. Για host-host, το SA mode μπορεί να είναι είτε tunnel είτε transport.

Περίπτωση 1. Η περίπτωση που παρέχουμε end-to-end ασφάλεια μεταξύ δύο host σε διαμέσου του internet (ή ενός intranet).



Σχήμα 5.5 Host to host SA

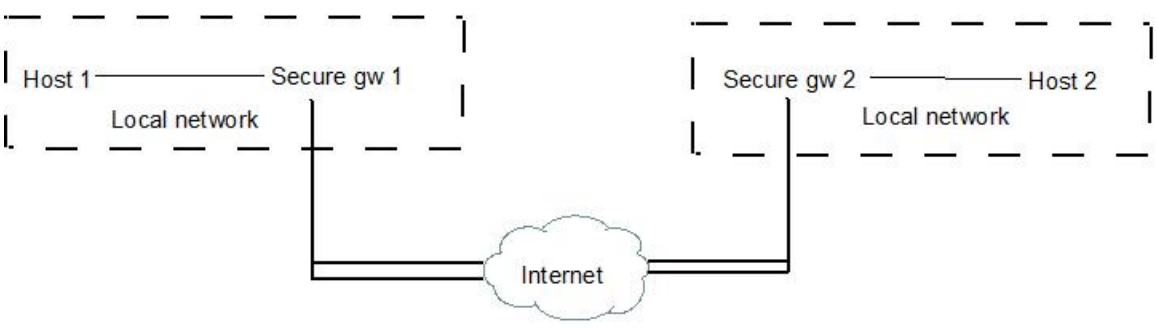
Σημειώστε ότι οι host μπορούν να υιοθετήσουν είτε το transport mode είτε tunnel mode. Έτσι τα header σε ένα πακέτο μεταξύ H1 και H2 θα μπορούσαν να μοιάσουν με ένα από τα εξής:

Transport	Tunnel
1. [IP1][AH][upper]	4. [IP2][AH][IP1][upper]
2. [IP1][ESP][upper]	5. [IP2][ESP][IP1][upper]
3. [IP1][AH][ESP][upper]	

Σχήμα 5.6 Header views

Σημειώνεται ότι δεν υπάρχει καμία απαίτηση να υποστηριχθεί συνδυασμός ESP ή AH, αλλά στο transport mode και το AH και το ESP μπορεί να εφαρμοστεί στο πακέτο. Σε αυτή την περίπτωση, η διαδικασία εγκαθίδρυσης των SA πρέπει να εξασφαλίσει ότι πρώτα το ESP και κατόπιν το AH θα εφαρμοστεί στο πακέτο.

Περίπτωση 2. Αυτή η περίπτωση επεξηγεί το απλό virtual private networks (VPN) δικτύων.



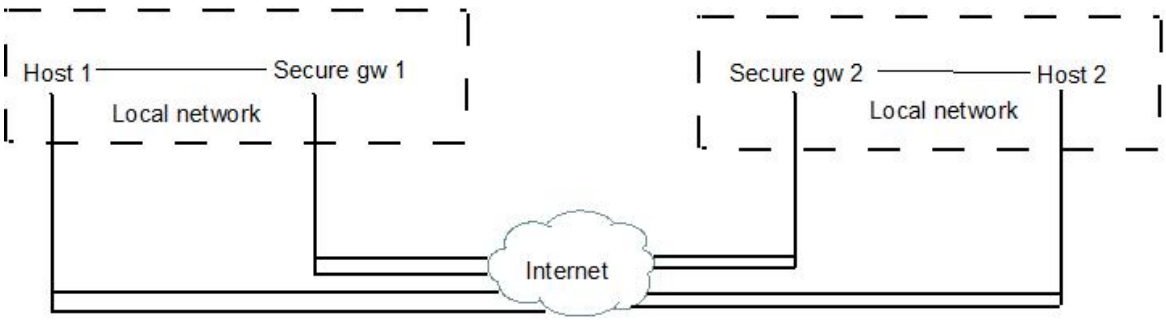
Σχήμα 5.7 VPN

Μόνο το tunnel mode απαιτείται εδώ. Έτσι οι επιγραφές σε ένα πακέτο μεταξύ SG1 και SG2 θα μπορούσαν να μοιάσουν με μία από τις εξής:

```
                Tunnel
--------------------
4. [IP2][AH][IP1][upper]
5. [IP2][ESP][IP1][upper]
```

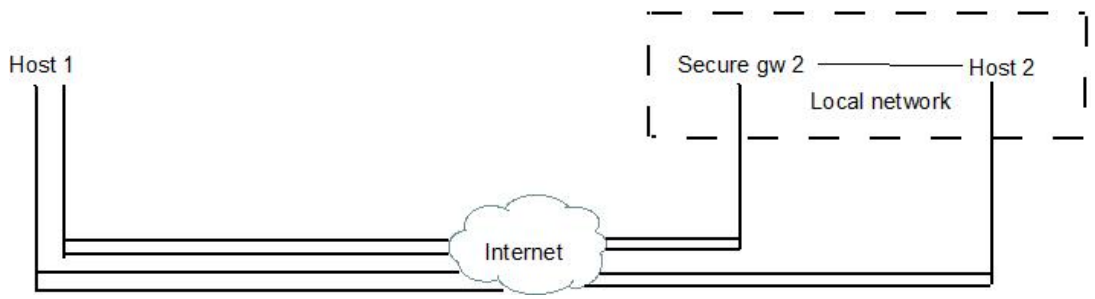
Σχήμα 5.8 Header views

Περίπτωση 3. Αυτή η περίπτωση συνδυάζει τις περιπτώσεις 1 και 2, προσθέτοντας τη end-to-end security μεταξύ του αποστολέα και του παραλήπτη host. Δεν επιβάλλει καμία νέα απαίτηση στους host ή στα secure gateway, εκτός για του ότι τα secure gateway πρέπει να διαμορφωθούν για να περάσουν το traffic του IPsec για τους hosts πίσω από αυτά.



Σχήμα 5.9 VPN with host to host SA

Περίπτωση 4. Αυτή καλύπτει την περίπτωση όπου ένας μακρινός host (H1) χρησιμοποιεί το Διαδίκτυο για να φθάσει στο secure gateway (SG2) και για να αποκτήσει πρόσβαση και έπειτα σε κάποιο κεντρικό υπολογιστή ή άλλη μηχανή (H2).



Σχήμα 5.10 Host to VPN

Μόνο tunnel mode απαιτείται μεταξύ H1 και SG2. Έτσι οι επιλογές για το SA μεταξύ H1 και SG2 θα ήταν μία από αυτές στην περίπτωση 2. Οι επιλογές για το SA μεταξύ H1 και H2 θα ήταν μία από αυτές στην περίπτωση 1.

Σημειώστε ότι σε αυτήν την περίπτωση, ο αποστολέας πρέπει να εφαρμόσει το transport header πριν από tunnel header. Επομένως διεπαφή του IPsec πρέπει να υποστηρίξει το configuration του Security Policy Database (SPD) και του Security Association Database (SAD) για να εξασφαλίσει αυτήν την σειρά της εφαρμογής των header στο IPsec. Όπως σημειώνεται παραπάνω, η υποστήριξη για επιπρόσθετους συνδυασμούς του AH και του ESP είναι προαιρετική. Η χρήση άλλων, προαιρετικών συνδυασμών μπορεί να έχει επιπτώσεις στη δυσλειτουργία της επικοινωνίας.

5.5.5 Security Association Database

Σε κάθε εφαρμογή του IPsec υπάρχει μια Security Association Database, στην οποία κάθε καταχώρηση καθορίζει τις παραμέτρους που σχετίζονται με ένα SA. Κάθε SA έχει μια καταχώρηση στο SAD.

5.5.6 Secure Police Database

Ένα SA είναι ένα μια υποδομή που χρησιμοποιείται για να επιβάλει μια πολιτική ασφαλείας στο περιβάλλον IPsec. Κατά συνέπεια το απαραίτητο στοιχείο του SA είναι Security Policy Database (SPD) που διευκρινίζει ποιες υπηρεσίες πρόκειται να προσφερθούν στα διαγράμματα δεδομένων IP.

5.5.7 SA και Key Management

Το IPSec παρέχει υποστήριξη και για χειροκίνητη και αυτοματοποιημένη δημιουργία SA και cryptographic key management. Τα πρωτόκολλα του IPSec, το AH και το ESP, είναι κατά ένα μεγάλο μέρος ανεξάρτητα από τις σχετικές τεχνικές διαχείρισης των SA, αν και οι τεχνικές αυτές έχουν επιπτώσεις σε μερικές από τις υπηρεσίες ασφάλειας που προσφέρονται από τα πρωτόκολλα. Παραδείγματος χάριν, η προαιρετική υπηρεσία anti-replay attack για το AH και το ESP απαιτούν την αυτοματοποιημένη διαχείριση SA.

5.5.7.1 Χειροκίνητες Τεχνικές

Η απλούστερη μορφή διαχείρισης είναι χειροκίνητη διαχείριση, στην οποία, κάποιο πρόσωπο διαμορφώνει χειροκίνητα τα κλειδιά σε κάθε σύστημα και στα στοιχεία των SA management σχετικά με την ασφαλή επικοινωνία με τα άλλα συστήματα. Οι χειροκίνητες τεχνικές είναι πρακτικές στα μικρά, στατικά περιβάλλοντα αλλά δεν έχουν καλό scalability. Παραδείγματος χάριν, μια επιχείρηση θα μπορούσε να δημιουργήσει ένα VPN χρησιμοποιώντας IPsec στα secure gateway. Εάν ο αριθμός περιοχών είναι μικρός, και δεδομένου ότι όλες οι περιοχές είναι κάτω από την έκταση μιας ενιαίας διοικητικής περιοχής, αυτό είναι πιθανό να είναι ένα εφικτό σενάριο για τις χειροκίνητες τεχνικές διαχείρισης. Σε αυτήν την περίπτωση, το secure gateway επιλεκτικά διαλέγει να προστατεύσει την κυκλοφορία σε άλλες περιοχές μέσα στην οργάνωση χρησιμοποιώντας ένα με χειροκίνητη διαμορφωμένο κλειδί, προστατεύοντας την κυκλοφορία και για άλλους προορισμούς.

5.5.7.2 Αυτοματοποιημένα SA και διαχείριση κλειδιών

Η ευρέως διάδοση και χρήση του IPSec απαιτούν ένα Internet standard που να είναι scalable, automated και SA management protocol. Τέτοια υποστήριξη απαιτείται για να διευκολύνει τη χρήση των χαρακτηριστικών γνωρισμάτων anti-replay attack στο AH και ESP, και για να προσαρμόσει την κατόπιν παραγγελίας δημιουργία του SA. Το βασικό αυτοματοποιημένο πρωτόκολλο που επιλέχτηκε γιατί η χρήση με IPSec είναι Internet key exchange (IKE).

Όταν ένα αυτοματοποιημένο διοικητικό SA/key πρωτόκολλο χρησιμοποιείται, η παραγωγή από αυτό το πρωτόκολλο μπορεί να χρησιμοποιηθεί για να παραχθούν κλειδιά, π.χ., για ένα ESP SA.

Το Key Management System μπορεί να παρέχει μια χωριστή σειρά bits για κάθε κλειδί ή μπορεί να παραγάγει μια σειρά bits από την οποία όλα τα κλειδιά εξάγονται από αυτή. Εάν μια ενιαία σειρά bits παράγεται, τότε χρειάζεται προσοχή διότι πρέπει να εξασφαλιστεί ότι τα μέρη του συστήματος που χαρτογραφούν τη σειρά των bits στα απαραίτητα κλειδιά το κάνουν τον ίδιο τρόπο και στις δύο άκρες του SA. Για να εξασφαλίσει ότι οι εφαρμογές του IPsec σε κάθε τέλος του SA χρησιμοποιούν τα ίδια

bits για τα ίδια κλειδιά και ανεξάρτητα από ποιο μέρος του συστήματος διαιρεί τη σειρά των bits σε μεμονωμένα κλειδιά, το κλειδί κρυπτογράφησης πρέπει να ληφθεί από τα πρώτα bits και το κλειδί του authentication πρέπει να ληφθεί από τα υπόλοιπα bits. Ο αριθμός bits για κάθε κλειδί καθορίζεται στη σχετική προδιαγραφή αλγορίθμου. Στην περίπτωση των πολλαπλάσιων κλειδιών κρυπτογράφησης ή των πολλαπλάσιων κλειδιών πιστοποίησης, η προδιαγραφή για τον αλγόριθμο πρέπει να διευκρινίσει τη σειρά στην οποία πρόκειται να επιλεχτούν τα bits που παρέχονται στον αλγόριθμο.

6. Πρόνοιες και αδυναμίες για τα πρωτόκολλα βασισμένα στο Mobile IPv6

6.1 *Μέριμνες στο Mobile IPv6*

Το MIPv6 ο διάδοχος του IPv4 έχει σχεδιαστεί σε νέα βάση για τις νέες ανάγκες. Μέσα σε αυτές τις ανάγκες υπάρχει και η ασφάλεια.

6.1.1 Denial-of-Service attack

Το return routability procedure προστατεύει ακόμα και από τις επιθέσεις εξαντλήσεων των πόρων γνωστές και ως Denial-of-Service. Συγκεκριμένα ο CN δεν διατηρεί κανένα state για κανένα MN έως ότου έρθει το authenticate Binding Update γι' αυτό τον κόμβο. Αυτό επιτυγχάνεται με μέσο των keygen tokens που προέρχονται από τα node keys τα οποία δεν είναι διακριτά από τους MN. Τα keygen tokens μπορούν να ανακτηθούν από τον CN και να συγκριθούν με τα CoA και home address, που περιέχονται στο BU. Αυτή η διαδικασία προστατεύει τον CN από την εξάντληση των πόρων.

6.1.2 Replay attack

Η διαδικασία του return routability που έχει περιγραφεί για το MIPv6 μπορεί να το προστατέψει από το replay attack. Εφόσον τα binding updates φυλάσσονται, τότε με της σύγκριση του MAC address και του sequence number μπορεί να διακριθεί εάν αυτό το binding update είναι καινούριο ή αποτέλεσμα του replay attack.

6.1.3 Απειλές σχετικές με τα Binding Updates

Το return routability procedure προστατεύει από απειλές που σχετίζονται με τα πλαστά BU εκτός από μια εξαίρεση. Η εξαίρεση αυτή είναι εάν ο επιτιθέμενος είναι σε θέση να κάνει monitoring το μονοπάτι μεταξύ του home agent και του correspondent node.

6.1.4 Απειλή κατά του confidentiality

Το MIPv6 παρέχει όλους τους μηχανισμούς εκείνους για να κάνει την επικοινωνία ασφαλή σε σχέση με το να γνωρίζουμε με το ποιόν επικοινωνούμε. Αλλά τι γίνεται με την εμπιστευτικότητα της επικοινωνίας; Εδώ θα πρέπει να επικαλεστούμε τους μηχανισμούς του IPSec που μας παρέχουν τέτοιες ιδιότητες. Θέλουμε να προσδώσουμε end-to-end εμπιστευτικότητα, άρα μια λογική λύση είναι να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP. Το ESP προσφέρει κρυπτογράφηση και πιστοποίηση (ανάλογα με τον αλγόριθμο τον οποίο έχει επιλεγεί).

6.1.5 Απειλή κατά του integrity

Εδώ θα πρέπει να επικαλεστούμε τους μηχανισμούς του IPSec που μας παρέχουν τέτοιες ιδιότητες. Επομένως εφόσον έχουμε να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP, για να προσδώσουμε εμπιστευτικότητα, μπορούμε επίσης σε αυτό το SA να χρησιμοποιήσουμε και ένα αλγόριθμο για εξασφάλιση της ακεραιότητας.

6.2 *Μέριμνες στο Hierarchical Mobile IPv6 (HMIPv6)*

Το HMIP εισάγει μια νέα έννοια, δηλαδή τη Mobility Anchor Point που δρα ως local Home Agent. Είναι κρίσιμο ότι η σχέση ασφάλειας μεταξύ του κινητού κόμβου και του MAP είναι ισχυρή και πρέπει να μεσολαβεί το αμοιβαίο πιστοποίηση, ακεραιότητα, και την προστασία από το replay attack. Η εμπιστευτικότητα μπορεί να απαιτηθεί για την κυκλοφορία του payload, αλλά δεν απαιτείται για τη δέσμευση για αναπροσαρμογές στο MAP. Η απουσία οποιασδήποτε από αυτές τις προστασίες μπορεί να δώσει τη δυνατότητα στους κακόβουλους κινητούς κόμβους να προσποιηθούν τους νόμιμους ή ένα MAP. Οποιεσδήποτε από αυτές τις επιθέσεις έχουν αναμφισβήτητα τις ανεπιθύμητες επιδράσεις στην επικοινωνία του κινητού κόμβου με όλους τους αντίστοιχους κόμβους που έχουν τη γνώση του RCoA του κινητού κόμβου.

6.2.1 Μέριμνα ασφάλειας μεταξύ Mobile node - MAP

Προκειμένου να επιτραπεί ένας κινητός κόμβος για να χρησιμοποιήσει την υπηρεσία του MAP, χρειάζεται ένα αρχική πιστοποίηση για να επιτρέψει σε έναν κινητό κόμβο για να χρησιμοποιήσει το MAP. Η πιστοποίηση μπορεί να γίνει βάση της ταυτότητας του κινητού κόμβου, που ανταλλάχτηκε κατά τη διάρκεια του SA negotiation process. Η έγκριση μπορεί να χορηγηθεί βασισμένη στη ταυτότητα του κινητού κόμβου, βασισμένη στην ταυτότητα του Certificate Authority (CA) που ο MAP εμπιστεύεται. Σημειώστε ότι αυτό το επίπεδο έγκρισης είναι ανεξάρτητο από την έγκριση της χρήσης του RCoA. Ομοίως, ο κινητός κόμβος θα εμπιστευόταν το MAP εάν παρουσίαζε μία πιστοποίηση που υπογράφηκε από το ίδιο CA ή από ένα άλλο CA.

Το HMIPv6 χρησιμοποιεί μια πρόσθετη εγγραφή μεταξύ του κινητού κόμβου και του τρέχοντος MAP όπου ανήκει. Όταν κινείται ένας κινητός κόμβος σε μια νέα περιοχή (δηλαδή εξυπηρετείται από έναν νέο MAP), λαμβάνει ένα RCoA, ένα LCoA και τους καταλόγους για τη σύνδεση μεταξύ αυτών των δύο διευθύνσεων με το νέο MAP. Ο MAP έπειτα ελέγχει εάν το RCoA δεν έχει καταχωρηθεί ακόμα και, σε αυτή την περίπτωση, δημιουργεί μια binding cache entry με το RCoA και το LCoA. Όποτε ο κινητός κόμβος παίρνει ένα νέο LCoA, πρέπει να στείλει νέο BU που διευκρινίζει τη σύνδεση μεταξύ RCoA και του νέου LCoA του. Αυτό το BU πρέπει να επικυρωθεί, διαφορετικά οποιοσδήποτε host θα μπορούσε να στείλει BU για το RCoA του κινητού κόμβου και να υποκλέψει τα πακέτα του κινητού κόμβου. Εντούτοις, επειδή το RCoA είναι προσωρινό και δεν είναι συνδεδεμένο σε έναν ιδιαίτερο κόμβο, ένας κινητός κόμβος δεν είναι απαραίτητο αρχικά (πριν από την πρώτη αναπροσαρμογή συνδέσεων) να αποδείξει ότι είναι κύριο του RCoA του όταν καθιερώνει έναν security association με το MAP. Ένας MAP πρέπει μόνο να εξασφαλίσει ότι το BU για ένα ιδιαίτερο RCoA εκδόθηκε από τον ίδιο κινητό κόμβο που καθιέρωσε το σύνδεσμο ασφάλειας για εκείνο το RCoA.

Ο MAP δεν πρέπει να έχει την προγενέστερη γνώση της ταυτότητας του κινητού κόμβου ούτε της Home Address του. Κατά συνέπεια το SA μεταξύ του κινητού κόμβου και του MAP μπορεί να καθιερωθεί χρησιμοποιώντας οποιοδήποτε κλειδί από τα πρωτόκολλα καθιερώσεων όπως το IKE. Το return routability process δεν είναι απαραίτητη.

Ο MAP πρέπει να δημιουργήσει το SA για το RCoA (όχι το LCoA). Αυτό μπορεί να εκτελεσθεί με το IKE. Ο κινητός κόμβος χρησιμοποιεί το LCoA του ως διεύθυνση προέλευσης, αλλά διευκρινίζει ότι το RCoA πρέπει να χρησιμοποιηθεί στο SA. Αυτό επιτυγχάνεται με τη χρήση του RCoA ως ταυτότητα για το IKE.

Οι δεσμευτικές αναπροσαρμογές μεταξύ του MAP και του κινητού κόμβου πρέπει να προστατευθούν είτε με το AH είτε με το ESP με transport mode. Όταν το ESP χρησιμοποιείται, ένας αλγόριθμος authentication πρέπει να χρησιμοποιηθεί.

6.2.2 Denial-of-Service attack

Ομοίως με το Mobile IPv6.

6.2.3 Replay attack

Ομοίως με το Mobile IPv6.

6.2.4 Απειλές σχετικές με τα Binding Updates

Στο mobile IPv6 καθορίζει το return routability process που επιτρέπει να μπορεί να εξακριβωθεί η ταυτότητα κάποιου κόμβου. Το HMIPv6 έχει τους ίδιους μηχανισμούς άμυνας για τις απειλές που απορρέουν από τα spoofed binding updates.

6.2.5 Απειλή κατά του confidentiality

Ομοίως με το Mobile IPv6.

6.2.6 Απειλή κατά του integrity

Ομοίως με το Mobile IPv6.

6.3 *Μέριμνες στο Fast Handoff Mobile IPv6 (FMIPv6)*

6.3.1 Insecure FBU

Σε αυτήν την περίπτωση, τα πακέτα που στάλθηκαν σε μια διεύθυνση θα μπορούσαν να κλαπούν, ή να επαναπροσανατολιστούν σε κάποιο «ανυποψίαστο» κόμβο. Αυτού του τύπου η επίθεση είναι η ίδια με αυτήν Home agent και των Mobile Node.

Ως εκ τούτου, ο Previous Access Router πρέπει να εξασφαλίσει ότι το FBU έφθασε από τον κόμβο που έχει το συγκεκριμένο PCoA και όχι από κάποιον που έκανε spoof το PCoA του κόμβου που κάνει το handoff. Ο Access Router και οι host του μπορούν να χρησιμοποιήσουν οποιοδήποτε διαθέσιμο μηχανισμό για να καθιερώσουν SA για να εξασφαλίσει πιστοποίηση για τα FBU. Ο γράφων αυτής της διπλωματικής εργασίας προτείνει τη δημιουργία ενός SA από τον Mobile Node προς τον PAR με πρωτόκολλο ασφάλειας AH σε tunnel mode.

Εάν ένας Access Router μπορεί να εξασφαλίσει ότι η διεύθυνση IP σε ένα πακέτο θα μπορούσε να έχει μόνο προέλθει από τον κόμβο του οποίου Link-Στρώμα Address είναι στην cache του γειτονικού router. Ως εκ τούτου ένας spoofed κόμβος δεν μπορεί να χρησιμοποιήσει τη διεύθυνση IP ενός θύματος για τον κακόβουλο επαναπροσανατολισμό της κυκλοφορίας. Μια τέτοια λειτουργία συστήνεται να υπάρχει τουλάχιστον στα neighbor discovery message και στα RtSolPr message.

6.3.2 Secure FBU

Το secure FBU εξασφαλίζει το κακόβουλο επαναπροσανατολισμό FBU. Σε αυτήν την περίπτωση, το FBU εξασφαλίζεται, αλλά ο προορισμός του είναι ένας ανυποψίαστος κόμβος λόγω της κακόβουλης πρόθεσης. Αυτή η ευπάθεια μπορεί να οδηγήσει σε ένα MN με SA με Access Router να επαναπροσανατολίζει την κυκλοφορία σε μια ανακριβή διεύθυνση.

Εντούτοις, ο στόχος του κακόβουλου επαναπροσανατολισμού κυκλοφορίας περιορίζεται σε έναν Access router με τον οποίο έχει ένα SA με τον PAR. Ο PAR πρέπει να ελέγξει ότι το NCoA στο οποίο PCoA δεσμεύεται πραγματικά να ανήκει στο πρόθεμα του NAR. Για να το κάνουν αυτό, HI και HAck ανταλλάσσουνε.

Εντούτοις, δεδομένου ότι NAR το handover state που αντιστοιχεί σε NCoA έχει σύντομη διάρκεια ζωής, άρα η έκταση αυτής της ευπάθειας είναι αμφισβητήσιμα μικρή.

6.3.3 Αποστολή ενός FBU από το NAR

Ένας κακόβουλος MN μπορεί να στείλει ένα FBU από NAR με τη σύνδεση που παρέχει τη διεύθυνση ενός ανυποψίαστου MN ως τη NCoA. Δεδομένου ότι το FBU είναι εμφωλευμένο στο FNA, ο NAR πρέπει να ανιχνεύσει τη σύγκρουση με τη διεύθυνση που είναι κατά την επεξεργασία του FNA και έπειτα να απορρίψει το FBU. Όταν ένας NAR είναι ανίκανος να ανιχνεύσει τις συγκρούσεις διευθύνσεων, είναι ευπαθής στον επαναπροσανατολισμό προς ανυποψίαστους κόμβους.

6.3.4 Denial-of-Service attack

Ομοίως με το Mobile IPv6.

6.3.5 Replay attack

Ομοίως με το Mobile IPv6.

6.3.6 Απειλές σχετικές με τα Binding Updates

Ομοίως με το Mobile IPv6.

6.3.7 Απειλή κατά του confidentiality

Ομοίως με το Mobile IPv6.

6.3.8 Απειλή κατά του integrity

Ομοίως με το Mobile IPv6.

6.4 *Seamless Mobile IPv6 (S-MIP)*

Στο έγγραφο του S-MIP δεν υπάρχουν πληροφορίες σχετικά με το πώς το πρωτόκολλο προστατεύεται από κακόβουλες ενέργειες. Ακόμα δεν είναι φανερό αν μπορεί να εφαρμόσει τις μεθόδους του Mobile IPv6 για να προστατευτεί. Έτσι παίρνουμε σαν δεδομένο ότι είναι εντελώς γυμνό από θέματα ασφάλειας και ότι πρέπει να εφαρμόσουμε την ασφάλεια του IPSec σε κάθε ανταλλαγή πακέτων.

6.4.1 Denial-of-Service attack

Το denial-of-Service είναι να υπερφορτώνουμε ένα συστατικό του δικτύου με άχρηστες πληροφορίες. Για να αντιμετωπιστεί πρέπει να εφαρμοστεί ένα local security policy που να διεξάγει traffic analysis. Ειδικότερα, το οποιοδήποτε συστατικό του δικτύου θα πρέπει να απορρίπτει οποιοδήποτε traffic προέρχεται από κάποιον που δεν είναι πιστοποιημένο. Γι' αυτό χρειάζεται να δημιουργηθεί ένα SA πριν αρχίσει να στέλνεται το traffic προς κάποιο συστατικό του δικτύου. Το SA θα χρησιμοποιεί το AH σε tunnel mode και θα κάνει πιστοποίηση τον κόμβο. Με αυτό τον τρόπο παρεμποδίζεται το να υπερφορτώνουν κακόβουλοι τους πόρους του δικτύου.

6.4.2 Replay attack

Το replay attack αναφέρεται στο να σταλούν σε κάποιο κόμβο παλιά πιστοποιημένα Binding update με σκοπό να κάνει κάποιο κόμβο να στέλνει παλιό traffic προς κάποιον και να τον φορτώνει. Για να αποφευχθεί αυτό πρέπει τα παλιά BU να φυλάσσονται σε μία δομή σύμφωνα με το MAC address του αποστολέα. Έτσι αποφεύγουμε το γεγονός να τα αναπαράγει κάποιος.

6.4.3 Απειλές σχετικές με τα Binding Updates

Εδώ έχουμε να αντιμετωπίσουμε τα πλαστά BU. Θα πρέπει σε κάθε επικοινωνία να εγκαθιδρύσουμε δυο SA για αμφίδρομη πιστοποίηση. Τα SA θα χρησιμοποιούν το AH σε tunnel mode. Ειδικότερα για το S-MIP θα πρέπει σε κάθε handoff ο nAR να πιστοποιεί τον εαυτό του στον oAR με ένα SA θα χρησιμοποίει το AH σε tunnel

mode. Αυτό για να μη μπορεί κάποιος να προσποιηθεί ένα AR του δικτύου για να αρχίσει τη διαδικασία του handoff και να εισάγει τον εαυτό του σε κάποιον άλλον AR. Ένδειξη του ότι κάτι τέτοιο πάει να γίνει. Είναι να λάβει ο αυθεντικός oAR Hack για τα οποία δεν έχει δώσει αυτό HI message.

6.4.4 Απειλή κατά του confidentiality

Εδώ θα πρέπει να επικαλεστούμε τους μηχανισμούς του IPSec που μας παρέχουν τέτοιες ιδιότητες. Θέλουμε να προσδώσουμε end-to-end εμπιστευτικότητα, άρα μια λογική λύση είναι να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP. Το ESP προσφέρει κρυπτογράφηση και πιστοποίηση (ανάλογα με τον αλγόριθμο τον οποίο εχει επιλεγεί).

6.4.5 Απειλή κατά του integrity

Εφόσον έχουμε να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP, για να προσδώσουμε εμπιστευτικότητα, μπορούμε επίσης σε αυτό το SA να χρησιμοποιήσουμε και ένα αλγόριθμο για εξασφάλιση ακεραιότητας.

6.5 *Fast Handover for Hierarchical MIPv6 (F-HMIPv6)*

Οι μέριμνες ασφαλείας του F-HMIPv6 συμφωνούν με εκείνες του FMIPv6 και του HMIPv6. Σημειώνουμε ότι ο MN και ο MAP θα μπορούσαν να έχουν ένα SA του IPSec, κατά συνέπεια τα μηνύματα RtSolPr και PrRtAdv μπορούν επίσης να προστατευθούν με το IPSec. Επιπλέον, ο MAP πρέπει να εξασφαλίσει ότι το RtSolPr και τα πακέτα FBU προέρχονται από ένα MN που έχει πράγματι το RCoA που ισχυρίζεται ότι έχει. Διαφορετικά, ένας κακόβουλος ο κόμβος θα μπορούσε να προσπαθήσει να αναπροσανατολίσει σε κάποιο Access Router.

6.5.1 Denial-of-Service attack

Για να αντιμετωπιστεί πρέπει να εφαρμοστεί ένα local security policy που να διεξάγει traffic analysis. Ειδικότερα το οποιοδήποτε συστατικό του δικτύου θα πρέπει να απορρίπτει οποιοδήποτε traffic προέρχεται από κάποιον που δεν είναι πιστοποιημένο. Γι' αυτό χρειάζεται να δημιουργηθεί ένα SA πριν αρχίσει να στέλνεται το traffic προς κάποιο συστατικό του δικτύου. Το SA θα χρησιμοποιεί το AH σε tunnel mode και θα πιστοποιεί τον κόμβο. Με αυτό τον τρόπο παρεμποδίζεται το να υπερφορτώνουν κακόβουλοι τους πόρους του δικτύου.

6.5.2 Replay attack

Το replay attack αναφέρεται στο να σταλούν σε κάποιο κόμβο παλιά πιστοποιημένα Binding update με σκοπό να κάνει κάποιο κόμβο να στέλνει παλιό traffic προς κάποιον και να τον φορτώνει. Για να αποφευχθεί αυτό πρέπει τα παλιά BU να φυλάσσονται σε μία δομή σύμφωνα με το MAC address του αποστολέα. Έτσι αποφεύγουμε το γεγονός να τα αναπαράγει κάποιος.

6.5.3 Απειλές σχετικές με τα Binding Updates

Το return routability procedure προστατεύει από απειλές που σχετίζονται με τα πλαστά BU εκτός από μια εξαίρεση. Η εξαίρεση αυτή είναι εάν ο επιτιθέμενος είναι σε θέση να κάνει monitoring το μονοπάτι μεταξύ του home agent και του correspondent node.

6.5.4 Απειλή κατά του confidentiality

Ομοίως με το Mobile IPv6.

6.5.5 Απειλή κατά του integrity

Ομοίως με το Mobile IPv6.

6.6 *Flow-based Fast Handover for MIPv6 (FFHMIPv6)*

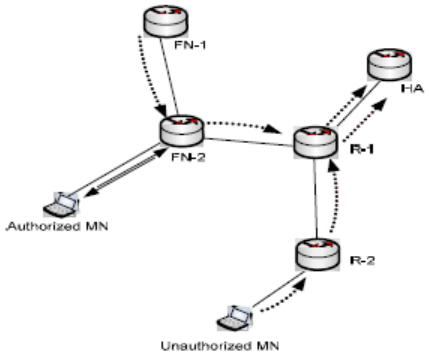
6.6.1 Ευπάθειες που αφορούν το FFHMIPv6

Σενάριο απειλής 1:

Η απειλή ασφάλειας έρχεται κατά τη διάρκεια του FFHBU επειδή το FFHBU προέρχεται από την νέα CoA όχι την παλιά CoA. Το ερώτημα εδώ είναι πώς ο router παραλήπτης προσδιορίζει ότι το μήνυμα FFHBU προέρχεται από το εξουσιοδοτημένο MN.

Αντιμετώπιση

Για να αντιμετωπιστεί αυτή η απειλή πρέπει ο νόμιμος MN να μπορεί να διαπιστωθεί εάν είναι πραγματική πηγή από το FFHBU όταν αλλάζει από την παλιά CoA του στη νέα CoA. Εάν η παράδοση του FFHBU στον HA δεν εξασφαλίζει την ασφάλεια τότε θα μπορούσε να έχει ανεπιθύμητες συνέπειες. Στο σχήμα μετά από ένα handover από ξένο δίκτυο (Foreign Network – FN-1) στο ξένο δίκτυο (FN-2), ο



Σχήμα 6.1 FFHBU flow

εξουσιοδοτημένος MN χρησιμοποιεί τη νέα CoA για να στείλει το FFHBU στον HA μέσω του Router - 1 (R-1). Δεδομένου ότι το FFHMIPv6 δεν διευκρινίζει έναν μηχανισμό όπου τα CR, ο HA και ο CN μπορούν να προσδιορίσουν εάν το FFHBU προέρχεται από εξουσιοδοτημένο MN το αναρμόδιο MN από το router - 2 (R-2) θα μπορούσε επίσης να στείλει το FFHBU στο HA που προσποιείται ότι είναι εξουσιοδοτημένο MN εάν η αληθινή πηγή του FFHBU δεν είναι προσδιορισμένη. Για να αποφευχθούν αυτού του είδους προβλήματα υπάρχουν δύο ενέργειες που το εξουσιοδοτημένο MN πρέπει να κάνει:

1. Υποθέτοντας ότι στους δρομολογητές εξασφαλίζεται καλά η ασφάλεια, κάθε εξουσιοδοτημένος MN πρέπει να κρατήσει σύνδεση με την παλιά CoA του και να πάρει ένα κρυπτογραφημένο μήνυμα από την κατεύθυνση της ροής του από τον τελευταίο προωθητή δρομολογητή (FN-1). Οι πληροφορίες για την παλιά CoA απαιτούνται από τη νέα CoA και κατά μήκος της ροής πληροφορίας κατά την αποστολή του FFHBU στον HA. Στο σχήμα, ο εξουσιοδοτημένος MN και ο αναρμόδιος MN έχουν διαφορετική παλιά και νέα CoA όπως και ροή πληροφορίας, επομένως οι δρομολογητές, ο CR και ο HA θα είναι σε θέση να προσδιορίσουν την αληθινή πηγή του FFHBU. Ο router - 1 (R-1) υποτίθεται ότι έχει flow state πληροφορίες που αποθηκεύονται στην cache μνήμη του. Στην λήψη ενός πακέτου FFHBU στον HA του MN ή στον CN του MN, πρέπει να ελεγχθεί η νέα CoA και η παλιά CoA μαζί με την κατεύθυνση ροής του εξουσιοδοτημένου MN ενάντια στην flow state πληροφορία του για να ελέγξει εάν είναι οι ίδιες πριν διαβιβαστεί το πακέτο στον επόμενο CR, που θα το οδηγήσει τελικά στον HA. Εάν είναι ψεύτικο απλώς κάνει drop το FFHBU.

2. Η δεύτερη ενέργεια που πρέπει να κάνει ο εξουσιοδοτημένος MN είναι να αποδείξει την ταυτότητά του στον HA σε περιπτώσεις που παραβιάζεται η ασφάλεια στους router. Αυτό μπορεί να γίνει για παράδειγμα εάν ο πρώτος router είναι σε θέση να αποδείξει την πηγή του FFHBU ότι είναι από τον εξουσιοδοτημένο MN με την πιο πάνω μέθοδο και να διαβιβάσει το FFHBU στον επόμενο router. Ο δεύτερος δρομολογητής όμως, δέχεται επίθεση προωθώντας ένα τροποποιημένο FFHBU στον HA. Κάτω από τέτοιες καταστάσεις ο HA πρέπει να είναι σε θέση να ξέρει εάν το FFHBU προέρχεται από τον κακόβουλο MN ή είναι τροποποιημένο. Ένας τρόπος να αποφευχθεί αυτή η απειλή ασφαλείας είναι ο MN να στείλει τον encrypted identification κώδικα του μαζί με το FFHBU στον HA του, τον οποίο αποκρυπτογραφείται μόνο από τον HA και ότι ο HA μπορεί να το επικυρώσει. Το λανθασμένο FFHBU δεν επικυρώνεται ως εκ τούτου αποβάλλεται από τον HA. Δεδομένου ότι όλοι οι MN είναι εξουσιοδοτημένοι χρήστες του εγχώριου δικτύου, είναι κάθε ένας προσδιορισμένος με τη MAC/Physical διεύθυνση του ή το λογαριασμό σύνδεσης χρήστη (user login accounts) στα αντίστοιχά τους

δίκτυα. Ένας κώδικας identification από αυτές τις πληροφορίες θα μπορούσε να παραχθεί, από έναν server, για κάθε συσκευή ή χρήστη στο δίκτυο.

Σενάριο απειλής 2:

Στο FFHMIPv6, ο δρομολογητής διαδραματίζει τους ρόλους διατήρησης των states, τον κατευθυντή του traffic στη παλιά CoA και στη νέα CoA, και διαμορφώνει τελικά ένα IPv6 tunnel προκειμένου να κατευθυνθεί η κυκλοφοριακή ροή στη νέα CoA. Επομένως, σε ένα περιβάλλον δικτύου με πολυάσχολους και πολλαπλάσιους MN, ένας ενιαίος δρομολογητής πρέπει να διατηρήσει πολλές flow-state πληροφορίες με διαφορετικές ετικέτες ροής. Κάτω από αυτό τον τύπο κατάστασης εάν το προαναφερόμενο FFHMIPv6 οι παράμετροι δρομολόγησης δεν προστατεύονται αρκετά. Ο επιτιθέμενος μπορεί να προσπαθήσει να πειράξει με τις state πληροφορίες και τις κατευθύνσεις κυκλοφοριακής ροής που είναι αποθηκευμένες στην cache μνήμη του δρομολογητή. Επίσης ο επιτιθέμενος μπορεί να προσπαθήσει να αλλάξει την παλιά CoA έτσι ώστε το FFHBU να μην είναι σωστό. Αυτό θα μπορούσε να επιφέρει ως αποτέλεσμα denial-of-service attack. Με την αλλαγή του flow label ή του τύπου του identifier του FFHMIPv6, ο επιτιθέμενος μπορεί να διακόψει την επικοινωνία (denial-of-service attack).

Αντιμετώπιση

Προβλήματα ασφαλείας που αναφέρονται από την $2_η$ περίπτωση υποθέτουμε ότι η επικοινωνία μεταξύ του MN και του HA δεν είναι ασφαλισμένη για λόγους εκτός της αρμοδιότητας του FFHMIPv6. Βασικά, αυτό είναι μια ανησυχία της ασφάλειας των router. Κάτω από αυτές τις περιστάσεις, οι ιδέες που αναφέρθηκαν στην $1_η$ περίπτωση θα μπορούσαν μόνο να δώσουν μια μερική λύση στο πρόβλημα επειδή είναι επιτυχείς μόνο εάν ο λαμβάνων router (R-1) είναι ασφαλισμένος. Εάν ο επιτιθέμενος έχει πρόσβαση στο router, τότε μπορεί να αλλάξει την flow state information cache του router συμπεριλαμβανομένου της παλιάς CoA. Με αυτόν τον τρόπο γίνεται ο μηχανισμός άχρηστος. Εδώ, ο επιτιθέμενος θα μπορούσε να έχει δύο διαφορετικά αποτελέσματα, είτε να τροποποιήσει τις πληροφορίες στην cache του router μαζί με αυτή στέλνεται από τον εξουσιοδοτημένο MN έτσι ώστε να μπορεί να κάνει denial-of-service σε εξουσιοδοτημένο MN ή να τις ταιριάξει αυτές του αναρμόδιου MN, έτσι ο επιτιθέμενος μπορεί να νομιμοποιήσει τα FFHBU και να τα χρησιμοποιήσει για τον σκοπό του. Επομένως το FFHMIPv6 πρέπει να εφαρμόσει δικό του

μηχανισμό ασφάλειας ως δεύτερο επίπεδο άμυνας στην περίπτωση των router ή της παραβίασης ασφάλειας δικτύων, έτσι ώστε να μην χρησιμοποιείται ως spring board ή για άλλο είδος επιθέσεων. Ως εκ τούτου το κομμάτι της λύση πρέπει να αποτελεί ο εξουσιοδοτημένος MN όπως αναφέρθηκε στη 1η λύση.

Σενάριο απειλής 3:

Στο FFHMIPv6 προτείνεται το FFHBU να στέλνεται μόνο στον HA χωρίς να είναι αναγκαίο να στέσλνεται στον CN. Αυτή η τροποποίηση της λειτουργίας του FFHMIPv6 πήρε την υπόθεση ότι το FFHMIPv6 δεν κινδυνεύει από τις απειλές ασφάλειας που αναφέρθηκαν πιο πάνω (περίπτωση 1 και 2). Στο αρχικό FFHMIPv6, στέλνοντας FFHBU και στους δύο (HA και CN) ξεχωριστά υπάρχει το πλεονέκτημα ότι μόλις το FFHBU ολοκληρωθεί, η επικοινωνία μεταξύ MN και CN μπορεί να συνεχιστεί ακόμα κι αν οι συνδέσεις μεταξύ MN και HA ή MN και CN είναι συμβιβασμένες. Όμως, στέλνοντας το FFHBU από τον MN στον CN μέσο του HA θα ενεργούσε ως καθυστέρηση ή βάζοντας σε κίνδυνο την επικοινωνία μεταξύ του MN και του CN εάν οι συνδέσεις μεταξύ του MN και του HA ή του HA και του CN είναι συμβιβασμένες.

Αντιμετώπιση

Η απειλή ασφάλειας που προσδιορίζεται στην 3η περίπτωση προκύπτει επειδή η αρχική ιδέα του FFHBU έχει αλλάξει. Στην ανανεωμένη δοκιμή αξιολόγησης απόδοσης, μόνο ένα FFHBU στέλνεται για τον HA και για τον CN και για τον HA. Αυτή η τροποποίηση του FFHBU στην αρχική λειτουργία του FFHMIPv6 έγινε χωρίς εξέταση των απειλών ασφάλειας του FFHMIPv6 που προσδιορίσαμε στην 1η και 2η περίπτωση. Εάν οι ιδέες που αναφέρθηκαν στις πιο πάνω λύσεις είναι υλοποιημένες και στην σύνδεση του MN με τον HA και στην σύνδεση του HA με τον CN δεν θα υπάρχει κανένα πρόβλημα. Εάν όμως η σύνδεση του MN με τον HA είναι ασφαλισμένη ενώ του HA με τον CN δεν είναι ή η σύνδεση του MN με τον HA δεν είναι ασφαλισμένη ενώ η σύνδεση του HA με τον CN είναι ασφαλής, τότε θα στείλει το FFHBU και στον CN και στον HA και έτσι είναι ο καλύτερος τρόπος να κρατήσει ασφαλείς τις επικοινωνίες και να αποφευχθεί η απειλή ασφάλειας που αναφέρεται στην 3η περίπτωση. Αυτή η ιδέα φαίνεται στο πιο κάτω σχήμα.

6.6.2 Denial-of-Service attack

Για να αντιμετωπιστεί πρέπει να εφαρμοστεί ένα local security policy που να διεξάγει traffic analysis. Ειδικότερα το οποιοδήποτε συστατικό του δικτύου θα πρέπει να απορρίπτει οπουδήποτε traffic προέρχεται από κάποιον που δεν είναι πιστοποιημένο. Για αυτό χρειάζεται να δημιουργηθεί ένα SA πριν αρχίσει να στέλνεται το traffic προς κάποιο συστατικό του δικτύου. Το SA θα χρησιμοποιεί το AH σε tunnel mode και θα κάνει πιστοποιεί τον κόμβο. Με αυτό τον τρόπο παρεμποδίζεται το να υπερφορτώνουν κακόβουλοι τους πόρους του δικτύου.
Ακόμα πρέπει να ληφθούν υπόψη σχετικά σημεία της παραγράφου 6.6.1.

6.6.3 Replay attack

Το replay attack αναφέρεται στο να σταλούν σε κάποιο κόμβο παλιά πιστοποιημένα Binding update με σκοπό να κάνει κάποιο κόμβο να στέλνει παλιό traffic προς κάποιον και να τον φορτώνει. Για να αποφευχθεί αυτό πρέπει τα παλιά BU να φυλάσσονται σε μία δομή σύμφωνα με το MAC address του αποστολέα. Έτσι αποφεύγουμε το γεγονός να τα αναπαράγει κάποιος.

6.6.4 Απειλή κατά του confidentiality

Εδώ θα πρέπει να επικαλεστούμε τους μηχανισμούς του IPSec που μας παρέχουν τέτοιες ιδιότητες. Θέλουμε να προσδώσουμε end-to-end εμπιστευτικότητα, άρα μια λογική λύση είναι να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP. Το ESP προσφέρει κρυπτογράφηση και πιστοποίηση (ανάλογα με τον αλγόριθμο τον οποίο έχει επιλεγεί).

6.6.5 Απειλή κατά του integrity

Εφόσον έχουμε να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP, για να προσδώσουμε εμπιστευτικότητα, μπορούμε επίσης σε αυτό το SA να χρησιμοποιήσουμε και ένα αλγόριθμο για εξασφάλιση της ακεραιότητας.

6.7 *Terminal Independent Mobility for IPv6 TIMIP*

Για το TIMIP δε γίνεται καμία αναφορά στο έγγραφο για το θέμα του security. Με τη δομή που έχει το TIMIP δείχνει ότι η πληροφορία παίρνει από πολλούς router μέχρι να φτάσει στον Access Network Gateway. Αν και η σύνδεση μεταξύ των router στη πυραμίδα γίνεται ενσύρματα, καλό θα ήταν στην μεταξύ τους επικοινωνία να εγκαθιδρυθούν αμφίδρομα SA σε tunnel mode ασφάλεια ESP που να παρέχει και πιστοποίηση.

6.7.1 Denial-of-Service attack

Για να αντιμετωπιστεί το Denial-of-Service πρέπει να εφαρμοστεί ένα local security policy στους AP που να διεξάγει traffic analysis. Ειδικότερα το οποιοδήποτε συστατικό του δικτύου θα πρέπει να απορρίπτει οπουδήποτε traffic προέρχεται από κάποιον που δεν είναι πιστοποιημένο. Γι' αυτό χρειάζεται να δημιουργηθεί ένα SA πριν αρχίσει να στέλνεται το traffic προς κάποιον AP του δικτύου. Το SA θα χρησιμοποιεί το AH σε tunnel mode και θα κάνει πιστοποίηση στον κόμβο. Με αυτό τον τρόπο παρεμποδίζεται το να υπερφορτώνουν κακόβουλοι τους πόρους του δικτύου.

Ειδικότερα για το TIMIP θα πρέπει το traffic analysis να είναι εκτενές και αν χρειαστεί να δράσει, αυτό να γίνεται άμεσα. Διότι όσο πιο πάνω είναι στη πυραμίδα ένας router τόσο πιο πολύ φόρτο έχει να διαχειριστεί, άρα μπορεί να κατακλειστεί από φόρτο εργασίας πιο σύντομα απο ότι από σε ένα άλλο δίκτυο.

6.7.2 Replay attack

Για να αποφευχθεί το Replay attack πρέπει τα παλιά BU να φυλάσσονται σε μία δομή σύμφωνα με το MAC address του αποστολέα. Έτσι αποφεύγουμε το γεγονός να τα αναπαράγει κάποιος.

6.7.3 Απειλές σχετικές με τα Binding Updates

Το πρωτόκολλο πρέπει να είναι σε θέση να ξεχωρίσει τα πλαστά BU. Κάθε φορά όπου ο MN κάνει handoff ή γίνεται initialize σε ένα δίκτυο πρέπει να κάνει

6.7.4 Απειλή κατά του confidentiality

Εδώ θα πρέπει να επικαλεστούμε τους μηχανισμούς του IPSec που μας παρέχουν τέτοιες ιδιότητες. Θέλουμε να προσδώσουμε end-to-end εμπιστευτικότητα, άρα μια λογική λύση είναι να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP. Το ESP προσφέρει κρυπτογράφηση και πιστοποίηση (ανάλογα με τον αλγόριθμο τον οποίο εχει επιλεγεί).

6.7.5 Απειλή κατά του integrity

Εφόσον έχουμε να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP, για να προσδώσουμε εμπιστευτικότητα, μπορούμε επίσης σε αυτό το SA να χρησιμοποιήσουμε και ένα αλγόριθμο για εξασφάλιση του integrity.

6.8 *Enhanced TIMIP*

Το πρωτόκολλο αυτό έχει την ιδιαιτερότητα να δουλεύει σε δύο στρώμα. Το physical και το overlay που είναι ένα λογικό επίπεδο. Μέσα στο eTIMIP διακινούνται επιπλέον πληροφορίες σχετικές με το routing από τους TIMIP Router. Αν και η σύνδεση μεταξύ των router γίνεται ενσύρματα, καλό θα ήταν στη μεταξύ τους επικοινωνία να εγκαθιδρυθούν αμφίδρομα SA σε tunnel mode ασφάλεια ESP που να παρέχει και πιστοποίηση.

6.8.1 Denial-of-Service attack

Για να αντιμετωπιστεί το Denial-of-Service πρέπει να εφαρμοστεί ένα local security policy που να διεξάγει traffic analysis. Ειδικότερα το οποιοδήποτε συστατικό του

6.8.2 Replay attack

Για να αποφευχθεί το Replay attack πρέπει τα παλιά BU να φυλάσσονται σε μία δομή σύμφωνα με το MAC address του αποστολέα. Έτσι αποφεύγουμε το γεγονός να τα αναπαράγει κάποιος.

6.8.3 Απειλές σχετικές με τα Binding Updates

Το πρωτόκολλο πρέπει να είναι σε θέση να ξεχωρίσει τα πλαστά BU. Κάθε φορά όπου ο MN κάνει handoff ή γίνεται initialize σε ένα δίκτυο πρέπει να κάνει πιστοποιεί τον εαυτό του στον HA και στον CN. Γι' αυτό το λόγο πρέπει να εγκατασταθεί ένα SA σε tunnel mode με το ESP από τον host στον AH, και από τον HA στον CN. Μέσω του παραπάνω SA διασφαλίζεται ότι αυτός που στέλνει το BU είναι αυτός που ισχυρίζεται ότι είναι.

6.8.4 Απειλή κατά του confidentiality

Εδώ θα πρέπει να επικαλεστούμε τους μηχανισμούς του IPSec που μας παρέχουν τέτοιες ιδιότητες. Θέλουμε να προσδώσουμε end-to-end εμπιστευτικότητα, άρα μια λογική λύση είναι να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP. Το ESP προσφέρει κρυπτογράφηση και πιστοποίηση (ανάλογα με τον αλγόριθμο τον οποίο εχει επιλεγεί).

6.8.5 Απειλή κατά του integrity

Εφόσον έχουμε να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP, για να προσδώσουμε εμπιστευτικότητα, μπορούμε επίσης σε αυτό το SA να χρησιμοποιήσουμε και ένα αλγόριθμο για εξασφάλιση της ακεραιότητας.

6.9 *SIGMA*

Το SIGMA είναι ένα πρωτόκολλο το όποιο φιλοδοξεί να μειώσει το latency του handoff. Αλλάζει αρκετές έννοιες σε σχέση με τα υπόλοιπα πρωτόκολλα. Δίνει περισσότερες αρμοδιότητες στον DNS – Location Manager. Ουσιαστικά καταργεί το ρόλο του Home agent και τη θέση αυτού παίρνει ο DNS που γνωρίζει που βρίσκεται ο κάθε MN μέσα στο δίκτυο. Τα BU γίνονται πλέον απευθείας στο CN και αφότου έχει μπει στην ακτίνα του νέου AR τότε πλέον ενημερώνει τον Location Manager. Έχοντας μαζέψει όλες τις αρμοδιότητες του HA στον Location Manager, γίνεται αυτόματα και το single point of failure του δικτύου. Πράγμα που σημαίνει ότι αν χάσουμε για κάποιο λόγο τον Location Manager, το δίκτυο θα νεκρώσει. Άρα ίσως να χρειαζόμαστε επιπλέον προστασία για τον Location Manager.

Ακόμα εάν κάποιος αποκτήσει πρόσβαση στον Location Manager τότε όλοι οι MN του δικτύου γίνονται αυτόματα ευπαθείς σε ένα ειδικό τύπο επίθεσης, του steel address of stationary node,ή επιπλέον ο κακόβουλος να πειράξει τις εγγραφές του. Με αυτό τον τρόπο θα μπορούσε να παραπλανήσει τον CN. Λύση σε αυτή την επίθεση είναι ο DNS να έχει ένα πεδίο για κάθε εγγραφή ώστε να μπορεί να ελέγχει ακεραιότητα, και ακόμα να κρυπτογραφεί τα δεδομένα του.

6.9.1 Denial-of-Service attack

Για να αντιμετωπιστεί το Denial-of-Service πρέπει να εφαρμοστεί ένα local security policy που να διεξάγει traffic analysis. Ειδικότερα το οποιοδήποτε συστατικό του δικτύου θα πρέπει να απορρίπτει οπουδήποτε traffic προέρχεται από κάποιον που δεν είναι πιστοποιημένο. Γι’ αυτό χρειάζεται να δημιουργηθεί ένα SA πριν αρχίσει να στέλνεται το traffic προς κάποιον AP του δικτύου. Το SA θα χρησιμοποιεί το AH σε

tunnel mode και θα πιστοποιεί τον κόμβο. Με αυτό τον τρόπο παρεμποδίζεται τον να υπερφορτώνουν κακόβουλοι τους πόρους του δικτύου.

Ειδικότερα για τον Location Manager θα πρέπει να εξετάσουμε ξεχωριστά την επίθεση του flooding που έχει σαν αποτέλεσμα της το denial-of-service. Έαν κάποιος κακόβουλος καλέσει ένα μεγάλο stream πληροφορίας προς τον DNS τότε η πληροφορία θα κατακλείσει τους πόρους του. Η απάντηση σε αυτήν την επίθεση είναι ότι η επικοινωνία με τον DNS πρέπει να γίνεται μέσω firewall το οποίο θα ελέγχει την income πληροφορία από κάθε πηγή. Εάν το income ξεπεράσει κάποιο όριο τότε το firewall θα κάνει drop τη ροή αυτή.

6.9.2 Replay attack

Για να αποφευχθεί το Replay attack πρέπει τα παλιά BU να φυλάσσονται σε μία δομή σύμφωνα με το MAC address του αποστολέα. Έτσι, αποφεύγουμε το γεγονός να τα αναπαράγει κάποιος.

6.9.3 Απειλές σχετικές με τα Binding Updates

Το πρωτόκολλο πρέπει να είναι σε θέση να ξεχωρίσει τα πλαστά BU. Κάθε φορά όπου ο MN κάνει handoff ή γίνεται initialize σε ένα δίκτυο πρέπει να κάνει πιστοποιεί τον εαυτό του στον CN. Για αυτό το λόγο πρέπει να εγκατασταθεί ένα SA σε tunnel mode με το ESP από τον host στον CN. Μέσω του παραπάνω SA διασφαλίζεται ότι αυτός που στέλνει το BU είναι αυτός που ισχυρίζεται ότι είναι.

Σε αυτό το πρωτόκολλο συναντάμε το “zero receiver window”. Με αυτό τον τρόπο το πρωτόκολλο αυτό όταν ένας MN αφήνει την εμβέλεια ενός subnet στέλνει αυτό το μήνυμα για να μη δέχεται πακέτα σε αυτό το subnet. Δηλαδή ο MN κάνει reserve αυτή την IP για να είναι άμεσα έτοιμος να τη χρησιμοποιήσει με συνοπτικές διαδικασίες όταν έρθει ξανά στο subnet. Εύκολα μπορεί κάνεις να καταλάβει την απειλή που μπορεί να πραγματοποιηθεί από αυτή την ενέργεια. Για να γίνει λοιπόν αυτή η λειτουργία με ασφάλεια πρέπει να προηγείται πιστοποίηση του MN όταν στέλνει μήνυμα να ανοίξει ξανά το window. Η τακτική της προηγούμενης

παραγράφου μας εξασφαλίζει ότι αυτό δε θα είναι εφικτό αφού υπάρχει διαρκές πιστοποίηση.

6.9.4 Απειλή κατά του confidentiality

Εδώ θα πρέπει να επικαλεστούμε τους μηχανισμούς του IPSec που μας παρέχουν τέτοιες ιδιότητες. Θέλουμε να προσδώσουμε end-to-end εμπιστευτικότητα, άρα μια λογική λύση είναι να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP. Το ESP προσφέρει κρυπτογράφηση και πιστοποίηση (ανάλογα με τον αλγόριθμο τον οποίο εχει επιλεγεί).

6.9.5 Απειλή κατά του integrity

Εφόσον έχουμε εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP, για να προσδώσουμε εμπιστευτικότητα, μπορούμε επίσης σε αυτό το SA να χρησιμοποιήσουμε και ένα αλγόριθμο για εξασφάλιση της ακεραιότητας.

6.10 *P-SIGMA*

Το P-SIGMA είναι ένα πρωτόκολλο το όποιο φιλοδοξεί να μειώσει και αυτό το latency του handoff. Μία νέα έννοια εμφανίζεται, το paging gate way το οποίο όμως δεν εμπνέει ιδιαίτερη ανησυχία αφού η ασφάλεια του καλύπτεται από τα πιστοποιημένα συστήματα.

Το θέμα του Location Manager καλύφθηκε από το SIGMA στο ίδιο κεφάλαιο.

6.10.1 Denial-of-Service attack

Ομοίως με το SIGMA στο ίδιο κεφάλαιο.

6.10.2 Replay attack

Για να αποφευχθεί το Replay attack πρέπει τα παλιά BU να φυλάσσονται σε μία δομή σύμφωνα με το MAC address του αποστολέα. Έτσι αποφεύγουμε το γεγονός να τα αναπαράγει κάποιος.

6.10.3 Απειλές σχετικές με τα Binding Updates

Ομοίως με το SIGMA στο ίδιο κεφάλαιο. Με εξαίρεση του ότι δεν έχει αναφερθεί τίποτα για το "zero receive window" και ακόμα το SA σε tunnel mode με το ESP από τον host στον CN και στον PGW.

6.10.4 Απειλή κατά του confidentiality

Εδώ θα πρέπει να επικαλεστούμε τους μηχανισμούς του IPSec που μας παρέχουν τέτοιες ιδιότητες. Θέλουμε να προσδώσουμε end-to-end εμπιστευτικότητα, άρα μια λογική λύση είναι να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP. Το ESP προσφέρει κρυπτογράφηση και πιστοποίηση (ανάλογα με τον αλγόριθμο τον οποίο εχει επιλεγεί).

6.10.5 Απειλή κατά του integrity

Εφόσον έχουμε να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP, για να προσδώσουμε εμπιστευτικότητα, μπορούμε επίσης σε αυτό το SA να χρησιμοποιήσουμε και ένα αλγόριθμο για εξασφάλιση της ακεραιότητας.

6.11 *Mobile IP Fast Authentication MIFA*

Το MIFA εισάγει μια νέα έννοια, το L3-FHR το οποίο είναι ένα σύνολο από γειτονικούς FA. Το σύνολο αυτό από FA έχει την ιδιότητα να μπορεί να πιστοποιεί τους MN στο επίπεδο των AR. Όταν οι MN κινούνται σε αυτό το σύνολο δε χρειάζεται να πιστοποιείται στο HA. Έχει προβλεφτεί από το σχεδιαστή τα FA στο να έχουν SA, το οποίο δε διευκρινίζει. Το SA κατά την άποψη μου είναι λογικό να είναι

SA σε transport mode και θα χρησιμοποιούν το ESP, το οποίο θα κρυπτογραφεί τα μηνύματα για περισσότερη ασφάλεια.

6.11.1 Denial-of-Service attack

Για να αντιμετωπιστεί το Denial-of-Service πρέπει να εφαρμοστεί ένα local security policy που να διεξάγει traffic analysis. Ειδικότερα το οποιοδήποτε συστατικό του δικτύου θα πρέπει να απορρίπτει οποιοδήποτε traffic προέρχεται από κάποιον που δεν είναι πιστοποιημένο. Για αυτό χρειάζεται να δημιουργηθεί ένα SA πριν αρχίσει να στέλνεται το traffic προς κάποιον AP του δικτύου. Το SA θα χρησιμοποιεί το AH σε tunnel mode και θα πιστοποιεί τον κόμβο. Με αυτό τον τρόπο παρεμποδίζεται τον να υπερφορτώνουν κακόβουλοι τους πόρους του δικτύου.

6.11.2 Replay attack

Για να αποφευχθεί το Replay attack πρέπει τα παλιά BU να φυλάσσονται σε μία δομή σύμφωνα με το MAC address του αποστολέα. Έτσι αποφεύγουμε το γεγονός να τα αναπαράγει κάποιος.

6.11.3 Απειλές σχετικές με τα Binding Updates

Το πρωτόκολλο πρέπει να είναι σε θέση να ξεχωρίσει τα πλαστά BU. Κάθε φορά όπου ο MN κάνει handoff ή γίνεται initialize σε ένα δίκτυο πρέπει να κάνει πιστοποιεί τον εαυτό του στον HA και στον CN. Για αυτό το λόγο πρέπει να εγκατασταθεί ένα SA σε tunnel mode με το ESP από τον host στον AH και από τον HA στον CN. Μέσω του παραπάνω SA διασφαλίζεται ότι αυτός που στέλνει το BU είναι αυτός που ισχυρίζεται ότι είναι.

6.11.4 Απειλή κατά του confidentiality

Εδώ θα πρέπει να επικαλεστούμε τους μηχανισμούς του IPSec που μας παρέχουν τέτοιες ιδιότητες. Θέλουμε να προσδώσουμε end-to-end εμπιστευτικότητα, άρα μια λογική λύση είναι να εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP. Το ESP προσφέρει

κρυπτογράφηση και πιστοποίηση (ανάλογα με τον αλγόριθμο τον οποίο εχει επιλεγεί).

6.11.5 Απειλή κατά του integrity

Εφόσον έχουμε εγκαθιδρύσουμε δύο SA για αμφίδρομη επικοινωνία μεταξύ των host τα οποία σε transport mode θα χρησιμοποιούν το ESP, για να προσδώσουμε εμπιστευτικότητα, μπορούμε επίσης σε αυτό το SA να χρησιμοποιήσουμε και ένα αλγόριθμο για εξασφάλιση της ακεραιότητας.

7. Συμπεράσματα

Τα πρωτόκολλα τα οποία εξετάσαμε και αναλύσαμε σε αυτή τη διπλωματική είναι το Mobile IPv6 και άλλα τα οποία βασίζονται σε αυτό. Αυτά τα πρωτόκολλα έχουν ως στόχο τη βελτίωση της ποιότητας υπηρεσίας που προσφέρει το MIPv6. Ορισμένα από αυτά έχουν φτάσει σε επίπεδο του IETF και μεριμνούν για θέματα ασφαλείας, αν και δεν τα λύνουν εντελώς. Σαν μια λύση για να ρυθμιστεί το θέμα της ασφάλειας όπου υπάρχει προτείναμε το γνωστό IPSec. Το IPSec είναι το πρωτόκολλο το οποίο μας παρέχει όλα τα εργαλεία για να προσδώσουμε σε ένα πρωτόκολλο κρυπτογραφία, πιστοποίηση και ακεραιότητα.

Γεγονός είναι ότι οι μετρήσεις στα πρωτόκολλα για θέματα επίδοσης γίνονται χωρίς τη χρήση κάποιου μέτρου ασφαλείας, κάτι που σαφώς θα είχε αρνητικές έως και καταστροφικές επιπτώσεις στην απόδοση του πρωτόκολλου. Δε χρειάζεται ο μέγιστος βαθμός ασφάλειας σε όλα τα δίκτυα αλλά αν μια πρόταση ενός πρωτοκόλλου δουλεύει και πραγματοποιεί αυτό που υπόσχεται μονό υπό συνθήκες όπου η ασφάλεια απουσιάζει, καταλαβαίνουμε ότι αυτό το πρωτόκολλο δε είναι πρακτικό. Άρα δεν έχει και ελπίδες να αναπτυχτεί περεταίρω. Δεν είναι ανύπαρκτες οι εφαρμογές σήμερα που απαιτούν QoS, ασφάλεια και εκτελούνται εν κινήσει. Μπορούμε εύκολα να υποστηρίξουμε ότι όσο περνάει ο καιρός αυτές οι εφαρμογές να πληθαίνουν.

Τι θα ήταν αυτό που θα μας έδινε και QoS και επιδόσεις στους κινητούς κόμβους;

Θα ήταν καλό λοιπόν, να αναπτυχθούν οι μέριμνες για ασφάλεια έως και υψηλού βαθμού για το πρωτόκολλο μέσα στο κώδικα του πρωτοκόλλου και να γίνουν optimize για το πρωτόκολλο αυτό. Φυσικά θα πρέπει να μπορεί να γίνει και παραμετροποίηση του πρωτοκόλλου για το τι βαθμού ασφάλεια θα εφαρμόζει σε κάθε υλοποίηση του, διότι όπως προαναφέραμε δεν έχουν όλα τα δίκτυα τις ίδιες ανάγκες στην ασφάλεια. Πράγμα το οποίο θα έχει αρνητικές επιπτώσεις στη πολυπλοκότητα του.

Δεύτερον και πολύ ουτοπικό είναι να υπάρχει ένας επιπλέον επεξεργαστής σε κάθε συστατικό του δικτύου, ο οποίος θα είναι ειδικός για πράξεις που χρειάζονται για να

πετύχουμε ασφάλεια σε ένα πρωτόκολλο. Έτσι θα ήταν εφικτό να γίνει παραλληλοποίηση των διεργασιών ενός πρωτοκόλλου, να μη σπαταλιέται χρόνος στο να γίνουν αυτές οι πράξεις από τον επεξεργαστή και να γίνονται on-the-fly. Είναι μια λύση η οποία όπως καταλαβαίνουμε αυξάνει δραματικά και την πολυπλοκότητα αλλά και το κόστος. Όταν αυτός ο επεξεργαστής θα είναι σε idle κατάσταση θα μπορούσε να υποβοηθά και σε πράξεις που σχετίζονται πάλι με τη κινητικότητα του συγκεκριμένου συστατικού του δικτύου.

Ποια πράγματα πρέπει να προσέξουμε σε ένα πρωτόκολλο και ποια χαρακτηριστικά πρέπει να έχει ώστε να είναι ασφαλές;

Το πρώτο είναι αυτό που υιοθετεί το Mobile IPv6, return routability. Είναι ένας μηχανισμός όπου ο MN πιστοποιεί ότι είναι αυτός που ισχυρίζεται ότι είναι. Είναι ένας μηχανισμός που εκτελείται όποτε τον καλέσει κάποιος να εκτελεστεί, δηλαδή μπορεί να εκτελεστεί είτε για προληπτικούς λόγους, είτε όταν υπάρχουν υπόνοιες για κακόβουλο κόμβο.

Ένα άλλο είναι η διαδικασία του traffic analysis. Πρέπει να είναι συνεχής αυτή η διαδικασία και να υπάρχει σε οποιοδήποτε πρωτόκολλο. Ύποπτα πακέτα πρέπει να απορρίπτονται. Το traffic analysis πρέπει να το εκτελεί κάθε συστατικό του δικτύου.

8. Σύνοψη αποτελεσμάτων

	MN address stealing	Stationary address stealing	Future stealing address	Man in the middle	Denial of service	Replay binding updates	flooding	Return to home flooding	Unnecessary binding updates	Reflection attack
MIPv6	Return routability	Return routability	Return routability	SA με ESP	Traffic Analysis, Return routability	Αποθηκ-ευση των BU με MAC	Local policy	Local policy	Local policy	Local policy
HMIPv6	Return routability	Return routability	Return routability	SA με ESP	Traffic Analysis, Return routability	Αποθηκ-ευση των BU με MAC	Local policy	Local policy	Local policy	Local policy
FMIP	Return routability	Return routability	Return routability	SA με ESP	Traffic Analysis, Return routability	Αποθηκ-ευση των BU με MAC	Local policy	Local policy	Local policy	Local policy
S-MIP	SA με AH	SA με AH	SA με AH	SA με ESP	Traffic Analysis, SA με AH	Αποθηκ-ευση των BU με MAC	Local policy	Local policy	Local policy	Local policy
FHMIPv6	Return routability	Return routability	Return routability	SA με ESP	Traffic Analysis, SA με AH	Αποθηκ-ευση των BU με MAC	Local policy	Local policy	Local policy	Local policy
FFHMIPv6	V	V	V	SA με ESP	Traffic Analysis, SA με AH	Αποθηκ-ευση των BU με MAC	Local policy	Local policy	Local policy	Local policy
TIMIP	SA με ESP	SA με ESP	SA με ESP	SA με ESP	Traffic Analysis, SA με AH	Αποθηκ-ευση των BU με MAC	Local policy	Local policy	Local policy	Local policy
eTIMIP	SA με ESP	SA με ESP	SA με ESP	SA με ESP	Traffic Analysis, SA με AH	Αποθηκ-ευση των BU με MAC	Local policy	Local policy	Local policy	Local policy

SIGMA	SA με ESP	SA με ESP	SA με ESP	SA με ESP	Traffic Analysis, SA με AH	Αποθηκ-ευση των BU με MAC	Local policy	Local policy	Local policy	Local policy
P-SIGMA	SA με ESP	SA με ESP	SA με ESP	SA με ESP	Traffic Analysis, SA με AH	Αποθηκ-ευση των BU με MAC	Local policy	Local policy	Local policy	Local policy
MIFA	SA με ESP	SA με ESP	SA με ESP	SA με ESP	Traffic Analysis, SA με AH	Αποθηκ-ευση των BU με MAC	Local policy	Local policy	Local policy	Local policy

9. Ακρωνύμια

AH Authentication Header

AP Access Point

BA Binding Acknowledgments

BS Base Station

BU Binding Update

CN Correspondent Node

CoA Care of Address

DAD Duplicate Address Detection

DHCP Dynamic Host Configuration Protocol

ESP EncAPulating Secure Payload

F-HMIPv6 Fast Hierarchical MIPv6

FA Foreign Agent

FBack Fast Binding Acknowledgement

FBU Fast Binding Update

FFHMIPv6 Flow-based Fast Handover for MIPv6

FNA Fast Neighbor Advertisement

GSM Global System for Mobile communications

HA Home Agent

HACK Handoff Acknowledgment

HI Handoff Initiate

HMIPv6 Hierarchical Mobile IPv6

HA Home Address

ICMP Internet Control Message Protocol

IP Internet Protocol

L2 Στρώμα 2 of OSI model, or Data Link στρώμα

L3 Στρώμα 3 of OSI model, or Network στρώμα

LBU Local Binding Update

LCoA Local Care-of-Address

LM *Location Management*

MAP Mobility Anchor Point

MIPv4 Mobile IPv4

MIPv6 Mobile IPv6

MN Mobile Node

NA Neighbor Advertisement

NAR New Access Router

NCoA New Care of Address

PAR Previous Access Router

PCoA Previous Care of Address

PrRtAdv Proxy Router Advertisement

RBU Regional Binding Update

RCoA Regional Care-of-Address

RtSolPr Router Solicitation for Proxy Advertisement

RA Router Advertisement (message)

RFC Request for Comments

RS Router Solicitation (message)

S-MIP Seamless Mobile IP

SA Security Association

SAD Security Association Database

SPD Security Policy Database

VPN Virtual Private Network

IKE Internet key exchange

QoS Quality of Service

10. Βιβλιογραφία

[1] D. Johnson, C. E. Perkins and J. Arkko, “Mobility Support in IPv6”, IETF, RFC3775, June 2004.

[2] H. Soliman, C. Castelluccia, K. El-Malki and L. Bellier, “Hierarchical MIPv6 mobility management (HMIPv6)”, IETF, RFC4140 , August 2005.

[3] R.Koodli, "Fast Handovers for Mobile IPv6", IETF, RFC4068 , July 2005.

[4] R. Hsieh, Z.G. Zhou, and A. Seneviratne, “S-MIP: A Seamless Handoff Architecture for Mobile IP”, Apr. 2003.

[5] H. Jung, "Fast Handover for Hierarchical MIPv6 (F-HMIPv6)", IETF, April 2005.

[6] Miska Sulander, Timo H¨am¨al¨ainen, Ari Viinikainen and Jani Puttonen, “Flow-Based Fast Handover Method for Mobile IPv6 Network”.

[7] A. Grilo, P. Estrela, M. Nunes, Terminal Independent Mobility for IP (TIMIP)”, IEEE Communications, Vol. 39 Nº12, Dec 2001.

[8] P. Estrela, T. Vazão, M. Nunes, “Design and Evaluation of eTIMIP - Overlay Micro-Mobility Architecture based on TIMIP”, ICWMC 2006, Romania, July 2006.

[9] Shaojian Fu, Liran Ma, Mohammed Atiquzzaman, Yong-Jin Lee, “Architecture and Performance of SIGMA: A Seamless Mobility Architecture for Data Networks”.

[10] Abu S. Reaz, Mohammed Atiquzzaman, “P-SIGMA: Paging in End to End Mobility Management”.

[11] Ali Diab, Andreas Mitschele-Thiel, René Böringer, “Evaluation of Mobile IP Fast AuthenticationProtocol compared to Hierarchical Mobile IP”.

[12] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", RFC 4225, December 2005.

[13] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[14] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[15] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

11. Γενική βιβλιογραφία

[ΓΒ1]Charlie Kaufman, Radia Perlman and Mike Speciner "Network Security: Private Communication in a Public World", 1st edition, Prentice Hall, March 16 1995.

[ΓΒ2]Vassos Vassiliou, "Lectures EPL 420: High Speed Multimedia and Multiservice Networks", spring 2008.

12. Βιβλιογραφία εικόνων-σχημάτων

[Σχήμα 2.1] Vassos Vassiliou, “lectures EPL 420: High Speed Multimedia and Multiservice Networks”, spring 2008.

[Σχήμα 2.2] Vassos Vassiliou, “lectures EPL 420: High Speed Multimedia and Multiservice Networks”, spring 2008.

[Σχήμα 3.1] DMai Banh, “Quantification, Characterisation and Evaluation of Mobile IPv6 Handoff Delay”, http://caia.swin.edu.au/talks/CAIA-TALK-050309A.pdf

[Σχήμα 3.2] D. Johnson, C. E. Perkins and J. Arkko, “Mobility Support in IPv6”, IETF, rfc3775, June 2004.

[Σχήμα 3.3.X] H. Soliman, C. Castelluccia, K. El-Malki and L. Bellier, “Hierarchical MIPv6 mobility management (HMIPv6)”, IETF, RFC4140 , August 2005.

[Σχήμα 3.4] R.Koodli, "Fast Handovers for Mobile IPv6", IETF, RFC4068, July 2005.

[Σχήμα 3.5] R. Hsieh, Z.G. Zhou, and A. Seneviratne, “S-MIP: A Seamless Handoff Architecture for Mobile IP”, School of Electrical Engineering and Telecommunications, The University of New South Wales Sydney, Apr. 2003.

[Σχήμα 3.7] R. Hsieh, Z.G. Zhou, and A. Seneviratne, “S-MIP: A Seamless Handoff Architecture for Mobile IP”, School of Electrical Engineering and Telecommunications, The University of New South Wales Sydney, Apr. 2003.

[Σχήμα 3.7] H. Jung, "Fast Handover for Hierarchical MIPv6 (F-HMIPv6)", IETF, April 2005.

[Σχήμα 3.8] Miska Sulander, Timo H¨am¨al¨ainen, Ari Viinikainen and Jani Puttonen, “Flow-Based Fast Handover Method for Mobile IPv6 Network”, Department of

Mathematical Information Technology University of Jyv¨askyl¨a, 40014 Jyv¨askyl¨a, FINLAND.

[Σχήμα 3.9] A. Grilo, P. Estrela, M. Nunes, Terminal Independent Mobility for IP (TIMIP)", IEEE Communications, Vol. 39 Nº12, Dec 2001.

[Σχήμα 3.10] A. Grilo, P. Estrela, M. Nunes, Terminal Independent Mobility for IP (TIMIP)", IEEE Communications, Vol. 39 Nº12, Dec 2001.

[Σχήμα 3.11] A. Grilo, P. Estrela, M. Nunes, Terminal Independent Mobility for IP (TIMIP)", IEEE Communications, Vol. 39 Nº12, Dec 2001.

[Σχήμα 3.12] P. Estrela, T. Vazão, M. Nunes, "Design and Evaluation of eTIMIP - Overlay Micro-Mobility Architecture based on TIMIP", ICWMC 2006, Romania, July 2006.

[Σχήμα 3.13] Shaojian Fu, Liran Ma, Mohammed Atiquzzaman, Yong-Jin Lee, "Architecture and Performance of SIGMA: A Seamless Mobility Architecture for Data Networks", Telecommunications and Networks Research Lab School of Computer Science, University of Oklahoma, Norman, OK 73019-6151, USA.

[Σχήμα 3.14] Shaojian Fu, Liran Ma, Mohammed Atiquzzaman, Yong-Jin Lee, "Architecture and Performance of SIGMA: A Seamless Mobility Architecture for Data Networks", Telecommunications and Networks Research Lab School of Computer Science, University of Oklahoma, Norman, OK 73019-6151, USA.

[Σχήμα 3.15] Abu S. Reaz, Mohammed Atiquzzaman, "P-SIGMA: Paging in End to End Mobility Management", Telecommunications and Networks Research Lab School of Computer Science, University of Oklahoma, Norman, OK 73019-6151, USA.

[Σχήμα 3.16] Abu S. Reaz, Mohammed Atiquzzaman, "P-SIGMA: Paging in End to End Mobility Management", Telecommunications and Networks Research Lab

School of Computer Science, University of Oklahoma, Norman, OK 73019-6151, USA.

[Σχήμα 3.17] Ali Diab, Andreas Mitschele-Thiel, René Böringer, “Evaluation of Mobile IP Fast AuthenticationProtocol compared to Hierarchical Mobile IP”.

[Σχήμα 3.18] Ali Diab, Andreas Mitschele-Thiel, René Böringer, “Evaluation of Mobile IP Fast AuthenticationProtocol compared to Hierarchical Mobile IP”.

[Σχήμα 4.x] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", RFC 4225, December 2005.

[Σχήμα 5.x] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[Σχήμα 6.1] Miska Sulander, Timo Hamalainen, Ari Viinikainen and Jani Puttonen, “Flow-Based Fast Handover Method for Mobile IPv6 Network”, Department of Mathematical Information Technology University of Jyv¨askyl¨a, 40014 Jyv¨askyl¨a, FINLAND.