ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ: Τηλεπληροφορικής και Διοίκησης

ΓΚΟΥΝΗΣ ΓΙΩΡΓΟΣ
ΤΖΑΜΤΖΗΣ ΛΑΜΠΡΟΣ

ΔΙΑΠΛΑΝΗΤΙΚΑ ΔΙΚΤΥΑ (INTERPLANETARY NETWORKS)

ΙΟΥΛΙΟΣ 2005

ΠΕΡΙΕΧΟΜΕΝΑ

1 ΕΙΣΑΓΩΓΗ

Αυτή η εργασία περιγράφει το Διαπλανητικό(Interplanetary) Internet δηλαδή ένα σύστημα επικοινωνίας που παρέχει υπηρεσίες Διαδικτύου για διαπλανητικές αποστάσεις και συμβάλλει στην εξερεύνηση του διαστήματος. Οι επικοινωνίες αυτού του περιβάλλοντος χαρακτηρίζονται από αποδόσεις υψηλής καθυστέρησης στο εύρος ζώνης του(high bandwidth-delay) που προκύπτουν από τις μεγάλες καθυστερήσεις διάδοσης του σήματος, από την προσωρινή διακοπή της επικοινωνίας που επιφέρει μεγάλες περιόδους απομόνωσης και διαχωρισμού του δικτύου και από ασυνέχεια στις δυνατότητες των παρακείμενων δικτύων. Πολλά από αυτά τα χαρακτηριστικά μοιάζουν με αυτά που αντιμετωπίζουμε στις υπηρεσίες επικοινωνίας στο σημερινό Διαδίκτυο. Για παράδειγμα, τα terabit δίκτυα παρουσιάζουν αποδόσεις πολύ μεγάλης καθυστέρησης στο εύρος ζώνης, η κινητή επικοινωνία έχει σαν αποτέλεσμα τον διαχωρισμό-καταμερισμό των κόμβων και των υποδικτύων και η διασύνδεση τεχνολογιών διαφορετικού φυσικού επιπέδου καταλήγουν σε αστοχίες(mismatches).Είναι εφικτό να αντιμετωπίσουμε την κάθε μία από τις παραπάνω περιπτώσεις χωριστά με μια απ'άκρου-εις-άκρου λύση, αλλά είναι δύσκολο να βρούμε λύση που να τις ικανοποιεί όλες ταυτόχρονα.

Τα αποτελέσματα της μεγάλης καθυστέρησης εύρους ζώνης που μοιράζονται το InterPlanetary Network (IPN) και τα σημερινά πολύ υψηλών ταχυτήτων γήινα δίκτυα στηρίζουν τα μη συνομηλιτικά (non-chatty) πρωτόκολλα επικοινωνίας. Στο IPN,οι μακρές καθυστερήσεις δείχνουν ότι τα πρωτόκολλα που χρησιμοποιούν πολλά roundtrips (η διαδρομή ενός πακέτου για τον προορισμό και πίσω) προκειμένου να εκτελέσουν τις εργασίες τους έχουν ως αντίτιμο την σπατάλη σημαντικού χρόνου. Στα επίγεια terabit δίκτυα οι μεταγωγείς (switches) προωθούν τα δεδομένα πολύ γρήγορα αλλά χρειάζεται σχετικά αρκετός χρόνος αναδιαμόρφωσής τους, με αποτέλεσμα να πέφτει σημαντικά η απόδοση στην χρησιμοποίηση των πόρων. Και τα δύο περιβάλλοντα επωφελούνται από τα πρωτόκολλα που μεταφέρουν όσο το δυνατό περισσότερες πληροφορίες σε κάθε μεταβίβασή τους και ελαχιστοποιούν τον αριθμό των διαδρομών που χρειάζεται να κάνουν. Επομένως, ένα πρωτόκολλο μεταφοράς αρχείων που μπορεί να συμπεριλάβει τόσο όλα τα δεδομένα όσο και τις πληροφορίες που σχετίζονται με τον έλεγχο μαζί σε μία απλή ατομική δοσοληψία, ολοκληρώνει πιο γρήγορα την αποστολή του μέσα στο IPN και κάνει αποτελεσματικότερη και πιο αποδοτική τη χρήση των σύγχρονων υψηλής ταχύτητας επίγειων δικτύων.

Τα περισσότερα από τα προβλήματα που αναφέρθηκαν παραπάνω έχουν εξεταστεί και λυθεί, κάθε ένα χωριστά, κατά την διάρκεια της εξέλιξης του σημερινού Internet.Πολλές από τις λύσεις όμως παρουσίασαν παρακλάδια μέσα στην εξέλιξη του Διαδικτυακού δέντρου και εγκαταλείφτηκαν προκειμένου να διατηρηθεί η υπάρχουσα υποδομή που μειώνει τις περιβαλλοντικές διαφορές. Όμως αυτή η αποτελεσματική ομοιογένεια μειώνεται ούτως ή άλλως με τη ραγδαία ανάπτυξη των νέων τεχνολογιών με διαφορετικά θεμελιώδη χαρακτηριστικά, όπως οι ασύρματες επικοινωνίες και τα DWDM(Dense Wavelength Division Multiplexing) δίκτυα. Μία λύση είναι το ηλεκτρονικό ταχυδρομείο(e-mail) που παρέχει τον τρόπο να επικοινωνούν διαφορετικά δίκτυα που δεν είναι απαραίτητα διαρκώς συνδεδεμένα μεταξύ τους. Η προσέγγιση του τρόπου λειτουργίας του e-mail παρουσιάζει μεγάλο ενδιαφέρον. Καταρχήν δεν υπάρχει η απαίτηση συνεχόμενης ή άμεσης επικοινωνίας.

Εκτός αυτού, η διαδικασία του e-mail ενσαρκώνει την ιδέα αποθήκευσης και προώθησης (store-and-forward) σε διαφορετικά δίκτυα ή και σε προσωρινά αποσυνδεδεμένα δίκτυα. Τέλος, η ιδέα του ηλεκτρονικού ταχυδρομείου γενικά θεωρείται ένας μηχανισμός μη διαδραστικής επικοινωνίας και πιθανότατα να ικανοποιεί ένα περιβάλλον που παρουσιάζει μεγάλες καθυστερήσεις στην επικοινωνία.
Η προσέγγιση του e-mail όμως έχει και περιορισμούς. Χωρίς μηχανισμό αναμετάδοσης end-to-end το ηλεκτρονικό ταχυδρομείο δεν παρέχει πραγματική απ'άκρου-εις-άκρου αξιοπιστία. Ακόμη, το e-mail προσανατολίζεται για ανθρώπινη χρήση παρά για ενδοεπεξεργαστική επικοινωνία. Επιπρόσθετα, το πρωτόκολλο που παρέχει τις υπηρεσίες του e-mail στο Διαδίκτυο, το SMTP,είναι πλήρως αλληλεπιδραστικό στον έλεγχο κυκλοφορίας του, άσχετα αν η όλη ιδέα του e-mail είναι ελάχιστα διαδραστική.

Η προσέγγιση μεταφοράς πληροφοριών σε μεγάλες αποστάσεις αναφέρεται ως bundling,αφού το νέο επίπεδο που θα χρησιμοποιηθεί θα ονομάζεται bundle layer και με βάση αυτό θα «χτιστεί» ένα store-and-forward δίκτυο που θα επικαλύπτει τα ήδη υπάρχοντα δίκτυα πάνω από το επίπεδο μεταφοράς τους. Έτσι δύο κόμβοι γειτονικοί, όσο αφορά το bundling, μπορεί να είναι πολλά βήματα (hops) μακριά στο πλαίσιο της τοπολογίας των από κάτω δικτύων. Το bundle layer αφήνει τις εφαρμογές να επικοινωνούν όταν υπάρχει ασυνέχεια στην επικοινωνία και να επικοινωνούν αποτελεσματικά με το πλήθος των τεχνολογιών μεταφοράς που βρίσκονται από κάτω. Αυτή η ασυνέχεια στην επικοινωνία μπορεί να προέλθει από τις διακυμάνσεις στην διαθεσιμότητα της ζεύξης ή από παραπλανητικές ασυνέχειες που δημιουργούν τα firewalls.Για αποτελεσματική επικοινωνία, το bundle layer προσπαθεί να ελαχιστοποιήσει την αλληλεπίδραση του δικού του ελέγχου κυκλοφορίας και περιμένει τις εφαρμογές να δράσουν ομοίως. Το bundle layer παρέχει επίσης ένα επίπεδο έμμεσης δρομολόγησης ανάμεσα σε εφαρμογές και σε συγκεκριμένες υπηρεσίες των πρωτοκόλλων των δικτύων.Οι bundle εφαρμογές μπορούν να καθορίσουν τις ζητούμενες πληροφορίες διεκπεραίωσης,όπως η αξιοπιστία και η ποιότητα στις υπηρεσίες αιτήσεων (QoS) που διαθέτουν οι κατάλληλοι μηχανισμοί στα σημερινά δίκτυα.

Το bundling χρησιμοποιεί πολλές από τις τεχνικές του ηλεκτρονικού ταχυδρομείου,αλλά είναι για ενδοεπεξεργαστική επικοινωνία. Οι bundle κόμβοι χρησιμοποιούν τις δυνατότητες των υποκείμενων δικτύων συμπεριλαμβάνοντας πρωτόκολλα αναμετάδοσης επιπέδου μεταφοράς, για να πραγματοποιηθεί η μεταφορά των bundles μεταξύ των κόμβων. Προαιρετικά, η end-to-end αξιοπιστία στο bundle επίπεδο διευκολύνει την end-to-end αξιοπιστία στο επίπεδο εφαρμογής. Εξάλλου, το bundle επίπεδο επιτρέπει σε κάθε bundle κόμβο της διαδρομής να έχει την κηδεμονία του πακέτου. Όταν η κηδεμονία μεταφερθεί, ο αποδέκτης bundle κόμβος αναλαμβάνει την ευθύνη για την μεταφορά του πακέτου ανάλογα με τις πληροφορίες διακίνησής του και ο προηγούμενος κόμβος-κηδεμόνας μπορεί να ανακτήσει τους πόρους αποθήκευσής του. Το bundle πρωτόκολλο σχεδιάστηκε για να λειτουργεί σε μονόδρομες(simplex) γραμμές και σε γραμμές αμφίδρομης εναλλασσόμενης επικοινωνίας (half-duplex) και κηδεμονικές μεταφορές μπορούν να γίνουν μεταξύ μη γειτονικών bundle κόμβων. Τέλος, επειδή το bundle επίπεδο λειτουργεί σε δίκτυα που είναι συχνά αποσυνδεδεμένα, οι μηχανισμοί αξιοπιστίας του προσαρμόζουν τη λειτουργία των χρονοδιακοπτών για να διευθετήσουν αυτή την προσωρινή αποσύνδεση.

Για να εξηγήσουμε πώς το bundling πετυχαίνει την επικοινωνία δικτύων που αποσυνδέονται κατά περιόδους, κάποιος θα μπορούσε να φανταστεί ένα στροβοσκοπικό φως που τονίζει τα μέρη της τοπολογίας του δικτύου που είναι συνδεδεμένα κάποια συγκεκριμένη χρονική περίοδο. Αυτά τα φωτισμένα μέρη του δικτύου είναι διαθέσιμα για bundle προώθηση πληροφοριών. Αν φανταστεί κανείς μια υψηλής διάρκειας CRT να συλλαμβάνει μία διατεταγμένη ακολουθία φωτεινών σημείων που προχωρούν από την πηγή προς τον προορισμό θα καταλάβαινε τις διαθέσιμες δρομολογήσεις για προώθηση του bundle. Αυτό το περιβάλλον όμως απαιτεί έναν μηχανισμό δρομολόγησης βασισμένο και στην τρέχουσα επικοινωνία και σ'αυτήν που αναμένεται να γίνει. Αυτός ο μηχανισμός εκμεταλλεύεται αυτή την πρόβλεψη όπως φαίνεται από την μηχανική τροχιά ή από προγραμματισμένα γεγονότα του δικτύου.Αξίζει να σημειωθεί ότι ο μηχανισμός δρομολόγησης μπορεί να επιλέξει την αναβολή της επικοινωνίας έστω και αν ο δρόμος προς τον προορισμό υπάρχει, εάν αναμένεται σε μικρό χρονικό διάστημα να βρεθεί καλύτερη διαθέσιμη διαδρομή.

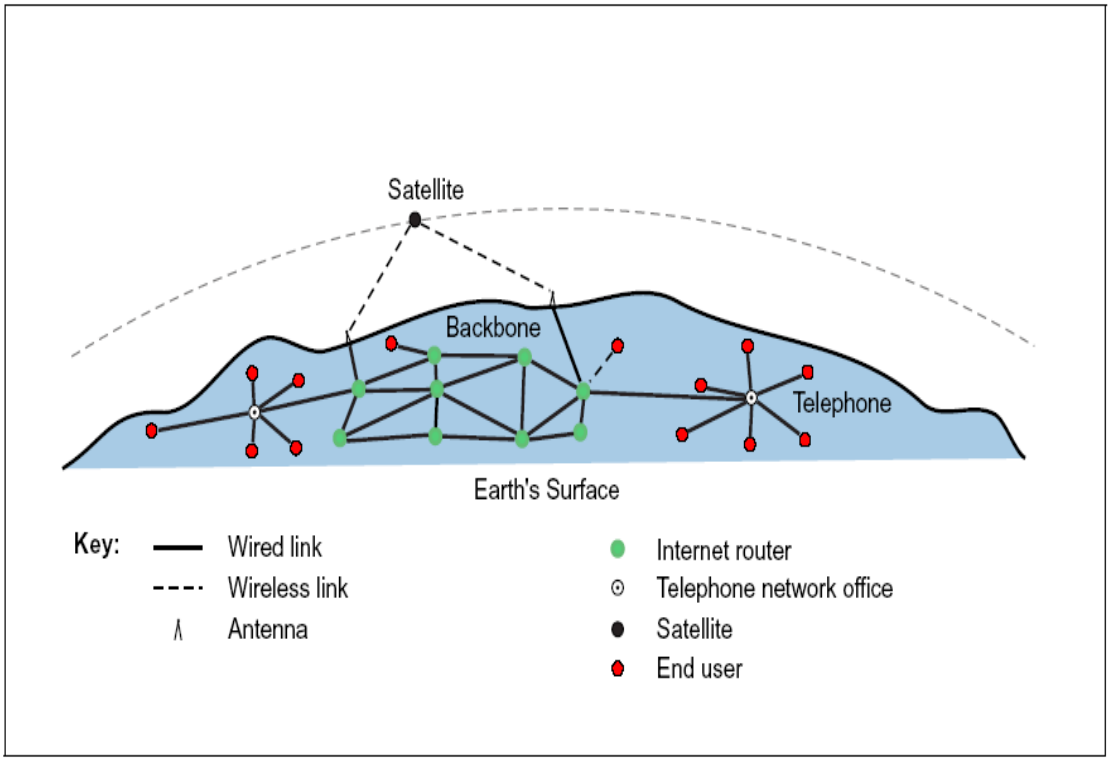
Είναι πιθανόν η λειτουργία του bundle επιπέδου να έχει ωφελιμότητα σε γενικές γραμμές και στο υπάρχων Διαδίκτυο. Το Internet εξελίσσεται συμπεριλαμβάνοντας πολύ διαφορετικές τεχνολογίες, αρχιτεκτονικές και εφαρμογές δικτύου. Μερικές από αυτές, όπως τα firewalls,έχουν ως αποτέλεσμα τον λογικό διαμερισμό του Internet,ενώ άλλες, όπως μεγάλοι ρυθμοί αστοχίας μπορεί να έχουν ως αποτέλεσμα την ανεπαρκή χρήση των πόρων του δικτύου. Το bundle επίπεδο επεκτείνει την αρχιτεκτονική του Διαδικτύου προσφέροντας σταθερή end-to-end επικοινωνία στο παρών και στα εξελισσόμενα διαμοιρασμένα περιβάλλοντα, προωθώντας την ανάπτυξη νέων εφαρμογών που μπορούν να λειτουργούν αξιόπιστα αφήνοντας τα δίκτυα να ενεργούν αποτελεσματικά.

2 ΤΟ ΔΙΑΔΙΚΤΥΟ ΣΗΜΕΡΑ

2.1 Εισαγωγή

Το Διαδίκτυο αποτέλεσε μια μεγάλη επιτυχία στη διασύνδεση τηλεπικοινωνιακών συσκευών σε όλη την υδρόγειο. Αυτό το κατάφερε με τη χρησιμοποίηση ενός ομοιογενούς συνόλου τηλεπικοινωνιακών πρωτοκόλλων, αποκαλούμενο *TCP/IP*. Όλες οι συσκευές στις εκατοντάδες χιλιάδες των υποδικτύων που αποτελούν το Διαδίκτυο χρησιμοποιούν αυτά τα πρωτόκολλα για τη δρομολόγηση δεδομένων και για εξασφάλιση της αξιοπιστίας των ανταλλασσόμενων μηνυμάτων.

Η συνδεσιμότητα στο διαδίκτυο στηρίζεται πρώτιστα στις ενσύρματες ζεύξεις, συμπεριλαμβανομένου του ενσύρματου τηλεφωνικού δικτύου, αν και νέες ασύρματες τεχνολογίες όπως μικρής εμβέλειας κινητές και δορυφορικές ζεύξεις εμφανίζονται συνεχώς. Αυτές οι συνδέσεις είναι συνεχώς ενωμένες στις απ'άκρου-εις-άκρου(end-to-end),χαμηλής καθυστέρησης διαδρομές μεταξύ πηγών και προορισμών. Έχουν χαμηλά ποσοστά λάθους και σχετικά συμμετρικά και αμφίδρομα ποσοστά μεταφοράς δεδομένων.



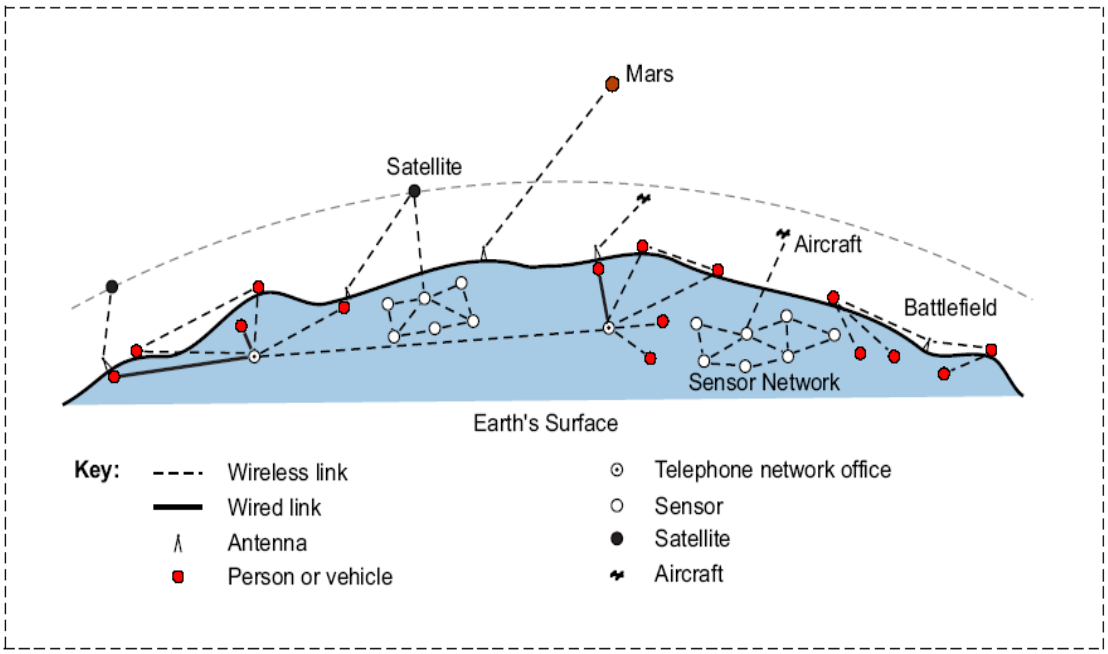
2.2 Εξελισσόμενα ασύρματα δίκτυα έξω από το Διαδίκτυο

Η επικοινωνία έξω από το Διαδίκτυο —όπου οι περιορισμένες ενεργειακά κινητές ασύρματες,
δορυφορικές και διαπλανητικές επικοινωνίες αναπτύσσονται —πραγματοποιείται σε ανεξάρτητα δίκτυα, το καθένα υποστηρίζοντας εξειδικευμένες τηλεπικοινωνιακές ανάγκες. Αυτά τα δίκτυα δεν χρησιμοποιούν Διαδικτυακά πρωτόκολλα και είναι

ασύμβατα μεταξύ τους —το καθένα είναι ικανό να μεταφέρει μυνήματα μέσα στο δίκτυό του ,αλλά μη ικανό να ανταλλάξει μυνήματα με άλλα δίκτυα.
Κάθε δίκτυο προσαρμόζεται σε μια συγκεκριμένη *τηλ*επικοινωνιακή *περιοχή,* στην οποία
τα επικοινωνιακά χαρακτηριστικά είναι σχετικά ομοιογενή.Τα όρια μεταξύ των περιοχών καθορίζονται από έννοιες όπως συνδεσιμότητα-καθυστέρηση ζεύξεις(link connectivity, link delay),ασσυμετρία ρυθμού μετάδοσης δεδομένων(data-rate asymmetry),ρυθμός λαθών(error rates), μηχανισμοί διευθυνσιοδότησης και αξιοπιστίας, και ποιότητα παρεχόμενων υπηρεσιών(quality-of-service).Σε αντίθεση με το Διαδίκτυο ,αυτά τα ασύρματα δίκτυα υποστηρίζουν μακροχρόνιες και μεταβλητές καθυστερήσεις, τυχαίες και μεγάλες περιόδους αποσύνδεσης, υψηλούς ρυθμούς λαθών, και μεγάλες αμφίδρομες ασσυμετρίες στο ρυθμό μετάδοσης των δεδομένων.

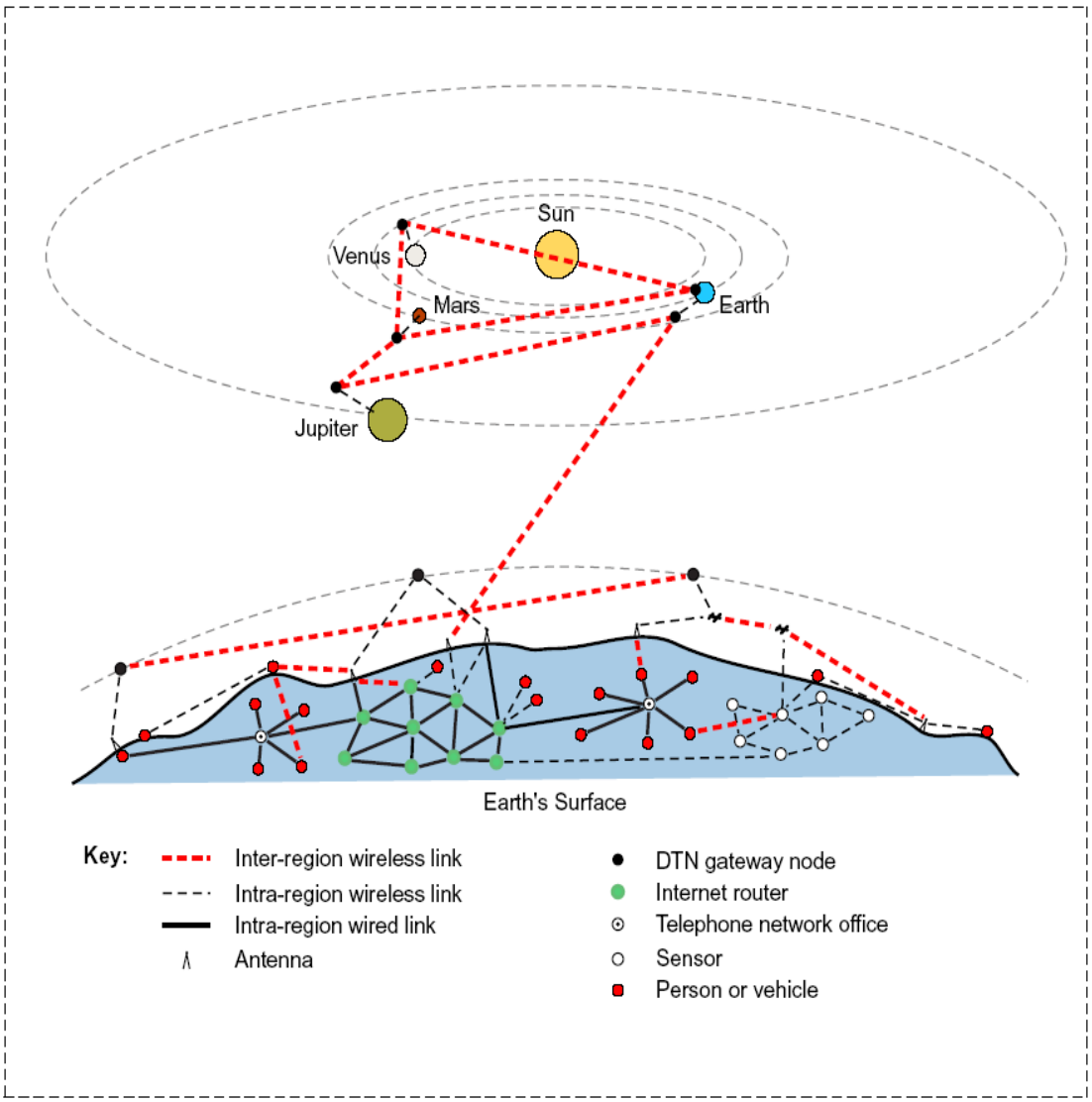
Παραδείγματα ασύρματων δικτύων εκτός του Διαδίκτυου αποτελούν:
Επίγεια πολιτικά δίκτυα που συνδέουν κινητές ασύρματες συσκευές.
Ασύρματα στρατιωτικά δίκτυα που συνδέουν στρατεύματα, αεροσκάφη, δορυφόρους και αισθητήρες (στο έδαφος ή στο νερό).
Διαστημικά δίκτυα, όπως το InterPlaNetary (IPN) Internet Project.

Η ένωση δύο δικτυακών περιοχών απαιτεί την μεσολάβηση ενός στοιχείου που μπορεί να μεταφράσει τα ασύμβατα χαρακτηριστικά μεταξύ αυτών των δικτύων και να χρησιμοποιηθεί σαν ενδιάμεσος-αποθήκη (buffer) για τις καθυστερήσης του δικτύου.



2.3 Η έννοια ενός ανεκτικού σε καθυστερήσεις δικτύου (DTN-Delay Tolerant Network)

Ένα DTN είναι ένα δίκτυο *περιφερειακών δικτύων*. Έιναι ένα στρώμα που επικαλύπτει τα περιφερειακά δίκτυα, συμπεριλαμβανομένου και του Διαδικτύου.
Τα DTN δίκτυα υποστηρίζουν την συνεργασία των περιφερειακών δικτύων με την προσαρμογή μεγάλων καθυστερήσεων μεταξύ και εντός των περιφερειακών δικτύων, και με την μετάφραση των μεταξύ των επικοινωνιακών τους χαρακτηριστικών. Με την παροχή αυτών των λειτουργιών, τα DTN δίκτυα διαθέτουν την ευελιξία και την περιορισμένη ενέργεια των εξελισόμενων ασύρματων τηλεπικοινωνιακών συσκευών. Οι ασύρματες DTN τεχνολογίες μπορούν να είναι διαφορετικές, συμπεριλαμβανομένων όχι μόνο των ραδιοσυχνοτήτων(RF) αλλά και της ultra-wide band (UWB), οπτικών και ακουστικών τεχνολογιών.

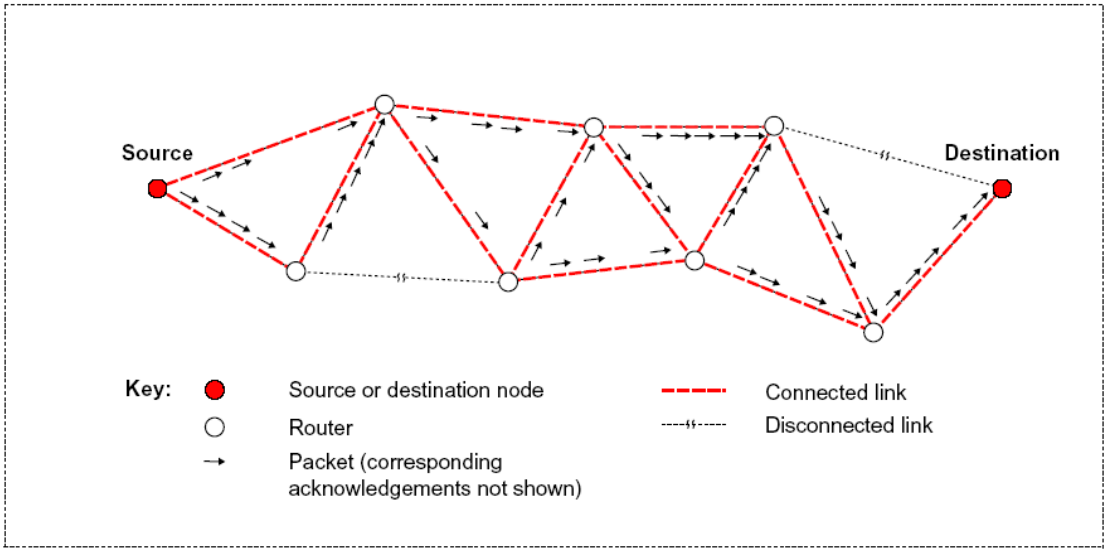


2.4 Μεταγωγή Πακέτου

Η επικοινωνία στο Διαδίκτυο βασίζεται στη μεταγωγή πακέτου(*packet switching).Τα πακέτα είναι κομμάτια ενός μέρους δεδομένων (π.χ κομμάτια ενός μυνήματος e-mail ή μίας ιστοσελίδας)* που ταξιδεύουν ανεξάρτητα από πομπό σε δέκτη μέσω ενός δικτύου ζεύξεων ενωμένων με δρομολογητές. Ο πομπός, ο δέκτης και οι δρομολογητές γενικά αποκαλούνται κόμβοι(nodes).
Κάθε πακέτο που αποτελεί μέρος ενός μυνήματος μπορεί να ακολουθήσει μια διαφορετική διαδρομή μέσα στο δίκτυο. Άν μία ζεύξη είναι αποσυνδεδεμένη, τα πακέτα μπορούν να ακολουθήσουν μία άλλη διαδρομή. Τα πακέτα περιέχουν τα προς μεταφορά δεδομένα (το ωφέλιμο φορτίο) και μία επικεφαλίδα(header-το κομμάτι ελέγχου του πακέτου). Η επικεφαλίδα περιέχει την διεύθυνση του προορισμού του πακέτου και άλλες πληροφορίες που καθορίζουν το πώς το πακέτο μετάγεται από τον ένα δρομολογητή στον άλλο. Τα πακέτα ενός απεσταλμένου μηνύματος μπορεί να φτάσουν σε διαφορετική σειρά, αλλά ο μηχανισμός μεταφοράς του προορισμού τα επαναφέρει στην σωστή σειρά.

Η δυνατότητα χρησιμοποίησης του Διαδικτύου εξαρτάται από μερικές σημαντικές υποθέσεις:

- Συνεχής, αμφίδρομη απ'άκρου-εις-άκρου διαδρομή*:* Μία συνεχώς διαθέσιμη αμφίδρομη
  σύνδεση μεταξύ της πηγής και του προορισμού για να υποστηρίξει *απ'άκρου-εις-άκρου* αλληλεπίδραση.
- Σύντομα round-trips*:* Μικρή και σχετικά ελεγχόμενη καθυστέρηση δικτύων στην αποστολή
  πακέτων δεδομένων και λήψη των αντίστοιχων πακέτων αναγνώρισης.
- Συμμετρικός ρυθμός μεταφοράς δεδομένων*:* Σχετικά συνεπής ρυθμός μεταφοράς δεδομένων και στις δύο κατευθύνσεις μεταξύ της πηγής και του προορισμού.
- Χαμηλά ποσοστά λάθους*:* Σχετικά μικρή απώλεια ή καταστροφή των δεδομένων σε κάθε ζεύξη.



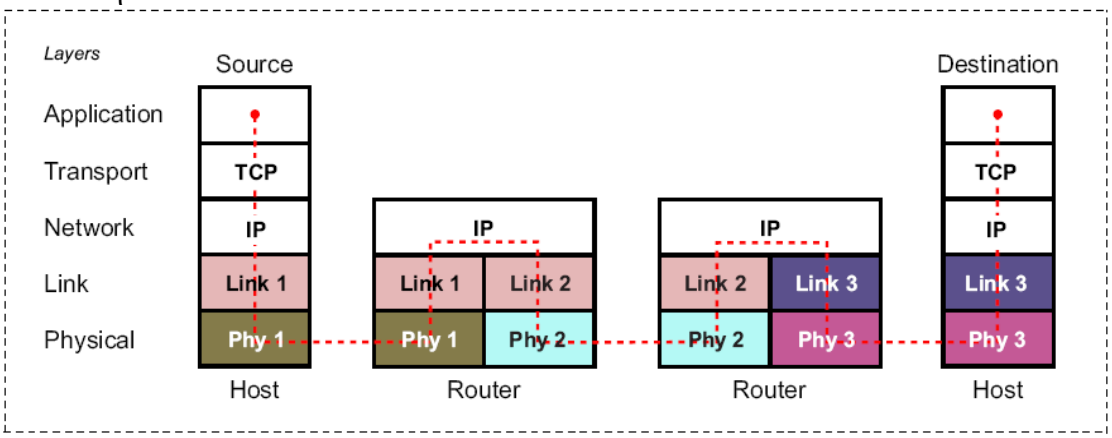
2.5 Στρώματα Πρωτοκόλλων

Τα μηνύματα κινούνται μέσω του Διαδικτύου από *τα στρώματα πρωτοκόλλων, ένα* σύνολο λειτουργιών διενεργηθείς από τους κόμβους των δικτύων πάνω στα δεδομένα που διακινούνται μεταξύ των κόμβων. *Οι hosts* (υπολογιστές ή άλλες συσκευές επικοινωνίας που είναι οι πηγές ή οι προορισμοί των μηνυμάτων) συνήθως υιοθετούν τουλάχιστον πέντε στρώματα πρωτοκόλλου, τα οποία πραγματοποιούν τις παρακάτω λειτουργίες:

• *Στρώμα εφαρμογής:* Παράγει ή αναλώνει τα δεδομένα των χρηστών (μηνύματα).
• *Στρώμα μεταφοράς:* κατάτμηση των μηνυμάτων σε κομμάτια και επανασυναρμολόγηση σε πλήρη μηνύματα, με έλεγχο λαθών και έλεγχο ροής. Στο διαδίκτυο χρησιμοποιείται το πρωτόκολλο TCP(Transmission Control Protocol).
• *Στρώμα δικτύου:* δρομολόγηση των προς αποστολή κομματιών μηνυμάτων μέσω ενδιάμεσων κόμβων, με τον τεμαχισμό και την επανασυναρμολόγησή τους αν είναι απαραίτητο. Στο διαδίκτυο χρησιμοποιείται το πρωτόκολλο *IP (Internet Protocol)*.
• *Στρώμα ζεύξης:* Από ζεύξη-σε-ζεύξη μετάδοση και υποδοχή των κομματιών των μηνυμάτων, με έλεγχο λαθών. Τα πιο σύνηθη πρωτόκολλα του στρώματος ζεύξης είναι το Ethernet για τοπικά δίκτυα (LAN) και το πρωτόκολλο PPP (Point-to-Point Protocol) για dial-up μόντεμ ή για ζεύξεις πολύ υψηλών ταχυτήτων.
• Στρώμα φυσικού μέσου*:* Από ζεύξη-σε-ζεύξη μετάδοση και υποδοχή ακολουθιών από bit. Τα πιο συνηθισμένα φυσικά μέσα μετάδοσης είναι καλώδια cat5, UTP (Unshielded Twisted Pair),τηλεφωνικά καλώδια, ομοαξονικά καλώδια, καλώδια οπτικών ινών και ραδιοκύματα (RF).

Οι δρομολογητές –για την δουλειά τους πού είναι να προωθούν δεδομένα (όπως φαίνεται παρακάτω) — υιοθετούν μόνο τα χαμηλότερα τρία στρώματα πρωτοκόλλων. Παρόλαυτα, οι δρομολογητές υιοθετούν και τα υψηλότερα στρώματα, αλλά για συντήρηση των πινάκων δρομολόγησης και άλλων πιο διοικητικών λειτουργιών.

Η εικόνα δείχνει τον βασικό μηχανισμό. Κάθε κόμβος της διαδρομής μπορεί να χρησιμοποιεί διαφορετική τεχνολογία στο στρώμα ζεύξης και στο φυσικό στρώμα, αλλά το πρωτόκολλο IP τρέχει σε όλους τους κόμβους και το πρωτόκολλο TCP τρέχει μόνο στη πηγή και στον προορισμό. Επίσης αρκετά άλλα διαδικτυακά πρωτόκολλα και εφαρμογές χρησιμοποιούνται για να παρέχουν υπηρεσίες δρομολόγησης, επιλογή διαδρομής, ανάλυση διευθύνσεων και υπηρεσίες ανάνηψης από λάθη.

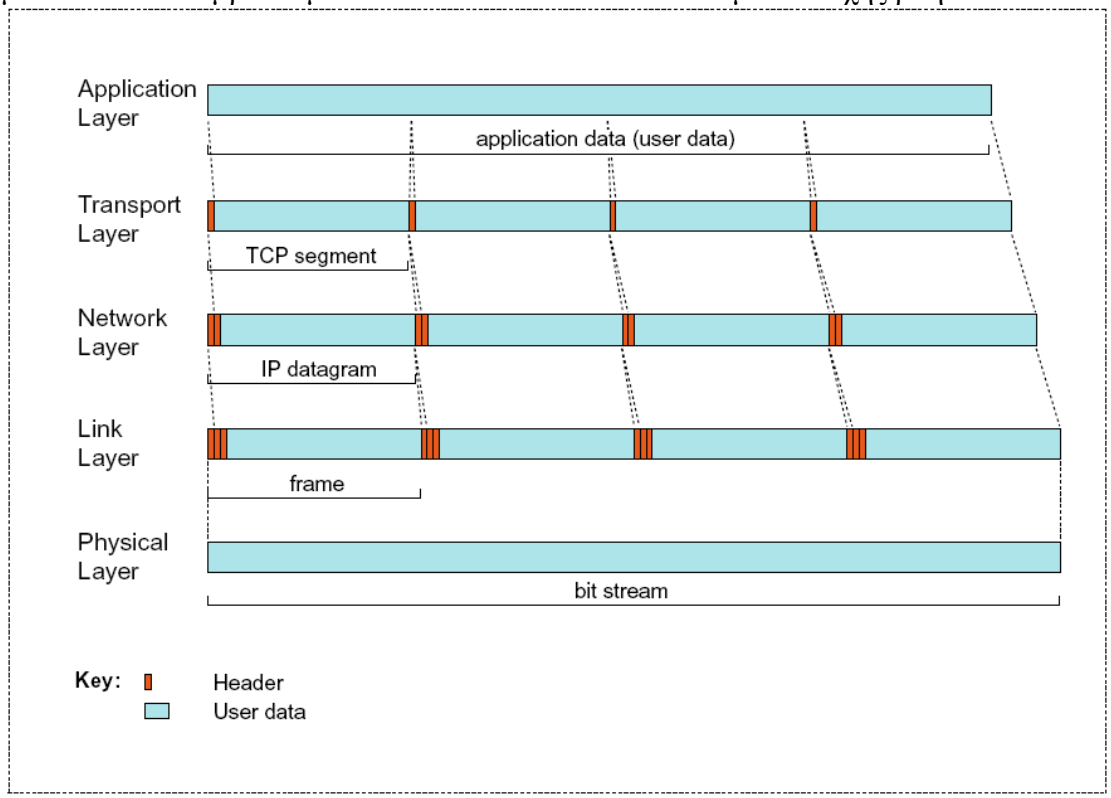


2.6 Ενθυλάκωση

Ο όρος πακέτο αναφέρεται στα στοιχεία που στέλνονται μέσω των φυσικών συνδέσεων ενός δικτύου. Αποκαλούνται πακέτα IP επειδή το πρωτόκολλο IP- το μόνο πρωτόκολλο που χρησιμοποιείται από όλους τους κόμβους στη διαδρομή- είναι το κυρίως υπεύθυνο για την καθοδήγηση των πακέτων, από κόμβο σε κόμβο και από πηγή σε προορισμό καθ'όλη την διαδρομή τους.

Τα πακέτα αποτελούνται από μια ιεραρχία από ενθυλακώσεις των δεδομένων πού πραγματοποιούνται από τα στρώματα των πρωτοκόλλων. Κατά την μετάδοση, τα υψηλότερου στρώματος δεδομένα και η επικεφαλίδα τους περικλείονται (ενθυλακώνονται) σε ένα χαμηλότερου στρώματος κομμάτι δεδομένων (πακέτο), στο οποίο δίδεται μία νέα επικεφαλίδα. Οι επικεφαλίδες χρησιμοποιούνται από τα αντίστοιχα τους στρώματα για να ελεγχθεί η επεξεργασία των ενθυλακωμένων δεδομένων. Διαδοχικές επικεφαλίδες προστίθενται καθώς τα δεδομένα μετακινούνται προς τα κάτω στη στοίβα πρωτοκόλλων από την εκπέμπουσα εφαρμογή που βρίσκεται στη πηγή προς το φυσικό επίπεδο. Οι επικεφαλίδες αφαιρούνται στο τέλος του προορισμού καθώς τα δεδομένα μετακινούνται προς τα πάνω στη στοίβα και στην εφαρμογή του προορισμού.

Το πρωτόκολλο TCP διαχωρίζει τα δεδομένα σε κομμάτια που ονομάζονται segments (τμήματα). Το πρωτόκολλο IP ενθυλακώνει τα segments του TCP σε *datagrams (διαγράμματα δεδομένων),*και μπορεί να χωρίσει τα segments σε τεμάχια (*fragments)(δεν φαίνονται στην εικόνα).*Τα πρωτόκολλα του στρώματος ζεύξης ενθυλακώνουν τα datagrams του IP σε πλαίσια (frames).Το φυσικό στρώμα μετά μεταδίδει και λαμβάνει μία ακολουθία από πλαίσια σαν μια συνεχής ροή από bit.

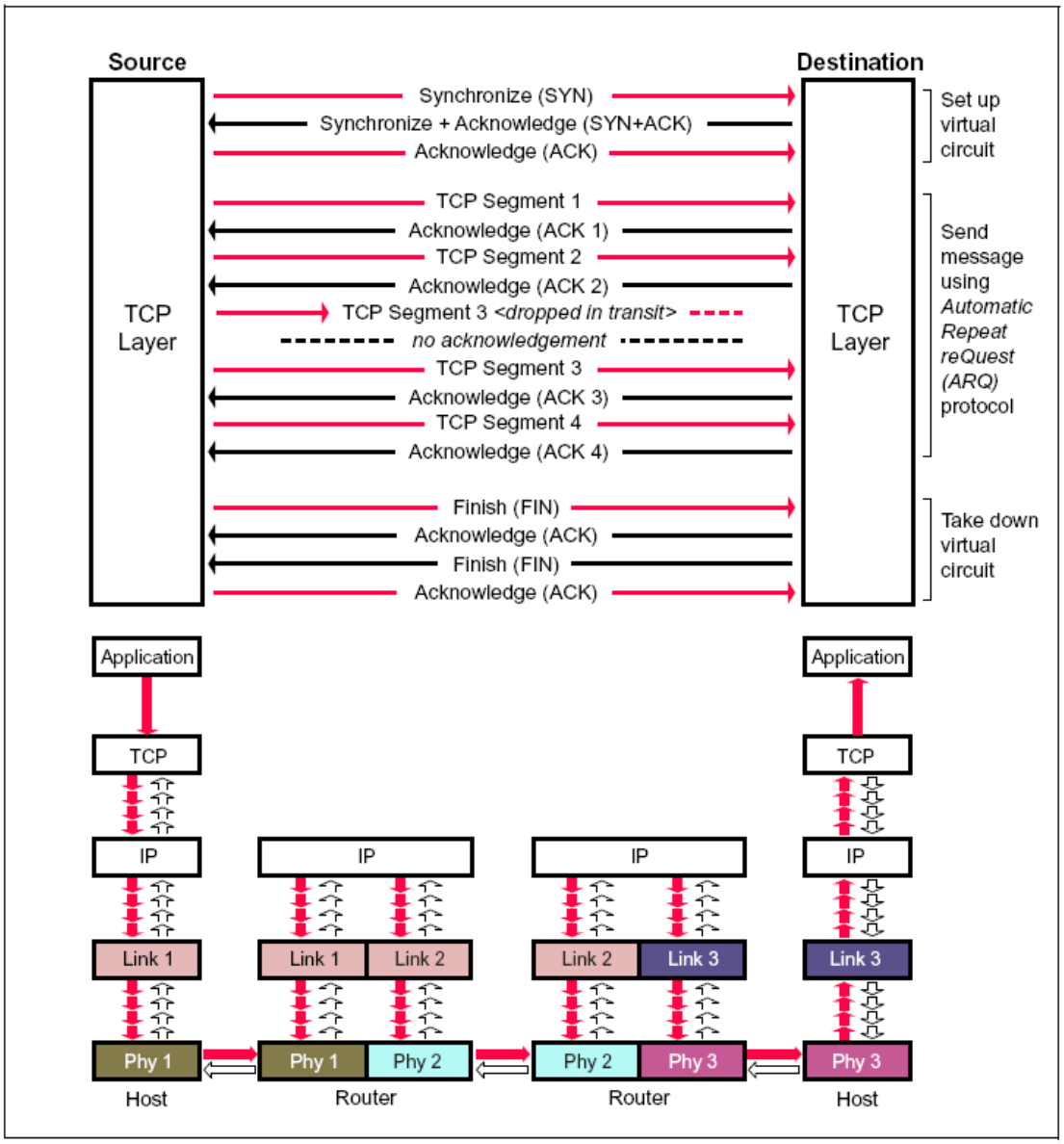


2.7 Συνομιλητικά πρωτόκολλα

Το πρωτόκολλο TCP θεωρείται συνομιλητικό (conversational-interactive),καθότι ένα ολόκληρο μήνυμα μίας κατεύθυνσης περιλαμβάνει πολλά από πηγή-σε-προορισμό round-trips:

- Εγκατάσταση σύνδεσης: Μία αναγνώριση τριών κατευθύνσεων των δύο ανταλλασσόμενων πλευρών (“Hello” handshake).
- Μεταφορά και επιβεβαίωση των *Segments:* κάθε segment του TCP πού στέλνεται από την πηγή επιβεβαιώνεται από τον προορισμό.
- Απόλυση σύνδεσης: Μία τεσσάρων κατευθύνσεων λήξη της συνεδρίας των δύο πλευρών (*"Goodbye"* handshake).

Η χρήση των θετικών ή αρνητικών αναγνωρίσεων για να ελεγχθεί η αναμετάδοση χαμένων ή αλλοιωμένων segments πραγματοποιείται από το πρωτόκολλο Automatic Repeat reQuest (ARQ).



2.8 Γιατί απαιτείται η χρήση ενός ανεκτικού σε καθυστερήσεις δικτύου (DTN);

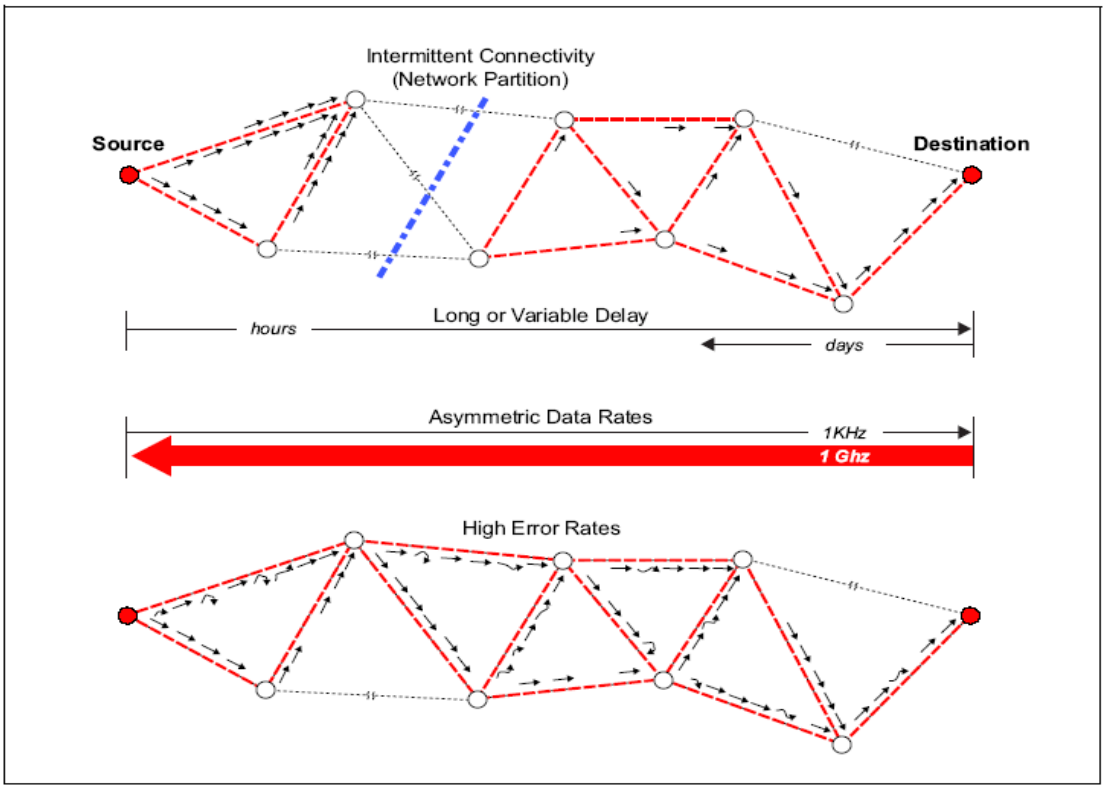
Πολλά εξελισσόμενα δίκτυα (κεφ 2.2) δεν είναι συμβατά με τις απαιτήσεις του Διαδικτύου (κεφ 2.4).Αυτά τα δίκτυα χαρακτηρίζονται από:

• Διακοπτόμενη Συνδεσιμότητα (*Intermittent Connectivity):* Αν δεν υπάρχει απ'άκρου-εις-άκρου διαδρομή μεταξύ της πηγής και του προορισμού, η απ'άκρου-εις-άκρου επικοινωνία χρησιμοποιώντας την σουίτα πρωτοκόλλων TCP/IP δεν μπορεί να λειτουργήσει. Απαιτούνται άλλα πρωτόκολλα.

• Μεγάλες ή *Μεταβλητές καθυστερήσεις:* Παράλληλα με την διακοπτόμενη συνδεσιμότητα, οι μεγάλες καθυστερήσεις στην μετάδοση μεταξύ των κόμβων και οι μεταβαλλόμενες καθυστερήσεις στη σειρά αναμονής των κόμβων συνεισφέρουν σε καθυστερήσεις στις απ'άκρου-εις-άκρου διαδρομές καθιστώντας άχρηστα τα πρωτόκολλα του Διαδικτύου και τις εφαρμογές που βασίζονται στην γρήγορη επιστροφή των επιβεβαιώσεων (ACK's) ή των δεδομένων.

• Ασύμμετροι Ρυθμοί Μεταφοράς Δεδομένων: Το Διαδίκτυο υποστηρίζει ελαφρά χαμηλές ασσυμετρίες σε αμφίδρομους ρυθμούς δεδομένων για χρήστες με καλωδιακή τηλεόραση ή πρόσβαση ADSL (ASYMMETRIC Digital Subscriber Line).Αλλά αν οι ασυμμετρίες είναι τεράστιες, τα συνομιλητικά πρωτόκολλα (κεφ 2.7) αχρηστεύονται.

• Υψηλά Ποσοστά Λαθών*:* Λάθη στη μεταφορά δεδομένων στις ζεύξεις απαιτούν διόρθωση (η οποία απαιτεί περισσότερα bit για μεταφορά και περισσότερη επεξεργασία) ή αναμετάδοση ολόκληρου του πακέτου (που έχει σαν αποτέλεσμα αύξηση της κίνησης στο δίκτυο). Για ένα δεδομένο ρυθμό λαθών σε μία ζεύξη, λιγότερες αναμεταδόσεις χρειάζονται για από κόμβου-εις-κόμβου αναμετάδοση παρά για απ'άκρου-εις-άκρου αναμετάδοση (γραμμική
αύξηση εναντίον εκθετικής αύξησης, ανά κόμβο).



3 Γιατί η χρήση μιας διαδεδομένης πλατφόρμας του Διαδικτύου δεν ενδύκνειται στο Διαπλανητικό Διαδίκτυο;

3.1 Προκαταρκτικές εκτιμήσεις

Σε επίπεδο τεχνολογιών, οι παρούσες δυνατότητες του Διαδικτύου αποδίδουν καλά στην Γη, όπου η καθυστέρηση μετάδοσης των κινούμενων με την ταχύτητα του φωτός σημάτων είναι μικρή.
Τα ανταλλασσόμενα πακέτα σύμφωνα με τις οδηγίες του πρωτοκόλλου TCP φτάνουν στους προορισμούς τους τυπικά σε κλάσματα του δευτερολέπτου. Τα πρωτόκολλα TCP/IP (ένα σύστημα από πάνω από 150 σχετικά επικοινωνιακά πρότυπα), αναμένεται συνεπώς να είναι ικανά να αποδώσουν εξίσου καλά και στην επιφάνεια άλλων πλανητών ή φεγγαριών, σε διαστημόπλοια και διαστημικούς σταθμούς σε τροχιά, και γενικά σε οτιδήποτε έχει να κάνει με ανταλλαγή δεδομένων σε σχετικά μικρές αποστάσεις, εξαρτώμενο βέβαια πάντα από την διαθεσιμότητα της απαραίτητης ενέργειας προκειμένου να διατηρηθεί μια καλή σχέση σήματος-προς-θόρυβο. Όσο ελκυστική και αν είναι όμως η υιοθέτηση παρόμοιων τεχνικών στην εξάπλωση του Διαδικτύου στο βαθύ διάστημα, υπάρχουν προβλήματα. Οι αποστάσεις μεταξύ των πλανητών είναι τεράστιες. Για παράδειγμα, οι καθυστερήσεις μετάδοσης –στην ταχύτητα του φωτός- στο roundtrip μεταξύ Γης και Άρη εκτείνονται ανάλογα με την τροχιά τους από 8 λεπτά έως και πάνω από 40 λεπτά. Αυτό κάνει τα συνομιλητικά πρωτόκολλα όπως το TCP σχετικά μη εφαρμόσιμα λόγω της μεγάλης τους εξάρτησης σε σχεδόν πραγματικού χρόνου ανταλλαγές δεδομένων μεταξύ των τηλεπικοινωνιακών μερών ενός δικτύου.

Επίσης αυτές οι τεράστιες αποστάσεις εξασθενούν το ρυθμό μετάδοσης των δεδομένων λόγω υποβάθμισης και μείωσης των ραδιοσημάτων.
Ακόμη, η ουράνια μηχανική του ηλιακού συστήματος έχει σαν αποτέλεσμα οι αποστάσεις μεταξύ των πλανητών να αλλάζουν με τον καιρό. Παρότι αυτές οι αλλαγές είναι υπολογίσιμες, προκαλούν μεταβολές στην καθυστέρηση, στην ικανότητα μετάδοσης και περιστασιακά στην συνδεσιμότητα λόγω απόκρυψης δορυφόρων από τους πλανήτες των οποίων την τροχιά διατρέχουν, ή επίγειων εγκαταστάσεων καθώς οι πλανήτες περιστρέφονται.

Το μέγεθος, το βάρος και πάνω απ’όλα η ενέργεια ενέχουν μεγάλες δυσκολίες για τα εγκατεστημένα στο διάστημα συστήματα επικοινωνιών, όπως ήταν επίσης κάποτε και για τα επίγεια κινητά συστήματα. Η εκτόξευση μάζας σε τροχιά, η είσοδος της στο βαρυτικό πεδίο ενός άλλου πλανήτη και η προσγείωσή της είναι προς το παρόν πολλή ακριβή. Η μάζα είναι ταυτόσημη με την τοπική διαθεσιμότητα σε ενέργεια. Η αποτελεσματική χρήση των καναλιών επικοινωνίας επιτρέπει περισσότερη πληροφορία να μεταφερθεί ανά μονάδα μεταδιδόμενης ενέργειας. Αλλά οι ενεργειακοί περιορισμοί εισάγουν ασυμμετρίες στις δυνατότητες μετάδοσης μεταξύ Γης για παράδειγμα, και απομακρυσμένων διαστημοπλοίων και πλανητών, δηλαδή μπορεί να υπάρχουν διαφορές μεταξύ του ρυθμού μετάδοσης των δεδομένων που μπορούν να ληφθούν από την Γη και του ρυθμού λήψης των δεδομένων από πηγές

εκτός Γης. Θεωρείται ότι θα είναι σύνηθης η δυνατότητα να δεχόμαστε μεταδόσεις από τον Άρη στα 100 kbps ενώ τα εγκατεστημένα στον Άρη συστήματα θα δέχονται από την Γη μόνο στα 1kbps.

Όλα αυτά τα φαινόμενα κάνουν το σχεδιασμό του backbone του διαπλανητικού συστήματος επικοινωνιών μια ιδιαίτερη πρόκληση. Το DSN (Deep Space Network) – το σημερινό διαπλανητικό backbone – χρησιμοποιεί τρία επίγεια τηλεπικοινωνιακά συγκροτήματα για την επικοινωνία με διαστημόπλοια, δορυφόρους σε τροχιά και επίγειες εγκαταστάσεις σε άλλα σώματα του ηλιακού συστήματος. Επειδή αυτοί οι πόροι πρέπει να μοιραστούν από πολλές αποστολές, είναι απαραίτητο να τους προγραμματίσουμε να στοχεύουν σε συγκεκριμένες κατευθύνσεις σε συγκεκριμένες στιγμές. Χρειάζεται συγχρονισμός μεταξύ των διαφόρων τμημάτων ενός τέτοιου συστήματος. Για παράδειγμα, ένα σήμα με πηγή τον Άρη μπορεί να κάνει 20 λεπτά να φτάσει στη Γη, κατά την οποία χρονική στιγμή άφιξης του σήματος η κατάλληλη κεραία του DSN θα πρέπει να είναι στραμμένη έτσι ώστε να δεχθεί την εκπομπή,20 λεπτά αφότου εστάλη. Αυτή η ίδια κεραία μπορεί μετά να πρέπει να επανατοποθετηθεί για να στείλει δεδομένα σε ένα άλλο σκάφος αλλού στο ηλιακό σύστημα, και ο δέκτης θα πρέπει να είναι έτοιμος να δεχθεί την εκπομπή την σωστή στιγμή. Κατά κάποιο τρόπο, αυτό το πρόβλημα μοιάζει με το πρόβλημα του προγραμματισμού τρένων στις σιδηροδρομικές γραμμές. Από τη στιγμή πού πολλά τρένα χρησιμοποιούν τις γραμμές, πρέπει να δρομολογηθούν έτσι ώστε να αποφευχθούν οι συγκρούσεις.

3.2 Το λειτουργικό περιβάλλον ενός IPN (InterPlanetary Network)

Υπάρχει ένας αριθμός από θεμελιώδης διαφορές μεταξύ του περιβάλλοντος των επίγειων επικοινωνιών και του περιβάλλοντος που προβλέπεται για το IPN. Αυτές οι διαφορές περιλαμβάνουν καθυστερήσεις, χαμηλό και ασύμμετρο εύρος ζώνης, διακοπτόμενη συνδεσιμότητα και ένα σχετικά υψηλό ποσοστό λαθών. Αν ληφθούν τα παραπάνω υπόψη επηρεάζεται όλο το επικοινωνιακό μοντέλο, μετατοπίζοντας μας από το παραδοσιακό μοντέλο της "τηλεφωνίας" που διατρέχει τις παρούσες επικοινωνίες του Διαδικτύου στο "ταχυδρομικό" μοντέλο. Για αυτό πρώτα θα περιγραφούν οι περιβαλλοντικές διαφορές μεταξύ επίγειων επικοινωνιών και του IPN και θα δοθεί μια εξήγηση στο γιατί το πρωτόκολλο του Διαδικτύου για ασφαλή μεταφορά, TCP, δεν είναι κατάλληλο για απ'άκρου-εις-άκρου επικοινωνία μέσα στο IPN.

Η πιο προφανής διαφορά μεταξύ της επικοινωνίας στη Γη και της επικοινωνίας μεταξύ πλανητών είναι η καθυστέρηση. Ενώ οι χρόνοι αποστολής και λήψης (roundtrip) πακέτων στο επίγειο Διαδίκτυο κυμαίνονται από χιλιοστά του δευτερολέπτου σε μερικά δευτερόλεπτα, οι χρόνοι αποστολής-λήψης για τον Άρη κυμαίνονται από 8 σε 40 λεπτά, ανάλογα με τις θέσεις των πλανητών, και οι χρόνοι των roundtrips μεταξύ Γης και Ευρώπης κυμαίνονται μεταξύ 66 και 100 λεπτών. Παράλληλα με την καθυστέρηση μετάδοσης, η επικοινωνία σε διαπλανητικές αποστάσεις τη σημερινή εποχή χρειάζεται ειδικό εξοπλισμό (τεράστιες κεραίες, υψηλής απόδοσης δέκτες, κτλ). Για τις περισσότερες διαστημικές αποστολές ο

εξοπλισμός αυτός παρέχεται από το DSN (Deep-Space Network) της NASA. Οι επικοινωνιακοί πόροι του DSN όμως υπερχρησιμοποιούνται υπερβαίνοντας τις δυνατότητες εξυπηρέτησης των συνδρομητών του, και κατά πάσα πιθανότητα αυτή η κατάσταση θα συνεχίσει και στο μέλλον. Παρότι μελέτες έχουν γίνει σχετικά με την δυνατότητα αναβάθμισης ή αντικατάστασης του παρών DSN, ο αριθμός των διαστημικών αποστολών πιθανότατα θα συνεχίσει να μεγαλώνει γρηγορότερα από την επίγεια υποδομή που απαιτείται για την υποστήριξη τους, κάνοντας την υπερχρησιμοποίηση των πόρων του DSN ένα μόνιμο πρόβλημα.

Αυτή η υπερεκμετάλλευση σημαίνει ότι οι roundtrip χρόνοι των πακέτων θα επηρεάζονται όχι μόνο από την καθυστέρηση μετάδοσης, αλλά επίσης και από την καθυστέρηση των δρομολογήσεων και των σειρών αναμονής που επιβάλλονται από τους επίγειους πόρους. Συνεπώς πακέτα δρομολογημένα για ένα συγκεκριμένο προορισμό μπορεί να βρίσκονται σε σειρά αναμονής μέχρι την επόμενη προγραμματισμένη περίοδο επαφής με τον προορισμό, που μπορεί να γίνει σε ώρες, ημέρες ή ακόμη και εβδομάδες. Παρότι η καθυστέρηση που προκαλείται από δρομολογήσεις και σειρές αναμονής είναι γενικότερα προβλέψιμη και αναμενόμενη, οι μεγάλες και μεταβαλλόμενες καθυστερήσεις κάνουν την σχεδίαση των χρονοδιακοπτών (timers), και συγκεκριμένα των χρονοδιακοπτών αναμετάδοσης ιδιαίτερα δύσκολη. Αυτό το γεγονός πάλι διαμορφώνει μία απομάκρυνση από το παρών μοντέλο του Διαδικτύου, καθώς οι σχεδιασμένες για το IPN εφαρμογές πιθανότατα θα χρειαστούν τρόπους παρακολούθησης και εποπτείας της προόδου μίας εν εξέλιξη επικοινωνίας και της πληροφόρησης των χρηστών σχετικά με την αναμενόμενη καθυστέρηση. Αυτή η δυνατότητα θα περιπλεχθεί όταν το IPN μετατοπιστεί από την αρχική γεωκεντρική προσέγγιση του σε ένα peer-to-peer δίκτυο, από τη στιγμή που η ενημέρωση των χρηστών για την πρόοδο της επικοινωνίας τους θα καταναλώνει πολύτιμο bandwidth.

Ο συνδυασμός των τεράστιων αποστάσεων, της ακρίβειας και δυσκολίας εγκατάστασης μεγάλων κεραιών σε απομακρυσμένους πλανήτες, και η δυσκολία παραγωγής ενέργειας στο διάστημα, όλα συνηγορούν στο ότι το διαθέσιμο εύρος ζώνης του IPN πιθανότατα θα είναι κατώτερο των επίγειων συστημάτων. Ένα άλλο χαρακτηριστικό που επικρατεί στις σημερινές διαστημικές αποστολές είναι η ασυμμετρία του εύρους ζώνης, όπου τα δεδομένα μεταδίδονται σε διαφορετικούς ρυθμούς σε διαφορετικές κατευθύνσεις. Η σημερινές αποστολές συνήθως σχεδιάζονται με πολύ μεγαλύτερο ρυθμό μετάδοσης δεδομένων στην επιστροφή (από το διάστημα προς την Γη) από τον ρυθμό μετάδοσης των εντολών. Ο λόγος για αυτή την ασυμμετρία είναι απλός: κανένας ποτέ δεν θέλησε ένα υψηλού ρυθμού κανάλι εντολών, αντίθετα κρίθηκε καλύτερη η ύπαρξη ενός αξιόπιστου καναλιού εντολών παρά ενός γρήγορου. Αυτή η σχεδιαστική επιλογή έχει οδηγήσει σε ασυμμετρίες στο ρυθμό μετάδοσης της τάξεως του 100:1, μερικές φορές πλησιάζοντας το 1000:1. Η επιθυμία για ένα πολύ αξιόπιστο κανάλι εντολών πιθανότατα θα εξακολουθήσει να υπάρχει, έτσι ώστε οποιοδήποτε πρωτόκολλο μεταφοράς σχεδιασμένο για χρήση στο IPN θα πρέπει να λειτουργεί με ένα σχετικά χαμηλό εύρος ζώνης στο κανάλι εξόδου προς το διάστημα.

Οι δυσκολίες της παραγωγής ενέργειας πάνω και γύρω από άλλους πλανήτες θα έχει επίσης ως αποτέλεσμα υψηλούς ρυθμούς λαθών. Οι παρούσες διαστημικές αποστολές λειτουργούν με πάρα πολύ υψηλούς ρυθμούς λαθών (της τάξεως του 10e-1, ή ένα

λάθος σε κάθε δέκα bits)οι οποίοι μετά διορθώνονται με τη χρήση υψηλής κωδικοποίησης.

3.3 ΘΕΜΑΤΑ ΤΗΣ IPN ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ

3.3.1 Καθυστερήσεις από την ταχύτητα του φωτός

Η καθυστέρηση που προκαλείται από την ταχύτητα του φωτός μεταξύ Γης και Άρη, για παράδειγμα, είναι ακριβώς 4 λεπτά όταν η Γη και ο Άρης βρίσκονται στην μικρότερη απόσταση μεταξύ τους. Ο χρόνος του φωτός για να διατρέξει μία φορά την μεγαλύτερη απόσταση τους ξεπερνάει τα 20 λεπτά. Η καθυστέρηση της ταχύτητας του φωτός στους εξώτερους πλανήτες γίνεται πολύ μεγαλύτερη. (Η καθυστέρηση του φωτός για τον Δία κυμαίνεται μεταξύ 30 και 45 λεπτών, για τον Κρόνο μεταξύ 70 και 90 λεπτών). Όπως θα δούμε ,καθυστερήσεις αυτής της έκτασης έχουν σημαντική επίδραση στην εφαρμοσιμότητα της παραδοσιακής Διαδικτυακής πλατφόρμας σε διαπλανητικές αποστάσεις.

3.3.2 Επεισοδιακή Συνδεσιμότητα

Ο όρος "επεισοδιακή συνδεσιμότητα" αναφέρεται στην ικανότητα να εγκαθίσταται και να διατηρείται ένα συνεχές επικοινωνιακό κανάλι μεταξύ των τοπικών και απομακρυσμένων άκρων ενός δικτύου. Στο διαπλανητικό Διαδίκτυο δεν υπάρχει εγγύηση ότι κάποιο από τα άκρα μιας επικοινωνίας θα είναι στη Γη. Είναι κατανοητό ότι μια αποστολή σε αστεροειδή μπορεί να επικοινωνεί με ένα σταθμό στον Άρη, οπότε επόμενες αναφορές στο Deep Space Network είναι απλά για παράδειγμα και δεν αποτελεί τον κανόνα.

Σήμερα, το DSN χρησιμοποιεί τρεις κύριους επίγειους σταθμούς εξοπλισμένους με κεραίες 70 μέτρων υποστηρίζοντας τις διαστημικές αποστολές. Αυτοί οι τρεις επίγειοι σταθμοί είναι τοποθετημένοι σε διαστήματα 120 μοιρών μεταξύ τους πάνω στον πλανήτη (Goldstone, California, USA; Madrid, Spain; και Canberra, Australia) για να διασφαλιστεί ότι η περιστροφή της Γης δεν εμποδίζει την συνεχή ορατότητα. Αν ήταν δυνατό να διασφαλιστεί από κάποιον η συνεχής χρήση του DSN, θα μπορούσε να στοχεύει συνεχώς από την Γη στην επιφάνεια του Άρη. Η περίοδος περιστροφής του Άρη είναι λίγο πιο πάνω από αυτή της Γης, οπότε θα ήταν δυνατό να υπάρχει σύνδεση με ένα σημείο στην επιφάνεια του Άρη για μια περίοδο μέχρι και 12 ωρών τη φορά. Αν ένα σύνολο διασυνδεδεμένων δορυφόρων αναπτύσσονταν σε Αεροστατική τροχιά (το αντίστοιχο για τον Άρη της Γεωστατικής), θα ήταν δυνατό να διατηρηθεί συνεχής 24ωρη σύνδεση π.χ με ένα lander στην επιφάνεια του Άρη.

Παρ'όλ'αυτά, βραχυπρόθεσμα τέτοια συνδεσιμότητα δεν θα είναι εφικτή. Οι τροχιακές παρεμβολές, κατά τις οποίες τα τηλεπικοινωνιακά συστήματα χάνουν την "όρασή" τους λόγω των θέσεων των πλανητικών σωμάτων, είναι και θα συνεχίσουν να είναι μια σημαντική πηγή διακοπτόμενης συνδεσιμότητας μέσα στο διαπλανητικό Διαδίκτυο. Ακόμη και αν ένα σχετικά συνεχές τηλεπικοινωνιακό σύστημα μπορούσε να αναπτυχθεί για να υποστηρίξει την επικοινωνία μεταξύ Γης και Άρη, άλλα στοιχεία του διαπλανητικού Διαδικτύου δεν θα ήταν τόσο προνομιούχα στη διασύνδεσή τους. Σκεφτείτε μία αποστολή σε ένα αστεροειδή, στην οποία δεν δικαιολογείται η πολυδάπανη και πολύπλοκη υποδομή. Σε αυτήν την περίπτωση η

επικοινωνία με ένα απομακρυσμένο σύστημα μπορεί να εμποδίζεται από την περιστροφή του αστεροειδούς ή από την τροχιά του σκάφους.

Υπάρχουν και πρακτικά προβλήματα πού επιβάλλουν διακοπές σύνδεσης. Το DSN είναι υπερχρησιμοποιούμενο. Οι αποστολές πρέπει να δρομολογηθούν για εξυπηρέτηση από το DSN, και αυτά τα κομμάτια χρόνου σε καμία περίπτωση δεν αποτελούν αδιάκοπη συνδεσιμότητα. Πρέπει να σημειωθεί ότι το DSN δεν λειτουργεί σαν μέσο ευρείας εκπομπής (broadcasting), αλλά σαν απ'άκρου-εις-άκρου σύστημα επικοινωνίας. Οι κεραίες πρέπει να στοχεύσουν και να ακολουθήσουν το απομακρυσμένο σύστημα, ενώ ο χρόνος που απαιτείται για επανατοποθέτηση και επαναστόχευση είναι σεβαστός. (Ο τυπικός χρόνος για την φάση επανατοποθέτησης για μια συγκεκριμένη επαφή είναι μία με μιάμιση ώρα).

3.3.3 Ασύμμετροι Ρυθμοί Μετάδοσης

Ο όρος "ασύμμετροι ρυθμοί μετάδοσης" σημαίνει ότι ένα σύστημα μπορεί να έχει διαφορετικό ρυθμό μετάδοσης δεδομένων στην εξερχόμενη κίνησή του από ότι στην εισερχόμενη. Αυτή η περίπρωση δεν είναι συνηθισμένη στα σημερινά δίκτυα, αν και το ADSL και τα DirecPC συστήματα εμφανίζουν αυτό το χαρακτηριστικό σε ένα περιορισμένο βαθμό βέβαια. Το σύστημα DirecPC χαρακτηρίζεται από ασυμμετρία μέχρι και 15:1 (400000 bps λήψη, 28800 bps εκπομπή, ή 13.9:1), ενώ το ADSL εμφανίζει ασυμμετρία έως και 100:1 (π.χ 1.544 Mbps λήψη, 16000 bps εκπομπή, ή 96.5:1). Η ασυμμετρία στον ρυθμό μετάδοσης σε διαστημικές αποστολές είναι συνήθως της τάξεως του 1000:1 ή και περισσότερο.

3.3.4 Αναλογία Σήματος προς Θόρυβο (Signal to Noise Ratio-SNR)

Σε ένα σύστημα επικοινωνιών, ο πομπός στέλνει κάποια σύμβολα στον δέκτη, όπου κάθε σύμβολο αντιστοιχεί σε ένα αριθμό από bit πληροφορίας. Η δουλειά του δέκτη είναι να αποφασίσει, βασιζόμενος στο ληφθέν σήμα και τον θόρυβο, τι νομίζει ότι τα μεταδοθέντα σύμβολα ήταν ώστε να ανακατασκευάσει την αυθεντική ροή της πληροφορίας. Σε οποιοδήποτε σύστημα υπάρχει κάποιος θόρυβος που διαταράσσει το μεταδιδόμενο σήμα πριν αυτό φτάσει τον δέκτη. Αυτός ο θόρυβος μπορεί να αναγκάσει τον δέκτη να κάνει λάθη στις αποφάσεις του για τα ληφθέντα σύμβολα. Μία παράμετρος που αποτελεί μέτρο για το πόσο επιρρεπής είναι ο δέκτης στο να κάνει λάθη είναι η αναλογία του εισερχόμενου σήματος προς τον θόρυβο στον δέκτη, ή signal-to-noise ratio (SNR). Όσο μεγαλύτερο είναι το SNR, λιγότερο πιθανό είναι ο δέκτης να κάνει λάθος στην αποκωδικοποίηση κάποιου συμβόλου. Για ένα δεδομένο ρυθμό μετάδοσης, δεδομένη κωδικοποίηση, και σχέδιο διαμόρφωσης, υπάρχει μία χαρτογράφηση από το ληφθέν SNR των χαρακτηριστικών των λαθών της αποκωδικοποιημένης πληροφορίας. Όταν τα λάθη είναι σχετικά σπάνια και με μεγάλα κενά, είναι σωστό να αναφερόμαστε στο ρυθμό λαθών των bit (bit error rate-BER) του συστήματος σαν τον ρυθμό στον οποίο ο δέκτης κάνει λάθη στην αποκωδικοποιημένη ροή των bit. Ενώ τα συστήματα που βασίζονται στις οπτικές ίνες μπορούν να επιτύχουν χαμηλούς ρυθμούς λαθών έως και 10-12 με 10-15, οι διαστημικές αποστολές συνήθως λειτουργούν με μη κωδικοποιημένο BER της τάξεως του 10-1. Χρησιμοποιούν ένα σύνθετο κώδικα αποτελούμενο από έναν κώδικα με χαρακτηριστικά: rate 7, constraint-length 1/2 inner convolutional code και

ένα κώδικα με χαρακτηριστικά: 223,255 Reed-Solomon outer code ώστε να ρίξουν τον ρυθμό λαθών στο επίπεδο του 10-9 ή και λιγότερο.

3.3.5 Περίληψη

Από αυτά τα αρχιτεκτονικά θέματα,μόνο οι μικρές καθυστερήσεις θεωρούνται αμετάβλητες. Παρόλαυτα, για το προσεχές μέλλον, η επεισοδιακή συνδεσιμότητα θα συνεχίσει να υπάρχει, τουλάχιστον σε ορισμένες περιοχές του διαπλανητικού Διαδικτύου. Αυτό μπορεί να θεωρηθεί ανάλογο με την βαθμιαία εξέλιξη των διαδικτυακών δυνατοτήτων στις αναπτυσσόμενες περιοχές του πλανήτη σήμερα. Τέλος, οι ασύμμετροι ρυθμοί μετάδοσης και η χαμηλή αναλογία σήματος προς θόρυβο είναι επίσης δεδομένα που θα συνεχίσουν να υφίστανται, αν και η εξέλιξη στην μετατροπή ενέργειας θα κάνει αυτά τα ζητήματα λιγότερα σημαντικά.

3.4 Ένα Υποθετικό Διαδίκτυο στο Διάστημα.

Η προηγούμενη ενότητα περιέγραψε τα αρχιτεκτονικά χαρακτηριστικά του διαπλανητικού Διαδικτύου. Αυτή η ενότητα περιγράφει τις επιπτώσεις αυτών των χαρακτηριστικών στα διαδικτυακά πρωτόκολλα που χρησιμοποιούνται σήμερα.

Στην πιθανότητα χρήσης του TCP σε πολύ μεγάλες καθυστερήσεις, πρέπει να ληφθεί υπόψη ότι το TCP χρησιμοποιεί απ'άκρου-εις-άκρου σηματοδοσία προκειμένου να διατηρήσει μία συνεχής άποψη της κατάστασης των άκρων της σύνδεσης και του δικτύου. Αν υποτεθεί ότι το TCP μπορεί να διαμορφωθεί έτσι ώστε να λειτουργεί σε τόσο μεγάλες καθυστερήσεις (θεωρητικά δυνατό, αλλά όπως θα δούμε παρακάτω πρακτικά δύσκολο) μπορούμε να αποφύγουμε τις πιο πολλές δυσκολίες που αναπτύσσονται στα άκρα Παρ'όλαυτα, αυτή η θεωρία δεν παίρνει υπόψη της το γεγονός ότι το TCP πρέπει να αντιμετωπίσει τα προβλήματα και τις αλλαγές στην κατάσταση του δικτύου. Αυτή η ευθύνη είναι προβληματική σε περιβάλλοντα μεγάλων καθυστερήσεων, από τη στιγμή που το TCP χρησιμοποιεί απ'άκρου-εισ-άκρου σηματοδοσία για τους ελέγχους του. Το σήμα ενός γεγονότος(π.χ συμφόρηση) πρέπει να μεταδοθεί στον παραλήπτη (από ένα τυχαίο σημείο μεταξύ του αποστολέα και του παραλήπτη), και μετά να αναμεταδοθεί στον αποστολέα για απάντηση. Με το TCP, το σήμα συμφόρησης θεωρείται ένα χαμένο πακέτο, το οποίο όταν εντοπιστεί από τον παραλήπτη λόγω διακοπής στην αριθμητική ακολουθία, σηματοδοτείτε πίσω στην πηγή μέσω διπλών επιβεβαιώσεων (ACKs). Ο αποστολέας αντιδράει σε αυτό το σήμα κόβοντας τον ρυθμό αποστολής του στο μισό, το οποίο λαμβάνεται από το σημείο στο οποίο εκδηλώθηκε η συμφόρηση ακριβώς ένα roundtrip μετά από την αρχική εκπομπή του σήματος (ή χαμένου πακέτου).

3.5 Θεωρητικά Αποτελέσματα

Η επίτευξη των θεωρητικών αποτελεσμάτων γίνεται με την χρήση των εξισώσεων που αναλύονται στο έργο του M. Mathis "The Macroscopic Behavior of the TCP Congestion Avoidance Algorithm" για να χαρακτηρίσουμε ένα ανώτατο όριο για

την απόδοση των διακινούμενων δεδομένων (throughput) που είναι δυνατό να υποστηριχθούν σαν αποτέλεσμα των μηχανισμών ελέγχου συμφόρησης του TCP. Οι εικόνες 1 και 2 δείχνουν το ανώτατο όριο στον ρυθμό δεδομένων που μπορεί να επιτευχθεί βάση αυτών των εξισώσεων, οι οποίες εφαρμόστηκαν στους σχετικά μεγάλους χρόνους της ταχύτητας του φωτός, που σχετίζεται με την διαπλανητική επικοινωνία. Η εικόνα 1 δείχνει την περίπτωση όπου η πιθανότητα να χαθεί κάποιο πακέτο είναι υπερβολικά μικρή (κατά μέσο όρο 1 πακέτο στα 100 εκατομμύρια θεωρείται χαμένο). Η αιτία της απώλειας είναι αδιάφορη. Μπορεί να προέρχεται από συμφόρηση του δικτύου, από αλλοίωση της πληροφορίας του πακέτου κτλ. Από τη στιγμή πού το μέσο μήκος μίας σύνδεσης TCP είναι πολύ λιγότερο από 100 εκατομμύρια πακέτα, πρέπει να σημειωθεί ότι το στιγμιαίο throughput μπορεί να ξεπεράσει αυτό το ανώτατο όριο. Η εικόνα 2 δείχνει το ανώτατο όριο του throughput υποθέτοντας ότι η πιθανότητα να χαθεί πακέτο είναι 1 στα 5000 (αυτή η εικόνα προέκυψε από το έργο του V. Paxson “Measurements and Analysis of End-to-End Internet Dynamics”, ως ο ρυθμός αλλοίωσης των πακέτων στο Διαδίκτυο). Αυτές οι εικόνες δείχνουν το όριο που καθορίζεται από τον αλγόριθμο αποφυγής συμφόρησης του TCP στο throughput. Να σημειωθεί ότι από τη στιγμή που οι πιο πολλές συνδέσεις αποτελούνται από λιγότερα από 100 εκατομμύρια πακέτα σε διάρκεια, και στην πραγματικότητα είναι λιγότερο από 5000 πακέτα σε διάρκεια, τα αποτελέσματα που παρουσιάζονται εδώ πιθανότατα δεν θα επηρεάζουν σε απόλυτο βαθμό την απόδοση μιας TCP σύνδεσης. Αντίθετα, τα αποτελέσματα από την έναρξη του αργού στο ξεκίνημα αλγόριθμου του TCP θα έχουν πολύ μεγαλύτερη επίδραση.

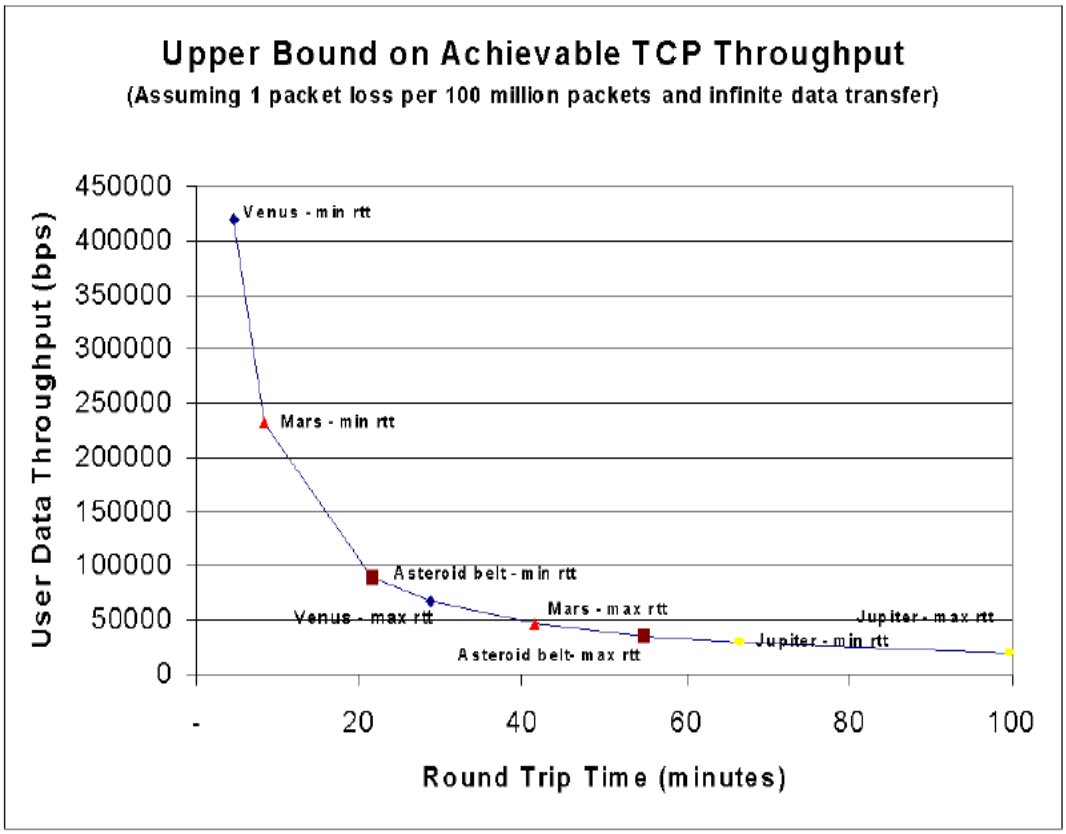


Figure 1. Upper Bound On TCP Throughput for Various Interplanetary Round Trip Times Assuming 1e-8 Packet Loss Rate

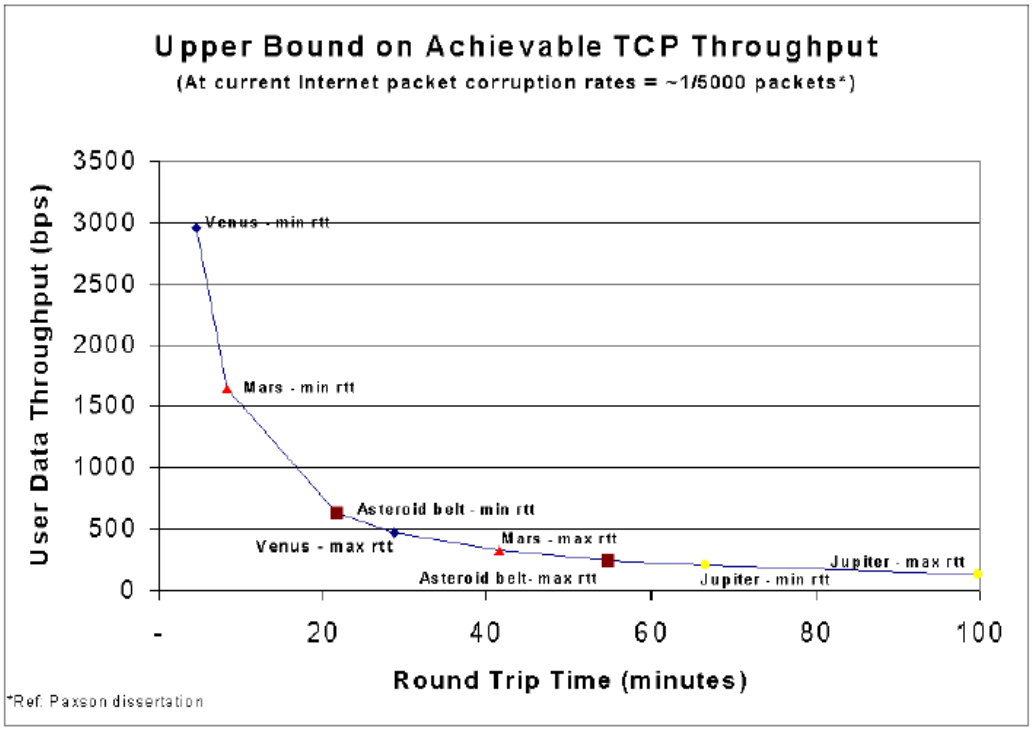


Figure 2. Upper Bound On TCP Throughput for Various Interplanetary Round Trip Times Assuming 2e-4 Packet Loss Rate

Οι εικόνες 3 και 4 παρουσιάζουν τα αποτελέσματα του αλγόριθμου του TCP σε ένα στιγμιαίο ρυθμό μετάδοσης και στο ποσοστό χρησιμοποίησης του καναλιού αντίστοιχα. Τα στοιχεία που έχουμε ως δεδομένα είναι μία καθυστέρηση 240 δευτερολέπτων μίας κατεύθυνσης (κάτι λιγότερο από την κοντινότερη προσέγγιση του Άρη), και ένα κανάλι του 1 Mbps. Η εικόνα 3 δείχνει ότι, μετά από μία ώρα λειτουργίας, ο στιγμιαίος ρυθμός μετάδοσης της TCP σύνδεσης είναι ακόμη πολύ κάτω από τα 5 kbps. (Οι εικόνες 3 και 4 δεν υπολογίζουν την καθυστέρηση από την εγκατάσταση της σύνδεσης). Η αιτία του χαμηλού ρυθμού μετάδοσης είναι το γεγονός ότι ο αργός αλγόριθμος του TCP εμποδίζει το ρυθμό μετάδοσης με το να αυξήσει το ρυθμό κατά ένα επιπλέον πακέτο ανά επιβεβαίωση που δέχεται. Καθώς ο χρόνος ενός roundtrip αυξάνεται, ο στιγμιαίος ρυθμός επηρεάζεται αντίθετα, δηλαδή μειώνεται. Παρομοίως, η εικόνα 4 δείχνει το ποσοστό χρησιμοποίησης ενός καναλιού 1 Mbps. Μετά από ακριβώς μία ώρα λειτουργίας, το κανάλι χρησιμοποιείται λιγότερο από 0.3%. Λαμβάνοντας υπόψη το χρόνο που θέλει για να μετακινηθεί ένα κομμάτι δεδομένων, στο παράδειγμα μπορεί να μεταφερθεί ακριβώς 1 MByte δεδομένων σε 90 λεπτά μέσω ενός καναλιού 1 Mbps.

Να σημειωθεί εδώ ότι η χρήση του DNS (Domain Name System) σε δίκτυα με μεγάλες καθυστερήσεις ενέχει έναν αριθμό από σημαντικά προβλήματα. Αν μία εφαρμογή σε έναν απομακρυσμένο πλανήτη ήθελε να επιλύσει ένα όνομα τοποθεσίας στη Γη σε μια διεύθυνση, θα μπορούσε να χρησιμοποιήσει έναν από τους τρεις τρόπους που υπάρχουν σήμερα στο Διαδίκτυο: Θα μπορούσε να θέσει ερώτημα σε έναν name server (διακομιστή DNS) στην Γη. Θα μπορούσε να θέσει ερώτημα σε έναν τοπικό δευτερεύων name server. Ή θα μπορούσε να διατηρεί μία στατική λίστα από ονόματα host ή διευθύνσεις. Ρωτώντας έναν name server στη Γη έχει σαν αποτέλεσμα μία καθυστέρηση ίση με τον χρόνο ενός roundtrip κατά την έναρξη της επικοινωνίας. Αυτή η καθυστέρηση μπορεί να είναι σημαντική όσον αφορά τον διαθέσιμο χρόνο επικοινωνίας, καθότι οι καθυστερήσεις είναι μεγάλες και η διάρκεια των επαφών είναι συνήθως μικρή. Εναλλακτικά, θα μπορούσε να διατηρείται ένας δευτερεύων server τοπικά, αλλά οι ενημερώσεις (updates) των ζωνών του δικτύου θα απασχολούσαν ολόκληρο το κανάλι επικοινωνίας εξαιρώντας άλλα δεδομένα. Τέλος, θα μπορούσε να διατηρείται μία στατική λίστα με τα ονόματα των host, αλλά αυτή η λύση έχει το μειονέκτημα ότι δεν αποδίδει το ίδιο καλά όσο το δίκτυο μεγαλώνει. Μία ελκυστική λύση είναι να χρησιμοποιηθεί ένα σύστημα παρόμοιο με τον Mail Exchanger του Domain Name System,όπου καθορίζεται ένας ενδιάμεσος host για να επικοινωνήσει σε περίπτωση που ο πρωταρχικός host είναι μη προσβάσιμος.

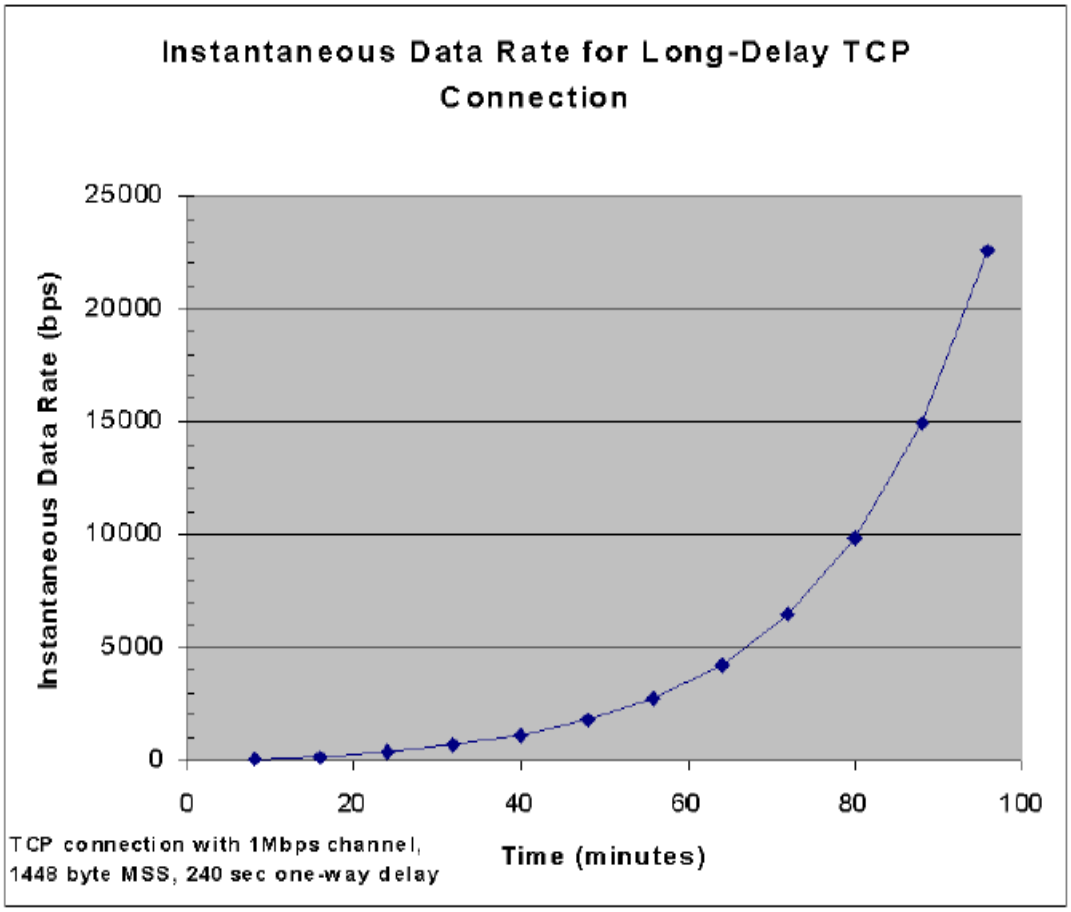


Figure 3. Instantaneous Data Rate for TCP Connection with Eight-Minute RTT)

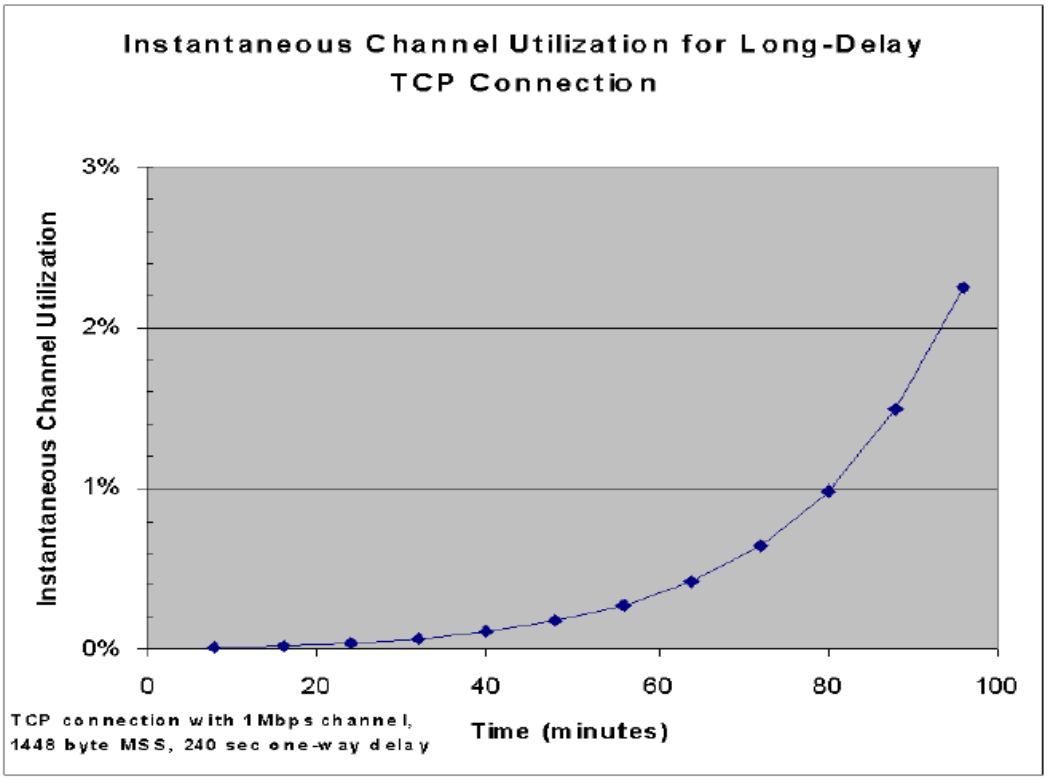


Figure 4. Instantaneous Channel Utilization for TCP Connection with Eight Minute RTT and 1 Mbps Channel

3.6 Εργαστηριακά Αποτελέσματα

Τα αποτελέσματα αυτής της ενότητας βασίζονται σε εργαστηριακά τεστ όπου χρησιμοποιήθηκε ένας εξομοιωτής BER (bit-error-rate) και καθυστέρησης με hosts που έτρεχαν εμπορικές υλοποιήσεις διαδικτυακών πρωτοκόλλων. Ελέγχθηκε η μεταφορά αρχείων (μέσω του FTP), και το ηλεκτρονικό ταχυδρομείο (μέσω του SMTP).

3.6.1 Χαρακτηριστικά του Εξεταζόμενου Συστήματος

Η εικόνα 5 δείχνει την διαμόρφωση του συστήματος που χρησιμοποιήθηκε για να συγκεντρωθούν τα αποτελέσματα . Ο εξομοιωτής βάζει σε σειρά αναμονής πακέτα βασιζόμενος στο μέγεθος της σειράς και στον χρόνο εξυπηρέτησης για κάθε πακέτο. Ένα Ethernet LAN φιλοξενεί όλα τα τερματικά που χρησιμοποιήθηκαν στο τεστ, και ο εξομοιωτής ζεύξης είναι διαμορφωμένος για ρυθμό δεδομένων 1000000 bps προς κάθε κατεύθυνση. Να υπενθυμίσουμε ότι οι ρυθμοί μετάδοσης δεδομένων είναι συνήθως ασύμμετροι. Παρόλαυτα , στο συγκεκριμένο πείραμα δεν υπάρχουν τέτοιοι περιορισμοί στο τηλεπικοινωνιακό σύστημα, ούτε εισήχθησαν σημαντικοί ρυθμοί λαθών.

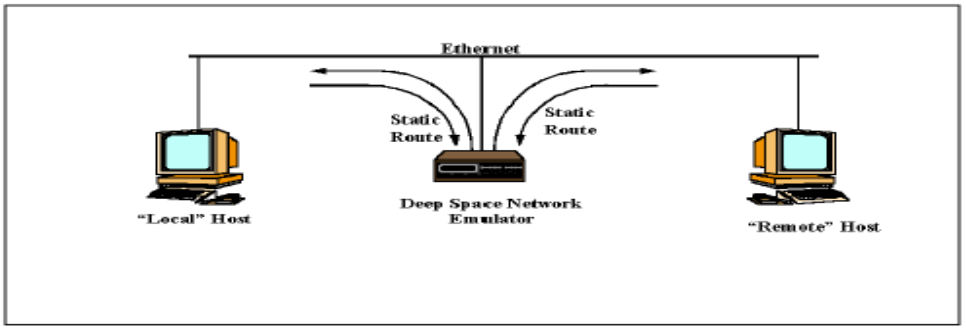


Figure 5. Laboratory Test Configuration for End-to-End Internet Testing

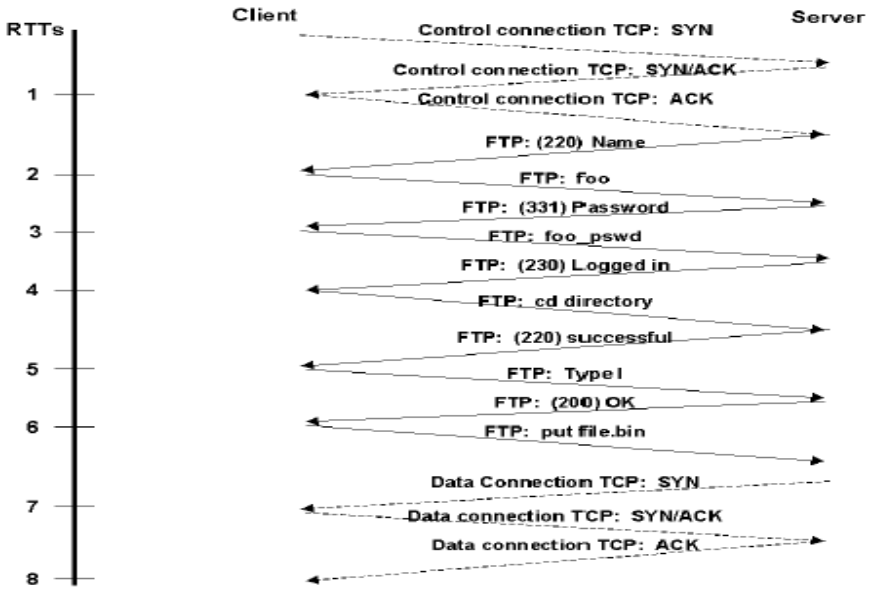


Figure 6. Typical Interaction Between FTP Client and Server

3.6.2 Παράδειγμα: Μεταφορά Αρχείου

Η εικόνα 6 δείχνει την τυπική ροή μίας σύνδεσης FTP για την λήψη ή αποστολή ενός αρχείου. Να σημειωθεί ότι χρειάζονται τυπικά οκτώ roundtrips για να ξεκινήσουν τα δεδομένα του αρχείου να μεταδίδονται. Παρόλο που αυτό το χρονικό διάστημα δεν δείχνει μεγάλο, σκεφτείτε την περίπτωση όπου κάθε roundtrip διαρκεί οκτώ λεπτά. Αυτό σημαίνει ότι πάνω από μία ώρα θα περάσει πριν αρχίσει πραγματικά η μεταφορά του αρχείου. (Θυμηθείτε ότι το roundtrip για τον Άρη είναι το λιγότερο 8.5 λεπτά, και ότι κυμαίνεται μεταξύ 8.5 και 40 λεπτών, που σημαίνει ότι η ίδια διαδικασία μπορεί να πάρει πάνω από 5 ώρες για να ξεκινήσει. Επίσης πρέπει να τονιστεί ότι στη σημερινή πραγματικότητα είναι γεγονός ότι ο χρόνος του DSN που αντιστοιχεί σε κάθε χρήστη είναι περιορισμένος, και ότι πιθανότατα η διαδικασία μεταφοράς ενός αρχείου δεν θα τελειώσει ή ούτε καν θα αρχίσει αφού ο χρόνος που αντιστοιχεί στον χρήστη θα έχει τελειώσει.)

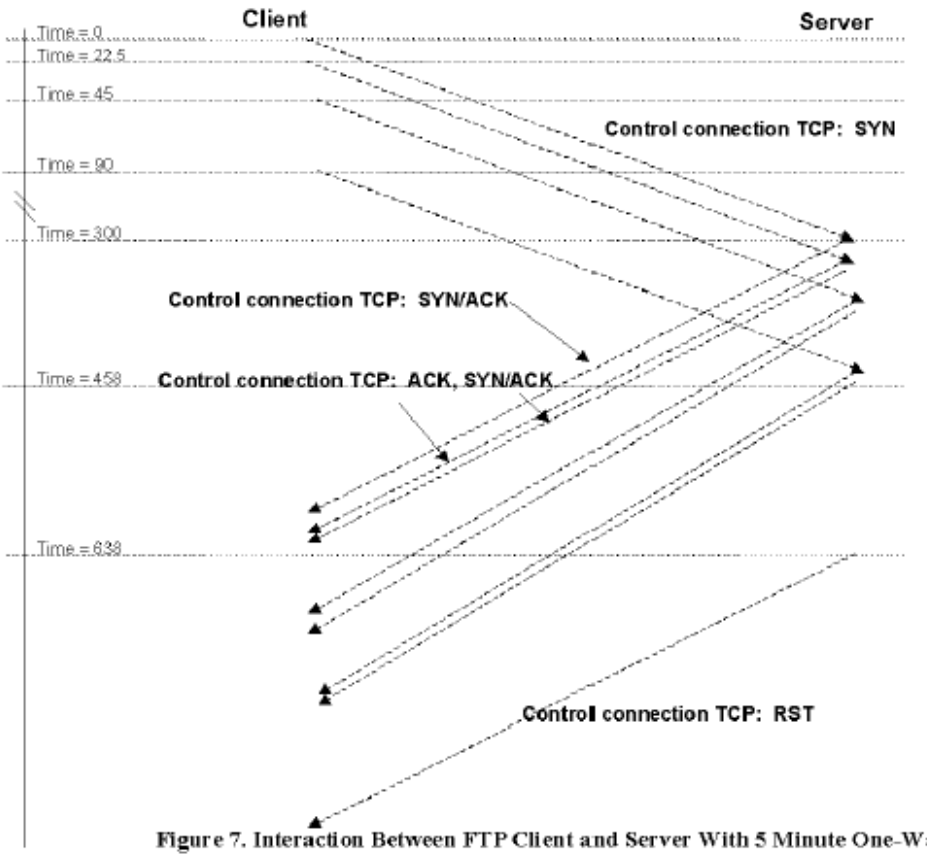


Figure 7. Interaction Between FTP Client and Server With 5 Minute One-Way Delay, Minimum RTO = 20sec (max value settable in Solaris 2.7)

Η εικόνα 7 δείχνει την πραγματική συναλλαγή των πακέτων μεταξύ δύο host που επιχειρούν μία συνομιλία FTP επί μίας καθυστέρησης 5 λεπτών και μίας κατεύθυνσης. Τα λειτουργικά και στους 2 host ήταν Solaris 2.7 και η τιμή για τον μικρότερο χρόνο αναμετάδοσης στα TCP σε κάθε host καθορίστηκε στην μέγιστη δυνατή τιμή των 20 δευτερολέπτων. Το ακόλουθο απόσπασμα από τον κανονισμό RFC 1123 έχει σαν σκοπό να εμποδίσει τους διακομιστές FTP από το να περιμένουν αιώνια έναν πελάτη που έχει crashάρει. Συνιστά οι διακομιστές FTP να υιοθετούν μία διαδικασία διακοπής λόγω απραγίας (idle timeout) και προτείνει η μικρότερη τιμή διακοπής να είναι μεγαλύτερη ή ίση με 5 λεπτά (στην πραγματικότητα,πολλοί διακομιστές χρησιμοποιούν μια τιμή 900 δευτερολέπτων ή 15 λεπτών).

4.1.3.2 Idle Timeout

> A Server-FTP process SHOULD have an idle timeout, which will Terminate the process and close the control connection if the server is inactive (i.e., no command or data transfer in progress) for a long period of time. The idle timeout time SHOULD be configurable, and the default should be at least 5 minutes.

Η περιγραφή της απραγίας έχει σημασία: “no command or data transfer in progress.” Στην εικόνα 8 η μετάδοση του μηνύματος 230 που τελειώνει το τρίτο roundtrip ολοκληρώνει την εντολή μεταφοράς απο την οπτική γωνία του διακομιστή. Ο

διακομιστής δεν έχει τρόπο να ρωτήσει τον πελάτη για να εξακριβώσει ότι το μήνυμα δεν έχει επιβεβαιωθεί, και πιστεύει ότι η σύνδεση έχει παύσει. Θα πάρει τουλάχιστον ένα roundtrip από τη στιγμή που το μήνυμα 230 εστάλη μέχρι να ληφθεί κάποια εντολή από τον πελάτη. Αν αυτός ο χρόνος ξεπεράσει τα 5 λεπτά , ο διακομιστής μπορεί να τερματίσει την σύνδεση λόγω απραγίας και να είναι σε απόλυτη προσαρμογή με το πνεύμα του RFC 1123. Από τη στιγμή που δεν θα διαμορφωθούν (και δεν πρέπει) όλοι οι διακομιστές FTP για να υποστηρίζουν τους χρόνους απραγίας του διαπλανητικού Διαδικτύου, αυτό αποτελεί ένα μεγάλο πρόβλημα στην απ'άκρου-εις-άκρου χρήση του FTP.

Γενικότερα, το FTP πιθανώς δεν θα λειτουργήσει καν σε περιβάλλοντα με μεγάλες καθυστερήσεις , αλλά ακόμα και αν λειτουργήσει θα είναι απελπιστικά αναποτελεσματικό.

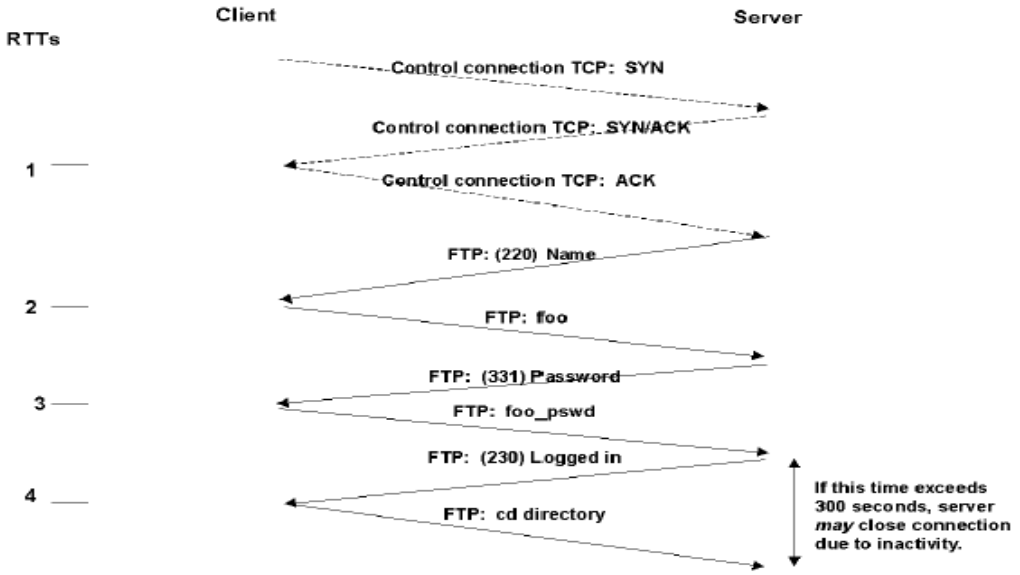


Figure 8. Effects of FTP Application Level Timers on Long Delay Connections

3.6.3 Παράδειγμα: Μεταφορά Ηλεκτρονικού Ταχυδρομείου

Από όλες τις υπάρχουσες εφαρμογές του Διαδικτύου, το πρωτόκολλο SMTP(Simple Mail Transfer Protocol) μοιάζει να είναι το πιο αρμόζον για την χρήση σε ένα διαπλανητικό περιβάλλον, χάρη στην λογική αποθήκευσης και προώθησης (store-and-forward)που το χαρακτηρίζει. Αυτή η συμπεριφορά αποθήκευσης και προώθησης είναι ιδανική για την λειτουργία σε περιβάλλοντα όπου δεν υπάρχει συνεχής σύνδεση μεταξύ όλων των hosts. Το μοντέλο SMTP εξελίχθηκε για να αντιμετωπίσει αυτά τα προβλήματα, αν και οι λόγοι για την διακοπτόμενη συνδεσιμότητα ήταν διαφορετικοί από αυτούς του διαπλανητικού Διαδικτύου. Παρόλαυτα βλέπουμε ότι ενώ το μοντέλο του ηλεκτρονικού ταχυδρομείου είναι ιδανικό για τις διαπλανητικές επικοινωνίες, το SMTP σαν πρωτόκολλο δυστυχώς δεν είναι.

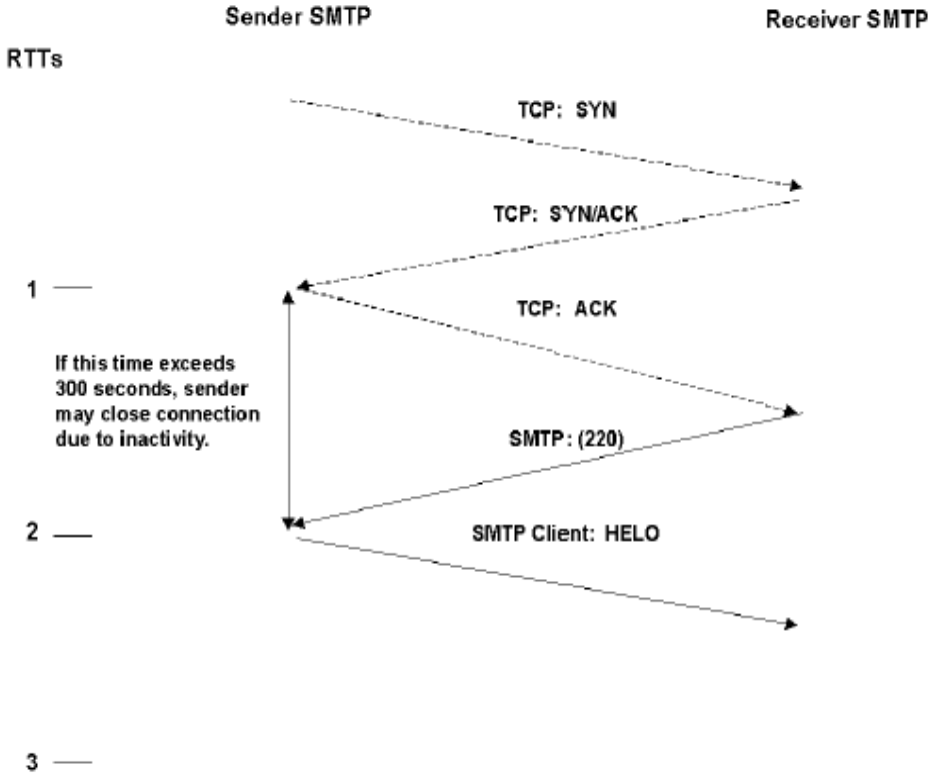


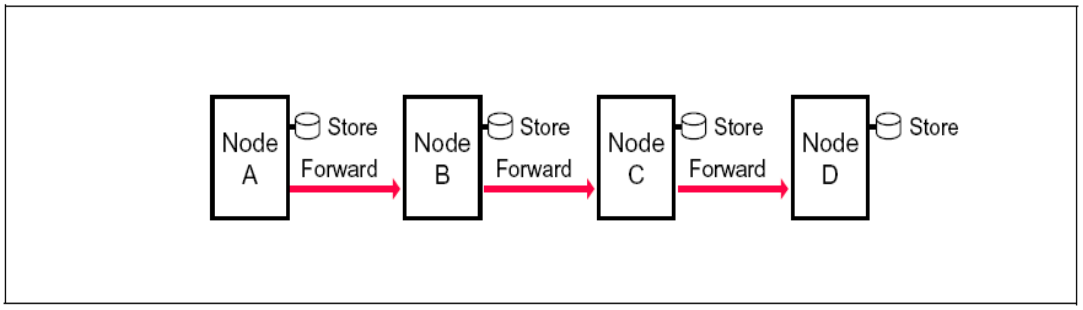
Figure 9. Effects of SMTP Application Level Timers on Long Delay Connections

Παρόμοια με το FTP, το RFC 1123 καθορίζει τα timeouts και για τους αποστολείς του SMTP. Το αρχικό περιθώριο είναι το λιγότερο 5 λεπτά, και όπως φαίνεται στην εικόνα 9, αν ο χρόνος του roundtrip είναι μεγαλύτερος , ο αποστολέας έχει το ελεύθερο να θεωρήσει ότι ο παραλήπτης δεν απαντάει και να διακόψει την σύνδεση. Ακόμη, οι παραλήπτες που χρησιμοποιούν το SMTP πρέπει (σύμφωνα με το RFC 1123) να έχουν περιθώρια που θα καθορίζουν πόσο πρέπει να περιμένουν για εντολές από τον αποστολέα. Σαν αποτέλεσμα, και οι δύο SMTP οντότητες θα πρέπει να διαμορφωθούν στις διαπλανητικές απαιτήσεις.

Επίσης παρόμοια με το FTP, υπάρχει μεγάλη αλληλεπίδραση και συνομιλία μεταξύ των συμμετεχόντων σε έναν διάλογο SMTP. Η αλληλεπίδραση αυτού του είδους είναι ακατάλληλη για τις μεγάλες καθυστερήσεις που περιλαμβάνει το διαπλανητικό περιβάλλον. Παρόλαυτα το μοντέλο του σύγχρονου e-mail, ή αλλιώς η τεχνική της μεταγωγής μηνύματος μέσω της προώθησης και αποθήκευσης(store-and-forward message switching), είναι κατάλληλο.

3.7 Επίλογος: Μεταγωγή Μηνύματος μέσω Προώθησης και Αποθήκευσης

Τα δίκτυα DTN ξεπερνούν τα προβλήματα που σχετίζονται με την διακοπτόμενη συνδεσιμότητα, τις μεγάλες ή μεταβαλλόμενες καθυστερήσεις, τους ασύμμετρους ρυθμούς μετάδοσης και τους υψηλούς ρυθμούς λαθών χρησιμοποιώντας την μεταγωγή μηνύματος μέσω της προώθησης και αποθήκευσης.Αυτη είναι μια παλιά μέθοδος χρησιμοποιούμενη από τα ταχυδρομικά συστήματα από την αρχαιότητα. Ολόκληρα μηνύματα (ολόκληρα κομμάτια από δεδομένα χρηστών) -ή κομμάτια από τέτοια μηνύματα- μετακινούνται (προωθούνται) από τον αποθηκευτικό χώρο ενός κόμβου στον αποθηκευτικό χώρο ενός άλλου κόμβου, ακολουθώντας μια διαδρομή που τελικά καταλήγει στον παραλήπτη. Οι μέθοδοι αποθήκευσης και προώθησης χρησιμοποιούνται σήμερα στα συστήματα ηλεκτρονικού ταχυδρομείου, αν και αυτά τα συστήματα δεν είναι σχηματισμοί μιας κατεύθυνσης (όπως φαίνεται παραπάνω) αλλά σχηματισμοί άστρου. Και η πηγή και ο προορισμός ανεξάρτητα επικοινωνούν με μία κεντρική αποθηκευτική μονάδα στο κέντρο των ζεύξεων.



Οι αποθηκευτικοί χώροι (όπως σκληροί δίσκοι) μπορούν να κρατούν τα μηνύματα επ' άπειρον. Παίρνουν τον χαρακτηρισμό μόνιμη αποθήκευση (persistent storage), σε αντίθεση με την προσωρινή αποθήκευση των κυκλωμάτων μνήμης. Οι δρομολογητές του Διαδικτύου χρησιμοποιούν την προσωρινή μνήμη για να αποθηκεύσουν τα εισερχόμενα πακέτα για μερικά χιλιοστά του δευτερολέπτου καθώς περιμένουν για την επόμενη δρομολόγηση (ερευνώντας τον πίνακα δρομολόγησης τους και κάποιο διαθέσιμο port εξερχόμενης κίνησης).

Οι δρομολογητές ενός DTN χρειάζονται μόνιμη αποθήκευση για τις σειρές αναμονής τους για έναν ή περισσότερους από τους ακόλουθους λόγους: Μία ζεύξη για την επόμενη μετάδοση του πακέτου μπορεί να μην είναι διαθέσιμη για πολύ καιρό, ένας κόμβος μπορεί να δέχεται ή να στέλνει δεδομένα πολύ πιο γρήγορα ή πιο αξιόπιστα από τον άλλο κόμβο, ένα μήνυμα μόλις μεταδοθεί μπορεί να χρειαστεί να αναμεταδοθεί αν υπάρξει λάθος κατά την διαδρομή του προς ένα άλλο κόμβο ή αν ο κόμβος που πρόκειται να το δεχτεί αρνηθεί για οποιοδήποτε λόγο την παραλαβή του μηνύματος.

Με την μεταφορά ολόκληρων μηνυμάτων (ή κομματιών) σε μία μεταφορά, η τεχνική μεταγωγής μηνύματος παρέχει τους κόμβους του δικτύου με άμεση γνώση του μεγέθους των μηνυμάτων, και για αυτό δημιουργούνται οι προϋποθέσεις για ενδιάμεσο αποθηκευτικό χώρο

4 CCSDS File Delivery Protocol (CFDP)

4.1 Εισαγωγή

Για ακριβώς 20 χρόνια, η Συμβουλευτική Επιτροπή για Διαστημικά Συστήματα Δεδομένων, ή αλλιώς CCSDS (Consultative Committee for Space Data Systems) – ένας διεθνής οργανισμός που υποστηρίζεται από 34 διαστημικές υπηρεσίες- ανέπτυσσε ένα βασικό σύνολο από τεχνικές επικοινωνίας στο διάστημα , οι οποίες τώρα είναι σε ευρεία χρήση στον κόσμο της διαστημικής κοινότητας. Στην πραγματικότητα, πάνω από 200 αποστολές έχουν δρομολογηθεί για να χρησιμοποιήσουν τις δυνατότητες της CCSDS.

Οι εργασίες τυποποίησης τις CCSDS καλύπτουν πέντε περιοχές λειτουργίας, όπως φαίνεται στο σχήμα 1.

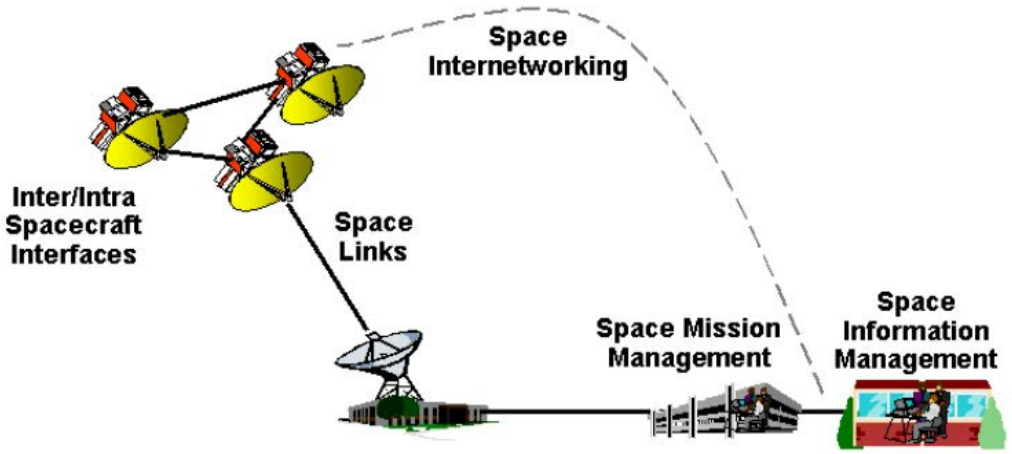


Figure 1: CCSDS Standardization Domains

1. Διεπαφές χειρισμού δεδομένων μέσα ή μεταξύ διαστημοπλοίων, συμπεριλαμβανομένων των μηχανισμών που επιτρέπουν σε ένα φορτίο να συνδεθεί στο σύστημα δεδομένων του σκάφους ή σε ένα προσεδαφισμένο όχημα να συνομιλήσει με έναν δορυφόρο μέσω μίας διαστημικής ζεύξης.
2. Ζεύξη δεδομένων που συνδέει ένα διαστημόπλοιο με το επίγειο σύστημα του.
3. Απ' άκρου-εις-άκρου διαδρομές δεδομένων που υλοποιούν αυτές τις διαστημικές ζεύξεις προκειμένου να υποστηρίξουν τη ροή των δεδομένων μεταξύ εδάφους και διαστήματος.
4. Υπηρεσίες διοίκησης αποστολών (όπως χειρισμό και έλεγχο συστημάτων) που μετατίθενται από ένα οργανισμό σε άλλον.
5. Υπηρεσίες διάδοσης δεδομένων για περιγραφή,διαμοιρασμό και αρχειοθέτηση της επιστημονικής πληροφορίας που λαμβάνεται από κάθε αποστολή.

Αυτή η ενότητα επικεντρώνεται στις τρεις πρώτες κατηγορίες των προτύπων δηλαδή στην μεταφορά της πληροφορίας από και προς το διάστημα.

4.2 Δυνατότητες τις CCSDS

Τα πρότυπα της επικοινωνίας στο διάστημα που έχει καθορίσει η CCSDS είναι διαμορφωμένα σε επίπεδα έτσι ώστε να σχηματίζουν μία στοίβα μεταξύ τους όπως δείχνει η εικόνα 2. Τα επίπεδα της διαστημικής επικοινωνίας είναι έτσι οργανωμένα ώστε να παραπέμπουν στο πολύ γνωστό μοντέλο του OSI (Open Systems Interconnection).

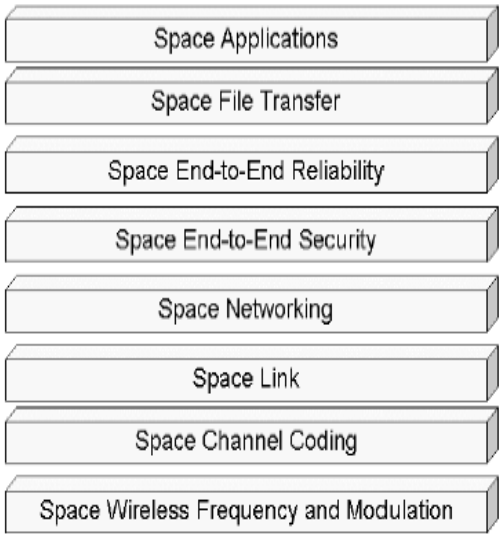


Figure 2: Space Protocol Stack

Στην κορυφή της στοίβας βρίσκονται οι εφαρμογές των χρηστών που τρέχουν σε υπολογιστές στο διάστημα ή στο έδαφος. Όταν δύο εφαρμογές πρέπει να ανταλλάξουν πληροφορίες, στηρίζονται στα επίπεδα πρωτοκόλλων επικοινωνιών που βρίσκονται από κάτω τους. Αυτά τα επίπεδα περιέχουν πολλαπλές επιλογές που μπορούν να επιλεχθούν για να εξυπηρετηθούν οι ανάγκες των αποστολών, και πολλά από τα επίπεδα μπορούν να μην χρησιμοποιηθούν αν δεν απαιτείται.

Ασύρματα Πρότυπα. Αυτά τα πρότυπα καθορίζουν τις συχνότητες και τους αποτελεσματικούς τύπους διαμόρφωσης που θα χρησιμοποιηθούν για να δημιουργηθεί το κανάλι που θα συνδέει το διαστημόπλοιο με τους επίγειους σταθμούς του ή με άλλα διαστημόπλοια.

Πρότυπα Κωδικοποίησης. Αυτές οι δυνατότητες "καθαρίζουν" τα λάθη από αυτά τα ασύρματα κανάλια και τα κάνουν καταλληλότερα για αυτόματη μεταφορά δεδομένων. Τα πρότυπα κωδικοποίησης της CCSDS περιλαμβάνουν μια ποικιλία από υψηλής απόδοσης τεχνολογίες όπως Convolutional κώδικες, Reed-Solomon και Turbo.

Πρότυπα Ζεύξης. Αυτά είναι τα "πλαίσια" που μεταφέρουν δεδομένα υψηλοτέρων επιπέδων διαμέσου της διαστημικής ζεύξης και καθορίζονται από πρότυπα Τηλεμετρίας και Τηλεντολών πακέτων της CCSDS(Packet Telemetry, Packet Telecommand). Το CCSDS Telecommand παρέχει αξιοπιστία μέσω ενός

πρωτοκόλλου αναμετάδοσης πλαισίων ‘go-back-n’ , που λέγεται Command Operation Procedure (COP). Το σύστημα AOS (Advanced Orbiting Systems) επεκτείνει την Τηλεμετρία Πακέτων ώστε να μπορεί να χειριστεί υψηλού ρυθμού μετάδοση δεδομένων, και χρησιμοποιείται από τον Διεθνή Διαστημικό Σταθμό και από πολλές αποστολές σε τροχιά γύρω από την Γη. Ένα νέο πρωτόκολλο ονόματι CCSDS Proximity-1, παρέχει αξιόπιστη επικοινωνία μικρής εμβέλειας, όπως μεταξύ προσεδαφισμένων οχημάτων και δορυφόρων, ή μεταξύ πολλών διαστημοπλοίων που βρίσκονται σε σχηματισμό. Προέρχεται από το CCSDS Telecommand και παρέχει αμφίδρομη αξιοπιστία του επιπέδου ζεύξης μέσω ενός παράγωγου του σχεδίου αναμετάδοσης COP.

Πρότυπα Δικτύωσης. Η ζεύξη στο διάστημα είναι απλά ένα στοιχείο της απ’άκρου-εις-άκρου διαδρομής των δεδομένων μεταξύ ενός διαστημοπλοίου και ενός χρήστη. Προκειμένου να περάσει όλη τη διαδρομή, η πληροφορία δρομολόγησης πρέπει να συσχετιστεί με κάθε κομμάτι των δεδομένων του χρήστη. Το πακέτο CCSDS (το “packet” τμήμα του Packet Telemetry and Telecommand) χρησιμοποιείται σαν δικτυακό πρωτόκολλο για το CCSDS για πάνω από μια δεκαετία. Εκμεταλλεύεται το γεγονός ότι για τις πιο πολλές σημερινές αποστολές υπάρχει μία υψηλά προβλέψιμη διαδρομή δρομολόγησης των δεδομένων μεταξύ ενός οργάνου και ενός χρήστη, οπότε είναι μικρή η ανάγκη για προσαρμοζόμενη δρομολόγηση των πακέτων. Το σύνολο των CCSDS προτύπων που έχουν περιγραφεί ως τώρα αντιπροσωπεύουν αυτά που χρησιμοποιούνται από την πλειοψηφεία των σημερινών αποστολών.
Οι λεπτομέρειες της στοίβας φαίνονται στην εικόνα 3. Κάθε ένα τετράγωνο αντιπροσωπεύει μια υπηρεσία στην οποία μπορεί να έχει πρόσβαση μία εφαρμογή χρήστη που επιθυμεί να επικοινωνήσει διαμέσου μιας ζεύξης στο διάστημα.

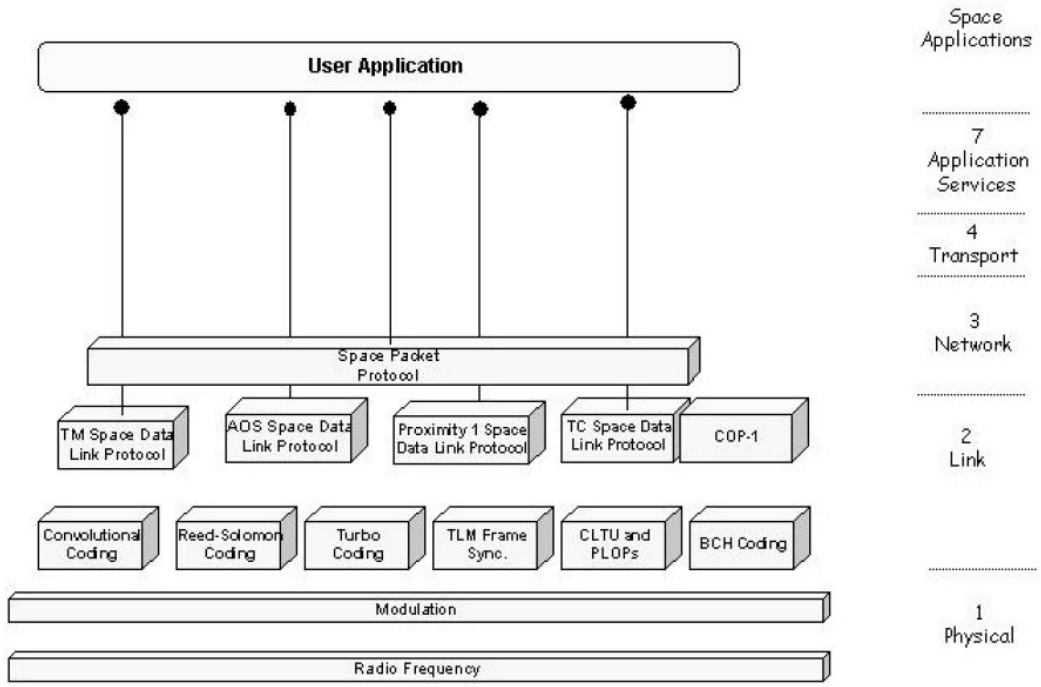


Figure 3: Typical Current CCSDS Stack

Πρόσφατα, το CCSDS πρόσθεσε την δυνατότητα να επιτρέπεται στα συστήματα των αποστολών να έχουν την δικιά τους διεύθυνση IP στο Διαδίκτυο. Αυτό επιτυγχάνεται είτε με την απευθείας χρήση του πρωτοκόλλου IP, ή από μια μορφή του IP που ονομάζεται Network Protocol (NP),και που είναι στοιχείο μίας τεσσάρων μερών στοίβας πρωτοκόλλων γνωστή ως Space Communication Protocol Standards (SCPS). Και οι δύο αυτές δυνατότητες επιτρέπουν στα πακέτα να δρομολογούνται δυναμικά μέσω διαφόρων διαδρομών με έναν ασυνδεσμικό τρόπο.

Πρότυπα Ασφάλειας. Καθώς οι αποστολές γίνονται πιο διαδικτυακά προσβάσιμες, γίνονται και πιο ευαίσθητες σε επιθέσεις. Βασική εξακρίβωση στοιχείων και κρυπτογράφηση μπορεί να υλοποιηθεί μέσα στα πρότυπα του CCSDS αλλά πιο ισχυρές απ'άκρου-εις-άκρου τεχνικές μπορούν να προστατέψουν όλη την ροή των δεδομένων. Δύο επιλογές πρωτοκόλλων υπάρχουν: Το Internet Protocol Security (IPSec) και ένα πρωτόκολλο του SCPS, το Security Protocol (SP). Και τα δύο παρέχουν πολλαπλά επίπεδα προστασίας των δεδομένων:

Έλεγχο Πρόσβασης: Παρεμπόδιση μη εξουσιοδοτημένων χρηστών να στείλουν δεδομένα.
Επιβεβαίωση Στοιχείων: Εγγύηση για την ταυτότητα του αποστολέα.
Ακεραιότητα: Προστασία από την σκόπιμη ή τυχαία τροποποίηση των δεδομένων κατά την μετάδοση.
Εμπιστευτικότητα: προστασία από την κοινοποίηση του περιεχομένου των δεδομένων.

Πρότυπα Αξιοπιστίας απ'Άκρου-εις-Άκρου. Όλα τα πρότυπα μέχρι αυτό το επίπεδο έχουν κυρίως συνδεθεί με την ευθύνη του να φτάσει ένα πακέτο δεδομένων μεταξύ δύο συστημάτων. Συνδυάζοντας ισχυρή κωδικοποίηση καναλιού με αναμετάδοση του επιπέδου ζεύξης, και υποθέτοντας ότι δεν υπάρχει απώλεια στη Γη ή στο διαστημόπλοιο ή στο τοπικό δίκτυο του Άρη, υπάρχει μια μεγάλη πιθανότητα ότι το πακέτο θα παραληφθεί.

Παρόλαυτα, αν το πακέτο χαθεί λόγω υπερχείλισης του buffer κάπου στην απ'άκρου-εις-άκρου διαδρομή, ή καταστραφεί από λάθη αναμετάδοσης στην πληροφορία κατά την μεταφορά, θα υπάρξει ένα κενό στα δεδομένα του χρήστη. Ο μόνος τρόπος για να γεμίσει αυτό το κενό είναι μέσω απ'άκρου-εις-άκρου αναμετάδοση. Αυτή η αναμετάδοση μπορεί να γίνει με τρεις τρόπους: Χειροκίνητα από ανθρώπους. Από τυχαίο κώδικα που τρέχει σε κάθε μια από τις εφαρμογές που στέλνουν και λαμβάνουν δεδομένα. Ή καλώντας ένα επικοινωνιακό πρωτόκολλο γενικών καθηκόντων που είναι σχεδιασμένο για αυτή τη δουλειά.

Για επικοινωνίες μικρής καθυστέρησης, το CCSDS συνιστά μια λύση που βασίζεται στο Internet Transmission Control Protocol (TCP) και σε επεκτάσεις του TCP στο SCPS, γνωστές ως "TCP Tranquility". Για αυτές τις εφαρμογές που δεν χρειάζονται τις υπηρεσίες του TCP, το Internet User Datagram Protocol (UDP) μπορεί να χρησιμοποιηθεί για να διαχωρίσει και να ενθυλακώσει τα δεδομένα των χρηστών.

Πρότυπα Μεταφοράς Αρχείων στο Διάστημα. Αυτό το επίπεδο –το πρώτο από διάφορες "υπηρεσίες εφαρμογών" που πιθανότατα θα αναπτυχθούν στο κοντινό μέλλον- υποστηρίζει άμεσα τις εφαρμογές των χρηστών που τρέχουν απ'άκρου-εις-άκρου. Στα πρόσφατα χρόνια έχει υπάρξει μια ραγδαία αλλαγή προς την οργάνωση

της μεταφοράς των αρχείων στο διάστημα σε αυτάρκη και αυτόνομα αρχεία στα οποία μπορούν να δοθούν διαφορετικές προτεραιότητες. Αυτό είναι ιδιαίτερα σημαντικό καθώς η επίγεια υποδομή όπως το DSN υπερχρησιμοποιείται, έτσι ώστε μια μεγάλη ποσότητα κίνησης μεταξύ των διαστημοπλοίων και του εδάφους μπορεί να μετακινηθεί και να επιβεβαιωθεί μέσα σε ένα μικρό διάστημα και οι πόροι να απελευθερωθούν για να εξυπηρετήσουν κάποιο άλλο διαστημόπλοιο. Το CCSDS στην παρούσα φάση υποστηρίζει δυο βασισμένα σε αρχεία πρότυπα:

1. Το Internet File Transfer Protocol (FTP), και τις προσαρμοσμένες στο διάστημα επεκτάσεις του, που αποτελούν μέρος του SCPS. Αυτές προορίζονται για χρήση κυρίως σε μικρής καθυστέρησης παρόμοια με το Διαδίκτυο περιβάλλοντα, και τοποθετούνται σε ένα κατώτερο του TCP επίπεδο.
2. Το CCSDS File Delivery Protocol (CFDP). Αυτό είναι ένα πρωτόκολλο ανεκτικό σε καθυστερήσεις του οποίου το μοντέλο λειτουργίας χαρακτηρίζεται ως αποθήκευσης και προώθησης(store-and-forward), παρόμοια με το e-mail που μεταβιβάζει τα αρχεία σαν συννημένα. Το πρωτόκολλο στην παρούσα σχεδίαση του περιέχει τον δικό του μηχανισμό αξιοπιστίας και δεν έχει κάποια δυνατότητα αναμετάδοσης. Λειτουργεί από σημείο-σε-σημείο διαμέσου μιας ζεύξης και αποτελείται από τρία τμήματα: Εντολές χειρισμού αρχείων που επιτρέπουν τη δημιουργία και ανταλλαγή αρχείων. Εντολές αποθήκευσης αρχείων που χρησιμοποιούνται για τον έλεγχο απομακρυσμένων συστημάτων αρχείων(file systems) Και ένα πρωτόκολλο αξιοπιστίας που διασφαλίζει ότι όλα τα κομμάτια ενός αρχείου παραλαμβάνονται σωστά μέσω της ζεύξης, με οποιοδήποτε χαμένο κομμάτι να αναμεταδίδεται αυτόματα.

Το CFDP έχει επίσης την δικιά του έννοια “κηδεμονικής μεταφοράς” όπου ένας αποστολέας μπορεί να μεταδώσει ένα αρχείο σε κάποιον παραλήπτη μέσω μιας ζεύξης και, με την παραλαβή ολόκληρου του αρχείου, ο παραλήπτης μπορεί να ειδοποιήσει τον αποστολέα ότι θα αναλάβει την όποια περαιτέρω προώθηση του αρχείου στο επόμενο hop. Αυτό επιτρέπει στον αποστολέα να απελευθερώσει τους τοπικούς επεξεργαστικούς και αποθηκευτικούς του πόρους και να τους διοχετεύσει στην παραλαβή νέων δεδομένων-μία σημαντική δυνατότητα για την μετάδοση δεδομένων από και προς πηγές με περιορισμένους πόρους. Για αποστολές που δεν θέλουν να πραγματοποιήσουν μεταφορά αρχείων, οι εφαρμογές μπορούν να παρακάμψουν τις διαδικασίες μεταφοράς αρχείων και να έχουν πρόσβαση κατευθείαν στα υποκείμενα επίπεδα.

Η στοίβα των CCSDS πρωτοκόλλων που προκύπτει φαίνεται στο σχήμα 4, που δείχνει πώς το βασικό σετ δυνατοτήτων του CCSDS που είναι τώρα σε ευρεία χρήση έχει επεκταθεί στα ανώτερα στρώματα και μπορεί τώρα να υποστηρίξει τρεις λειτουργίες της διαστημικής δικτύωσης:

1. Συμβατική χαμηλής καθυστέρησης απ’άκρου-εις-άκρου διαδικτύωση, χρησιμοποιώντας επεκτάσεις για το διάστημα στην παραδοσιακή πλατφόρμα του TCP/IP.
2. Κηδεμονική, ανεκτική σε καθυστερήσεις μεταφορά αρχείων, χρησιμοποιώντας το CFDP.
3. Δικτύωση Intranet εντός ενός διαστημοπλοίου.

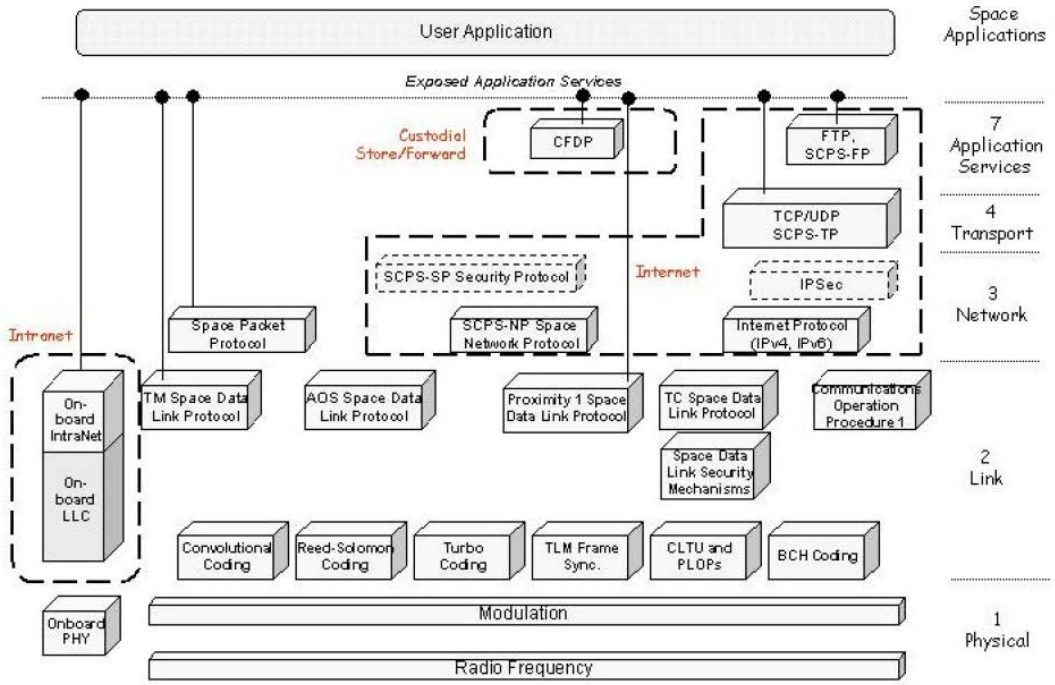


Figure 4: The "Emerging" CCSDS Stack

4.3 Διαπλανητικό Διαδίκτυο

Η βασική αρχιτεκτονική ιδέα του διαπλανητικού Διαδικτύου αποτελείται από τοπικά χαμηλής καθυστέρησης Διαδίκτυα, κατανεμημένα σε όλο το ηλιακό σύστημα, σε διαστημόπλοια σε κίνηση, αλλά και πάνω και γύρω από πλανήτες, που συνδέονται μεταξύ τους μέσω ενός backbone δικτύου μεγάλης καθυστέρησης στο διάστημα. Με τον ίδιο τρόπο που η πλατφόρμα του TCP/IP ενώνει το Διαδίκτυο της Γης σαν ένα "δίκτυο δικτύων", μια νέα πλατφόρμα πρωτοκόλλων που λέγεται πρωτόκολλο συσσώρευσης (bundling protocol) ενώνει το διαπλανητικό Διαδίκτυο σαν ένα "δίκτυο Διαδικτύων" υποστηρίζοντας διαπλανητικό διάλογο. Αυτή η αρχιτεκτονική φαίνεται στο σχήμα 5.

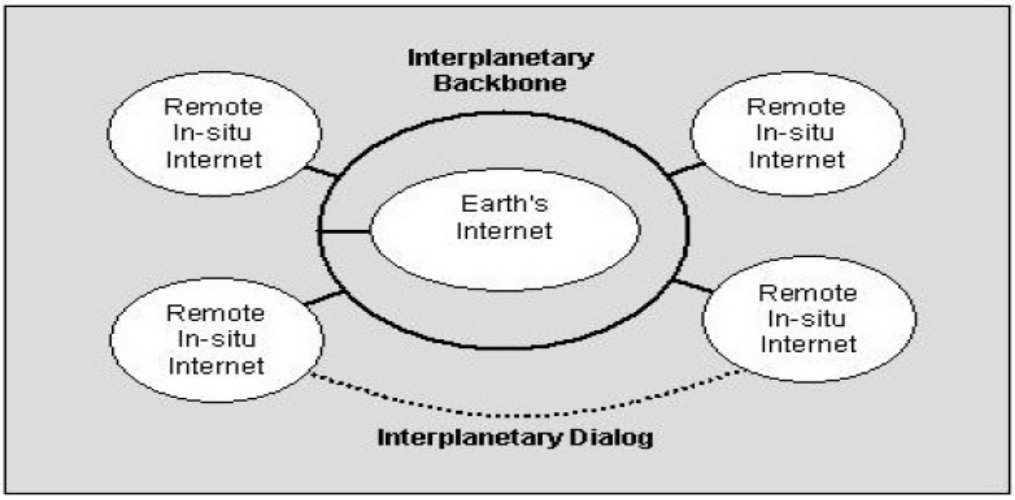


Figure 5: "Interplanetary Internet" Architecture

Η αρχιτεκτονική αυτή αναγνωρίζει ότι στο περιβάλλον του διαστήματος μια πραγματικού χρόνου απ'άκρου-εις-άκρου διαδρομή μεταξύ δύο χρηστών μπορεί να μην υπάρξει ποτέ σαν μια ενιαία συνδεδεμένη οντότητα. Αντίθετα, οι επικοινωνίες πρέπει να προκύπτουν με την ένωση μιας σειράς από χρονικά χωριστές μεταβάσεις πακέτων από ένα κόμβο στον επόμενο(hops). Η πλατφόρμα του *bundling* protocol είναι ο μηχανισμός μέσω του οποίου προκύπτει αυτή η ένωση. Μια λειτουργία δρομολόγησης θα καθοδηγεί τα bundles (τα πακέτα που θα μετακινούνται μέσω του *bundling* protocol) μέσω μιας ενωμένης σειράς από Διαδίκτυα, όπως το Internet protocol (IP) στην Γη δρομολογεί δεδομένα διαμέσου μιας σειράς από ανεξάρτητα δίκτυα πάνω στον πλανήτη. Για να εξασφαλιστεί αξιοπιστία της απ'άκρου-εις-άκρου μεταφοράς, τα bundles θα περιέχουν επίσης και μηχανισμούς αναμετάδοσης ανάλογους με αυτούς που παρέχει το Transmission Control Protocol (TCP) του Διαδικτύου στη Γη.

Το *bundling* protocol λειτουργεί στο διαστημικό περιβάλλον με δύο τρόπους:

1.Λειτουργεί με έναν τρόπο αποθήκευσης και προώθησης, παρόμοια με το e-mail, όπου τα bundles αποθηκεύονται σε δρομολογητές κατά μήκος της διαδρομής μέχρι να υπάρξει διαδρομή για να συνεχίσουν την πορεία τους.
2.Αποφεύγει την ανάγκη ο αποστολέας να πρέπει να αποθηκεύει δεδομένα μέχρι να παραληφθεί επιβεβαίωση από την άλλη άκρη, λειτουργώντας με έναν κηδεμονικό τρόπο. Σε αυτή τη λειτουργία, ενδιάμεσοι κόμβοι του δικτύου μπορούν να αναλάβουν την ευθύνη τα bundles να φτάσουν στον προορισμό τους, επιτρέποντας στους αποστολείς (και στους προηγούμενους "κηδεμόνες") να ανακατανείμουν τους πόρους τους σε νέες λειτουργίες.

Παρόλο που οι επικοινωνίες στο διάστημα (με τις τεράστιες καθυστερήσεις μετάδοσης) είναι προφανή παραδείγματα ανεκτικών σε καθυστερήσεις δικτύων (DTNs), αναμένεται αυτός ο τρόπος λειτουργίας να γίνει πολύ σημαντικός και για τις γήινες επικοινωνίες καθώς τα όρια του Διαδικτύου εξαντλούνται. Άλλες εφαρμογές που μπορούν να χρησιμοποιήσουν αυτές τις τεχνικές περιλαμβάνουν π.χ υπερφορτωμένες στρατιωτικές επικοινωνίες. Το κόστος ανάπτυξης συνεπώς του *bundling* protocol πιθανότατα θα μοιραστεί σε μια μεγάλη κοινότητα.

4.4 Το CFDP και η θέση του στο *bundling* protocol

Το CCSDS File Delivery Protocol (σχήμα 6) είναι μια πρωτοτυπική μορφή του *bundling* protocol. Το CFDP αποτελείται από τρία τμήματα:

1. Μηχανισμοί χειρισμού των αρχείων.
2. Μηχανισμοί αξιοπιστίας από σημείο-σε-σημείο,πού βασίζονται σε κατώτερα επίπεδα.
3. Υπηρεσίες μεταφοράς δεδομένων στο επίπεδο ζεύξης.

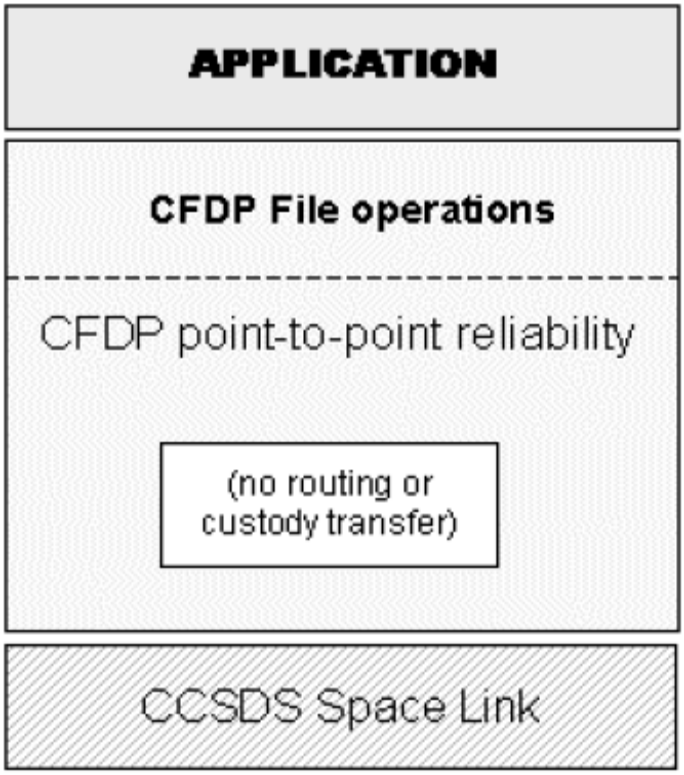


Figure 6: Current CFDP Architecture

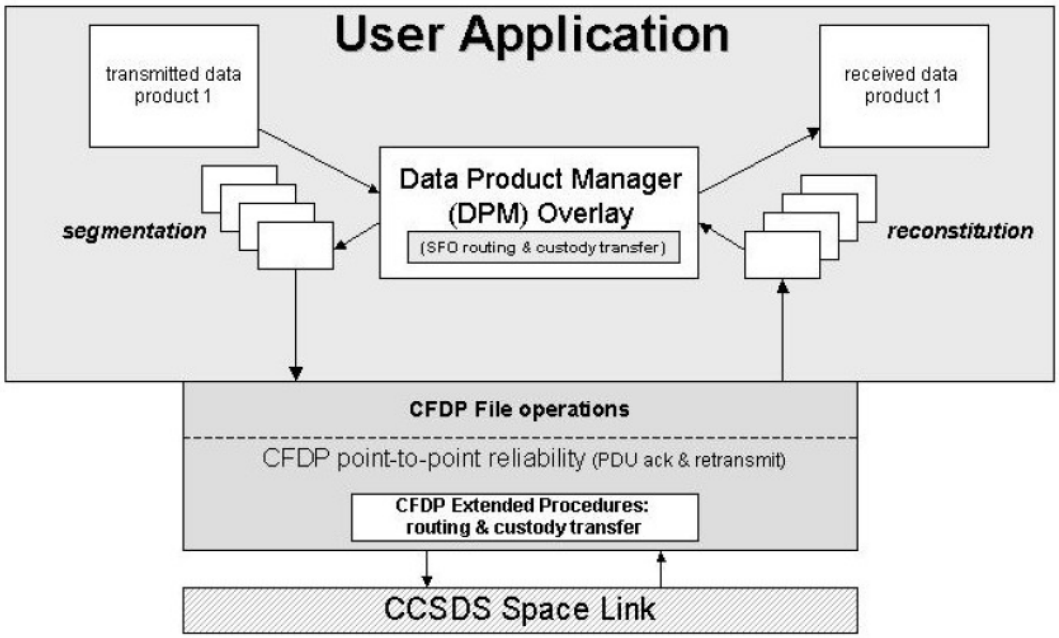


Figure 7: Extensions to CFDP

Η δυνατότητες του CFDP περιλαμβάνουν:
a. Διαδικασίες που επεκτάθηκαν και που υποστηρίζουν δρομολόγηση και κηδεμονική μεταφορά.
b. Δυνατότητα αποθήκευσης και προώθησης πού αναβαθμίζει αυτές τις διαδικασίες με το να παρέχει ανίχνευση διαδρομής και διαγνωστικές λειτουργίες και επιτρέποντας την συνέχιση από ένα γνωστό σημείο όπου υπήρξε λάθος.
c. Μια επιπλέον δυνατότητα στην εφαρμογή χρήστη– ένα "Data Product Manager" – που επιτρέπει λειτουργία για αποστολές που χρησιμοποιούν πολλαπλούς δορυφόρους.

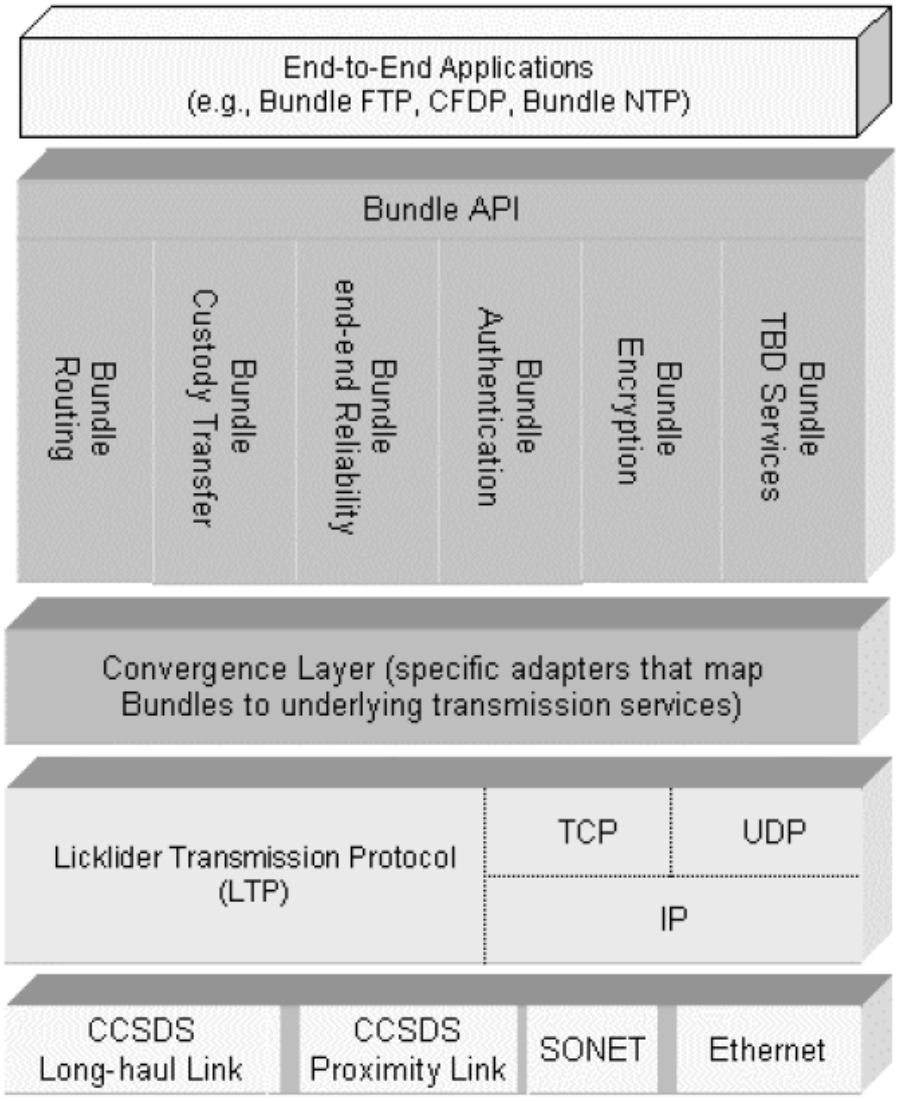


Figure 8: Current *bundling* Architecture

Η αρχιτεκτονική του *bundling* protocol διαφέρει από το CFDP σε μερικά βασικά σημεία:

1.Δεν περιορίζεται στο να υποστηρίζει απλώς μεταφορά αρχείων, αλλά μπορεί να χειριστεί κυριολεκτικά οποιαδήποτε απ'άκρου-εις-άκρου εφαρμογή. Αναπόφευκτα, το CFDP τελικά θα μετακινηθεί προς τα πάνω στην στοίβα για να γίνει μια από αυτές τις εφαρμογές.
2.Οι εσωτερικές του λειτουργίες είναι πιο ξεκάθαρα σχεδιασμένες από του CFDP, έτσι ώστε να είναι πιο εύκολο να εξελιχθεί με τον καιρό.
3.Θα παρέχει ένα πλούσιο σύνολο από υπηρεσίες εφαρμογών, συμπεριλαμβάνοντας μια πιο ώριμη δυνατότητα κηδεμονικής μεταφοράς από ότι είναι εφικτό με το CFDP.

5 BUNDLE

5.1 Το Επίπεδο Bundle Τερματίζει τα Τοπικά Πρωτόκολλα Μεταφοράς και Λειτουργεί απ' άκρου-εις-άκρου.

Στα Διαπλανητικά Δίκτυα (InterPlanetary Networks), δεν μπορούμε ποτέ να είμαστε σίγουροι ότι υπάρχει άμεση συνδεσιμότητα μεταξύ πηγής και προορισμού. Αυτό σημαίνει ότι δεν μπορούμε να υποθέσουμε ότι τα bit που εκπέμπονται από μια πηγή μπορούν να ταξιδέψουν, αντιμετωπίζοντας μόνο καθυστερήσεις δρομολόγησης και μετάδοσης. Οι αιτίες των καθυστερήσεων μπορούν να είναι πολλές, από φυσικές (ο προορισμός είναι στην άλλη άκρη ενός μακρινού πλανήτη και δεν μπορεί να επικοινωνήσει με τίποτα την παρούσα στιγμή), ή σχετιζόμενες με το πρόγραμμα εξυπηρέτησης της δεδομένης χρονικής στιγμής (η απαιτούμενη πύλη του IPN εξυπηρετεί άλλους πελάτες εκείνη τη στιγμή), ή σχετικές με την διαχείριση του δικτύου (η πηγή είναι σε λειτουργία-επαφή μόνο την ημέρα, ο προορισμός μόνο την νύχτα).Για τις ζεύξεις μεγάλης απόστασης του backbone, η πληροφορία θα πρέπει να αποθηκεύεται για κάποιο χρονικό διάστημα καθώς οι κεραίες που θα χρησιμοποιούνται για τις ζεύξεις θα είναι κατευθυντικές (directional).

Συνεπώς αναλόγως με το πρόγραμμα των συμμετεχόντων κόμβων και την πιθανότητα της κίνησης υψηλής προτεραιότητας να διακόψει την επικοινωνία, οι κόμβοι που αποτελούν το IPN μπορεί να πρέπει να αποθηκεύσουν δεδομένα για ώρες, ημέρες, ή και εβδομάδες πρίν να μπορέσουν να τα προωθήσουν ξανά. Επίσης, τα πολύ διαφορετικά επικοινωνιακά περιβάλλοντα που θα συνθέτουν το IPN, όπως οι οπτικές ίνες στη Γη και οι ασύρματες επικοινωνίες γύρω από τον Άρη, συνιστούν την χρήση διαφορετικών πρωτοκόλλων μεταφοράς για τα ετερόκλητα αυτά περιβάλλοντα. Είναι λογικό λοιπόν οι κόμβοι του IPN να τερματίζουν τα πρωτόκολλα του επιπέδου μεταφοράς που χρησιμοποιούνται στις αντίστοιχες περιοχές του IPN, κρατώντας τα δεδομένα σε κάποιο υψηλότερο επίπεδο πριν τα προωθήσουν, πιθανώς χρησιμοποιώντας κάποιο διαφορετικό πρωτόκολλο του επιπέδου μεταφοράς.

Αυτό το υψηλότερο επίπεδο αποκαλείται, "επίπεδο bundle", και το πρωτόκολλο που χρησιμοποιείται για να σταλούν δεδομένα μεταξύ των διαφόρων κόμβων του IPN "bundling protocol". Ο όρος "bundle" χρησιμοποιείται για να δείξουμε την ιδιότητα αποθήκευσης και προώθησης των επικοινωνιών όπου έχει επιτευχθεί όσο το δυνατόν μεγαλύτερη αλληλεπίδραση. Μία ερώτηση μεταφοράς αρχείου bundle για παράδειγμα, μπορεί να περιέχει τα στοιχεία εξακρίβωσης του χρήστη (login/password, κτλ), την περιοχή του προς λήψη αρχείου, και που πρέπει να παραδοθεί αυτό το αρχείο στο IPN domain του παραλήπτη. Όλη αυτή η πληροφορία θα μεταδοθεί σαν ένα bundle, και θα επιστραφεί το ζητούμενο αρχείο. Χρησιμοποιείται ο όρος bundle αντί για συναλλαγή για να αποφευχθούν παραλληλισμοί με διαδικασίες δύο και τριών φάσεων που είναι συνηφασμένες με την επεξεργασία συνναλαγών.

Στην παραδοσιακή δικτυακή ορολογία είναι γενικότερα το πρωτόκολλο επίπεδου μεταφοράς που λειτουργεί απ'άκρου-εις-άκρου. Από τη στιγμή που οι κόμβοι του IPN τερματίζουν τα πρωτόκολλα του επιπέδου μεταφοράς προκειμένου να αποθηκεύσουν δεδομένα και να τα επιτρέψουν να χρησιμοποιήσουν ένα πρωτόκολλο μεταφοράς κατάλληλο για την περιοχή του IPN όπου θα σταλούν, είναι το επίπεδο bundle στο IPN που λειτουργεί απ'άκρου-εις-άκρου.

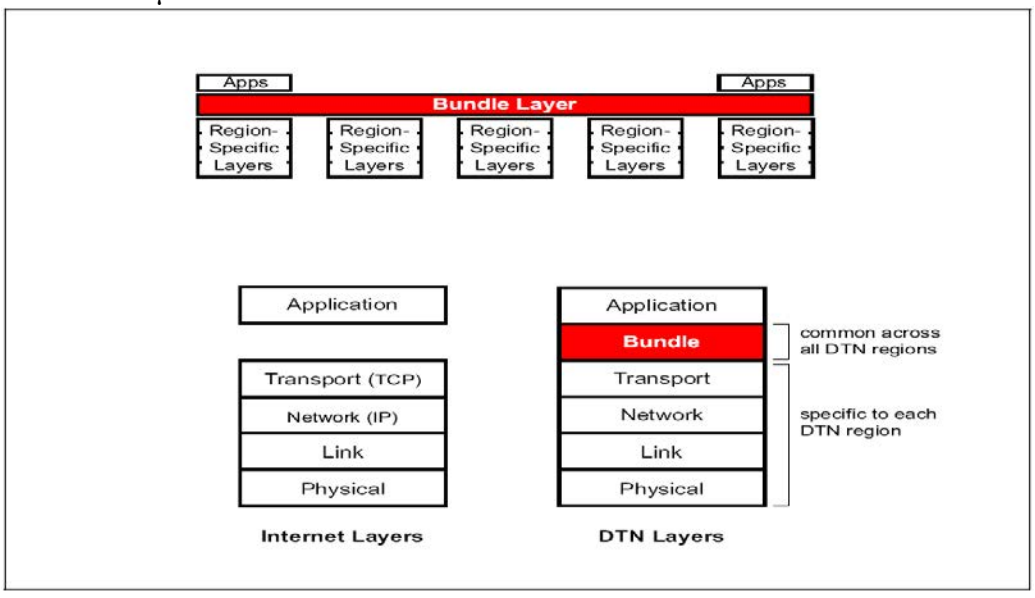
Πρέπει να σημειωθεί ότι τερματίζοντας τα πρωτόκολλα μεταφοράς στους IPN κόμβους αποσυνδέονται τα διαδίκτυα σε διαφορετικές IPN περιοχές σε έναν σημαντικό βαθμό. Αυτό έχει ως θετικό αποτέλεσμα την αποσύνδεση και των ρυθμών εξέλιξης αυτών των διαδικτύων: Αλλαγές στο Διαδίκτυο της Γης δεν είναι απαραίτητο να υπαγορεύσει αναγκαστικά αλλαγές και στα άλλα διαδίκτυα. Αυτό είναι σημαντικό σε ένα περιβάλλον όπου οι πόροι είναι και θα συνεχίσουν να είναι πολύ περιορισμένοι.

5.2 Το Επίπεδο Bundle

Η αρχιτεκτονική IPN υλοποιεί μεταγωγή μηνύματος αποθήκευσης και προώθησης τοποθετώντας ένα νέο επίπεδο –γνωστό ως bundle- στην κορυφή χαμηλότερων ετερογενών και σχετικών με κάθε περιοχή επιπέδων. Το επίπεδο bundle δένει μεταξύ τους αυτά τα επίπεδα έτσι ώστε οι εφαρμογές να μπορούν να επικοινωνούν διαμέσου πολλαπλών περιοχών του IPN.

Τα bundles αποκαλούνται επίσης και μηνύματα. Το επίπεδο bundle αποθηκεύει και προωθεί ολόκληρα bundles μεταξύ κόμβων. Ένα συγκεκριμένο πρωτόκολλο του επιπέδου bundle χρησιμοποιείται πάνω σε όλα τα δίκτυα (περιοχές) που αποτελούν ένα DTN. Τα επίπεδα κάτω από το bundle επίπεδο (από το επίπεδο μεταφοράς και κάτω) επιλέγονται για την καταλληλότητα τους στο επικοινωνιακό περιβάλλον κάθε περιοχής.

Η εικόνα δείχνει την θέση του επιπέδου bundle και συγκρίνει τα επίπεδα του Διαδικτύου με τα επίπεδα του DTN.

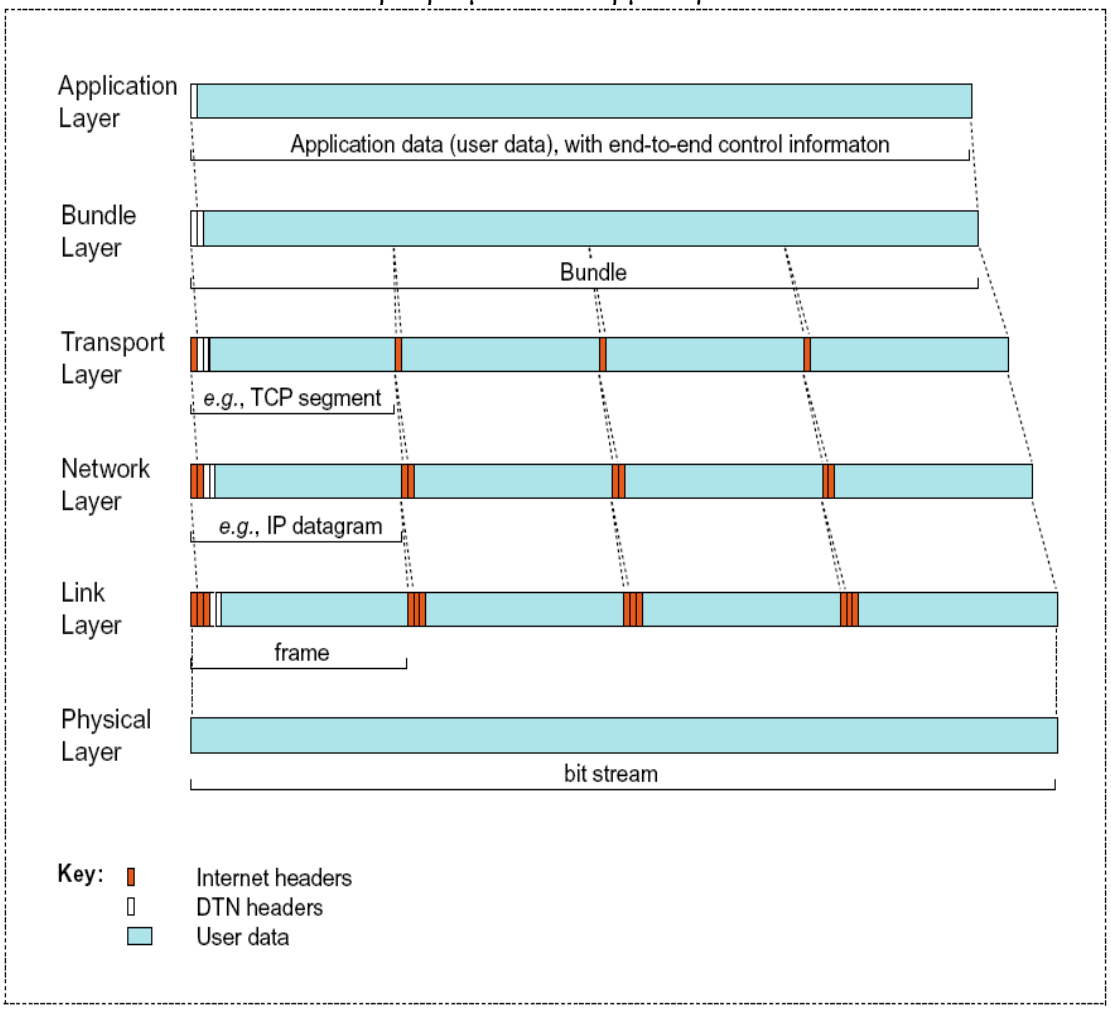


5.3 Τα bundles και η ενθυλάκωση στο επίπεδο bundle

Τα bundles αποτελούνται από τρία πράγματα γενικά:
1.Τα δεδομένα χρήστη της εφαρμογής στην πηγή.
2.Πληροφορία ελέγχου, που παρέχεται από την εφαρμογή στην πηγή για την εφαρμογή στον προορισμό, που περιγράφει πώς να επεξεργαστεί, αποθηκευτεί, απορριφθεί και γενικά να χειριστεί τα δεδομένα χρήστη ο προορισμός.
3.Μια bundle επικεφαλίδα (bundle header), που ενσωματώνεται από το επίπεδο bundle.
Όπως και τα δεδομένα χρήστη, τα bundles μπορεί να είναι τυχαία μεγάλα.

Τα bundles επεκτείνουν την ιεραρχία της ενθυλάκωσης δεδομένων που πραγματοποιείται από τα πρωτόκολλα του Διαδικτύου. Το παράδειγμα παρακάτω δείχνει πώς λειτουργεί η ενθυλάκωση του επίπεδου bundle στο πλαίσιο των χαμηλότερου επιπέδου TCP/IP.

Το επίπεδο bundle μπορεί να σπάσει ολόκληρα bundles (ολόκληρα μηνύματα) σε κομμάτια (fragments) (δεν φαίνεται στην εικόνα), όπως το επίπεδο του IP μπορεί να σπάσει τα datagrams σε fragments.Αν τα bundles έχουν χωριστεί σε κομμάτια το επίπεδο bundle στον τελικό προορισμό τα συναρμολογεί.



5.4 Πληροφορία πού Μεταφέρεται με το Επίπεδο Bundle.

Για να φέρει εις πέρας τις απ'άκρου-εις-άκρου μεταφορές που είναι απραίτητες στο IPN, το επίπεδο bundle πρέπει να κουβαλήσει κάποια πληροφορία από άκρο σε άκρο. Σε αυτήν την ενότητα αναφέρεται η πληροφορία που πρέπει να μεταφερθεί, καθώς και πια από αυτά τα δεδομένα μπορούν να παρασχεθούν από την εφαρμογή που χρησιμοποιεί την υπηρεσία του bundle.

* Bundle Identifier: Αυτός είναι ένας μονοτονικά αυξανόμενος αριθμός που μεταφέρεται με το bundle, και επίσης επιστρέφεται στην εφαρμογή για να υποστηριχθεί η επεξεργασία της επιβεβαίωσης επιστροφής. Δεν είναι απαραίτητα ένας αύξων αριθμός, και γι'αυτό δεν υπάρχει η απαίτηση ο αριθμός του Bundle Identifier να αυξάνει συνεχόμενα. Η απαίτηση για μονοτονικότητα προέρχεται από την ανάγκη να παρασχεθεί αντοχή απέναντι στις αποτυχίες συστήματος.

* Remote entity name: Αυτό είναι το IPN όνομα του απομακρυσμένου στοιχείου bundle.Παρέχεται από την τοπική εφαρμογή χρησιμοποιώντας την υπηρεσία του bundle.

* Source entity name: Αυτό είναι το IPN όνομα του απομακρυσμένου στοιχείου bundle. Παρέχεται από την τοπική υπηρεσία bundle, καθώς ένας host μπορεί να έχει πολλαπλά ονόματα και ένα μπορεί να επιλεγεί βάση των αποφάσεων δρομολόγησης ή άλλων κριτηρίων αδιαφανών στην εφαρμογή. Το όνομα της πηγής μπορεί να επιστραφεί στην εφαρμογή για να υποστηριχθεί η επεξεργασία της επιβεβαίωσης επιστροφής.

* Authentication information: Αυτή είναι πληροφορία, όπως μια ψηφιακή υπογραφή, που περνάει από την εφαρμογή στο επίπεδο bundle προκειμένου να αναγνωριστεί η πηγή του bundle (μόνο η πηγή του bundle ποια είναι, το άτομο, μέρος, διεύθυνση κτλ δεν είναι ακόμα αναγνωρίσιμα). Αυτή η πληροφορία ελέγχεται για την εγγύτητα της και στο στοιχείο του bundle στην πηγή και στο στοιχείο στον προορισμό. Η πληροφορία της ταυτοποίησης μπορεί επίσης να χρησιμοποιηθεί για σκοπούς έλεγχου πρόσβασης μέσα στο δίκτυο.

* Source application instance handle: Είναι παρόμοιο με το νούμερο του port στην πηγή στο ότι αναγνωρίζει την αποστέλλουσα εφαρμογή. Αφού τα bundles είναι εγγενώς μη διαδραστικά, η τυπική χρήση για το handle είναι να ξαναενεργοποιήσει την εφαρμογή της πηγής όταν μια επιβεβαίωση επιστροφής φτάσει. Αυτό θα μπορούσε να γίνει ώρες, μέρες ή και βδομάδες μετά από την αρχική εκπομπή, οπότε το handle θα είναι μια αναφορά σε μια δομή που επιτρέπει στην εφαρμογή να επανέλθει στην τελευταία γνωστή κατάσταση της. Το source application instance handle μπορεί να χρησιμοποιηθεί στον προορισμό σαν ένας identifier, αλλά μπορεί να είναι και περιττό με την απ'άκρου-εις-άκρου πληροφορία ταυτοποίησης για αυτήν την περίπτωση. Αυτό το handle παρέχεται από την εφαρμογή της πηγής.

* Destination application instance handle: Αυτό είναι ουσιαστικά το identifier του port στον προορισμό. Όπως και με τα ports, αυτά πρέπει να είναι γνωστά και να παρέχονται από την εφαρμογή της πηγής.

* Size of data: Αποτελεί την δήλωση του μεγέθους του bundle,σε bytes. Παρέχεται από την εφαρμογή της πηγής, και χρησιμοποιείται αρχικά για να επιβεβαιωθεί ότι υπάρχει αρκετός χώρος για να αποθηκευτεί το bundle για την αρχική του μετάδοση. Οι κόμβοι που παραλαμβάνουν τα μεταδιδόμενα bundles χρησιμοποιούν αυτή την πληροφορία με τον ίδιο τρόπο: σαν ένα μέσο για να γίνει ο υπολογισμός του αν υπάρχει χώρος στην αρχή της διαδικασίας. Στον σχηματισμό του αρχικού bundle,το επίπεδο bundle στην πηγή μπορεί να χρησιμοποιήσει το μέγεθος των παραμέτρων των δεδομένων σαν έναν έλεγχο της ακαιρεότητας της ποσότητας των δεδομένων που πραγματικά παραλήφθηκαν.

* Handling instructions: Αυτές είναι παράμετροι που παρέχονται από τον χρήστη με το bundle που μεταβιβάζει τις προτιμήσεις του χρήστη στο δίκτυο. Ουσιαστικά αυτές οι παράμετροι περιλαμβάνουν μερικά ή όλα από τα ακόλουθα: προταιρεότητα, ποιότητα υπηρεσίας (quality of service-QoS), εναπομείναν χρόνος μετά το πέρας του οποίου το περιεχόμενο του bundle δεν έχει καμιά χρησιμότητα (χρόνος ζωής όπως καθορίζεται από τον χρήστη), απαιτήσεις αξιοπιστίας, και οποιαδήποτε πληροφορία χειρισμού λαθών. Όλα αυτά είναι κυρίως αιτήματα, και πιθανώς το επίπεδο bundle να παρακάμψει μερικά ή όλα από αυτά τα αιτήματα ή να αποτύχει στο αίτημα αν η τοπική πολιτική δεν επιτρέπει στον συγκεκριμένο χρήστη να κάνει το συγκεκριμένο αίτημα την συγκεκριμένη στιγμή.

* Data Descriptor: Είναι ένας αποθηκευτικός αριθμός που παράγεται από το επίπεδο bundle. Ο αναλυτικός ορισμός του και η χρήση του δεν έχουν ακόμη καθοριστεί.

* Time to Live: Αυτός είναι ο χρόνος μετά το πέρας του οποίου το bundle πρέπει να απορριφθεί από το δίκτυο.

* Loose/Strict Source Route and Record: Αυτή η πληροφορία παρέχεται από την εφαρμογή της πηγής για να επιτευχθεί η διόρθωση των λαθών και μειονεκτημάτων στην αρχιτεκτονική και λειτουργία του δικτύου. Αποτελείται από μια λίστα από ονόματα των κόμβων του IPN μέσω των οποίων το bundle πρέπει να περάσει στον δρόμο του για τον προορισμό, και η πρόθεση είναι να συμπεριφέρεται παρόμοια με την αντίστοιχη επιλογή μέσα στο IP.

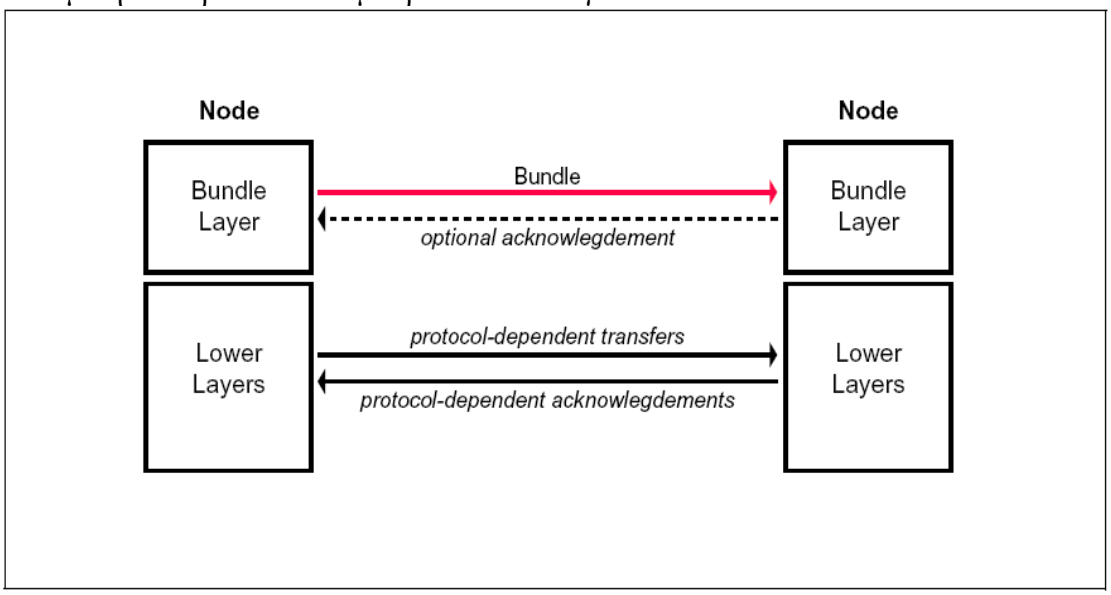
* Current bundle custodian: Το πρωτόκολλο του bundle υποστηρίζει λειτουργία αποθήκευσης και προώθησης στην οποία η κηδεμονία ενός bundle (δηλαδή η ευθύνη για εξασφάλιση αξιόπιστης παραλαβής) μπορεί να μεταφερθεί από τον ένα κόμβο στον άλλο καθώς το bundle προχωράει μέσα στο IPN. Δεν υπάρχει η απαίτηση για κάθε κόμβο που συναντάει το bundle, εκείνος ο κόμβος να αναλαμβάνει κηδεμονία. Σαν αποτέλεσμα, είναι απαραίτητο να αναγνωριστεί ο κόμβος που έχει την κηδεμονία, προκειμένου να ζητηθεί αναμετάδοση ή μεταφορά της κηδεμονίας σε κάποιον άλλο κόμβο.

* User data: Αυτά είναι όλα τα δεδομένα που η απομακρυσμένη οντότητα απαιτεί να πραγματοποιήσουν την λειτουργία για την οποία προορίζονται. Από τη στιγμή που τα περιβαλλοντικά χαρακτηριστικά του IPN κάνουν την διαδραστικότητα δύσκολη, η έννοια είναι όλη η πληροφορία που απαιτείται για να πραγματοποιηθεί μια συγκεκριμένη συναλλαγή να παρέχεται σε ένα μόνο bundle.

5.5 Ένα Μη Συνομιλητικό Πρωτόκολλο

Σε ζεύξεις με διακοπτόμενη συνδεσιμότητα και μεγάλες καθυστερήσεις, τα συνομιλητικά πρωτόκολλα όπως το TCP που περιλαμβάνουν πολλά απ'άκρου-εις-άκρου roundtrips μπορεί να καθυστερήσουν πάρα πολύ, σε σημείο να μην είναι αποδεκτός ο χρόνος που θα κάνουν ή να αποτύχουν τελείως να μεταδοθούν. Για αυτό το λόγο, τα επίπεδα bundle στο DTN μπορεί να επικοινωνούν μεταξύ τους χρησιμοποιώντας απλές συνόδους με ελάχιστα ή καθόλου roundtrips. Οποιαδήποτε επιβεβαίωση από τον κόμβο-παραλήπτη είναι προαιρετική, αναλόγως με την ποιότητα υπηρεσίας (QoS) που έχει επιλεγεί.

Τα χαμηλότερων επιπέδων πρωτόκολλα που υποστηρίζουν συναλλαγές με το επίπεδο bundle μπορούν φυσικά να είναι συνομιλητικά, όπως το TCP. Αλλά σε ζεύξεις διακοπτόμενης σύνδεσης με μεγάλες καθυστερήσεις, μη συνομιλητικά ή ελάχιστα συνομιλητικά πρωτόκολλα μπορούν να επιλεγούν.

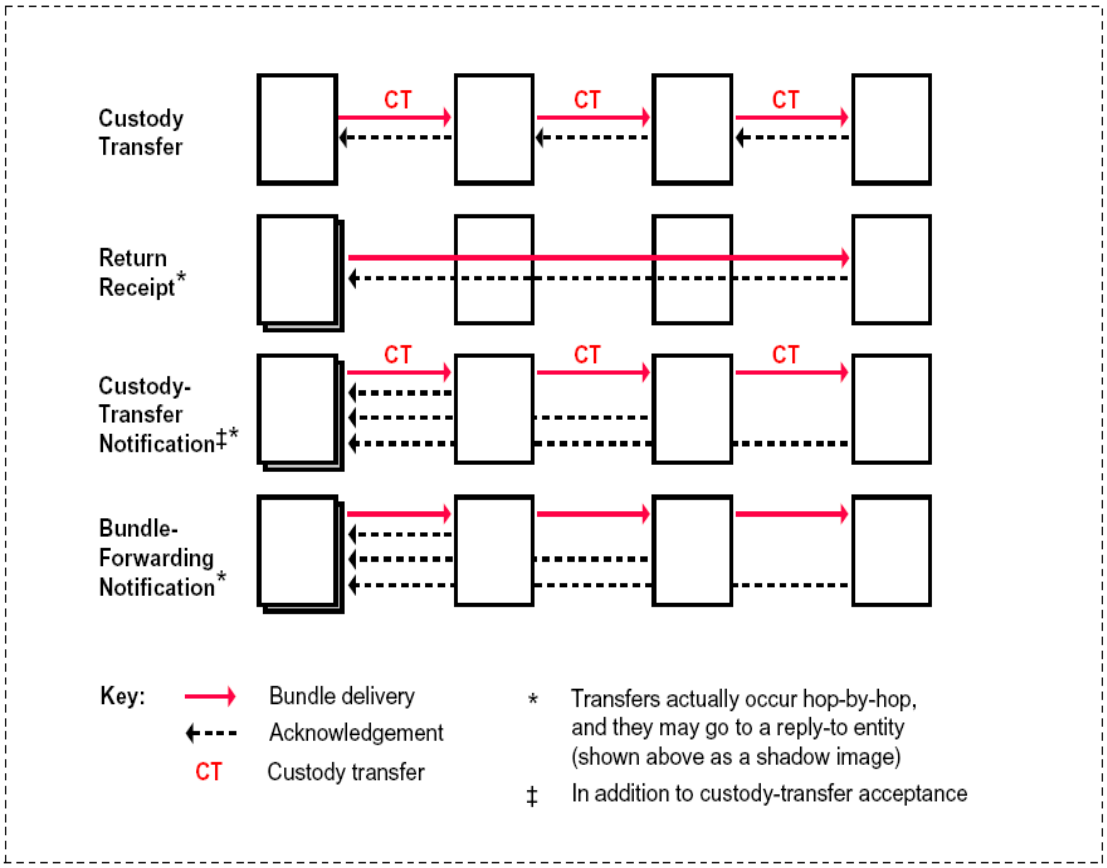


5.6 Ποιότητα Υπηρεσίας στο Bundle

Το επίπεδο bundle παρέχει έξι κατηγορίες QoS για ένα bundle:

1. Custody Transfer: Μεταφορά της ευθύνης αναμετάδοσης σε ένα κόμβο που δέχεται το σήμα, έτσι ώστε ο κόμβος που το στέλνει να μπορεί να ανακτήσει τους πόρους του. Ο κόμβος που δέχεται το σήμα επιστρέφει μια επιβεβαίωση αποδοχής της κηδεμονίας στον προηγούμενο κόμβο-κηδεμόνα.

2. Return Receipt: Επιβεβαίωση στην πηγή, ότι το bundle παραλήφθηκε από την εφαρμογή του προορισμού.
3. Custody-Transfer Notification: Ειδοποίηση στην πηγή, όταν ένας κόμβος αποδέχεται μια μεταβίβαση της κηδεμονίας ενός bundle.
4. Bundle-Forwarding Notification: Ειδοποίηση στην πηγή, όποτε το bundle προωθείται σε άλλο κόμβο.
5. Priority of Delivery: Bulk, Normal ή Expedited.
6. Authentication: Η μέθοδος (π.χ ψηφιακή υπογραφή), που χρησιμοποιείται για να επιβεβαιωθεί η ταυτότητα του αποστολέα και η ακεραιότητα του μηνύματος.



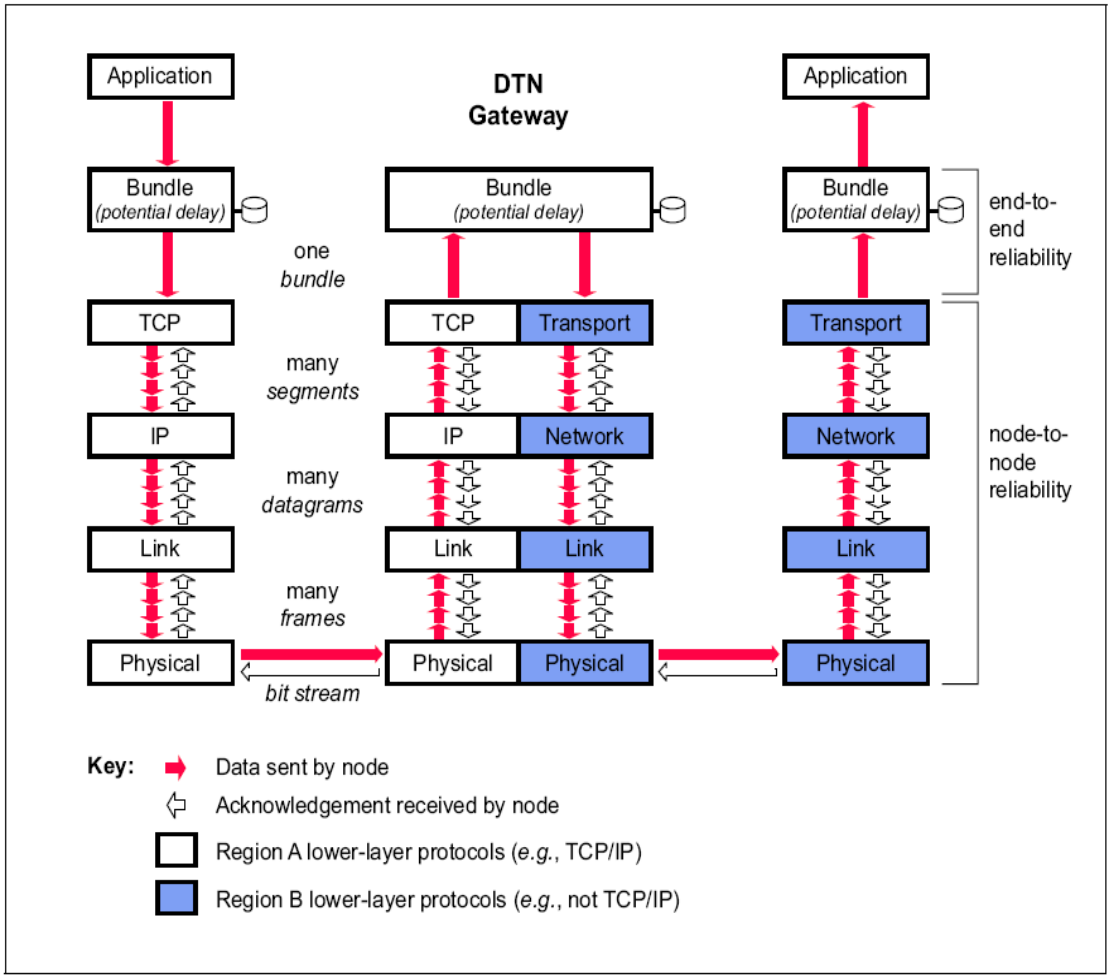
5.7 Απομόνωση της Καθυστέρησης μέσω Τερματισμού του Επιπέδου Μεταφοράς

Στο Διαδίκτυο, το πρωτόκολλο TCP παρέχει απ'άκρου-εις-άκρου (πηγής-σε-προορισμό) αξιοπιστία αναμεταδίδοντας οποιοδήποτε κομμάτι που δεν επιβεβαιώνεται από τον προορισμό. Το δίκτυο, η ζεύξη, και το φυσικό επίπεδο παρέχουν άλλους τύπους υπηρεσιών ακεραιότητας δεδομένων. Σε ένα DTN,το επίπεδο bundle βασίζεται σε αυτά τα χαμηλότερου επιπέδου πρωτόκολλα για να εγγυηθεί την αξιοπιστία της επικοινωνίας.

Παρόλαυτα, οι δρομολογητές και οι πύλες του DTN-κόμβοι που προωθούν bundles μέσα ή μεταξύ DTN περιοχών αντίστοιχα-τερματίζουν τα πρωτόκολλα μεταφοράς στο επίπεδο bundle.Τα επίπεδα bundle συνεπώς δρουν σαν αναπληρώσεις για τις

απ'άκρου-εις-άκρου πηγές και προορισμούς. Επιπλέον, έτσι τα συνομιλητικά πρωτόκολλα των χαμηλότερων επιπέδων στις χαμηλής καθυστέρησης περιοχές είναι απομονωμένες στο επίπεδο bundle από μεγάλες καθυστερήσεις σε άλλες περιοχές της απ'άκρου-εις-άκρου διαδρομής.

Μόνο το επίπεδο bundle υποστηρίζει απ'άκρου-εις-άκρου αποστολή μηνυμάτων. Τα bundles τυπικά παραλαμβάνονται ατομικά, από ένα κόμβο στον επόμενο, ανεξάρτητα από άλλα bundles εκτός από προαιρετικές απαντήσεις, αν και ένα bundle επίπεδο μπορεί να σπάσει ένα απλό bundle σε πολλαπλά κομμάτια.



5.8 Κηδεμονικές Μεταφορές

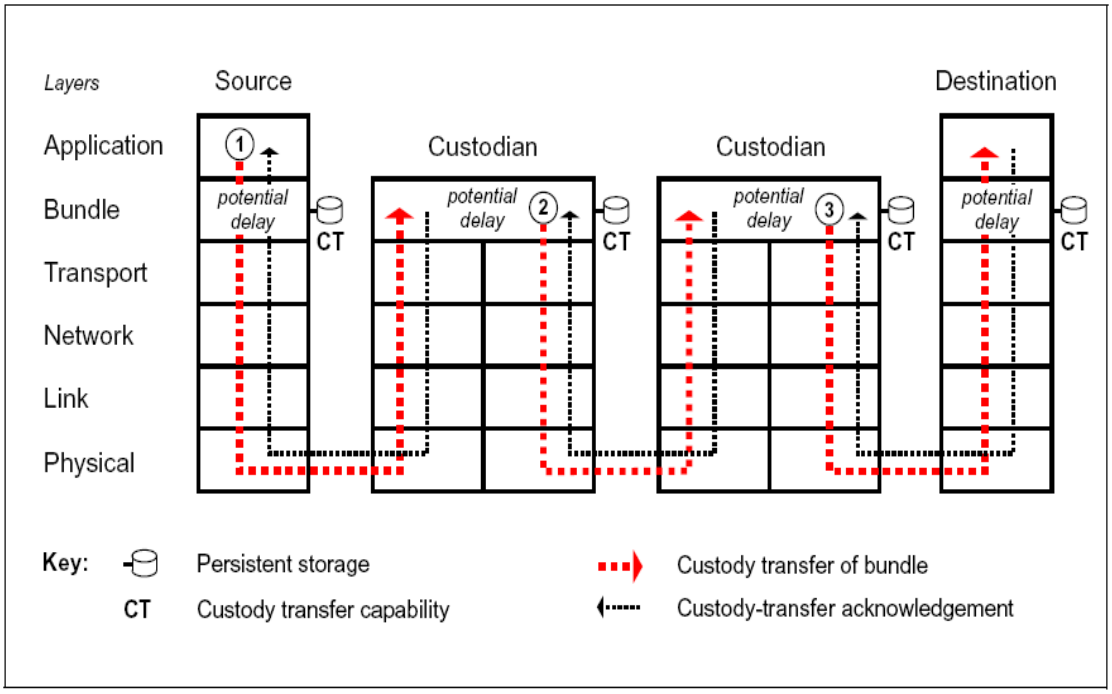
Τα DTN δίκτυα υποστηρίζουν από κόμβο-σε-κόμβο αναμετάδοση χαμένων ή κατεστραμμένων δεδομένων και στο επίπεδο μεταφοράς και στο bundle επίπεδο. Παρόλαυτα, επειδή κανένα πρωτόκολλο του επιπέδου μεταφοράς (τα πρωταρχικά μέσα αξιόπιστης μεταφοράς) δεν λειτουργεί απ'άκρου-εις-άκρου διαμέσου ενός DTN, απ'άκρου-εις-άκρου αξιοπιστία μπορεί να επιτευχθεί μόνο στο bundle επίπεδο.

Το επίπεδο bundle υποστηρίζει την από κόμβο σε κόμβο αναμετάδοση μέσω κηδεμονικών μεταφορών. Τέτοιες μεταφορές κανονίζονται μεταξύ των bundle

επιπέδων των διαδοχικών κόμβων, στο αρχικό αίτημα της εφαρμογής στην πηγή. Όταν ο τρέχων κηδεμόνας του bundle επιπέδου στέλνει ένα bundle στον επόμενο κόμβο, ζητάει μια κηδεμονική μεταφορά και ξεκινάει ένα χρονοδιακόπτη αναμετάδοσης time-to-acknowledge. Αν το bundle επίπεδο του επόμενου hop αποδεχτεί την κηδεμονία, επιστρέφει μια επιβεβαίωση στον αποστολέα. Αν δεν επιστραφεί επιβεβαίωση πριν λήξει ο χρονοδιακόπτης time-to-acknowledge του αποστολέα, ο αποστολέας αναμεταδίδει το bundle. Η τιμή που δίνεται στον χρονοδιακόπτη αναμετάδοσης μπορεί είτε να μοιραστεί στους κόμβους μαζί με πληροφορία δρομολόγησης, είτε να υπολογιστεί τοπικά, βάση της προηγούμενης εμπειρίας μετάδοσης σε κάποιο συγκεκριμένο κόμβο.

Ο κηδεμόνας ενός bundle πρέπει να αποθηκεύσει ένα bundle μέχρι είτε κάποιος άλλος κόμβος να αποδεχτεί την κηδεμονία ή να λήξει ο χρόνος ζωής (time-to-live) του bundle,το οποίο είναι πολύ μεγαλύτερο από το time-to-acknowledge του κηδεμόνα. Παρόλαυτα ο χρόνος του time-to-acknowledge πρέπει να είναι αρκετά μεγάλος για να δώσει στα υποκείμενα πρωτόκολλα μεταφοράς κάθε ευκαιρία να τελειώσουν μια αξιόπιστη μετάδοση.

Οι κηδεμονικές μεταφορές δεν παρέχουν εγγυημένη απ'άκρου-εις-άκρου αξιοπιστία. Αυτό μπορεί να γίνει μόνο αν μια πηγή ζητήσει και την κηδεμονική μεταφορά και το return receipt(κεφ 5.6). Σε αυτήν τη περίπτωση, η πηγή πρέπει να διατηρήσει ένα αντίγραφο του bundle μέχρι να παραλάβει ένα return receipt, και θα το αναμεταδώσει αν δεν παραλάβει return receipt.



6 ΘΕΜΑΤΑ ΔΡΟΜΟΛΟΓΗΣΗΣ

6.1 Εισαγωγή

Η επικοινωνία σε ένα Delay Tolerant Network (DTN) μπορεί να είναι είτε μεταξύ περιοχών είτε εντός μιας περιοχής. Ενώ αυτή η αρχιτεκτονική δεν προσδιορίζει συγκεκριμένες μεθόδους για ανταλλαγή πληροφοριών δρομολόγησης, είναι παραδεχτό το γεγονός ότι οι μηχανισμοί για την ανταλλαγή πληροφοριών bundle δρομολόγησης μεταξύ περιοχών είναι διαφορετικοί από αυτούς που ανταλλάσσουν πληροφορίες εντός μιας περιοχής. Ακόμη, η αρχιτεκτονική αναγνωρίζει ότι οι μηχανισμοί για εντός περιοχής μεταφορά σε ένα τμήμα του DTN μπορεί να είναι ακατάλληλοι για χρήση σε άλλα τμήματά αυτού του DTN και ότι δεν απαιτείται ομοιογένεια του πρωτοκόλλου δρομολόγησης εντός περιφέρειας σε όλο το DTN.

6.2 Καταστάσεις Δρομολόγησης

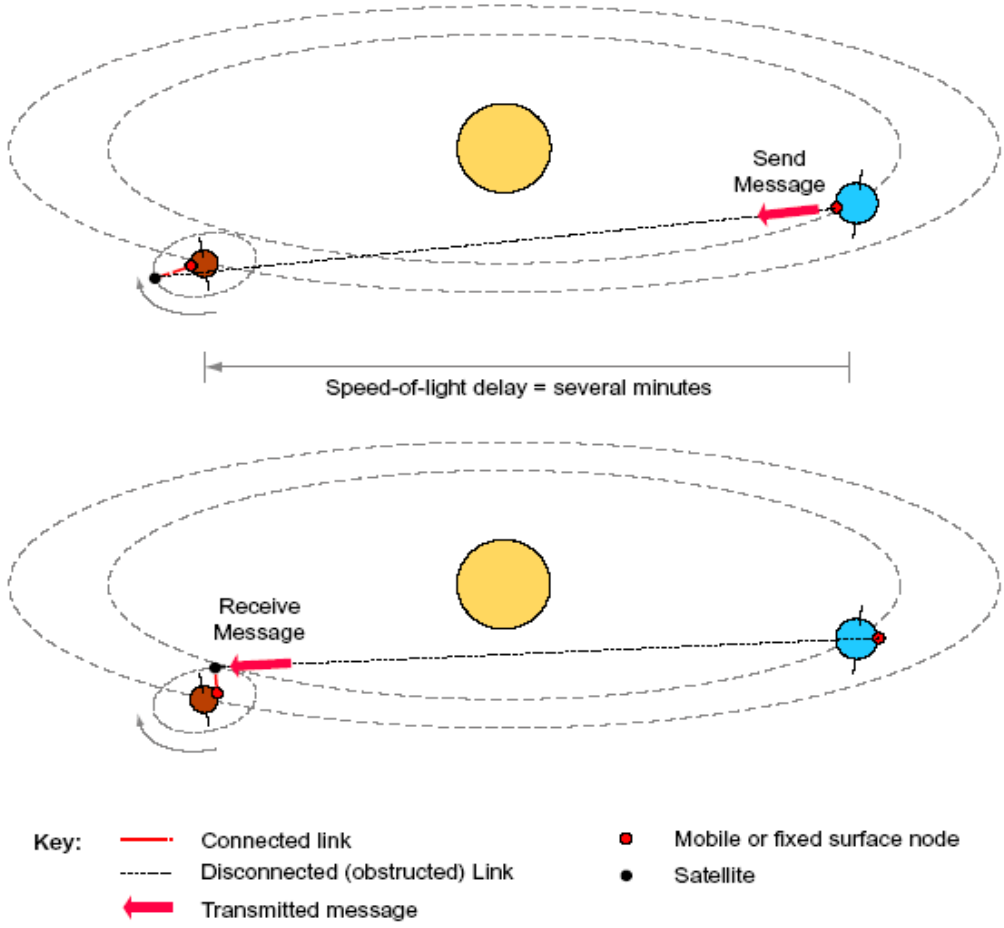
Τα DTN πρέπει να λειτουργούν σύμφωνα με της περισσότερες ή και όλες τις παρακάτω καταστάσεις δρομολόγησης. Αυτές οι καταστάσεις παρουσιάζονται περισσότερο σαν πληροφορία παρά σαν απαιτήσεις για όλα τα DTN,αν και πολλές από αυτές ίσως να απαιτούνται για ένα συγκεκριμένο DTN.

Συνεχείς(διαρκείς) Επικοινωνίες: Οι συνεχείς επικοινωνίες είναι συνδιαλέξεις με έναν γειτονικό DTN κόμβο και είναι μονίμως διαθέσιμες ή μπορούν να γίνουν διαθέσιμες αν ζητηθεί. Στον κόσμο του IP,οι DSL(Digital Subscriber Line) συνδέσεις είναι ένα παράδειγμα του παρόντος κειμένου, ενώ οι dial-up συνδέσεις είναι ένα παράδειγμα του επόμενου.

Διακοπτόμενες-Προγραμματισμένες Επικοινωνίες:

Στο διάστημα τα πάντα βρίσκονται σε συνεχή κίνηση και οι καθυστερήσεις της ταχύτητας του φωτός είναι σημαντικές (δεκάδες λεπτά μέσα στο ηλιακό μας σύστημα).Τα προγραμματισμένα δρομολόγια είναι αυτά όπου υπάρχει συμφωνία να εγκατασταθεί μια γραμμή επικοινωνίας μεταξύ δύο κόμβων σε συγκεκριμένη στιγμή,για συγκεκριμένη χρονική διάρκεια.Αν οι κόμβοι επικοινωνίας κινούνται στις αναμενόμενες διαδρομές,μπορούν να προβλέψουν ή να λάβουν προγραμματισμένο χρόνο για τις μελλοντικές τους θέσεις και επομένως να κανονίσουν τις μελλοντικές συνδιαλέξεις επικοινωνίας.

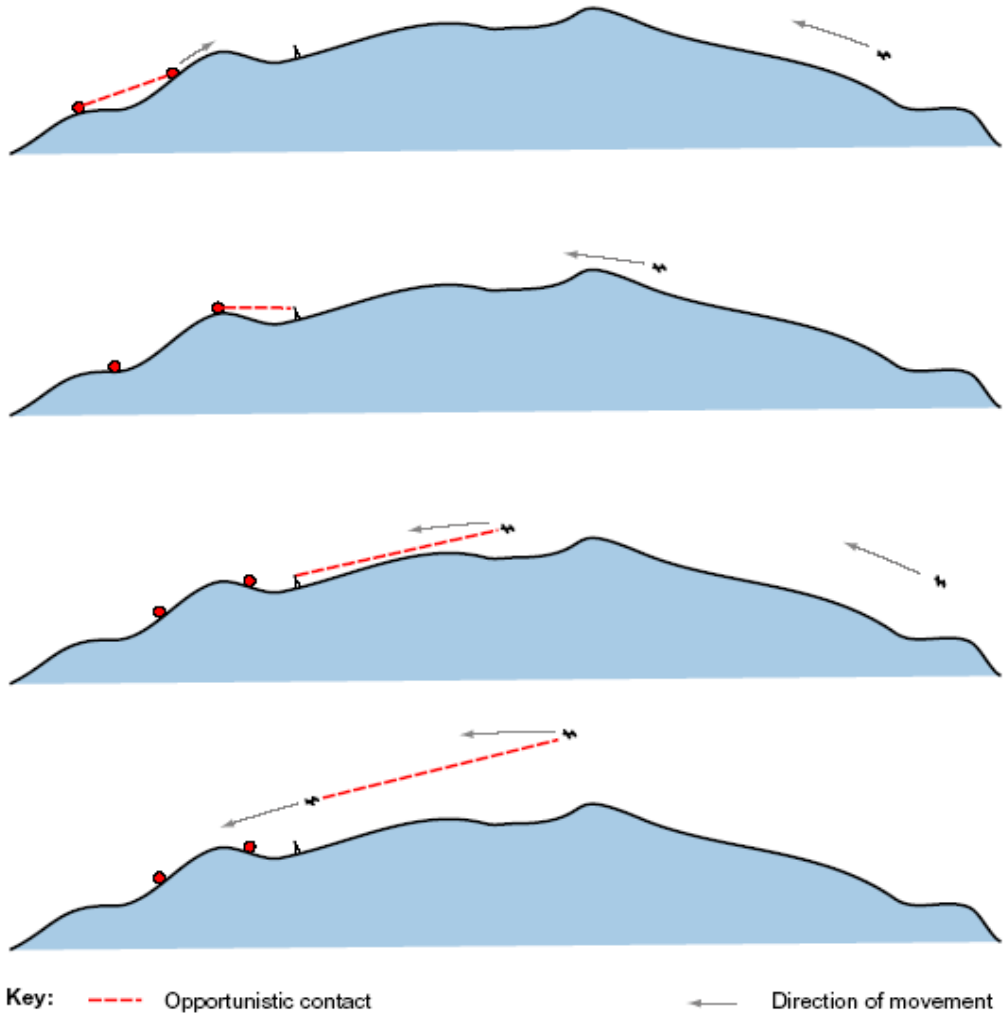
Οι προγραμματισμένες επικοινωνίες μπορεί να περιλαμβάνουν την αποστολή μηνύματος μεταξύ κόμβων που δεν βρίσκονται σε άμεση επικοινωνία,όπως φαίνεται στο σχήμα παρακάτω.Επίσης,μπορεί να περιλαμβάνουν την αποθήκευση πληροφορίας μέχρι αυτή να προωθηθεί ή μέχρι η εφαρμογή-παραλήπτης να προλάβει τον ρυθμό μετάδοσης δεδομένων του αποστολέα.



Διακοπτόμενες-Ευκαιριακές Επικοινωνίες:

Οι κόμβοι του δικτύου ίσως χρειαστεί να επικοινωνήσουν κατά την διάρκεια ευκαιριακών επαφών,όπου ο αποστολέας και ο δέκτης επικοινωνούν σε απρογραμμάτιστο χρόνο. Άνθρωποι, οχήματα, αεροσκάφη ή δορυφόροι που βρίσκονται σε κίνηση μπορεί να χρειαστεί να επικοινωνήσουν και να ανταλλάξουν πληροφορίες όταν τυχαίνει να είναι σε απόσταση ικανή και χωρίς εμπόδια για επικοινωνία.

Όλοι μας χρησιμοποιούμε ευκαιριακές επικοινωνίες:όταν κατά τύχη συναντάμε τον συγκεκριμένο άνθρωπο που θέλαμε να μιλήσουμε,του μιλάμε.Το ίδιο μοντέλο μπορεί να εφαρμοστεί και στην ηλεκτρονική επικοινωνία.Για παράδειγμα,τα ασύρματα PDA μπορούν να σχεδιαστούν και να προγραμματιστούν να στέλνουν και να δέχονται πληροφορίες όταν συγκεκριμένοι άνθρωποι που κουβαλάν μαζί τους τα PDA βρίσκονται σε ακτίνα επικοινωνίας.



<u>Διακοπτόμενες-Προβλεπόμενες Επικοινωνίες:</u> Οι προβλεπόμενες επικοινωνίες είναι αυτές που βασίζονται σε μη σταθερό πρόγραμμα,αλλά σχετίζονται με τις ευκαιριακές επικοινωνίες,όπου η μη συνεχής επαφή με τον γειτονικό κόμβο ξεκινά σε συγκεκριμένη χρονική περίοδο και διατηρείται για ορισμένη διάρκεια.Έχοντας μεγαλυτερη σιγουριά ότι η επικοινωνία θα πραγματοποιηθεί,ένας DTN κόμβος μπορεί να κατανείμει σ'αυτήν την περίοδο προβλεπόμενης επαφής τα πακέτα που ούτως ή άλλως θα διαθέτονταν με άλλες επαφές.Οι αλγόριθμοι για την καθιέρωση του προβλεπόμενου χρόνου και της διάρκειας μιας επαφής,ο βαθμός αβεβαιότητας γι'αυτούς τους υπολογισμούς και τις εκτιμήσεις,ο χρόνος για να εγκαταλείψουμε την προσπάθεια για προβλεπόμενη επικοινωνία και οι γραμμές κατεύθυνσης για την κατανομή πακέτων σε τέτοιου είδους επικοινωνίες,είναι όλα ζητήματα ανοιχτά προς έρευνα.

6.3 Δρομολόγηση Προσανατολισμένης Επικοινωνίας

Για να παρθούν αποφάσεις δρομολόγησης για τον διαμοιρασμό των πακέτων σε μελλοντικές επικοινωνίες,χρειάζεται ένας DTN κόμβος που να μπορεί να εκτιμήσει ποια επικοινωνία με άλλα σημεία του δικτύου θα προκύψει μέσω αυτής της επαφής.Βασιζόμενοι στην αναμενόμενη επικοινωνία του δικτύου με κάθε μία από τις διακοπτόμενες επικοινωνίες και στα όμοια χαρακτηριστικά επικοινωνίας για τους

διαρκώς συνδεδεμένους γειτονικούς κόμβους,ένας DTN κόμβος μπορεί να «αποφασίσει» για το πώς θα κατανείμει τα πακέτα στις επικοινωνίες.Θα μπορούσε να σκεφτεί κάποιος για τον καταμερισμό των πακέτων στις επικοινωνίες ότι μπορεί να γίνει με τη δημιουργία διατεταγμένης λίστας αναφορών για τα πακέτα που αποθηκεύονται και δίνοντας αυτήν τη λίστα στο πιο κάτω επίπεδο του πρωτοκόλλου για την μεταφορά στην αρχή της επικοινωνίας.Τα πακέτα που δεν μεταφέρθηκαν κατά την επικοινωνία θα επιστρέφουν στην λίστα για να κατανεμηθούν στις επαφές που θα προκύψουν.Με αυτήν την προσέγγιση το Bundle επίπεδο είναι απολύτως ελεύθερο να ρυθμίσει την προώθηση των πακέτων για τις επόμενες επικοινωνίες, βασιζόμενο στη λήψη νέων και ίσως υψηλής προτεραιότητας πακέτων.Τέλος, είναι πιθανό το Bundle επίπεδο να μπορεί να κάνει αλλαγές στη λίστα αναφορών κατά τη διάρκεια της συνδιάλεξης,αν επιτρέπεται από την εφαρμογή.

6.4 Πρωτόκολλα Δρομολόγησης

Αν και δεν έχουν αναπτυχθεί ακόμη πρωτόκολλα δρομολόγησης γι'αυτήν την αρχιτεκτονική πιθανολογικά χρειάζονται τουλάχιστον δύο:ένα που να υποστηρίζει δρομολόγηση εντός των περιοχών του DTN και τουλάχιστον ένα για την υποστήριξη δρομολόγησης μεταξύ των περιοχών.Είναι πιθανό πως ένα inter-region πρωτόκολλο δρομολόγησης,για δίκτυο που έχει μία ή περισσότερες ζεύξεις με 40λεπτη καθυστέρηση προς τη μία κατεύθυνση και δύο βδομάδες αποσύνδεση(κάτι τέτοιο μπορεί να συμβεί σε διαστημική αποστολή) να είναι εντελώς διαφορετικό με ένα inter-region πρωτόκολλο δρομολόγησης που υποστηρίζει ένα δίκτυο με αισθητήρια συνδεδεμένο στο διαδίκτυο μέσω ενός δορυφόρου χαμηλής τροχιάς γύρω από τη γη.

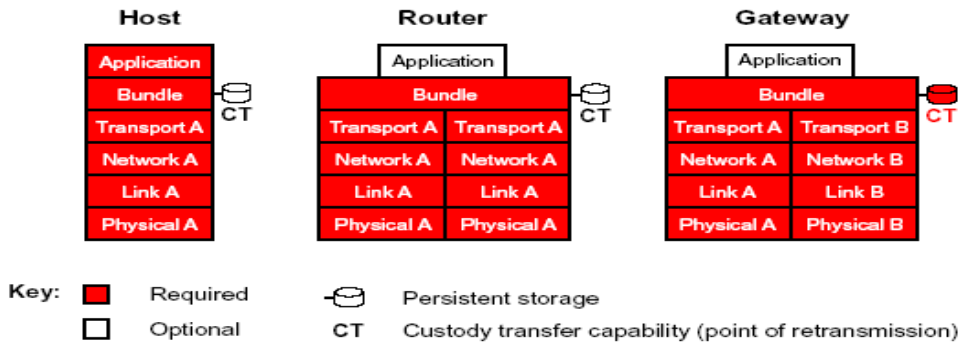
Σκοπός είναι,τα πρωτόκολλα δρομολόγησης για να υποστηρίξουν την διακοπτόμενη επικοινωνία,να διατηρήσουν τις πληροφορίες της κατάστασης της ζεύξης ενός βήματος και τον τύπο της συνολικής πορείας και απόστασης πέρα από το ένα βήμα(hop).Η προσπάθεια να διατηρηθεί μια ακριβής εικόνα του δικτύου επικοινωνίας πέραν του ενός hop,όταν οι διαδρομές αποτελούνται από προγραμματισμένες ή πιθανές επαφές αμφιβόλου χωρητικότητας, είναι ανώφελη.Από την άλλη μεριά όμως,μια πιθανολογική εικόνα επικοινωνίας μπορεί να πραγματοποιηθεί και να δημοσιοποιηθεί με τέτοιον τρόπο που να επιτρέπει την αποτελεσματική χρήση αυτών των διακοπτόμενων συνδέσεων.Το γεγονός ότι δεν υπάρχει απαίτηση για προσωρινή end-to-end διαδρομή,κάνει το όλο εγχείρημα να φαίνεται εφικτό.

7 ΘΕΜΑΤΑ ΤΟΠΟΛΟΓΙΑΣ

7.1 DTN Κόμβοι

Σε ένα DTN,ο κόμβος είναι μια οντότητα με ένα επίπεδο bundle.Ένας κόμβος μπορεί να είναι ξενιστής (host),δρομολογητής (router), πύλη (gateway) ή και συνδυασμός αυτών,λειτουργώντας ως πηγή,προορισμός ή μεταδότης πακέτων.

Ξενιστής(Host): Στέλνει και/ή δέχεται πακέτα(bundles),αλλά δεν τα μεταβιβάζει. Ένας ξενιστής μπορεί να είναι η πηγή ή ο προορισμός της μεταφοράς του πακέτου.Τα bundle επίπεδα των ξενιστών που λειτουργούν σε γραμμές μεγάλων καθυστερήσεων,χρειάζονται μόνιμη αποθήκευση στην οποία να βάζουν σε σειρά τα πακέτα μέχρι οι ζητούμενες συνδέσεις αποστολής των πακέτων να είναι διαθέσιμες.Οι ξενιστές προαιρετικά μπορούν να υποστηρίξουν κηδεμονικές μεταφορές.
Δρομολογητής: Μεταβιβάζει πακέτα σε μια απλή περιοχή του DTN, και μπορεί προαιρετικά να γίνει ξενιστής.Τα bundle επίπεδα των δρομολογητών που λειτουργούν σε ζεύξης μεγάλων καθυστερήσεων, χρειάζονται μόνιμη αποθήκευση στην οποία να βάζουν σε σειρά τα πακέτα μέχρι οι ζητούμενες συνδέσεις να είναι διαθέσιμες.Οι δρομολογητές προαιρετικά μπορούν να υποστηρίξουν κηδεμονικές μεταφορές.
Πύλη: Προωθεί πακέτα ανάμεσα σε δύο ή περισσότερες DTN περιοχές και προαιρετικά μπορεί να γίνει ξενιστής.Τα bundle επίπεδα των πυλών πρέπει να διαθέτουν μόνιμη αποθήκευση και να υποστηρίζουν κηδεμονικές μεταφορές.Οι πύλες μπορούν να κάνουν μετατροπές μεταξύ των πρωτοκόλλων χαμηλότερων επιπέδων των περιοχών που καλύπτουν.



Οι κόμβοι σε ένα IPN έχουν αρκετές υπευθυνότητες.Σαν μέρη της store-and-forward αλυσίδας,έχουν την ευθύνη για την κατανομή των πόρων ώστε να υποστηρίξουν την μεταφορά των πακέτων.Αυτοί οι πόροι συμπεριλαμβάνουν εκτός των άλλων και την χωρητικότητα ενδιάμεσης μνήμης και μεταφοράς.

Ακόμη, οι IPN κόμβοι έχουν την ευθύνη πραγματικά να φέρουν σε πέρας τη μεταφορά των πακέτων.Οι απαιτήσεις αξιοπιστίας για τις μεταφορές πακέτων ορίζονται από την εφαρμογή που χρησιμοποιείται και περιλαμβάνουν αξιόπιστες και μη αξιόπιστες μεταφορές(πιθανώς με κάποιες ενδιάμεσες αξιόπιστες υπηρεσίες).Οι

IPN κόμβοι είναι υπεύθυνοι για το ποιος μηχανισμός αξιοπιστίας θα εφαρμοστεί από αυτούς που υπάρχουν στα κατώτερα επίπεδα(επίπεδο μεταφοράς και κάτω) και κατά πόσο θα αυξήσουν αυτούς τους μηχανισμούς για να επιτευχθεί η αναμενόμενη αξιοπιστία.

Τέλος,οι IPN κόμβοι ευθύνονται για τη δρομολόγηση των πακέτων ανάμεσα στα domain του IPN.Αυτοί οι κόμβοι πιθανώς να εξαρτώνται από τις υπηρεσίες των τοπικών δικτύων για τη δρομολόγηση μεταξύ των domains.

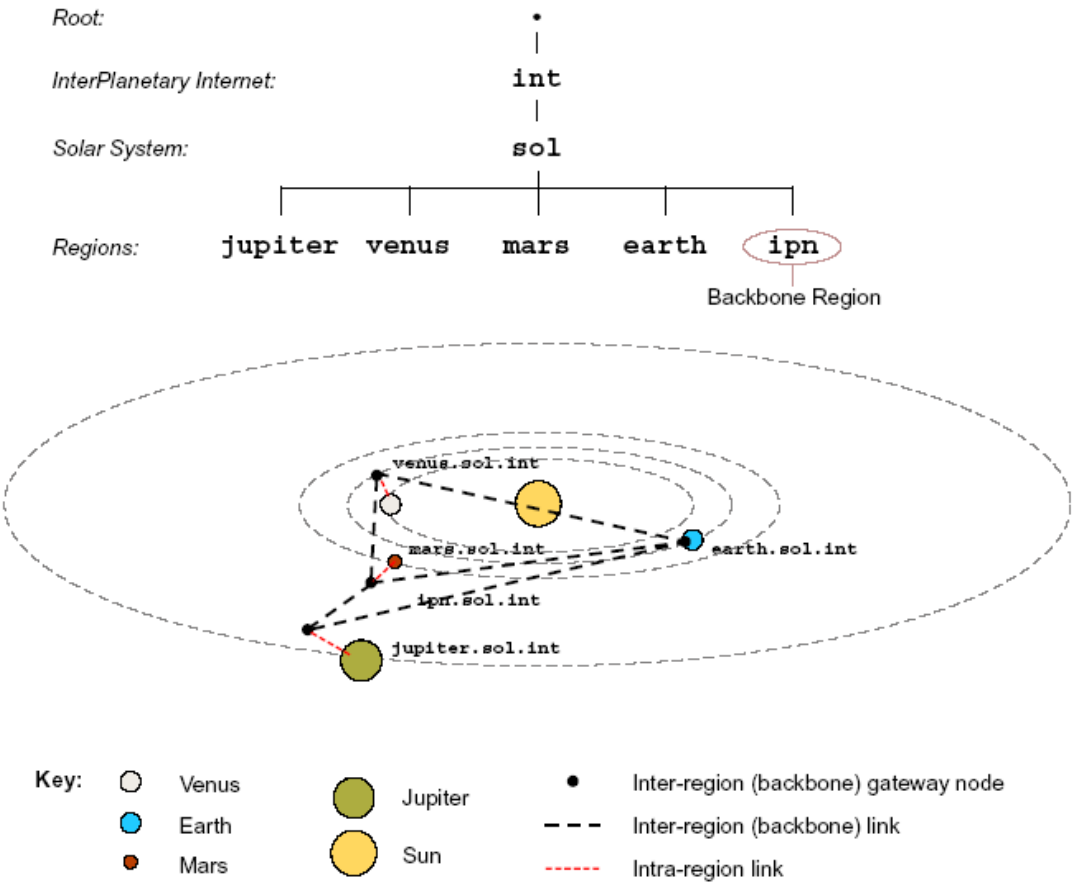
7.2 Περιοχές DTN

Το DTN είναι ένα δίκτυο δικτύων,όπου το κάθε ένα από αυτά τα δίκτυα είναι μια περιοχή,της οποίας τα επικοινωνιακά χαρακτηριστικά είναι ομοιογενή.Για παράδειγμα,μια περιοχή μπορεί να είναι το Internet της γης,ένα ασύρματο δίκτυο Προσωπικού Ψηφιακού Βοηθού(PDA),ένα δίκτυο με αισθητήρια,ένα στρατιωτικής τακτικής δίκτυο,η επιφάνεια ενός πλανήτη ή ένα διαστημόπλοιο.

Σ'αυτό το σημείο αξίζει να προσδιοριστούν οι απαιτήσεις των DTN περιοχών:

- Κάθε DTN περιοχή πρέπει να έχει έναν αναγνωριστικό μέρος που μοιράζεται σε όλους τους DTN κόμβους της περιοχής.Η περιοχή πρέπει να προσδιορίσει τις ονοματολογικές συμβάσεις που θα χρησιμοποιηθούν εντός της περιοχής σαν αναγνώριση οντότητας.
- Κάθε κόμβος που είναι μέλος της περιοχής πρέπει να έχει ένα μοναδικό αναγνωριστικό που να προκύπτει από το αναγνωριστικό μέρος της περιοχής.Να έχουμε υπόψη όμως ότι για μερικούς τύπους περιοχών,ένας κόμβος μπορεί να αποτελείται από τη συλλογή υπολογιστικών στοιχείων,πιθανώς γεωγραφικά διαμοιρασμένων.Ένα απλό μοναδικό αναγνωριστικό μπορεί συλλογικά να αναφέρεται σ'αυτούς .Ακόμη,η απαίτηση για μοναδικό αναγνωριστικό εφαρμόζεται μόνο σε κόμβους που σκοπεύουν να λάβουν δεδομένα από άλλους DTN κόμβους.
- Κάθε πιθανό μέλος της περιοχής για να γίνει μέλος πρέπει να έχει τη δυνατότητα να επικοινωνεί με τα άλλα μέλη της περιοχής χωρίς να στηρίζεται στους DTN κόμβους εκτός περιοχής.(Αν και ένας DTN κόμβος ίσως να μην είναι άμεσα προσβάσιμος .Σε αυτήν την περίπτωση απαιτείται store-and-forward χειρισμός από άλλους DTN κόμβους μέσα στην ίδια περιοχή.)

Το σχήμα παρακάτω δείχνει μερικές πιθανές περιοχές που βασίζονται στη διαστημική ιεραρχία.Η περιοχή ipn.sol.int αποτελεί το backbone των πυλών του IPN για συνδέσεις ευρείας περιοχής.

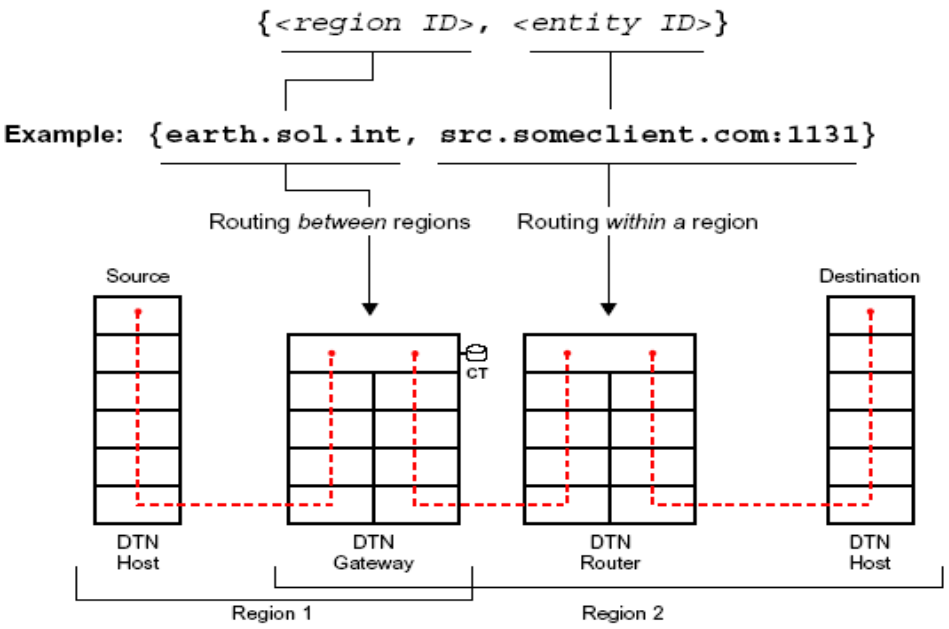


7.3 Ονοματολογίες και Διευθύνσεις

Κάθε DTN κόμβος έχει δύο μέρη ονοματολογίας :ένα για τον κωδικό περιοχής (region ID)(ή απλά όνομα περιοχής) και ένα για τον κωδικό της οντότητας (entity ID)(ή όνομα οντότητας).Η δρομολόγηση μεταξύ των περιοχών βασίζεται μόνο στους κωδικούς περιοχής,οι οποίοι είναι ενωμένοι με τις διευθύνσεις ανταπόκρισής τους στο DTN.Η δρομολόγηση μέσα στις περιοχές βασίζεται μόνο στους κωδικούς οντότητας,οι οποίοι είναι συσχετισμένοι με τις διευθύνσεις ανταπόκρισης μόνο μέσα στην συγκεκριμένη περιοχή.Έπομένως, κάθε περιοχή χρησιμοποιεί διαφορετική αντιστοιχία κωδικών οντότητας για τις διευθύνσεις και δε χρειάζεται καθόλου εύρος ζώνης για να αντιγραφούν οι αντιστοιχίες των ονομάτων και διευθύνσεων μεταξύ των περιοχών.

Οι πύλες ανήκουν σε δύο ή περισσότερες περιοχές και μετακινούν τα πακέτα (bundles) μεταξύ των περιοχών.Μ'αυτόν τον τρόπο,οι πύλες έχουν πολλαπλούς κωδικούς περιοχής.Οι κωδικοί περιοχής χρησιμοποιούν την ίδια σύνταξη όπως γίνεται και στο διαδίκτυο με το Domain Name System (DNS).

Μια οντότητα μπορεί να είναι ξενιστής (ένας DTN κόμβος), μια εφαρμογή, ένα πρωτόκολλο, μία διεύθυνση(URL),ένα port(χρησιμοποιείται για να βρεθεί η bundle υπηρεσία σε ένα host) ή κάτι άλλο.



8 IPN ΠΑΡΑΔΕΙΓΜΑΤΑ

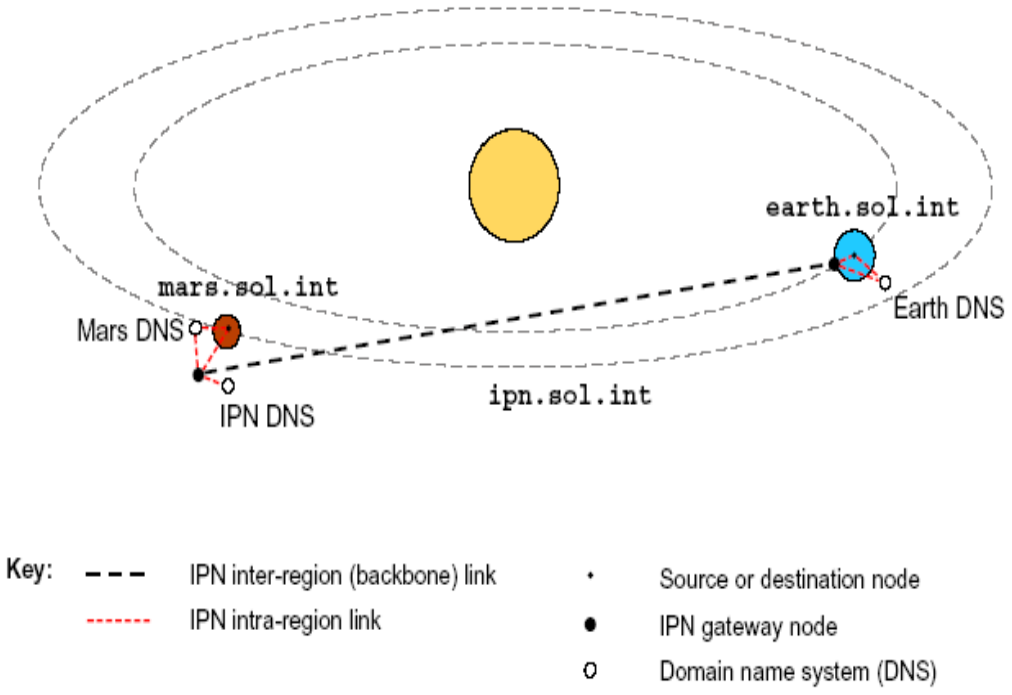
8.1 Σύνδεση Backbone

Είναι σημαντικό να κατανοήσουμε τη δρομολόγηση που χρειάζεται στις πύλες του IPN.Αντίθετα με τις χερσάιες επικοινωνίες,οι γραμμές επικοινωνίας μεγάλων αποστάσεων στο IPN είναι κατευθηντικές,κινητές και υψηλά προγραμματισμένες.Αυτό έχει μεγάλη σημασία,επειδή η κατευθηντικότητα σε συνδυασμό με την κινητικότητα σημαίνει ότι ο μεταδότης και ο λήπτης πρέπει να ανιχνεύσουν ο καθένας την τροχιά του άλλου,άρα και τη θέση που βρίσκονται,προκειμένου να εγκαταστήσουν και να διατηρήσουν τη ζεύξη επικοινωνίας.Στο IPN,η κινητικότητα εξαρτάται από την μηχανική των τροχιών και έτσι είναι σχετικά προβλέψιμη.Όμως, αυτό σημαινει ότι τους κόμβους πού φυσιολογικά θα τους θεωρούσαμε σταθερούς, όπως για παράδειγμα οι κεραίες στην επιφάνεια της γης,είναι στην ουσία κινητές λόγω της περιστροφικής κίνησης της γης γύρω από τον εαυτό της και γύρω από τον ήλιο.(Σ'αυτό το παράδειγμα,περιοριζόμαστε στο τοπικό ηλιακό μας σύστημα και δεν εξετάζουμε την κίνηση του ήλιου μας σχετικά με τα ουράνια σώματα έξω από το ηλιακό μας σύστημα.) Μπορούμε να περιγράψουμε την προβλέψιμη πλευρά της κίνησης ενός κόμβου με έναν πίνακα με τις θέσεις των ουράνιων σωμάτων σε συγκεκριμένα διαστήματα του χρόνου.Ο κατευθηντικός μεταδότης και λήπτης πρέπει να ξέρουν ο ένας τη θέση του άλλου για να εγκατασταθεί η ζεύξη μεταξύ τους.Επιπλέον,οι πόροι επικοινωνίας που θα χρειαστούν είναι εξαιρετικά προγραμματισμένοι.Δεν είναι αρκετό για τον λήπτη να υποδείξει τον ενδεχόμενο στόχο και απλά να περιμένει.Για παράδειγμα ένας χερσαίος κόμβος τυπικά θα πρέπει να υποδεικνύει αρκετούς στόχους διαδοχικά αλλά ένας διαπλανητικός κόμβος δε θα έχει αρκετή ισχύ απλά να περιμένει για εισερχόμενα μηνύματα.Αντίθετα,το πρόγραμμα των πιθανοτήτων επικοινωνίας πρέπει να υπολογίζεται και μετά να καθορίζεται με σχεδιασμένες υποδείξεις επικοινωνίας.Μια ευκαιρία επικοινωνίας δείχνει ότι τα σημεία προορισμού θα μπορούσαν να εγκαταστήσουν μια σύνδεση αν εντόπιζαν το καθένα τη θέση του άλλου την κατάλληλες στιγμές.Αναφερόμαστε σε ένα σχεδιασμένο παράδειγμα επικοινωνίας σαν μια συμφωνία μεταξύ των δύο ομάδων να έρθουν σε επαφή και να επικοινωνήσουν για ορισμένη περίοδο του χρόνου.Τα πρωτόκολλα που εγκαθιστούν την προγραμματισμένη επικοινωνία μεταξύ όλων των πιθανών ζευγαριών,θα εξελιχθούν από κάτι που αρχικά γινόταν χειροκίνητα σε κάτι περισσότερο αυτόματο καθώς το IPN αναπτύσσεται.

Η προγραμματισμένη φύση της σύνδεσης στο InterPlanetary Internet, ιδιαίτερα στις ζεύξεις του βαθύ διαστήματος,σημαίνει ότι από τη στιγμή που θα γίνει η λήψη του πακέτου σε μια πύλη του IPN,μερικές ή όλες από τις πιθανές εξερχόμενης κίνησης διαδρομές,μπορεί να είναι «πεσμένες». Η πύλη πρέπει να αποθηκεύσει το πακέτο μέχρι η κατάλληλη ζεύξη να είναι διαθέσιμη και μετά να μεταφέρει το πακέτο μέσω αυτής της ζεύξης. Μια από τις βασικές διαφορές μεταξύ του Διαπλανητικού με του χερσαίου Internet,είναι αυτή η αναγκαστική χρήση των store-and-forward μηχανισμών για τη δρομολόγηση των πακέτων.

8.2 Παράδειγμα IPN

Έχοντας υπόψη τα παραπάνω,ας δούμε το παρακάτω παράδειγμα με σχεδιαγράμματα.Στο παράδειγμα χρησιμοποιούνται τρεις περιοχές συνδεδεμένες από δύο πύλες με ένα DNS για κάθε περιοχή.



Ο παρακάτω πίνακας δείχνει τα ονόματα των κόμβων που χρησιμοποιήθηκαν στο παράδειγμα.Για να γίνει απλούστερο,όλες οι εφαρμογές του bundle επιπέδου στης Γης και στου Άρη τις περιοχές χρησιμοποιούν το πρωτόκολλο μεταφοράς TCP και βρίσκονται στην TCP πόρτα 6769.

Node	IPN Regions	Node Names
Source	earth.sol.int	{earth.sol.int, src.jpl.nasa.gov:6769}
Earth Gateway	earth.sol.int ipn.sol.int	{earth.sol.int, ipngw1.jpl.nasa.gov:6769} {ipn.sol.int, ipngw1.jpl.nasa.gov}
Mars Gateway	ipn.sol.int mars.sol.int	{ipn.sol.int, ipngw2.nasa.mars.org} {mars.sol.int, ipngw2.nasa.mars.org:6769}
Destination	mars.sol.int	{mars.sol.int, dst.jpl.nasa.gov:6769}

Προτού ξεκινήσουν οι μεταφορές το επίπεδο Bundle όλων των κόμβων,συγχρονίζουν το χρόνο μεταξύ τους.Αυτό χρειάζεται για το σταθερό υπολογισμό του προγράμματος επαφών και για τον χρόνο ζωής του bundle(πακέτου) στο DTN.

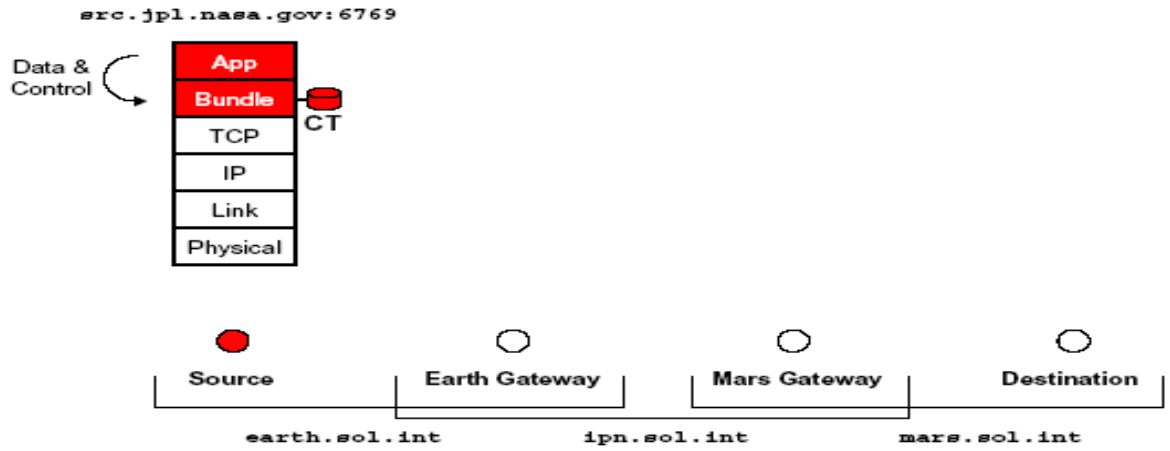
8.2.1 ΒΗΜΑ 1ο:ΔΗΜΙΟΥΡΓΙΑ BUNDLE ΣΤΗΝ ΠΗΓΗ

Η εφαρμογή της πηγής επικαλείται το bundle επίπεδό της,ζητώντας μεταφορά του πακέτου με επικεφαλίδα,όπως φαίνεται στον πίνακα παρακάτω.Τα δεδομένα της πηγής του χρήστη περιέχουν πληροφορίες για την εφαρμογή του προορισμού για επεξεργασία,αποθήκευση,διάθεση και αντιμετώπιση προβλημάτων των δεδομένων.Αυτά τα δεδομένα του χρήστη δεν είναι εμφανή στα επίπεδα bundle που ελέγχουν τη μεταφορά.

Item	Value
Source	{earth.sol.int, src.jpl.nasa.gov:6769}
Destination	{mars.sol.int, dst.jpl.nasa.gov:6769}
Class of service (CoS)	• Custody transfer • Normal priority • Time-to-live = 36 hours
Signature	*<bundle-specific encrypted signature using source's private key>*
User Data	Application-specific data, including instructions to the destination application for processing, storage, disposal, and error-handling. (User data is not visible to bundle layers.)

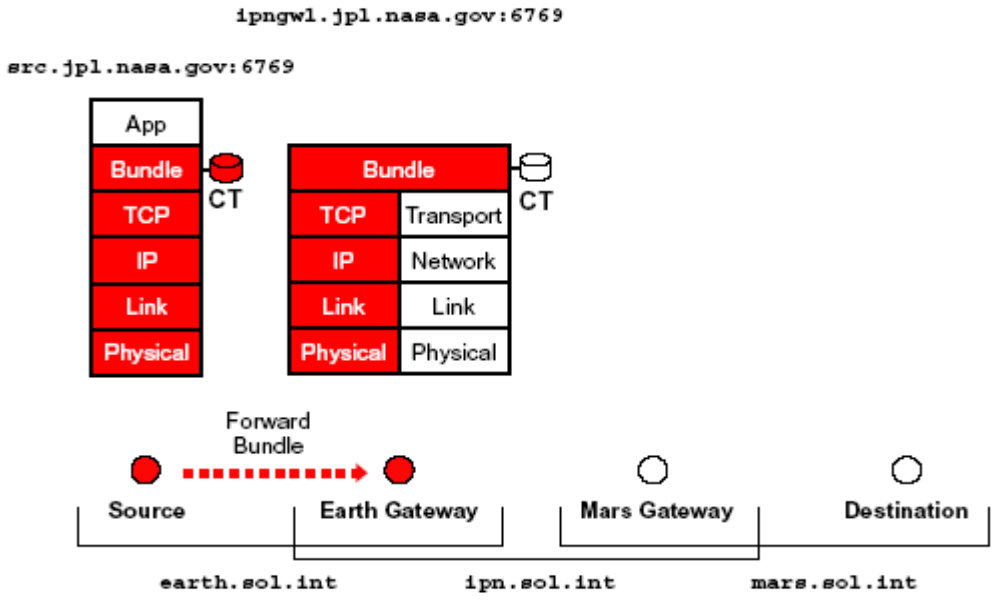
Το επίπεδο bundle της πηγής επιβεβαιώνει την υπογραφή της πηγής, δημιουργεί ένα πακέτο,επισυνάπτει την δική του υπογραφή μετά από την επικεφαλίδα του πακέτου και αποθηκεύει το αποτέλεσμα στην αποθήκη διαρκείας.Η αποθήκευση απαιτείται ακόμη και αν υπάρχει ευκαιρία για άμεση προώθηση,επειδή το επίπεδο bundle αποδέχεται τη μεταφορά με κηδεμονία και πρέπει γι'αυτό το λόγο να είναι

προετοιμασμένο να μεταφέρει ξανά το πακέτο αν δε λάβει αναγνώριση μέσα στον απαιτούμενο χρόνο από τον λήπτη που έλαβε το πακέτο.



8.2.2 ΒΗΜΑ 2ο :ΜΕΤΑΦΟΡΑ ΑΠΟ ΤΗΝ ΠΗΓΗ

Το bundle επίπεδο της πηγής συμβουλεύεται τον δικό του πίνακα δρομολόγησης και βρίσκει κατά πρώτον ότι η πύλη της Γης {earth.sol.int,ipngw1.jpl.nasa.gov : 6769} είναι ο επόμενος διαθέσιμος σταθμός να δεχτεί κηδεμονικές μεταφορές για την επικείμενη διαδρομή προς τον προορισμό και κατά δεύτερον ότι το TCP είναι το κατάλληλο πρωτόκολλο μεταφοράς.Επίσης,το bundle επίπεδο της πηγής προδιορίζει ότι υπάρχει συνεχής σύνδεση με την πύλη της Γης.Το bundle επίπεδο μεταφέρει ένα αντίγραφο του πακέτου στην πύλη της γης μέσω TCP, ξεκινάει έναν χρονοδιακόπτη αναμετάδοσης time-to-acknowledge,για να ξαναστείλει το πακέτο αν χρειαστεί,και περιμένει την επιβεβαίωση ασφαλής μεταφοράς από την πύλη.

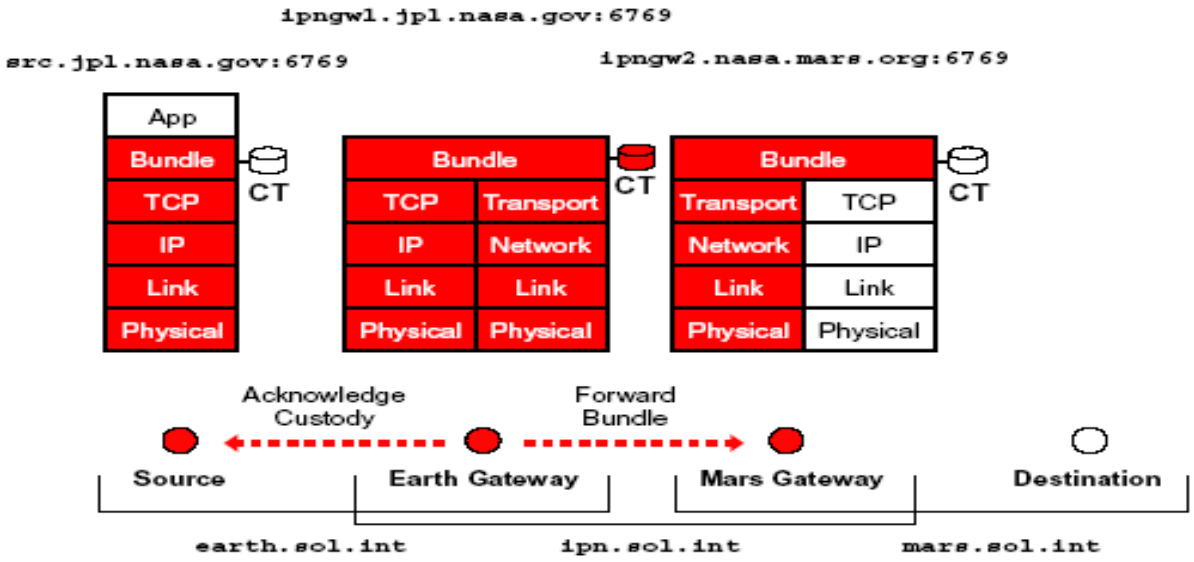


8.2.3 ΒΗΜΑ 3ο : ΕΠΕΞΕΡΓΑΣΙΑ ΚΑΙ ΠΡΟΩΘΗΣΗ ΠΑΚΕΤΟΥ ΠΡΩΤΟΥ ΒΗΜΑΤΟΣ

Όταν το επίπεδο bundle της πύλης της γης δεχτεί το πακέτο μέσω TCP, τερματίζει τη συνδιάλεξη.Από τη στιγμή που αυτό είναι το σύνορο ασφαλείας για το Διαπλανητικό Internet,το bundle επίπεδο της πύλης της γης επαληθεύει την υπογραφή της εφαρμογής της πηγής και το κατάλληλο επίπεδο υπηρεσιών(QoS), είτε χρησιμοποιώντας τα αποθηκεμένα αντίγραφα πιστοποιητικών του γειτονικού χρήστη και πιστοποιητικό δικαιοδοσίας δημόσιων κλειδιών είτε αποκτώντας τα απαιτούμενα πιστοποιητικά και κλειδιά.Έπειτα,τα συγκρίνει με την υπογραφή της λίστας του ελέγχου προσπέλασης.Αφού εξασφαλίσει την πρέπουσα μεταφορά,το bundle επίπεδο της πύλης της γης αντικαθιστά την υπογραφή του bundle επιπέδου της πηγής με τη δικιά της,αφήνωντας όμως την υπογραφή της εφαρμογής της πηγής ανέπαφη.Μετά από αυτό, αποθηκεύει το πακέτο που έλαβε στην διαρκή αποθήκη.

Το επίπεδο bundle της πύλης της γης προστρέχει στον δικό του πίνακα δρομολόγησης και βρίσκει ότι η πύλη του Άρη {mars.sol.int, ipngw2.jpl.nasa.mars.org: 6769} είναι ο επόμενος διαθέσιμος σταθμός να δεχτεί κηδεμονικές μεταφορές για την επικείμενη διαδρομή προς τον προορισμό.Υπολογίζει ότι η πύλη του Άρη θα είναι προσβάσιμη στις 11 της επόμενης μέρας, εξασφαλίζει ότι ο χρόνος ζωής του πακέτου είναι προσιτός γι'αυτή την καθυστέρηση και προσθέτει το πακέτο στη λίστα επαφών του για την προώθησή του.

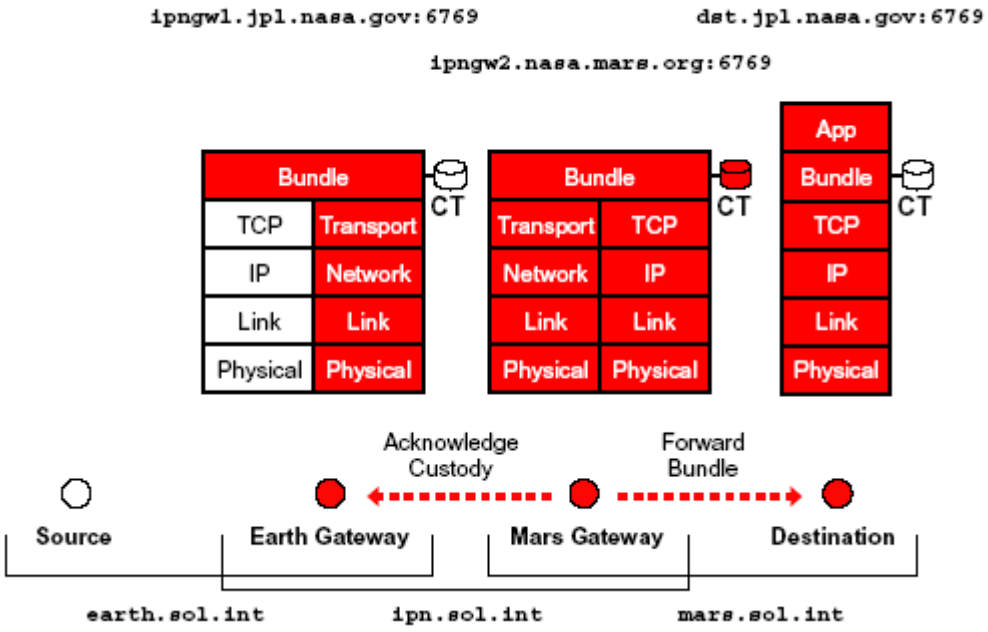
Έπειτα,το bundle επίπεδο της πύλης της γης αναλαμβάνει την κηδεμονία του πακέτου,ενημερώνει αυτήν την πληροφορία στην επικεφαλίδα του πακέτου και το επιβεβαιώνει αυτό με αναγνώριση στο επίπεδο bundle της πηγής,η οποία διαγράφει με τη σειρά της τα αντίγραφα κηδεμονίας του πακέτου που είχε.Όταν έρθει η ώρα της ζητούμενης επικοινωνίας,το bundle επίπεδο της πύλης της γης εγκαθιστά τη σύνδεση με το κατάλληλο πρωτόκολλο μεταφοράς ευρείας περιοχής και προωθεί το πακέτο.



8.2.4 ΒΗΜΑ 4ο : ΔΕΥΤΕΡΟ ΒΗΜΑ ΕΠΕΞΕΡΓΑΣΙΑΣ ΚΑΙ ΠΡΟΩΘΗΣΗΣ ΠΑΚΕΤΟΥ

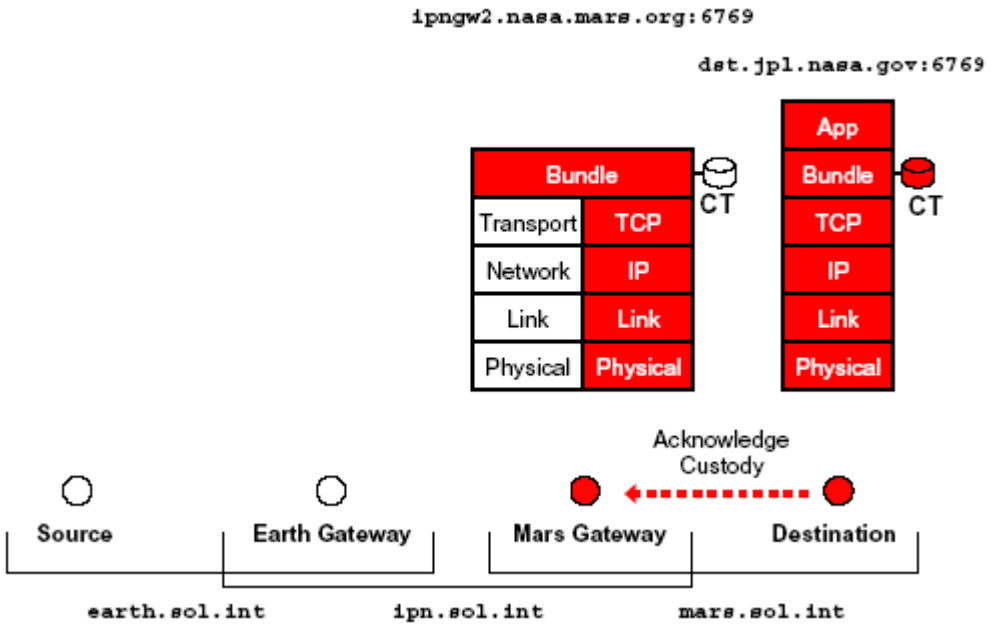
Όταν το bundle επίπεδο της πύλης του Άρη λαμβάνει το πακέτο, τερματίζει τη συνδιάλεξη μεταφοράς ευρείας περιοχής και ελέγχει την υπογραφή του bundle επιπέδου της πύλης της γης,χρησιμοποιώντας τα αποθηκευμένα αντίγραφα των πιστοποιητικών του γειτονικού δρομολογητή και το πιστοποιητικό δικαιοδοσίας δημόσιων κλειδιών. Προσδιορίζει ότι το πακέτο έχει προωθηθεί από την προσδοκώμενη πηγή και αντικαθιστά την υπογραφή του bundle επιπέδου της πύλης της γης με τη δική του,αφήνοντας την υπογραφή της εφαρμογής της πηγής ανέπαφη.Έπειτα,αποθηκεύει το πακέτο που έλαβε στην αποθήκη διαρκείας.

Το bundle επίπεδο της πύλης του Άρη προστρέχει στον πίνακα δρομολόγησής του και βρίσκει ότι ο επόμενος σταθμός προς τον προορισμό είναι ο εαυτός του.Προσδιορίζει ότι ο προορισμός είναι άμεσα διαθέσιμος,ότι το κατάλληλο πρωτόκολλο μεταφοράς είναι το TCP και εξασφαλίζει ότι ο χρόνος ζωής του πακέτου είναι επαρκής σε σχέση με την καθυστέρηση.Έπειτα,το bundle επίπεδο της πύλης του Άρη δέχεται την επιτήρηση του πακέτου,ενημερώνει γι'αυτήν την πληροφορία την επικεφαλίδα του πακέτου και το εξασφαλίζει αυτό με την αναγνώριση του bundle επιπέδου της πύλης της Γης,η οποία διαγράφει το κηδεμονικό της αντίγραφο του πακέτου.Τέλος,το bundle επίπεδο εγκαθιστά επαφή με το bundle επίπεδο του προορισμού,μέσω του TCP πρωτοκόλλου και προωθεί το πακέτο.



8.2.5 ΒΗΜΑ 5ο : ΠΑΡΑΛΑΒΗ ΠΑΚΕΤΟΥ ΑΠΟ ΤΟΝ ΠΡΟΟΡΙΣΜΟ

Όταν το bundle επίπεδο του προορισμού παραλάβει το πακέτο μέσω του TCP,τερματίζει τη συνδιάλεξη του TCP και ελέγχει την υπογραφή του bundle επιπέδου της πύλης του Άρη, χρησιμοποιώντας τα δικά του αποθηκευμένα αντίγραφα των πιστοποιητικών του γειτονικού δρομολογητή και το πιστοποιητικό δικαιοδοσίας των δημόσιων κλειδιών. Προσδιορίζει ότι το πακέτο έχει προωθηθεί από την προσδοκώμενη πηγή. Έπειτα,αποθηκεύει το πακέτο που έλαβε στην αποθήκη διαρκείας, δέχεται την κηδεμονία του πακέτου και το εξασφαλίζει αυτό με την αναγνώριση του bundle επιπέδου της πύλης του Άρη,η οποία διαγράφει το ασφαλές της αντίγραφο του πακέτου.Το bundle επίπεδο του προορισμού αφυπνίζει την εφαρμογή του προορισμού αναγνωρίζοντάς την από τον κωδικό οντότητας.Έχοντας υπόψη το τμήμα ελέγχου των δεδομένων του χρήστη που στάλθηκαν από την πηγή,η εφαρμογή του προορισμού μπορεί να δημιουργήσει μια επιβεβαίωση του επιπέδου εφαρμογής σε ένα νέο πακέτο και να το στείλει στην πηγή.



8.3 Συνθήκες Σφάλματος στο Bundle Επίπεδο

Σ'αυτό το σημείο αξίζει να περιγράψουμε τις συνθήκες σφάλματος που μπορούν να εμφανιστούν στο bundle επίπεδο κατά τη διάρκεια της δημιουργίας και της μεταφοράς του πακέτου.Όταν αυτά τα σφάλματα προκληθούν στην IPN περιοχή του αποστολέα,είναι πιθανόν να χειριστεί ένα διάλογο πραγματικού χρόνου για να τα διορθώσει προτού προωθηθεί το πακέτο.Και λέμε είναι πιθανό γιατί έστω και αν δύο

κόμβοι βρίσκονται στην ίδια IPN περιοχή,μπορεί να μην υπάρχει η δυνατότητα για επικοινωνία σε πραγματικό χρόνο.Ένα παράδειγμα γι'αυτή την περίπτωση θα ήταν αν ένα lander βρισκόταν στην αντίθετη πλευρά του πλανήτη από την IPN πύλη και χρησιμοποιούσε πακέτα για να επικοινωνήσει με την πύλη μέσα από έναν χαμηλής τροχιάς δορυφόρου,με τον δορυφόρο να θεωρείται κόμβος.

Τα σφάλματα που μπορούν να εμφανιστούν στο bundle επίπεδο φαίνονται στο παρακάτω πίνακα.Οι αριθμοί των σφαλμάτων που έχουν αστερίσκο (*) δεξιά τους,σημαίνει ότι δίνεται αναφορά πίσω στην εφαρμογή αποστολής για το λόγο του σφάλματος

ΣΦΑΛΜΑ	ΠΕΡΙΓΡΑΦΗ	ΠΟΥ ΜΠΟΡΕΙ ΝΑ ΠΡΟΚΛΗΘΕΙ ΤΟ ΣΦΑΛΜΑ
1*	Άγνωστη Περιοχή Προορισμού	Μεσολαβητής Πακέτου Πηγής
2*	Άκυρη Εφαρμογή Πηγής	Μεσολαβητής Πακέτου Πηγής
3*	Σφάλμα Σύνταξης Παραμέτρου Πακέτου	Μεσολαβητής Πακέτου Πηγής
4*	Σφάλμα Σημασιολογίας Παραμέτρου Πακέτου	Μεσολαβητής Πακέτου Πηγής
5*	Άκυρο Όνομα Κόμβου στο LSRR ή SSRR	Οποιοσδήποτε Κόμβος
6	Ανεπαρκή Χώρος Ενδιάμεσης Μνήμης	Οποιοσδήποτε Κόμβος
7	Απρόσιτο DNS	Οποιοσδήποτε Κόμβος
8*	Υπέρβαση Χρόνου	Οποιοσδήποτε κόμβος εκτός του μεσολαβητή πηγής
9*	Μη Αποδεκτή Πρόσβαση στη Οντότητα Πηγής	Οποιοσδήποτε κόμβος εκτός του μεσολαβητή πηγής
10*	Άκυρο Όνομα Διεύθυνσης Προορισμού	Η IPN πύλη που υποστηρίζει την IPN περιοχή προορισμού
11*	Άκυρη Εφαρμογή Προορισμού	Προορισμός
12*	Μη Αποδεκτή end-to-end Προσπέλαση	Προορισμός

1. **<u>Άγνωστη Περιοχή Προορισμού</u>**:Αυτό το σφάλμα εμφανίζεται όταν ο μεσολαβητής πακέτου της πηγής πρέπει άμεσα να δημιουργήσει ένα πακέτο προορισμού για μία IPN περιοχή,η οποία δεν έχει αναγνωριστεί δηλαδή κάποια για την οποία δεν υπάρχει κατάλληλη διαδρομή που να γνωρίζει ο Διανεμητής Εφαρμογής (Dispatcher Application).Έχουμε υπόψη μας ότι μόνο το μέρος της IPN περιοχής του ονόματος προορισμού πρέπει να ερμηνευτεί έξω από την IPN περιοχή προορισμού.Συγκεκριμένα, το μέρος διαχείρισης του ονόματος προορισμού πρέπει να είναι ερμηνεύσιμο στο DNS της πηγής (αφού ξέρουμε ότι η πηγή ο προορισμός βρίσκονται σε διαφορετικές IPN περιοχές) και επομένως δεν είναι απαραίτητο να γίνει έλεγχος όταν το πακέτο δημιουργείται.
2. **<u>Άκυρη Εφαρμογή Πηγής</u>** :Αν το source application instance handle που παρέχεται από την εφαρμογή της πηγής είναι άκυρο,ο μεσολαβητής πακέτου της πηγής απαντάει με ΄΄Σφάλμα Άκυρης Εφαρμογής Πηγής ΄΄(Invalid Source Application Error). Αυτό θα μπορούσε να είναι μια περίπτωση για παράδειγμα,αν η εφαρμογή της πηγής πρόσφερε ένα instance handle που απευθυνόταν σε ένα σύστημα επεξεργασίας για το οποίο η εφαρμογή δε θα είχε προνόμια.

3. **Σφάλμα Σύνταξης Παραμέτρου Πακέτου**: Ο μεσολαβητής πακέτου της πηγής μπορεί να ελέγξει τη σύνταξη μερικών από τις παραμέτρους της δημιουργίας πακέτου(π.χ. μπορεί διαβεβαιώσει ότι η end-to-end και IPN ασφάλεια πρόσβασης είναι σωστά δομημένες).Αν μια παράμετρος βρεθεί συντακτικά ανακριβής ή φανερά λανθασμένη,ο μεσολαβητής πακέτου θα δώσει αναφορά πίσω στην πηγή για Σφάλμα Σύνταξης Παραμέτρου Πακέτου και η οποία θα περικλείει τουλάχιστον την παράμετρο που προκάλεσε το σφάλμα.
4. **Σφάλμα Σημασιολογίας Παραμέτρου Πακέτου**: Αν ο μεσολαβητής πακέτου της πηγής μπορεί να αναγνωρίσει μια συγκεκριμένη παράμετρο δημιουργίας πακέτου ως καλά δομημένη αλλά ακατάλληλη για χρήση,θα δώσει αναφορά στην εφαρμογή της πηγής για Σφάλμα Σημασιολογίας Παραμέτρου Πακέτου,η οποία θα περικλείει τουλάχιστον την παράμετρο που προκάλεσε το σφάλμα.
5. **Άκυρο Όνομα Κόμβου στο LSRR ή SSRR**: Αν ένα άκυρο όνομα κόμβου αποκαλυφθεί σε μια χαλαρή ή αυστηρή διαδρομή και εγγραφή πηγής,ο μεσολαβητής πακέτου που εντόπισε το σφάλμα θα το μεταβιβάσει πίσω στην εφαρμογή της πηγής.Θεωρούμε ότι μπορεί να είναι ωφέλιμο να έχουμε τους μεσολαβητές πακέτου να ελέγχουν την εγκυρότητα όχι μόνο του επόμενου βήματος στο δρομολόγιο της πηγής,αλλά όσων εισόδων μπορούν.Η αξία του ελέγχου πολλαπλών εισόδων είναι ο πιθανός εντοπισμός των σφαλμάτων,πριν το πακέτο περάσει κάποια από τις ευρείας περιοχής συνδέσεις.
6. **Ανεπαρκής Χώρος Ενδιάμεσης Μνήμης**: Αν ένας μεσολαβητής πακέτου δεν έχει επαρκή χώρο ενδιάμεσης μνήμης για να δεχτεί κάποιο πακέτο,το εγκαταλείπει και δημιουργεί σφάλμα ανεπαρκή χώρου ενδιάμεσης μνήμης.Σημειώνουμε ότι ένας κόμβος μπορεί να επιλέξει να εγκαταλείψει τα χαμηλής προτεραιότητας πακέτα,με σκοπό να παραχωρήσει χώρο στα υψηλής προτεραιότητας πακέτα. Αυτό το σφάλμα δε μεταβιβάζεται πίσω στην πηγή.
7. **Απρόσιτο DNS**: Αν ένας μεσολαβητής πακέτου χρειάζεται πρόσβαση στο DNS του και δεν μπορεί να πάρει πληροφορίες από αυτό,δημιουργεί ένα σφάλμα απρόσιτου DNS.Αυτή η πληροφορία δε μεταβιβάζεται πίσω στην εφαρμογή της πηγής.
8. **Υπέρβαση Χρόνου**: Αν ο χρόνος αναμονής του πακέτου(είτε η πηγή παρέχει TTL είτε το πακέτο είναι TTL) λήξει,η πηγή ειδοποιείται με ένα μήνυμα Υπέρβαση Χρόνου.Αυτά τα σφάλματα μεταβιβάζονται στην εφαρμογή της πηγής.
9. **Μη Αποδεκτή Πρόσβαση στην Οντότητα Πηγής**: Αυτό το σφάλμα αποδεικνύει ότι η οντότητα της πηγής δεν έχει πρόσβαση σε έναν απαιτούμενο πόρο του IPN κόμβου.Η πηγή μπορεί να μην έχει καμία εξουσιοδότηση να χρησιμοποιήσει τον κόμβο ή να μην της επιτρέπεται να χρησιμοποιήσει μια συγκεκριμένη προσαρμογή που απαιτεί το πακέτο.Επομένως,τα σφάλματα μη αποδεκτής πρόσβασης στην οντότητα της πηγής δείχνουν ότι η πηγή δεν έχει το δικαίωμα να χρησιμοποιήσει κάποιο συγκεκριμένο πόρο.Άλλα σφάλματα(π.χ. Ανεπαρκής Χώρος Ενδιάμεσης Μνήμης) υπογραμμίζουν ότι ένας συγκεκριμένος πόρος δεν είναι διαθέσιμος για κάποιο πακέτο.Για παράδειγμα,μια οντότητα στην επιφάνεια ενός πλανήτη μπορεί να έχει το δικαίωμα να επικοινωνήσει, χρησιμοποιώντας το bundle πρωτόκολλο,με μια άλλη οντότητα στην άλλη πλευρά του πλανήτη μέσω ενός χαμηλού ύψους δορυφόρο που είναι επίσης και IPN πύλη.Ο αποστολέας όμως μπορεί να μην επιτρέπεται να στείλει πακέτα στο διαπλανητικό χώρο.Σ'αυτήν

την περίπτωση τα πακέτα που στέλνονται και μπαίνουν σε τροχιά προορισμού για την άλλη πλευρά του πλανήτη δε θα προκαλέσουν σφάλματα,ενώ άλλα πακέτα με διεύθυνση προορισμού εκτός πλανήτη θα μπορούσαν να δημιουργήσουν προβλήματα.Τα σφάλματα μη αποδεκτής πρόσβασης στην οντότητα της πηγής μεταβιβάζονται πίσω στην εφαρμογή της πηγής.

10. **Άκυρο Όνομα Διεύθυνσης Προορισμού**: Όταν για πρώτη φορά το πακέτο βρει την κατεύθυνση της IPN περιοχής,το κομμάτι της διεύθυνσης του ονόματος προορισμού μπορεί να επιβεβαιωθεί.Αν αυτό το κομμάτι της διεύθυνσης δεν είναι έγκυρο,η πηγή ενημερώνεται με ένα μήνυμα για σφάλμα Άκυρου Ονόματος Διεύθυνσης Προορισμού.Όσο για το LSRR/SSRR,πιθανόν να ήταν ωφέλιμο να ελέγχουν το κομμάτι διεύθυνσης του ονόματος προορισμού όσο το δυνατό γρηγορότερα,προκειμένου να αποφευχθεί η μεταβίβαση των άκυρων ονοματολογικά πακέτων και των μηνύματα σφαλμάτων στο backbone.
11. **Άκυρη εφαρμογή Προορισμού**: Αν ο μεσολαβητής του πακέτου προορισμού δεν μπορεί άμεσα να εντοπίσει την εφαρμογή προορισμού (με βάση την εφαρμογή προορισμού άμεσου ελέγχου στο πακέτο),ειδοποιεί την εφαρμογή της πηγής με ένα μήνυμα για σφάλμα Άκυρης Εφαρμογής Προορισμού.
12. **Μη Αποδεκτή end-to-end Προσπέλαση:** Αν ο προορισμός του πακέτου δε δεχτεί το πακέτο εξαιτίας κάποιου σφάλματος ελέγχου προσπέλασης ή εγκυρότητας,τότε η εφαρμογή της πηγής ενημερώνεται με ένα μήνυμα για μη αποδεκτή end-to-end προσπέλαση.

9 ΑΣΦΑΛΕΙΑ ΣΤΟ IPN

Είναι κατανοητό ότι δεν υπάρχει λεπτομερής λίστα με τις απαιτήσεις ασφάλειας για το Διαπλανητικό Internet,περισσότερο αφού προς το παρόν δεν υπάρχουν IPN χρήστες και επειδή έστω και να υπήρχαν υποτιθέμενοι χρήστες δεν θα έδιναν τόσο μεγάλη σημασία στην ασφάλεια ώστε να εμπιστευτούμε απλά ένα σύνολο απαιτήσεων. Γνωρίζουμε όμως ότι το εύρος ζώνης των πόρων του Διαπλανητικού Internet θα είναι πολύτιμο.Μπορούμε επίσης να πούμε με σιγουριά ότι το IPN θα γίνει εξαιρετικός στόχος για τους hackers.Ακόμη,μπορούμε να προβλέψουμε ότι στο IPN θα διακινούνται πολύτιμα και προσωπικά δεδομένα.Συμπερασματικά δηλαδή,είναι αποδεκτό ότι θα απαιτούνται πολύμορφοι μηχανισμοί ασφαλείας και υπηρεσίες ώστε να εξασφαλιστεί η προστασία για τη διακίνηση των πακέτων στο IPN αλλά και για να διατηρηθεί η υποδομή του ίδιου του IPN.

Υπάρχουν λοιπόν δύο πλευρές για την ασφάλεια του IPN: προστασία της υποδομής του IPN και προστασία των δεδομένων που διακινούνται στο IPN.Η προστασία της υποδομής του IPN δεν είναι διαφορετική από την προστασία που απαιτείται για την υποδομή του Internet στη γη.Θα υπάρχει η ανάγκη για ασφαλή ανταλλαγή πληροφοριών δρομολόγησης μεταξύ των κόμβων,όπως επίσης και για τον ασφαλή χειρισμό αυτών.Για να προστατέψει από μόνο του την υποδομή του το IPN,οι IPN κόμβοι πρέπει να υποπτεύονται ο ένας τον άλλο.Μ'αυτόν τον τρόπο,ο κάθε IPN κόμβος θα επικυρώνει τον εαυτό του στους άλλους,ώστε να εξασφαλιστεί ότι δεν έχει παραποιημένα στοιχεία από κάποια αναξιόπιστη οντότητα. Έτσι όμως κάποιος μπορεί να σκεφτεί ότι θα προκληθούν απώλειες περισσότερες από τις απαιτούμενες αν πιστεύουμε ότι πάντα θα υπάρχει ένας μικρός,ελεγχόμενος αριθμός IPN κόμβων (όπως το αυθεντικό ARPANET).Με την ίδια λογική όμως κάποιος μπορεί να προβλέψει ότι θα μπορούσαν πολλοί IPN κόμβοι να βρίσκονται υπό την προστασία και τον έλεγχο πολλών οργανισμών-εταιριών(όπως στο σημερινό διαδίκτυο). Από τη στιγμή που προτιμάμε το IPN σε απλή κλίμακα,θέλουμε να δημιουργήσουμε από την αρχή αμοιβαίους μηχανισμούς ασφάλειας στην αρχιτεκτονική του IPN.Αξίζει να σημειωθεί ότι οι ίδιοι μηχανισμοί θα μπορούσαν να χρησιμοποιηθούν για την ασφάλεια τόσο της υποδομής του IPN όσο και των διακινούμενων δεδομένων.

9.1 Προϋποθέσεις Αναφορικά με τους Απαιτούμενους IPN Μηχανισμούς Ασφαλείας

Οι μηχανισμοί ασφάλειας που απαιτούνται για το IPN είναι:

- Έλεγχος πρόσβασης
- Απόδειξη γνησιότητας
- Ακεραιότητα δεδομένων
- Ιδιωτικότητα δεδομένων

Οι έλεγχοι πρόσβασης θα χρειάζονται γιατί οι βασισμένες στο διάστημα εργασίες του IPN θα έχουν περιορισμένους διαθέσιμους πόρους και γιατί θα είναι σπουδαίος στόχος για τους hackers.Με το να περιορίζουμε την πρόσβαση στους IPN πόρους,περιορίζουμε τη διάθεση του IPN μόνο σ'αυτούς τους χρήστες που απαιτούν

τις υπηρεσίες του και δεν το επιτρέπουν να υπερφορτωθεί από αυτούς που δεν έχουν δικαίωμα πρόσβασης στις IPN υπηρεσίες.

Η απόδειξη γνησιότητας της ταυτότητας θα είναι απαραίτητη για να πραγματοποιηθεί η παρέμβαση του ελέγχου πρόσβασης.Για να επιτραπεί ή όχι η πρόσβαση στο IPN θα χρειάζεται μια εγγυημένη ταυτότητα της πηγής της κυκλοφορίας δικτύου.Η ταυτότητα μπορεί να είναι ατομική (π.χ. ένας ανώτερος διερευνητής) ή μια τοποθεσία (π.χ. ένα κέντρο ελέγχου επιστήμης ή ένα κέντρο ελέγχου διαστημόπλοιων).

Η ακεραιότητα των δεδομένων θα χρειάζεται για να εξασφαλιστεί ότι τα ληφθέντα δεδομένα που κυκλοφόρησαν μέσα στο IPN είναι τα ίδια με τα πρωτότυπα που στάλθηκαν.Αυτό αποτελεί πραγματικότητα τόσο για την προοπτική υποδομής του IPN (π.χ. δεδομένα διαχείρισης) όσο και για την προοπτική του χρήστη (π.χ. επιστημονικά δεδομένα,σειρές εντολών).Η ακεραιότητα των δεδομένων εξασφαλίζει ότι οποιαδήποτε μη επιτρεπτή τροποποίηση των δεδομένων θα εντοπιστεί από τον παραλήπτη.

Η ιδιωτικότητα των δεδομένων είναι απαραίτητη ώστε να εξασφαλιστεί ότι μόνο αυτοί που έχουν το δικαίωμα να πάρουν δεδομένα που διακινούνται στο IPN ή προορίζονται για ή από την IPN υποδομή,θα έχουν το προνόμιο να το κάνουν αυτό.Αυτός ο μηχανισμός είναι γνωστός και ως ΄΄Εμπιστευτικός΄΄.

Στο περιβάλλον της ασφάλειας δικτύου υπάρχουν δύο γνωστά παραδείγματα:η hop-by-hop ασφάλεια που είναι γνωστή και ως ασφάλεια σύνδεσης και η end-to-end ασφάλεια.Στο hop-by-hop παράδειγμα,τα δεδομένα που μεταφέρονται στο δίκτυο προστατεύονται σε hop-by-hop βάση.Μ'αυτόν τον τρόπο,τα δεδομένα προστατεύονται στην πηγή τους, αλλά προκειμένου να δρομολογηθούν στον τελικό προορισμό τους χρειάζεται να είναι ΄΄ξεπροστατευμένα΄΄ σε ένα έμπιστο σημείο δρομολόγησης(π.χ. μια χερσαίας βάσης πύλη ή μια IPN πύλη) για να εξεταστούν για την επόμενη δρομολόγηση.Το έμπιστο σημείο δρομολόγησης πρέπει μετά να προστατέψει ξανά τα δεδομένα και να τα προωθήσει στο επόμενο σημείο δρομολόγησης.Κάθε διαδοχικό σημείο πρέπει να ΄΄ξεπροστατεύει΄΄ και να ΄΄ξαναπροστατεύει΄΄ τα δεδομένα μέχρι να φτάσουν στον τελικό προορισμό τους.Η αρνητική πλευρά αυτού του παραδείγματος ασφάλειας,είναι ότι εξαρτάται από το πώς η ασφάλεια βρίσκει εφαρμογή.Τα δεδομένα μπορεί να είναι εντελώς εκτεθειμένα καθώς βρίσκονται στη πύλη,η οποία θεωρείται ασφαλές σημείο.Αυτό σημαίνει ότι ενδεχομένως τα δεδομένα να είναι ευπρόσβλητα σε μη επιτρεπτές τροποποιήσεις και μη επιτρεπτές εμφανίσεις.

Το end-to-end παράδειγμα δε χρησιμοποιεί έμπιστες πύλες.Μάλιστα, θεωρεί ότι η διαδρομή μεταξύ της πηγής των δεδομένων και του προορισμού είναι επικίνδυνη και δεν μπορεί να είναι έμπιστη.Επομένως, τα δεδομένα προστατεύονται στην πηγή τους και δε μένουν απροστάτευτα μέχρι να φτάσουν στον προορισμό τους.Για να λειτουργήσει όμως αυτό το σύστημα,οι πληροφορίες δρομολόγησης πρέπει να παραμείνουν χωρίς προστασία,έτσι ώστε οι ενδιάμεσες πύλες να είναι ικανές να ρυθμίσουν την προώθηση των δεδομένων χωρίς να έχουν τη δυνατότητα να διαβάσουν ή να αλλάξουν τα δεδομένα.Ένα πρόβλημα με το end-to-end πρότυπο είναι ότι μπορεί να λειτουργήσει μόνο σε ένα δίκτυο που υπάρχουν end-to-end πρωτόκολλα(π.χ. το TCP). Εκεί πρέπει να υπάρχει ένα πρωτόκολλο κάτω από τα δεδομένα,που να παρέχει τη δυνατότητα να δρομολογεί.Ένα τέτοιο παράδειγμα είναι

το Internet Engineering Task Force's (IETF) Internet Protocol Security Protocol (IPSEC).Το IPSEC Encapsulating Security Payload (ESP) πρωτόκολλο προσφέρει end-to-end υπηρεσία ασφάλειας των επιπέδων των πρωτοκόλλων IP και TCP.

Στο IPN όμως τα IP και TCP δεν υποστηρίζουν απαραίτητα end-to-end πρωτόκολλα ή καλύτερα αυτά τα πρωτόκολλα μπορούν να τερματιστούν σε ένα τοπικό διαδίκτυο(π.χ. ένα τμήμα στη γη ή ένα ουράνιο σώμα) και να μην υποστηρίζουν end-to-end στο IPN.Τα δεδομένα θα υποστηρίζουν end-to-end μέσω του bundle πρωτοκόλλου που με τη σειρά του θα μεταφέρεται από άλλα IPN πρωτόκολλα(π.χ. LTP,TCP)χρησιμοποιώντας το μοντέλο Pony Express.Από τη στιγμή που το IPN πρέπει να δομηθεί πάνω σε μια store-and-forward βάση και εφόσον οι χρήστες μπορεί να μην εμπιστεύονται τις IPN πύλες,οι λύσεις του τύπου IPSEC δεν μπορούν να χρησιμοποιηθούν.Προκειμένου να δοθεί μια λύση end-to-end για την ασφάλεια,οι μηχανισμοί ασφάλειας μπορούν να εφαρμοστούν μόνο στα δεδομένα και όχι σε άλλα επίπεδα πρωτοκόλλων κάτω από το bundle πρωτόκολλο.Αυτός είναι ο τρόπος που δουλεύουν οι μηχανισμοί Secure Sockets Layer (SSL) (τώρα έχει καθοριστεί μέσα στο IETF όπως το πρωτόκολλο Transport Layer Security(TLS))και οι τεχνικές του ασφαλούς email όπως το S/MIME και OpenPGP.Ουσιαστικά,οι υπηρεσίες ασφάλειας εφαρμόζονται στο μέρος των δεδομένων του πακέτου αφήνοντας όλες τις επικεφαλίδες των πρωτοκόλλων του πακέτου ανοιχτές και διαθέσιμες για χρήση από ενδιάμεσα συστήματα.Για παράδειγμα,για να μεταδοθεί η στοιχειοσειρά ΄΄Hello World΄΄ μέσα στο διαδίκτυο,είναι αναγκαίο να τοποθετηθεί αυτή η στοιχειοσειρά μέσα σε μια TCP επικεφαλίδα,σε IP επικεφαλίδα και σε μια MAC (Media Access) επικεφαλίδα επιπέδου.Για να προσφερθούν οι end-to-end υπηρεσίες ασφάλειας,μόνο η στοιχειοσειρά ΄΄Hello World΄΄ θα είχε εφαρμοσμένες τις υπηρεσίες ασφάλειας(π.χ. μπορεί να είναι κρυπτογραφημένο ώστε να εξασφαλιστεί ιδιωτικότητα και εμπιστοσύνη).
Από την άλλη μεριά,οι TCP,IP και MAC επικεφαλίδες θα παραμείνουν όλες χωρίς να εφαρμοστούν οι υπηρεσίες ασφάλειας σ'αυτές.Παράλληλα όταν χρησιμοποιούνται οι τεχνικές IPSEC και ESP,η TCP επικεφαλίδα θα έχει εφαρμοσμένες τις υπηρεσίες ασφάλειας σ'αυτό για να το προστατέψει όπως και τα δεδομένα.Αν χειριζόμασταν την τεχνοτροπία του τούνελ,το ESP θα τοποθετούσε τις TCP και IP επικεφαλίδες μέσα σε ένα IP πακέτο.

Με βάση όλα τα παραπάνω,τα δεδομένα θα μεταφέρονται μέσα στο IPN σε πακέτα,χρησιμοποιώντας email όπως στα παραδείγματα αφού και η δανειζόμενη τεχνολογία της ασφάλειας του email είναι μια λύση για το IPN.

9.2 Ασφαλής Τεχνολογία E-mail

Από τη στιγμή που το ασφαλή ηλεκτρονικό ταχυδρομείο χρησιμοποιείται με μη αλληλεπιδραστική μέθοδο και αφού δεν είναι απαραίτητο οι δύο πλευρές να είχαν προηγουμένως επικοινωνία,αναπτύχθηκε μια τεχνική διαφορετική από αυτή που χρησιμοποιεί το IPSEC.Ένας τρόπος με τον οποίο το email θα μπορούσε με ασφάλεια να «κρύψει» τις πληροφορίες του(π.χ. κρυπτογραφημένες και/ή με ψηφιακή υπογραφή) είναι μέσω της χρήσης κρυπτογράφησης του δημόσιου κλειδιού.Χρησιμοποιώντας αυτή την τεχνολογία,ένας αποστολέας email θα χρησιμοποιούσε το δημόσιο κλειδί του προσδοκώμενου αποδέκτη ώστε να

κρυπτογραφήσει το υλικό (π.χ. το μήνυμα) και ο αποδέκτης θα χρησιμοποιούσε το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το υλικό.Επιπλέον,ο αποστολέας θα μπορούσε να υπογράψει ψηφιακά το μήνυμα(ώστε να αποδείξει τη γνησιότητα του μηνύματος)χρησιμοποιώντας το ιδιωτικό του κλειδί και ο αποδέκτης θα επαλήθευε τη γνησιότητα του μηνύματος χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα. Σχετικά μ'αυτή τη μέθοδο όμως υπάρχουν δύο προβλήματα για το IPN.

Το πρώτο πρόβλημα είναι ότι η κρυπτογράφηση του δημόσιου κλειδιού καταναλώνει αρκετή ισχύ από τον επεξεργαστή.Συνεπώς,γι'αυτή την περίπτωση η συνηθισμένη λύση είναι να χρησιμοποιηθούν αλγόριθμοι με συμμετρικό κλειδί(π.χ. κοινό μυστικό)για μεγάλες ποσότητες δεδομένων. Με αλλαγές στην τεχνολογία,αυτό το πρόβλημα πιθανό να εξαλειφτεί τουλάχιστον στα συστήματα στη γη.Από την άλλη,δεν είναι ξεκάθαρο αν τα διαστημικά συστήματα θα το εφαρμόσουν τόσο γρήγορα.Το δεύτερο πρόβλημα είναι ότι η κρυπτογράφηση του δημόσιου κλειδιού αναλώνει το εύρος.Ένα δημόσιο κλειδί συναλλάσσει τεχνολογία που επιτρέπει δύο οντότητες επικοινωνίας να παράγουν ένα κοινό συμμετρικό κλειδί ώστε να γνωρίζουν η κάθε μία το δημόσιο κλειδί της άλλης και να ανταλλάζουν μερικές τυχαίες πληροφορίες.Τέτοιου είδους συναλλαγή πληροφοριών είναι γνωστή ως Diffie-Helman συναλλαγή.Αξίζει όμως να σημειωθεί ότι αυτή η συναλλαγή πληροφοριών πρέπει να εκτελεστεί σε near-real-time περιβάλλον,προκειμένου το κοινό κλειδί να μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση μεταφορών.Κάτι τέτοιο δεν είναι πρακτικό στο IPN αφού δεν πραγματοποιούνται συναλλαγές δεδομένων πραγματικού χρόνου σε end-to-end βάσεις.Ωστόσο,η ασφαλής μέθοδος email μπορεί να χρησιμοποιηθεί και κάτω από το μοντέλο pony-express.

Η γενική τεχνική που χρησιμοποιείται από το ασφαλή μηχανισμό email είναι ότι η οντότητα αποστολέας αποφασίζει τι μηχανισμό ασφάλειας θα παράσχει(π.χ. κρυπτογράφηση για εμπιστοσύνη,ψηφιακή υπογραφή για γνησιότητα και πληρότητα ή και τα δύο).Αν τα δεδομένα που πρέπει να σταλούν μέσω email είναι κρυπτογραφημένα,ο αποστολέας παράγει ένα τυχαίο κλειδί που χρησιμοποιείται για να κρυπτογραφήσει τα δεδομένα.Ο αποστολέας μετά έχει στη θέση του το δημόσιο κλειδί του λήπτη ή απαιτεί το δημόσιο κλειδί του server για να αποκτήσει το δημόσιο κλειδί του λήπτη το οποίο θα περιέχεται στο ψηφιακό πιστοποιητικό.Σε βάρος του σχετικού εύρους,ο αποστολέας μπορεί να μεταβιβάσει το ψηφιακό πιστοποιητικό του μέσα στο μήνυμα του email,το οποίο ο λήπτης μπορεί να το επαληθεύσει ως αυθεντικό βασισμένος στη γνωστή αξιόπιστη υπογραφή του πιστοποιητικού.Το κλειδί που συνηθίζεται να κρυπτογραφεί τα δεδομένα,είναι και αυτό κρυπτογραφημένο χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη και έτσι το μήνυμα στέλνεται.Ο παραλήπτης χρησιμοποιεί το ιδιωτικό του κλειδί αρχικά για να αποκρυπτογραφήσει το κλειδί που έχει το κρυπτογραφημένο μήνυμα και μετά χρησιμοποιεί το αποκρυπτογραφημένο κλειδί για να αποκρυπτογραφήσει τα δεδομένα.Όταν χρησιμοποιηθεί η ψηφιακή υπογραφή,ο αποστολέας εκτιμά τα ασυνάρτητα δεδομένα του μηνύματος χρησιμοποιώντας έναν μεθοδικό αλγόριθμο όπως τον MD5 ή τον Secure Hash Algorithm(SHA-1).Αυτά τα ασυνάρτητα κρυπτογραφημένα δεδομένα στέλνονται μαζί με τα δεδομένα του μηνύματος.Ο παραλήπτης χρησιμοποιεί ένα αντίγραφο του δημόσιου κλειδιού του αποστολέα ώστε να πιστοποιήσει το γεγονός ότι το μήνυμα στάλθηκε από τον προσδοκώμενο αποστολέα.

Δεδομένου ότι το IPN και το ηλεκτρονικό ταχυδρομείο μπορούν να λειτουργήσουν πάνω στο ίδιο παράδειγμα,η αντίληψη του IPN σχετικά με το ΄΄bundle-space΄΄ είναι

ακριβώς ανάλογο με το κυρίως MIME σώμα στο ασφαλή email.Όπως εξηγήσαμε παραπάνω,στο ασφαλή email τα περιεχόμενα του μηνύματος είναι κρυπτογραφημένα με τη χρήση ενός συμμετρικού κλειδιου.Τα πραγματικά περιεχόμενα του μηνύματος είναι ΄΄κρατημένα΄΄(αυτό μπορεί να παραλληλιστεί με τα περιεχόμενα που είναι ΄΄bundled΄΄)σε ένα κομμάτι του MIME σώματος.Σχετικά με τα μέρη του MIME σώματος,αυτά είναι επίσης συνοδευόμενα από το κρυπτογραφημένο συμμετρικό κλειδί και τις ανάλογες πληροφορίες που χρειάζονται για την αποκρυπτογράφηση.

Ως εκ τούτου,παρόμοιες τεχνικές ασφαλείας μπορούν να εφαρμοστούν πάνω στην ιδέα του΄΄bundle-space΄΄ του IPN.Φαίνεται λοιπόν πως ο τρόπος που τα απαραίτητα bundle δεδομένα μεταφέρονται στο IPN είναι όμοιος με αυτόν της μεταφοράς ενός μηνύματος email.Επομένως και στις δυο περιπτώσεις μπορούν να εφαρμοστούν υπηρεσίες ασφαλείας προτού σταλούν όλα τα δεδομένα σαν προστατευόμενη οντότητα.

ΠΑΡΑΡΤΗΜΑ

ΒΙΒΛΙΟΓΡΑΦΙΑ

- A.J.Hooke <<Towards an Interplanetary Internet:A proposed strategy for standardization>>,California Institute of Technology
- S.Burleigh,V.Cerf,R.Durst <<The Interplanetary Internet:A communications infrastructure for Mars exploration>>,International Astronautical Federation
- R.Durst,D.Feighery,L.Scott <<Why not use the standard Internet Suite for the Interplanetary Internet?>>,The MITRE Corporation
- M.Mathis <<The macroscopic behaviour of the congestion avoidance Algorithm>>,Computer Communications Review
- V.Paxson <<Measurements and analysis of End-to-End Internet Dynamics>>,University of California,Berkeley
- F.Warthman <<Delay-Tolerant Networks: A tutorial>>,Warthman Associates
- V.Cerf,A.Hooke,L.Torgerson <<Interplanetary Internet: Architectural Definition>>,Worldcom/Jet Propulsion Laboratory
- V.Cerf,K.Fall,H.Weiss <<Delay-Tolerant Network Architecture: The evolving Interplanetary Internet>>,NASA/Jet Propulsion Laboratory