ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ:ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

Πρωτόκολλο Bluetooth, εφαρμογές στα ασύρματα δίκτυα.

ΤΣΙΛΙΚΟΣ ΓΕΩΡΓΙΟΣ
ΕΠΙΒΛΕΠΟΝ ΚΑΘΗΓΗΤΗΣ: ΛΑΜΠΡΟΥ ΑΘΑΝΑΣΙΟΣ

ΑΡΤΑ
ΦΕΒΡΟΥΑΡΙΟΣ 2004

ΣΥΝΕΡΓΑΤΗΣ ΚΑΘΗΓΗΤΗΣ
ΛΑΜΠΡΟΥ ΑΘΑΝΑΣΙΟΣ

ΤΣΙΛΙΚΟΣ ΓΕΩΡΓΙΟΣ

Φεβρουάριος 2004

ΑΡΤΑ

Πτυχιακή εργασία μέρος των απαιτήσεων του τμήματος
Τηλεπληροφορικής και διοίκησης

Η σκέψη ραδιουργεί...

ΠΕΡΙΛΗΨΗ

Το bluetooth μια νέα ανερχόμενη τεχνολογία στον τομέα την ασύρματης τεχνολογίας και αποτελεί το θέμα της παρακάτω εργασίας. Ένα εισαγωγικό κείμενο παρουσιάζεται στην σκηνή και αρχίζει την αφήγηση του στον κόσμο που βασιλεύει το ασύρματο πρότυπο bluetooth(κεφάλαιο 1). Έπειτα στο κεφαλαίο 2 αναλύεται η εγκατάσταση σύνδεσης μεταξύ 2 συσκευών καθώς και οι τεχνολογίες που χρησιμοποιούνται για την αποφυγή της παρεμβολής. Στο κεφάλαιο 3 προβάλουν τα πακέτα και η δομή τους καθώς και ο τρόπος διευθυνσιοδότησης των συσκευων. Επιπλέον περιγράφεται η τεχνολογία TDD καθώς και ο τρόπος μεταγωγής πακέτων. Στο κεφάλαιο 4 η Αρχιτεκτονική παίρνει τα ηνία και μας εξηγεί την δομή της λίστας πρωτοκόλλου του Bluetooth, όπως επίσης και τα διάφορα profile που χρησιμοποιούνται. Έπειτα στο κεφάλαιο 5 μαθαίνουμε να ασφαλίζουμε τις συνδέσεις που πραγματοποιούμε μεταξύ των συσκευών και στο κεφάλαιο 6 παρουσιάζονται τα μοντέλα χρήσης. Η σύγκριση με άλλες ασύρματες τεχνολογίες όπως η HomeRF,WI/FI και IRDA έρχεται να γεμίσει το 7^{ο} κεφάλαιο.
Η αυλαία πέφτει με τα συμπεράσματα και τη μελλοντική χρήση του Bluetooth να ολοκληρώνουν αυτό το project πάνω σε αυτήν την τεχνολογία.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 3 ν ΜΕΤΑΔΟΣΗ ΠΑΚΕΤΩΝ

ΚΕΦΑΛΑΙΟ 4 ν ΑΡΧΙΤΕΚΤΟΝΙΚΗ BLUETOOTH

ΚΕΦΑΛΑΙΟ 7 η ΣΥΓΚΡΙΣΗ ΜΕ ΑΛΛΑ ΑΣΥΡΜΑΤΑ ΠΡΟΤΥΠΑ

ΚΕΦΑΛΑΙΟ 8 η ΜΕΛΛΟΝ ΣΥΜΠΕΡΑΣΜΑΤΑ

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Θα μπορούσε να υποστηριχθεί ότι η ηλικία των ψηφιακών ηλεκτρονικών επικοινωνιών άρχισε όταν καταχώρησε ο Samuel F.B Morse τον ηλεκτρονικό τηλέγραφο το 1840 με δίπλωμα ευρεσιτεχνίας. Για μερικές δεκαετίες, ο κώδικας Morse ήταν ο ποιο διαδεδομένος τρόπος να εμφανίζει γράμματα, αριθμούς και στίξη, και το καλώδιο ήταν ο μόνος πρακτικός τρόπος για την μεταφορά πληροφορίας από την πηγή στον προορισμό. Ακόμα και τώρα, το καλώδιο και παρόμοια fiberoptic κανάλια επικρατούν στις αμέτρητες εφαρμογές. Εντούτοις, με τη σημερινή ανάγκη για κινητές, δυναμικές επικοινωνίες, η ασύρματη μετάδοση κερδίζει έδαφος γρήγορα ως πανταχού παρόν για την σύνδεση συσκευών μεταξύ τους. Η ασύρματη επικοινωνία έγινε εμπορικά βιώσιμη με την εμφάνιση της ραδιοφωνικής μετάδοσης, όπου μια ακριβή συσκευή αποστολής σημάτων στέλνει τα μονόδρομα σήματα σε χιλιάδες χαμηλού κόστους δέκτες. Μόνο πρόσφατα έχει γίνει πρακτικό και αρκετά ανέξοδο ώστε να «σπάσει» την κυριαρχία από τα χέρια των επαγγελματιών.

Πιθανόν το καλύτερο παράδειγμα από ευρέως διαδεδομένο για διπλής κατεύθυνσης επικοινωνίας φανερώθηκε από το αρχικό κυψελοειδές τηλεφωνικό δίκτυο με το όνομα Advanced Mobile Phone System(AMPS), όπου μια εκτενής μήτρα από κύτταρα επικοινωνούσε πέρα από τις σχετικά μικρές αποστάσεις με τα κινητά φορητά τηλεφωνά τους. Δεδομένου ότι ο αριθμός των χρηστών πολλαπλασιάζονταν, τα κύτταρα έγιναν μικρότερα για να επιτρέψουν την επαναχρησιμοποίηση συχνότητας, όπου 2 κύτταρα μοιράζονται το ίδιο σύνολο καναλιών, προσαρμόζοντας κατά συνέπεια περισσότερα τηλέφωνα. Επειδή το ραδιοφάσμα έχει ένα σταθερό εύρος ζώνης, περισσότεροι χρήστες μπορούν να φιλοξενηθούν μέσω την μειωμένης ισχύος χωρίς να προκαλέσουν παρεμβολές. Μια από τις πιο χρήσιμες εφαρμογές, μικρών αποστάσεων, διπλής κατεύθυνσης ψηφιακής επικοινωνίας είναι να επιτρέπει τους υπολογιστές να επικοινωνούν μεταξύ τους καθώς και με τα περιφερειακά τους όπως έκπτωτες και σαρωτές. Αυτό μπορεί να είναι τόσο απλό όσο μια σύνδεση μεταξύ ενός υπολογιστή με ένα ή περισσότερα περιφερειακά ή τόσο σύνθετο όσο διάφορες συσκευές που επικοινωνούν η μια με την άλλη υπό την μορφή τοπικού δικτύου(LAN). Το LAN μπορεί

να είναι είτε ενσύρματο είτε ασύρματο και συνήθως καλύπτει μια περιοχή από μερικά δωμάτια ή ορόφους σε ένα κτίριο. Το ποιο κοινό wireless local area network(WLAN) είναι το IEEE 802,11b αποκαλούμενο επίσης ως Wi-Fi.

Το Bluetooth συμμερίζεται την ιδέα του WLAN σε μια μικρότερη κλίμακα βέβαια, με την χαμηλής ισχύος 10μετρη απόσταση που καλύπτει, ταιριάζει περισσότερο για την σύνδεση συσκευών που βρίσκονται στο ίδιο δωμάτιο ή ακόμα και σε ένα άτομο. Αυτή η έννοια ονομαζόμενη σαν personal area network (PAN) προορίζεται πρώτιστα να αντικαταστήσει τα καλώδια με ασύρματες συνδέσεις. Μαζί με πολλές άλλες ασύρματες συσκευές, το Bluetooth χρησιμοποιεί τη χωρίς άδεια ζώνη συχνότητας 2,4 GHz για τη λειτουργία του. Αντίθετα στη δημοφιλή πεποίθηση, χωρίς άδεια δεν σημαίνει ανεξέλεγκτη χρήση των χωρίς άδεια συχνοτήτων όπως θα δούμε παρακάτω.

ΓΙΑΤΙ ΝΑ ΠΕΤΑΞΟΥΜΕ ΤΑ ΚΑΛΩΔΙΑ

Με την εμφάνιση των φτηνών και απλών διπλής κατεύθυνσης ψηφιακών ασύρματων συστημάτων, μια επιλογή είναι τώρα διαθέσιμη μεταξύ ενσύρματης και ασύρματης επικοινωνίας, και να αναρωτηθούμε γιατί κάποιος θα επέλεγε τα πρώτα. Αυτή είναι μια πολύ καλή ερώτηση, και αυτό θα ήταν χρήσιμο να εξετάσουμε τις χαρακτηριστικές διαφορές μεταξύ των ενσύρματων και ασύρματων επικοινωνιών για να αποκτήσουμε την επίγνωση ώστε να καταλάβουμε ποια μέθοδος είναι καλύτερη και για ποια ιδιαίτερη εφαρμογή. Αν και τα συνδεμένα με καλώδιο συστήματα θεωρούνται συνήθως ότι χρησιμοποιούν τους αγωγούς χαλκού για το κανάλι, παρόμοια χαρακτηριστικά εκθεμάτων οπτικών ινών υπάρχουν σε διάφορες περιοχές, οπότε θα αναφερθούμε και στις δύο μεθόδους .

Πλεονεκτήματα του ασύρματου δικτύου

Όταν οι κόμβοι συνδέονται μέσω του καλωδίου, είναι σαφές ότι είναι σχεδόν αδύνατη η ''κινητικότητα'' που επιτρέπεται ενώ η ασύρματη σύνδεση σπάζει αυτό ¨σχοινί" και διευκολύνει τη δυνατότητα να περιπλανηθεί ενώ η επικοινωνία μεταξύ των συσκευών συνεχίζεται. Ομοίως, η επικοινωνία μπορεί να καθιερωθεί από αρκετές διαφορετικές

θέσεις χωρίς απαίτηση μιας φυσικής βυσμάτωσης στο δίκτυο.

Είναι, φυσικά, προφανές ότι ένα ενσύρματο δίκτυο απαιτεί την τοποθέτηση πολλών καλωδίων επειδή κάθε κόμβος στο δίκτυο πρέπει να έχει φυσική πρόσβαση στο καλώδιο από την συγκεκριμένη θέση του. Αυτό μπορεί να προκαλέσει μεγάλους πονοκέφαλους όταν πρέπει να "παραβιαστούν" οι τοίχοι, τα πατώματα, και οι οροφές ενός υπάρχοντος κτιρίου για την εγκατάσταση καλωδίων. Πολλά κτήρια γραφείων, ειδικά τα παλαιά, έχουν ιστορική σημασία, και η αλλαγή της δομής τους για τα καλώδια συχνά δυσκολεύει. Η σύνδεση των υπολογιστών σε ένα τέτοιο κτήριο μέσω ενός WLAN είναι συχνά η μόνη λογική λύση. Τα νεώτερα κτήρια μπορούν να εγκαταστήσουν τα καλώδια του τοπικού LAN παράλληλα με οικοδόμηση, αλλά τα προβλήματα αντικατάστασης καλωδίων λόγω βελτίωσης, βλάβης η επεκτασιμότητας κρίνονται ακριβές και ενοχλητικές . Αφ' ετέρου, ένα WLAN μπορεί να αναβαθμιστεί απλά με την εγκατάσταση του νέων υλικού και του λογισμικού στους υπολογιστές.

Το καλώδιο που χρησιμοποιείται για τη σύνδεση ενός υπολογιστή με έναν απομακρυσμένο μπορεί να παρέχει τις πολύτιμες ενδείξεις για τη λειτουργία του. Μπορούμε να εξετάσουμε και τις άκρες του καλωδίου και να ανακαλύψουμε τις συνημμένες συσκευές που επικοινωνούν η μια με την άλλη. Οι συνδετήρες σε κάθε τέλος συσχετίζονται συχνά με το σκοπό για τον οποίο το καλώδιο χρησιμοποιείται, έτσι μπορούμε να διερευνήσουμε το καλώδιο και τον απομακρυσμένο που συνδέονται με το και να ξέρουμε αμέσως το υλικό και το λογισμικό που απαιτούνται για να έχει πρόσβαση σε αυτό απομακρυσμένο. Φυσικά, το συνηθισμένο αποτέλεσμα είναι ότι ένα καλώδιο απαιτείται για καθετί απομακρυσμένο. Όχι με την ασύρματη επικοινωνία: το μόνο φυσικό μέσο είναι μέσα στον αέρα, έτσι οι δυνατότητες σύνδεσης είναι πολύ πιο ευπροσάρμοστες χωρίς δημιουργούν χάος πίσω από κάθε υπολογιστή.

Πλεονεκτήματα του ενσύρματου δικτύου

Παρά τα σημαντικά μειονεκτήματα, τα συνδεμένα με καλώδιο δίκτυα θα παραμείνουν πιθανώς βιώσιμα για διάφορους λόγους. Το καλώδιο παρέχει ένα ολόκληρα δοσμένο, ήρεμο κανάλι για τους κόμβους στην πρόσβαση, έτσι η αξιοπιστία αυξάνεται. Υπάρχει

μικρή εξασθένηση σήματος μεταξύ της πηγής και του προορισμού σε ένα καλώδιο, έτσι οι κόμβοι μπορούν να διαβιβάσουν και να λάβουν ταυτόχρονα. Αυτό δεν σημαίνει ότι διάφορα μηνύματα μπορούν να σταλθούν μέσα καλώδιο συγχρόνως (τουλάχιστον όχι χωρίς χρησιμοποίηση των ειδικών τεχνικών διαμόρφωσης).Τα ασύρματα σήματα παρουσιάζουν σημαντική εξασθένηση μεταξύ της συσκευής αποστολής σημάτων και του δέκτη, ένα χαρακτηριστικό που θα ποσολογηθεί σε ένα επόμενο κεφάλαιο.

Η υψηλή εξασθένηση σημάτων μεταξύ της συσκευής αποστολής σημάτων και του δέκτη επίσης σημαίνει ότι η πιθανότητα λάθους bit (επίσης αποκαλούμενη το *ποσοστό λάθους κομματιών(bit error rate,* ή BER) είναι πολύ υψηλότερη στα ασύρματα απ'ό,τι στα συνδεμένα με καλώδιο συστήματα. Οι μεταφορές αρχείων πέρα από το δίκτυο συνήθως πραγματοποιηθούν λάθος, έτσι ώστε πρόσθετα bits προστίθενται στο αρχείο για τον έλεγχο λάθους. Το επακόλουθο είναι από πάνω συνήθως υψηλότερη στα ασύρματα δίκτυα, έτσι η αποδοτικότητά τους είναι χαμηλότερη. Οι περαιτέρω μειώσεις των BER μπορούν να ολοκληρωθούν με τη μείωση της ταχύτητας μετάδοσης στοιχείων στο ασύρματο δίκτυο για να αντισταθμίσουν την υψηλή μείωση. Εμπειρικά, ένα συνδεμένο με καλώδιο δίκτυο μπορεί να στείλει δεδομένα 10 χρόνους γρηγορότερα από έναν ασύρματο δίκτυο της ίδιας χρονικής(τεχνολογικής) στιγμής. Παραδείγματος χάριν, το *Universal Serial Bus* (USB) 1.x λειτουργεί με ταχύτητες περίπου 12 Mb/s, και το IEEE 1394 τις εργασίες σε 100 έως 400 Mb/s. Το Bluetooth λειτουργεί σε ένα ακατέργαστο ποσοστό 1 Mb/s, και το IEEE 802.11b ή WI-FI λειτουργεί μέχρι 11 Mb/s. (Είναι ενδιαφέρον να σημειωθεί ότι το ποσοστό δεδομένων ενός καναλιού τυπικής οπτικής ίνας υπερβαίνει το σύγχρονο συνδεμένο με καλώδιο κανάλι επίσης από έναν παράγοντα 10.)

Η ασφάλεια είναι ένα άλλο ζήτημα που είναι δύσκολο να εξεταστεί με τις ασύρματες συσκευές επειδή οι μεταδόσεις τους δεν περιορίζονται στα όρια ενός καλωδίου. Τα ασύρματα σήματα είναι ευκολότερα να παρεμποδιστούν, να διασπαστούνε, και να παρεμβάλλονται από παράσιτα, τα οποία απαιτούν τα αντίμετρα που δεν είναι συνήθως απαραίτητα κατά τη χρησιμοποίηση ενός καλωδίου.

Ήδη είστε πιθανώς έτοιμοι να αντιστρέψετε τη θέση σας και να ρωτήσετε γιατί κάποιος θα χρησιμοποιούσε την ασύρματη επικοινωνία. Το ραδιόφωνο πρόκειται σαφώς εδώ να μείνει λόγω της απίστευτης ευκολίας του πέρα από τη συνδεμένη με καλώδιο

πρόσβαση, και το Bluetooth έχει ενσωματώσει διάφορες έξυπνες τεχνικές για να ανακουφίσει μερικά από τα πιθανά μειονεκτήματά του έναντι της επικοινωνίας από ένα καλώδιο. Επειδή η ασύρματη επικοινωνία περιλαμβάνει τη χρησιμοποίηση ενός δημόσιου μέσου αποκαλούμενου *ράδιο φάσμα(radio spectrum)*, θα εξετάσουμε τους κανονισμούς που το Bluetooth και τα άλλα ασύρματα δίκτυα πρέπει να ακολουθήσουν.

ΚΑΝΟΝΙΣΜΟΣ ΤΩΝ ΖΩΝΩΝ ΧΩΡΙΣ ΑΔΕΙΑ

Μαζί με πολλές άλλες ασύρματες συσκευές, το Bluetooth χρησιμοποιεί τη χωρίς άδεια ζώνη συχνότητας 2,4 GHz για τη λειτουργία του. Αντίθετα στη δημοφιλή πεποίθηση, χωρίς άδεια δεν σημαίνει ανεξέλεγκτη, και πράγματι οι περισσότερες χώρες ρυθμίζουν αυστηρά τη χρήση των χωρίς άδεια συχνοτήτων. Η διαχείριση συχνότητας εμπίπτει στην (*Federal Communications Commission) ομοσπονδιακή Επιτροπή ανακοινώσεων* (FCC) στις Ηνωμένες Πολιτείες, αλλά άλλες κυβερνήσεις έχουν συχνά τους κανόνες που είναι αρκετά διαφορετικοί από, και ασυμβίβαστος μερικές φορές με, τους κανονισμούς της FCC. Φυσικά, αυτή η κατάσταση έχει τη δυνατότητα να αναγκάσει έναν ρυθμιστικό εφιάλτη για το Bluetooth στην αναζήτησή του να γίνει παγκόσμιο πρότυπο για το περιορισμένου φάσματος ασύρματη επικοινωνία.

Το 1992, η *διεθνής ένωση τηλεπικοινωνιών* (ITU), που είναι μέρος των Ηνωμένων Εθνών, διαμόρφωσε *τον τομέα της ραδιοεπικοινωνίας* (ITU-R) σε μία προσπάθεια να εξασφαλιστεί λογική, αποδοτική, και οικονομική η χρήση του φάσματος *ραδιοσυχνότητας* (RF). Κάθε λίγα χρόνια, η ITU διευθύνει μια *διάσκεψη παγκόσμιων ράδιο επικοινωνιών* (WRC), όπου τα έθνη μελών συμφωνούν σχετικά με τον τρόπο με τον οποίο το ραδιοφάσμα διατίθεται και χρησιμοποιείται. Επιπλέον, η *ειδική ομάδα ενδιαφέροντος* Bluetooth (SIG) συνεργάζεται με τις διάφορες κυβερνήσεις για να φέρει τους κανονισμούς τους σε ευθυγράμμιση με τις απαιτήσεις Bluetooth.

Το Bluetooth λειτουργεί σε 2,4 GHz επειδή αυτή είναι η μόνη πρακτική ζώνη συχνότητας που (συνήθως) διατίθεται παγκοσμίως και δεν απαιτεί καμία άδεια για να ενεργοποιήσει μια συσκευή αποστολής σημάτων. Αυτά είναι καλά νέα, φυσικά, αλλά υπάρχει ένας λόγος για το ότι η ζώνη είναι διαθέσιμη σε όλο τον κόσμο, και ο λόγος είναι οι φούρνοι μικροκυμάτων. Αυτοί οι φούρνοι έγιναν δημοφιλείς πολύ πριν να

προβλεφθεί οποιαδήποτε γενική χρήση αυτών των υψηλών συχνοτήτων, και η συχνότητα φούρνων μικροκυμάτων των 2,45 GHz επιλέχτηκε επειδή τα μόρια ύδατος απορροφούν εύκολα την ενέργεια RF σε αυτήν την συχνότητα και την μετατρέπουν στη θερμότητα. Αυτοί οι φούρνοι λειτουργούν σε αρκετά Watt της ισχύος, και όπως θα ανακαλύψουμε σε ένα επόμενο κεφάλαιο, αυτοί μπορούν να είναι μια σημαντική πηγή παρέμβασης σε Bluetooth και άλλους ασύρματους χρήστες στη ζώνη 2,4 GHz.

Αυτήν την περίοδο, η ζώνη 2.4GHz χρησιμοποιείται από:

- 2.4GHz ασύρματα τηλέφωνα
- 802.11 ασύρματα δίκτυα
- HomeRF ασύρματα δίκτυα
- Όργανα ελέγχου μωρών (νεώτερα πρότυπα)
- Openers γκαράζ-πόρτων (νεώτερα πρότυπα)
- Αστικά και προαστιακά ασύρματα συστήματα επικοινωνιών, συμπεριλαμβανομένης έκτακτης ανάγκης ραδιόφωνα
- Μερικές επικοινωνίες τοπικής κυβέρνησης στην Ισπανία, τη Γαλλία, και την Ιαπωνία
- Φούρνοι μικροκυμάτων

Η ΙΣΤΟΡΙΑ BLUETOOTH

Η ιδέα πίσω από το Bluetooth είχε την προέλευσή της το 1994 όταν άρχισε Ericsson την ιδέα της αντικατάστασης των καλωδίων που συνδέουν τα εξαρτήματα με τα κινητά τηλέφωνα και τους υπολογιστές με ασύρματες συνδέσεις. Δεδομένου ότι τεχνικές λεπτομέρειες άρχισαν να προκύπτουν, η Ericsson γρήγορα συνειδητοποίησε ότι η πιθανή αγορά για τα προϊόντα Bluetooth θα ήταν τεράστια, αλλά θα απαιτούνταν η συνεργασία σε όλο τον κόσμο για να πετύχουν τα προϊόντα. Επομένως, η Bluetooth SIG διαμορφώθηκε το 1998, και η πρώτη τεχνική προδιαγραφή Bluetooth έφθασε το 1999.

Αλλά γιατί να καλούμε ένα ασύρματο σύστημα Bluetooth; Δεν υπάρχει κανένας υπαινιγμός μέσα στο ίδιο το όνομα που να αντιπροσωπεύει ένα ασύρματο σύστημα επικοινωνιών. Ο Harald Bluetooth(Blatand στα δανικά) ήταν μονάρχης Βίκινγκ του 10ου αιώνα (γεννηθείς το 911 μχ) που κατόρθωσε να ενώσει τη Δανία και τη Νορβηγία, και επειδή η αρχική διαμόρφωση της έννοιας της ασύρματης αντικατάστασης καλωδίων άρχισε στην Σκανδιναβία, έβγαζε κάποιο νόημα για να αναγνωρίσει την προέλευση του Βίκινγκ. Επιπλέον, ενοποιώντας την προσέγγιση του Harald για κατάκτηση, συνεπλεξε ωραία με σκοπό την ένωση υπολογιστή και περιφερειακών μέσω μιας προδιαγραφής που θα επιτύγχανε ενδεχομένως την παγκόσμια αποδοχή.

Η ειδική ομάδα ενδιαφέροντος Bluetooth (Special interest group (SIG)

Ιδρυμένο από Ericsson, τη Nokia, την IBM, την Intel, και Toshiba, η Bluetooth SIG άρχισε το Φεβρουάριο 1998, Ακόμη και κατά τη διάρκεια της παιδικής ηλικίας του, το Bluetooth ήταν σαφώς προβλεπόμενο ως παγκόσμιο σύστημα επικοινωνιών όπως αποδεικνυόταν από Ericsson και τη Nokia που αντιπροσωπεύουν την Ευρώπη, IBM και Intel που αντιπροσωπεύουν την Αμερική, και Toshiba που αντιπροσωπεύει την Ασία. Στη SIG ενώθηκαν το Δεκέμβρη του 1999 οι 3Com, Lucent, Motorola και η Microsoft, και αυτές οι εννέα οντότητες καλούνται τώρα *υποστηρικτές(promoters) SIG*. Αυτή τη στιγμή δεν υπάρχει κανένα σχέδιο για πρόσθεση στον κατάλογο υποστηρικτών. Οι υποστηρικτές είναι αρμόδιοι για την υψηλού επιπέδου διοίκηση της SIG, και για την παροχή του εργατικού δυναμικού για να τρέξουν τις νομικές διαδικασίες, το μάρκετινγκ, και τις διαδικασίες πιστοποίησης.

Μερικές από τις σημαντικότερες λειτουργίες των SIG περιλαμβάνουν:

- Υποβολή αίτησης των διάφορων κυβερνητικών αντιπροσωπειών για να επιτρέψει το Bluetooth να λειτουργήσει στις χώρες τους χωρίς τις ειδικές απαιτήσεις ή περιορισμούς.
- Να χειρίζονται τα νομικά ζητήματα σχετικά με την ιδιότητα μέλους SIG, την πνευματική ιδιοκτησία, και χρήση του εμπορικού σήματος.

- Να διαχειρίζονται τη διαδικασία που εξετάζει τις συσκευές για να διασφαλίσει τη συμμόρφωση τους στην προδιαγραφή Bluetooth.
- Να διαχειρίζονται τις διαδικασίες δοκιμής διαλειτουργικότητας για να εξασφαλίσει ότι οι συσκευές Bluetooth από διαφορετικούς κατασκευαστές μπορούν να επικοινωνήσουν η μια με την άλλη.
- Διαχείριση των τεχνικών ομάδων εργασίας
- Δημιουργία και έκδοση της προδιαγραφής Bluetooth

Η υψηλότερη θέση ιδιότητας μέλους ανοικτή σε άλλες οντότητες (εταιρίες και άλλες ομάδες) είναι το συνδυαζόμενο μέλος Associate Member, που απαιτείται να υπογράψει ένα νομικό έγγραφο και να δώσει μια ετήσια αμοιβή ιδιότητας μέλους. Οι συνεταίροι έχουν την άδεια για να συμμετέχουν στο μάρκετινγκ και τις τεχνικές υποομάδες και τους δίνεται η πρόσβαση στην ομάδας εργασίας για τα επίσημα σχέδια εγγράφων στην έκδοση 0.5 και ανωτέρω. Οι Adopters, από την άλλη, παίρνουν μέρος στη SIG χωρίς καταβολή μιας αμοιβής, αν και ένα νομικό έγγραφο υπογράφεται, και τους επιτρέπεται να συμμετέχουν σε μερικούς ρυθμιστικά test, και σε ομάδες εμπειρογνωμόνων. Οι Adopters έχουν πρόσβαση στα επίσημα σχέδια εγγράφων ομάδας εργασίας στην έκδοση 0.9 και ανωτέρω.

Τα μέλη της SIG απαιτούνται προτού να μπορέσει η προδιαγραφή Bluetooth να χρησιμοποιηθεί στα σχέδια, και στο μέλος χορηγείται η πρόσβαση στην πνευματική ιδιοκτησία Bluetooth και το λογότυπο χωρίς πληρωμή των δικαιωμάτων. Τα SIG έγιναν μια μη κερδοσκοπική εταιρία στις αρχές του 2001, και ο εκτενής ισόχωρος του μπορεί να προσπελαστεί στη διεύθυνση www.Bluetooth.org.

ΠΙΝΑΚΑΣ 1.1 Δικαιώματα των διάφορων μελών

Activity	Associate Member	Adopter Member
Marketing meetings and reflector	Yes	No
Architecture Review Board votes, meetings, and reflector	Yes	No
Regulatory meetings, reflector, and database	Yes	Yes
Test meetings and reflector	Yes	Yes
Working group chairs, meetings, and reflector	Yes	No
Working group drafts	Yes	Yes
Expert group chairs	Yes	No
Expert group meetings and reflector	Yes	Yes

ΚΕΦΑΛΑΙΟ 2
ΚΑΘΙΕΡΩΣΗ PICONET

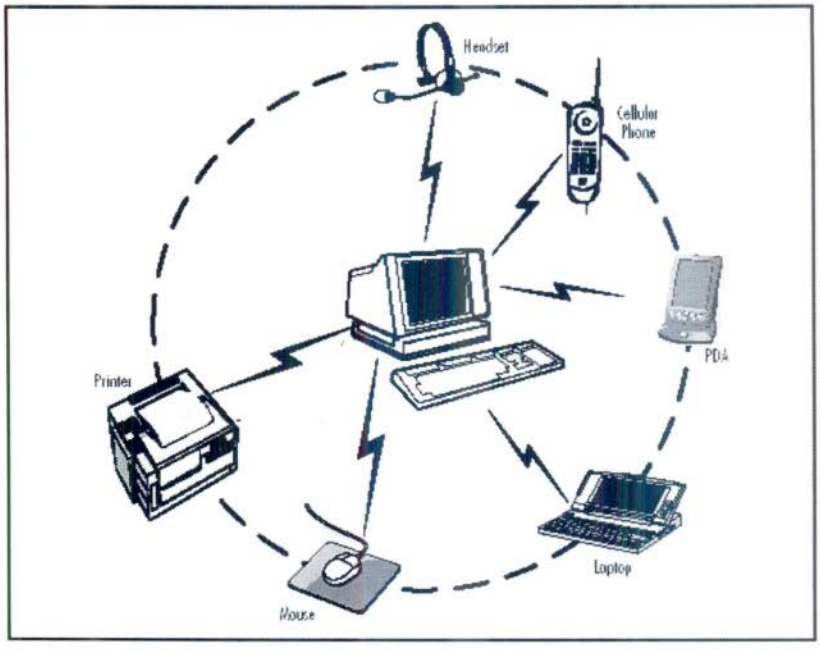
ΓΕΝΙΚΑ

Η προδιαγραφή Bluetooth καθορίζει μια μικρή (10 μέτρα) ή μια μέση απόσταση (100 μέτρα) ραδιοσύνδεσης ικανή για μετάδοση φωνής ή στοιχείων σε μια μέγιστη ικανότητα 720 kbps ανά κανάλι (με μια ακαθάριστη ρυθμοαπόδοση 1Mbit/sec). Η λειτουργία ραδιοσυχνότητας είναι στη χωρίς άδεια βιομηχανική, επιστημονική και ιατρική (ism) ζώνη στα 2,4 έως 2,48 GHz, που χρησιμοποιεί ένα φάσμα διάδοσης, hopping συχνότητας, πλήρης-διπλό σήμα σε μέχρι 1600 hops/sec. Οι μεταπηδήσεις σημάτων μεταξύ 79 συχνοτήτων σε διαστήματα 1 MHz χρησιμοποιούνται για να δώσουν έναν υψηλό βαθμό ασυλίας της παρέμβασης από τις εξωτερικές επιρροές. Αυτό οφείλεται κυρίως στον αριθμό ηλεκτρονικής διανομής προϊόντων σε αυτό το φάσμα συχνότητας. Η παραγωγή RF καθορίζετε ως 0 dBm (1 mW) στην επικοινωνία 10 μέτρων και -30 + 20 dBm (100 mW) στην έκδοση μεγαλύτερης απόστασης.

ΤΙ ΕΙΝΑΙ PICONET

Αφού περιγράψαμε παραπάνω τις διαφορές μεταξύ ασύρματων και ενσύρματων δικτύων παρακάτω θα εξετάσουμε πως γίνεται η σύνδεση των συσκευών όπως για παράδειγμα ενός υπολογιστή, ένα PDA, ένας εκτυπωτής και ένα κινητό. Πως όλες αυτές οι συσκευές μπορούν να συνδεθούν.

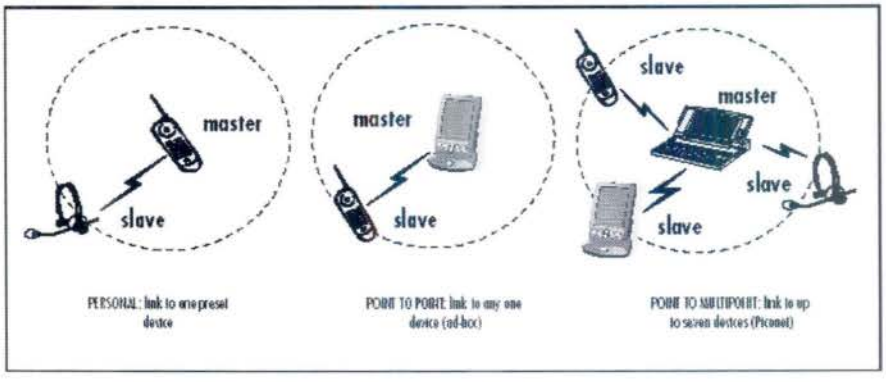
Το σχήμα 2.1 δείχνει την λύση για όλες αυτές τις Bluetooth-enable συσκευές. Η απλή πράξη της χρησιμοποίησης της τεχνολογίας Bluetooth ως αντικατάσταση καλωδίων αφαιρεί το πρόβλημα των πραγματικών φυσικών συνδέσεων και η ικανότητα ad hoc(μη προγραμματισμένης) σύνδεσης της τεχνολογίας μπορεί να επιτρέψει την επικοινωνία μεταξύ των συσκευών



ΣΧΗΜΑ 2.1 Ένα piconet

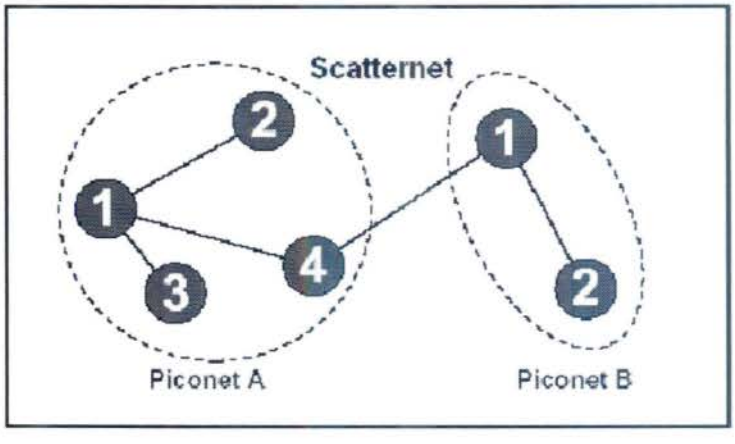
Αυτό το πλήρως ασύρματο σενάριο μπορεί να επιτευχθεί λόγω της master/slave φύσης της Bluetooth τεχνολογίας. Όλες οι συσκευές είναι ισότιμες, αναγνωριζόμενες από την μοναδική τους 48-bit διεύθυνση, και μπορεί να οριστούν ως master είτε κατά τη λειτουργία τους είτε από την επέμβαση χρηστών.

Ένας master μπορεί να συνδέσει μέχρι επτά slaves συγχρόνως, διαμορφώνοντας ένα piconet - αυτό το "point-to-multipoint" χαρακτηριστικό γνώρισμα ξεχωρίζει το Bluetooth από τις άλλες ασύρματες τεχνολογίες. Το σχήμα 2.2 δείχνει διάφορα σενάρια σύνδεσης.



ΣΧΗΜΑ 2.2 Διάφορα σενάρια συνδέσεων μεταξύ των συσκευών

Στο τελευταίο σενάριο, ένα μέλος ενός piconet μπορεί επίσης να ανήκει σε ένα άλλο piconet. Το σχήμα 2-3 επεξηγεί το *scatternet*, όπου ένας σκλάβος σε ένα piconet είναι επίσης ο Master ενός δεύτερου piconet που επεκτείνει έτσι τη δικτύωση μεταξύ των συσκευών. Μια συσκευή σε ένα PAN μπορεί να επικοινωνήσει με μια άλλη συσκευή σε διαφορετικό PAN!



ΣΧΗΜΑ 2.3 Ένα τυπικό scatternet

ΕΠΙΤΡΕΠΟΝΤΑΣ ΤΗΝ ΠΑΡΕΜΒΟΛΗ

Ασύρματα σημαίνει ραδιοσύνδεση -και οι ραδιοσυνδέσεις υπόκεινται στην παρεμβολή. Η παρεμβολή μπορεί να έχει αντίκτυπο και στην ποιότητα μιας audio σύνδεσης (Synchronous Connection Oriented [SCO]) και στην σύνδεση δεδομένων (Asynchronous Connectionless [ACL]). Τα υψηλά επίπεδα παρεμβολής μπορούν να διακόψουν τις επικοινωνίες για αρκετό χρόνο για να προκαλέσει τη λίστα πρωτοκόλλου(protocol stack) να εγκαταλείψει τη σύνδεση. Αν και αυτό εξετάζεται στη Bluetooth Προδιαγραφή με ένα σχέδιο μεταπήδησης συχνοτήτων που παρέχει ευρωστία, αυτό είναι ακόμα μια σοβαρή εκτίμηση για μερικές εφαρμογές.

Η τεχνολογία Bluetooth δεν πρέπει να χρησιμοποιηθεί για ασφαλείς ή κρίσιμες εφαρμογές όπου τα δεδομένα *πρέπει απολύτως* να περάσουν από το κανάλι απευθείας, επειδή υπάρχει πάντα μια πιθανότητα παρεμβολής που σταματά τη σύνδεση. Η παρεμβολή μπορεί να προέλθει από το ποικίλες πηγές όπως:

- Φούρνοι μικροκυμάτων
- Άλλα Bluetooth piconets(Αν και δεν έχουν μεγάλη επίδραση λόγω FHSS)
- Άλλα Συστήματα επικοινωνιών (όπως ieee 802.11b)
- Δίκτυα Home RF
- Κινητά τηλέφωνα

Frequency Hop Spread Spectrum (FHSS)

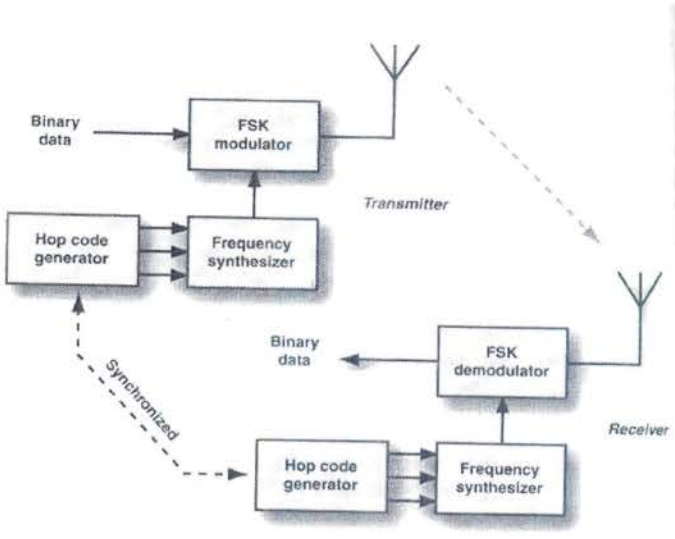
Αν σχεδιάζαμε ένα σύστημα επικοινωνιών για να λειτουργήσει σε ένα περιβάλλον που έχει μια υψηλή δυνατότητα για την παρέμβαση, τι θα έπρεπε η συχνότητα του φορέα να είναι; Μια καλή ιδέα θα ήταν να δημιουργηθούν διάφορες συχνότητες φορέων, ή κανάλια, και να επιλεχτεί αυτό που έχει ένα επίπεδο παρεμβολής κάτω από κάποιο κατώτατο όριο πριν από την έναρξη κάθε συνόδου επικοινωνίας. Η διαδικασία επιλογής καναλιών θα μπορούσε ακόμη και να είναι αυτόματη. Αυτή η μέθοδος χρησιμοποιείται με πολλά ασύρματα τηλέφωνα στις Ηνωμένες Πολιτείες για να αποφύγει παρέμβολη από τα τηλέφωνα των γειτόνων. Λειτουργεί καλά επειδή υπάρχει συνήθως ένα όριο στον αριθμό ασύρματων τηλεφώνων μέσα σε μια ιδιαίτερη περιοχή, και αρκετά κανάλια

υποδεικνύονται ώστε σχεδόν να εγγυηθούν ότι θα υπάρξει επικοινωνία σε οποιοδήποτε ιδιαίτερο χρόνο μέσα σε ένα σπίτι.

Για ένα Bluetooth piconet, εν τούτοις, είναι πιθανό ότι η παρεμβολή θα αλλάξει από στιγμή σε στιγμή στη ζώνη 2,4 GHz, και πολλές χρήσεις θα προσπαθήσουν να συνυπάρξουν σε αυτήν την ζώνη μεταξύ της απόστασης της μιας με της άλλης. Επιλογή ενός ενιαίου καναλιού και έπειτα να παραμείνει εκεί για μια ολόκληρη συνεδρίαση διατρέχει τον κίνδυνο μια ξαφνικής, καταστροφικής αύξησης της παρεμβολής όπου οι συμμετέχοντες Bluetooth συσκευές να μην είναι σε θέση ακόμη και να συντονίσουν μια αλλαγή καναλιών, και η επικοινωνία να χαθεί. Για να αποφύγει αυτήν την κατάσταση, το Bluetooth χρησιμοποιεί το FHSS ως τεχνική αποφυγής παρεμβολής.

Ένα block diagram ενός συστήματος επικοινωνιών Bluetooth FHSS παρουσιάζεται στο σχήμα 2-4. Το δυαδικά δεδομένα βασικής ζώνης είναι σε διαμόρφωση GFSK και διαβιβάζονται χρησιμοποιώντας ένα φέρον κύμα που καθορίζεται από τον frequency synthesizer. Αντί να δημιουργείται μόνο μια συχνότητα φέρον κύματος, ο synthesizer ελέγχεται από μια γεννήτρια Hop code που τον αναγκάζει να αλλάξει τη συχνότητα φορέα στο ονομαστικό ποσοστό 1.600 hops per sec. Ένα πακέτο δεδομένων Bluetooth στέλνεται ανά hop.

Το ίδιο αυτό το σχέδιο των μεταπηδήσεων φαίνεται να είναι τυχαίο αλλά δημιουργείται πραγματικά από ένα ψευδοτυχαίο αλγόριθμο στη γεννήτρια κώδικα hop. Η γεννήτρια είναι "αντεγραμένη" στο δέκτη ώστε να δημιουργήσει το ίδιο hopping σχέδιο που ο πομπός χρησιμοποιεί. Επικοινωνώντας, έπειτα, ο πομπός και ο δέκτης μεταπηδούν μαζί από κανάλι σε κανάλι. Επιπλέον, οι δύο συσκευές έχουν ήδη χρονικά συμφωνήσει σχετικά με την ακολουθία hop, έτσι ακόμα κι αν μερικά hop κανάλια περιέχουν παρεμβολές, το piconet θα επιζήσει επειδή όλα τα μέλη σύντομα θα μεταπηδήσουν μαζί από εκείνο το κανάλι.



ΣΧΗΜΑ 2.4 Διάγραμμα ενός FHSS συστήματος επικοινωνίας

Συγχρονισμός μεταξύ της επικοινωνίας των συσκευών

Για να επικοινωνήσουν δύο συσκευές χρησιμοποιώντας FHSS, πρέπει να συγχρονιστούν κατάλληλα έτσι ώστε να μεταπηδούν μαζί από κανάλι σε κανάλι. Αυτό σημαίνει ότι οι συσκευές πρέπει να:

- Χρησιμοποιούν το ίδιο σύνολο καναλιών.
- Χρησιμοποιούν την ίδια hopping ακολουθία μέσα σε εκείνο το σύνολο καναλιών.
- Να είναι συγχρονισμένες μέσα στη hopping ακολουθία.
- Εξασφαλίσουν ότι ένας διαβιβάζει ενώ άλλος λαμβάνει, και αντίστροφα.

Όλα αυτά τα αντικείμενα συγχρονισμού καθορίζονται από τον master στο piconet. Ο master περνά τις παραμέτρους συγχρονισμού FHSS σε έναν slave κατά τη διάρκεια της διαδικασίας page, που καλύπτεται αργότερα.

Hop Channel Set και περίοδος: Μια ραδιοζευξη FHSS είναι προγραμματισμένη να λειτουργήσει σε ένα ορισμένο σύνολο συχνοτήτων, το οποίο καλείται *σύνολο καναλιών [channel set]*. Για το Bluetooth, το σύνολο καναλιών αποτελείται από τις συχνότητες φορέα

$fc = 2.402 + K$ MHz $K = 0,1,. . .,78$

Κατά συνέπεια, υπάρχουν 79 πιθανές συχνότητες στο σύνολο καναλιών, κάθε μια χωρισμένη κατά διαστήματα 1 MHz και καλύπτοντας τις συχνότητες 2.402 έως 2.480 MHz. Το piconet μεταπηδά ψευδοτυχαία μέσα σε αυτά τα κανάλια. Κάθε κανάλι έχει 1 MHz εύρος, και η μετάδοση δεδομένων Bluetooth GFSK καταλαμβάνει αυτό το εύρος ζώνης.

ΕΞΕΤΑΣΗ ΤΗΣ ΙΣΧΥΟΣ ΚΑΙ ΤΗΣ ΑΠΟΣΤΑΣΗΣ

Η ισχύς είναι μια κρίσιμη εκτίμηση για τις ασύρματες συσκευές. Εάν ένα προϊόν πρόκειται να γίνει ασύρματο, από πού θα προέλθει η ισχύς του;

Συχνά το καλώδιο επικοινωνίας στις ενσύρματες επικοινωνίες ενεργεί επίσης ως καλώδιο ισχύος. Με το καλώδιο εκτός, το θέμα των μπαταριών παρουσιάζεται, και αναπόφευκτες ερωτήσεις προκύπτουν σχετικά με τη ζωή μπαταριών, τον εφεδρικό(standby) χρόνο, και τις φυσικές διαστάσεις.

Όταν τα καλώδια αντικαθίστανται με μια σύνδεση Bluetooth, ξαφνικά χρειαζόμαστε τη ισχύ να οδηγήσουμε τη σύνδεση, την ισχύ να οδηγήσουμε το μικροεπεξεργαστή που τρέχει τη λίστα πρωτοκόλλου Bluetooth, και την ισχύ(power) να ενισχύσουμε το ακουστικό σήμα σε ένα επίπεδο που ο χρήστης μπορεί να ακούσει. Με τις μικρές κινητές συσκευές προφανώς δεν θέλουμε να εγκαταστήσουμε τις τεράστιες μπαταρίες, έτσι η μικρή κατανάλωσης ισχύος είναι μια σημαντική εκτίμηση.

Κατηγορίες ισχύος πομπού

Οι συσκευές αποστολής σημάτων Bluetooth περιέρχονται σε τρεις βασικές κατηγορίες που καθορίζονται από τη μέγιστη παραγωγή ισχύς τους. Η κατηγορία 1 συσκευών αποστολής σημάτων είναι η ισχυρότερη στη μέγιστη ισχύ των 100 μ W (20 dBm), η κατηγορία 2 (πομπού) έχει μια μεγάλου μεγέθους ισχύς της τάξης των 2.5 mW (4 dBm), και η κατηγορία 3 (πομπού) παράγει 1 mW (0 dBm). Στη κατηγορία 1 ο πομπός πρέπει να έχει ένα χαρακτηριστικό γνώρισμα ελέγχου ισχύος για να μειώσει την ισχύ σε ένα επίπεδο επαρκές για την επικοινωνία προκειμένου να αποτραπεί η υπερβολική παρέμβαση σε άλλους χρήστες στη ζώνη. Οι άλλες δύο κατηγορίες δεν απαιτούν τον έλεγχο δύναμης, αλλά μπορεί να υιοθετηθεί ως προαιρετικό χαρακτηριστικό γνώρισμα.

Η κατηγορία 2 και η κατηγορία 3 Η συσκευή κατηγορίας 2 Bluetooth επιτρέπεται να έχει μια μέγιστη έξοδο ισχύος 4 dBm, με μια ονομαστική έξοδο ισχύος 0 dBm και της ελάχιστης ισχύος -6 dBm (εάν το power control εφαρμόζεται). Η μέγιστη παραγόμενη ισχύς για την κατηγορία 3 συσκευή αποστολής σημάτων Bluetooth είναι 0 dBm. Ο έλεγχος δύναμης είναι προαιρετικός, αλλά πιθανότατα δεν θα βρει εφαρμογή σε πολλές κατηγορίας 2 και κατηγορίας 3 συσκευές Bluetooth.

Bluetooth Radio Power Classes

Power Class	Max Output Power	Range
Class 1	100 mW	100 meters+
Class 2	2.5 mW	10 meters
Class 3	1 mW	1 meter

ΣΧΗΜΑ 2-5 Η προδιαγραφή Bluetooth καθορίζει τρεις κατηγορίες ισχύος για τις ράδιο συσκευές αποστολής σημάτων με μια παραγωγή ισχύος 1 mW. 2.5 mW,και 100 mW .Η παραγωγή ισχύος καθορίζει την απόσταση που η συσκευή είναι σε θέση να καλύψει και έτσι η λειτουργία του προϊόντος πρέπει να εξεταστεί όταν αποφασίσουμε ποια κατηγορία ισχύος θα χρησιμοποιηθεί

Η κατηγορία 1 Η μέγιστη εκπομπή ισχύος της κατηγορίας 1 για τις συσκευές Bluetooth φτάνει μέχρι 20 dBm, και μια μέθοδος έλεγχου της ισχύος(power control) απαιτείται για να κατεβούμε στα 4 dBm, ή χαμηλότερα εάν αυτό επιδιώκεται. Το χαμηλότερο όριο ισχύος προτείνεται για να είναι -30 dBm (1 μW), αλλά δεν είναι υποχρεωτικό για τα επίπεδα κάτω από 4 dBm.

Ο έλεγχος ισχύος εφαρμόζεται χρησιμοποιώντας έναν μηχανισμό ανατροφοδότησης μεταξύ του master και ενός slave στο piconet. Στην περιγραφή της λειτουργίας του, ας υποθέσουμε ότι η ισχύς της συσκευών αποστολής σημάτων του master ρυθμίζεται από έναν slave. Για να είναι δυνατός ο έλεγχος ισχύος , η συσκευή αποστολής σημάτων του master πρέπει να έχει την ικανότητα να αλλάξει το επίπεδο ισχύος της αυτόματα, και ο δέκτης του slave πρέπει να έχει ένα βαθμολογημένο RSSI [receive signal strength indicator]. Επιπλέον, πρέπει να υπάρχουν τα μέσα για το slave ώστε να κατευθύνει τον master για να ρυθμίσει την ισχύ του, είτε προς τα πάνω είτε προς τα κάτω. Αυτό γίνεται χρησιμοποιώντας τα πακέτα *πρωτοκόλλου διευθυντών συνδέσεων* (LMP), όπως περιγράφεται παρακάτω

Ένας πομπός έλεγχου ισχύος πρέπει να έχει τη δυνατότητα να ρυθμίσει το επίπεδο παραγωγής(output) της στα κομμάτια που κυμαίνονται στο μέγεθος μεταξύ 2 και 8 DB. Η σειρά ρύθμισης πρέπει να είναι μεταξύ 4 dBm (ή, προαιρετικά, χαμηλότερα) και του μέγιστου επιπέδου δύναμης (μέχρι 20 dBm). Για παράδειγμα, υποθέστε η μέγιστη παραγωγή ισχύος ότι ενός πομπού είναι 20 dBm. Η απαίτηση του έλεγχου ισχύος θα μπορούσε να καλυφτεί με την εφαρμογή ενός μεγέθους 8 DB, οπότε σ'αυτή την περίπτωση θα υπήρχαν μόνο τρία επίπεδα δύναμης: 20 ..12, και 4 dBm. Εάν ένα μέγεθος βημάτων 2 DB χρησιμοποιείται άντ' αυτού, θα απαιτούνταν εννέα επίπεδα ισχύος.

Ένας δεκτής συμμετέχοντας στη διαδικασία power control προσπαθεί να τοποθετήσει το επίπεδο ισχύος του εισερχόμενου σήματος στο Golden Receive Power Range όπως αναφέρεται στην προδιαγραφή Bluetooth. Έτσι όταν κάποια επίπεδα ισχύος βγουν έξω από αυτά όρια ενεργεί το power control.

ΕΓΚΑΤΑΣΤΑΣΗ ΣΥΝΔΕΣΕΩΝ

Τα Bluetooth piconets είναι ιδιαίτερα δυναμικά, αλλάζουν γρήγορα με την εμφάνιση και εξαφάνιση διάφορων συσκευών. Τα μέλη ενός piconet μπορούν να αλλάξουν, ή ολόκληρο το piconet μπορεί να διαλυθεί σε μια στιγμή. Σε ένα τέτοιο δυναμικό δίκτυο, δεν είναι εφαρμόσιμο να ξοδεύεται σημαντικός χρόνος αποκτώντας πληροφορίες για τις συσκευές και που διαμορφώνοντας το λογισμικό για να τους χρησιμοποιήσει: αυτή η διαδικασία πρέπει να είναι αυτόματη. Αυτό συνήθως γίνεται από δυο βαθμίδες διαδικασίας. Η πρώτη είναι για έναν p-master να ανακαλύψει ποιες άλλες Bluetooth συσκευές είναι σε απόσταση(inquiry), και το άλλο βήμα είναι να ξεκινήσει ο p-master την σύνδεση με την συγκεκριμένη συσκευή που ανταποκρίνεται στη διαδικασία inquiry (page)

Τι κάνει όμως MASTER μια συσκευή ενώ μια άλλη γίνεται *slave*; Κάθε συσκευή Bluetooth έχει την ικανότητα να είναι είτε *master* είτε *slave*,έτσι δεν υπάρχει κάτι στο hardware που να υπαγορεύει για το ποιος θα είναι ο Master. Αντιθέτως ως master ορίζεται η συσκευή που θα ξεκινήσει την καθιέρωση του piconet και slave είναι οι συσκευές που εισέρχονται στο Piconet. Με άλλα λόγια ο master είναι αυτός που ξεκινά την σύνδεση μέσω του page, και οι slave έχουν απαντήσει σε αυτό το page. Γνωρίζουμε ότι ο p-master πρέπει να στείλει το frequency hop synchronization (FHS) πακέτο του σε μια slave συσκευή ώστε αργότερα να χρησιμοποιήσει την ίδια συχνότητα hop και φάση που χρησιμοποιούνται από τον master.Αλλά σε ποια συχνότητα θα αλλάξουν το FHS πακέτο; Για την έρευνα ο Master μπορεί να μην γνωρίζει τίποτα για γειτονικές συσκευές ,το hop συχνότητας (βασικά, μια συχνότητα για αποστολή inquiry και άλλη για απάντηση στο inquiry) χρησιμοποιείται από όλες τις συσκευές για να αρχίσουν την ανακάλυψη συσκευών. Ένας p-slave άπαντα σε ένα inquiry στέλνοντας το δικό του FHS πακέτο μες στο οποίο είναι η Bluetooth device address(BD_ADDR).Τώρα ο p-master μπορεί να δημιουργήσει μια νέα hopping συχνότητα βασισμένη στην BD_ADDR για να στείλει διαδοχικά ένα Page για να καθιερώσει ένα piconet με αυτόν τον p-slave.

Δραστηριότητες συνδέσεων από σημείο σε σημείο

Υποθέστε ότι ένας p-master θέλει να ψάξει το χώρο για τις διαθέσιμες συσκευές Bluetooth και ίσως έπειτα να συνδεθεί με μια από αυτές σε ένα από σημείο σε σημείο piconet. Η σειρά των βημάτων που περιλαμβάνονται σε μια τέτοια προσπάθεια μπορεί να φανούν υπό μορφή διαγράμματος 2-6. Αυτό το διάγραμμα περιέχει ένα σύνολο καταστάσεων συνδεδεμένων με κάθε βήμα της καθιέρωσης ενός piconet και ένα σύνολο *μεταβάσεων* που απεικονίζουν την επιτρεπόμενη μετακίνηση από το κατάσταση σε κατάσταση . Μια συσκευή μπορεί να είναι μόνο σε μια κατάσταση τη φορά, αλλά μπορεί (όπου επιτρέπεται) να κινηθεί μεταξύ των καταστάσεων, μερικές φορές αρκετά γρήγορα.

Όταν μια συσκευή Bluetooth αρχικά τροφοδοτείται(power up), μπαίνει σε κατάσταση STANDBY, όπου το υλικό και το λογισμικό του αρχικοποιείται. Από αυτό τη κατάσταση, ένας p-master μπορεί να πάει είτε σε PAGE είτε σε INQUIRY, ανάλογα με εάν το σελιδοποιημένο το BD_ADDR της μονάδας είναι ή όχι γνωστό. Η κατάσταση ΕΡΕΥΝΑΣ επιτρέπει στον p-master να ανακαλύψει όλες τις BD_ADDR αυτών που απαντάνε οι p-slaves, και από εκεί μπορεί είτε να επιστρέψει σε STANDBY είτε να πάει στη κατάσταση PAGE για να καθιερώσουν ένα από σημείο σε σημείο piconet με έναν p-slave. Εάν η διαδικασία PAGE είναι επιτυχής, κατόπιν ο p-master γίνεται master και ο p-slave γίνεται slave του νέου piconet, και οι συσκευές αρχίζουν να ανταλλάσσουν τις παραμέτρους οργάνωσης δικτύων και τις πληροφορίες χρηστών. Κατά τη διάρκεια αυτής της περιόδου οι δύο συσκευές είναι σε κατάσταση CONNECT .

Ένας p-slave μπορεί περιοδικά να κινηθεί από το STANDBY για να αφουγκραστεί τα inquiry και τα page. Εάν σελιδοποιείται επιτυχώς, αλλάζει σε CONNECT δηλώνει μαζί με το νέο master. Ενώ στη κατάσταση CONNECT ο slave μπορεί να κανονίσει με τον master του να εισαχθεί σε έναν από τους τρεις χαμηλής ισχύος τρόπους αποκαλούμενους *sniff, hold,* και *park*. Ο sniff τρόπος επιτρέπει στο slave για να ελέγξει για μια κύρια μετάδοση λιγότερο συχνά απ'ό,τι σε κάθε άρτια αριθμημένη χρονική αυλάκωση. Ο τρόπος hold είναι ένας χρόνος κατά τη διάρκεια του οποίου ο slave μπορεί προσωρινά να βγει από το piconet χωρίς αν αποσυνδεθεί από τον master. Αφότου λήγει ο χρόνος hold ο slave άλλη μια φορά εκτελεί τα κανονικά καθήκοντα piconet. Ένας slave που είναι στη

κατάσταση park σταματά την AM_ADDR του και ενεργοποιεί το δέκτη του να ξανασυγχρονίζει περιοδικά το CLK του με εκείνο του master. Ο master πρέπει να ξεκινήσει την διαδικασία unpark για τον slave με ένα νέο AM_ADDR προτού να μπορέσει να συνεχίσει την κανονική επικοινωνία.

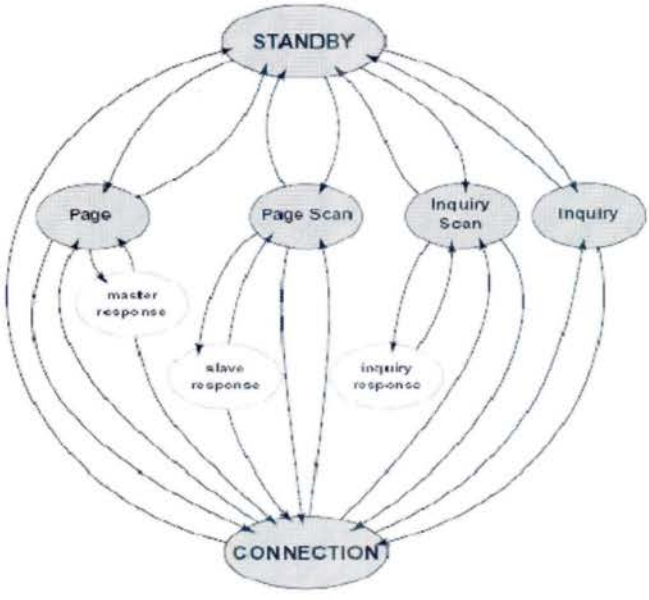
Από την κατάσταση CONNECT είτε ο master είτε ο slave μπορεί να αρχίσουν την αποσύνδεση, από το οποίο και τα δύο επιστρέφουν σε STANDBY εάν δεν συμμετέχουν σε άλλη δραστηριότητα Bluetooth.

Κατά συνέπεια, μόλις καθιερωθεί ένα piconet με έναν μόνο slave, κανένας πρόσθετος *slave* δεν μπορεί να παρουσιαστεί στο piconet. Κάποιο πρόσφατα Bluetooth chipsets έχουν αυτόν τον ιδιαίτερο περιορισμό. Τα πιο πρόσφατα σύνολα τσιπ είναι πιο ευπροσάρμοστα, επιτρέποντας όχι μόνο τα point-to-multipoint piconets, αλλά και scatternet διαδικασίες.

Γενική καθιέρωση Piconet

Οι πιο ευπροσάρμοστες συσκευές Bluetooth μπορούν να κινηθούν εύκολα μεταξύ των διαφορετικών καταστάσεων που ανήκουν είτε σε έναν p-master είτε έναν p-slave, ανάλογα με αυτό που οι στόχοι του τελικού χρήστη μπορούν να είναι. Για παράδειγμα, υποθέστε ότι ένας master ενός piconet με έναν ενιαίο slave θέλει να φέρει έναν νέο slave στο piconet. Σαφώς, ο master απαιτεί την ικανότητα να κινηθεί από την κατάσταση CONNECT πίσω στα PAGE ή INQUIRY states. Είναι επίσης σαφές ότι η αποστολή ενός page και ο εντοπισμός ένος page είναι χωριστές καταστάσεις επειδή το πρώτο ανήκει σε έναν p-master και το τελευταίο ανήκει σε έναν p-slave.

Το σχήμα 2-6 παρουσιάζει διάγραμμα καταστάσεων για κάθε συσκευή Bluetooth που είναι ικανή για λειτουργίες από σημείο σε σημείο, point-to-multipoint, και scatternet .



ΣΧΗΜΑ 2-6

Όπως πριν, η πρώτη κατάσταση είναι το STANDBY και από εκεί μπορεί να μπει σε ένα από τέσσερις καταστάσεις: PAGE, PAGE SCAN, INQUIRY, or INQUIRY SCAN. Αυτά καθορίζονται ως εξής:

PAGE : Χρησιμοποιείται από έναν p-master για να καθιερώσει ένα piconet με έναν p-slave του οποίου η BD_ADDR είναι γνωστή .

PAGE SCAN : Που χρησιμοποιείται από έναν p-slave για να αφουγκραστεί τη page διαδικασία .

INQUIRY : Που χρησιμοποιείται από έναν p-master για να ανακαλύψει το BD_ADDR και άλλες πληροφορίες των συσκευών μέσα στο βεληνεκές της συσκευής.

INQUIRY SCAN : Που χρησιμοποιείται από έναν p-slave για να αφουγκραστεί μια έρευνα

Το PAGE, PAGE SCAN, ΚΑΙ ΤΟ INQUIRY SCAN όλα αυτά έχουν τις απαντήσεις συνεργάσιμες με αυτά, τα οποία είναι:

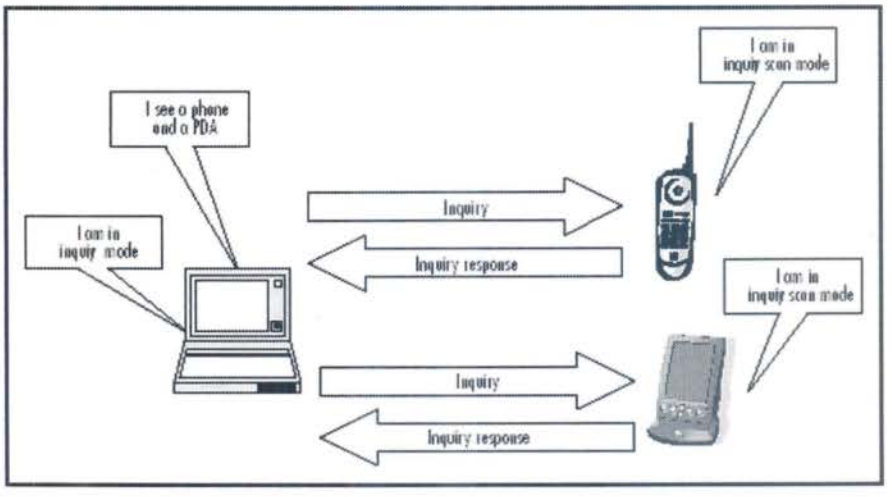
P-slave response after PAGE SCAN : εάν ένας P-slave ακούει το page του καθώς είναι στην κατάσταση PAGE SCAN, τότε άπαντα με την δικιά του device access code(DAC).

P-master response after PAGE : Όταν ο p-master ακούει την απάντηση του p-slave DAC, τότε άπαντα με την σειρά του ένα πακέτο FHS, δίνοντας με αυτόν το τρόπο αρκετές πληροφορίες να μεταπηδά με τον master κατά την διάρκεια μιας φυσιολογικής λειτουργίας του piconet.

P-slave response after INQUIRY SCAN : Εάν ένας p-slave ακούσει ένα inquiry όταν είναι σε κατάσταση INQUIRY SCAN, τότε άπαντα με το δικό του FHS πακετο. Η συσκευή που πραγματοποιεί το INQUIRY δεν αποδέχεται το πακέτο.

Χρόνοι Ανακάλυψης συσκευών

Προτού να μπορέσουν οποιεσδήποτε δύο συσκευές να περάσουν στην ανακάλυψη συσκευών, *πρέπει* να είναι *στην κατάσταση έρευνα[inquiry]* και κατάσταση *ανίχνευσης έρευνας[inquiry scan]* Η συσκευή έρευνας πρέπει να ανακαλύψει τις γειτονικές συσκευές, και η συσκευή ανίχνευσης έρευνας πρέπει να είναι πρόθυμη να ανακαλυφθεί όπως προαναφέρθηκε.



ΣΧΗΜΑ 2-7 Εικονική απεικόνιση εγκατάσταση σύνδεσης

Η συσκευή έρευνας διαβιβάζει μια σειρά πακέτων έρευνας Αυτά τα μικρά πακέτα στέλνονται γρήγορα σε μια ακολουθία διαφορετικών συχνοτήτων. Η συσκευή έρευνας αλλάζει συχνότητες 3200 φορές το δευτερόλεπτο (δύο φορές το ποσοστό για μια συσκευή σε μια κανονική σύνδεση). Αυτό το γρήγορο hopping συχνότητας επιτρέπει στον ερωτώντα να καλύψει μια απόσταση συχνοτήτων όσο ποιο γρήγορα γίνεται. Αυτά τα πακέτα δεν αναγνωρίζουν την συσκευή έρευνας από καμιά άποψη. Είναι πακέτα ταυτότητας που περιέχουν έναν κωδικό πρόσβασης έρευνας που οι συσκευές ανίχνευσης έρευνας[inquiry scan] θα αναγνωρίσουν.

Η συσκευή που βρίσκεται σε κατάσταση inquiry scan [ανίχνευσης έρευνας] αλλάζει τις συχνότητες πολύ αργά ακριβώς μία φορά κάθε 1,28 δευτερόλεπτα. Επειδή η συσκευή inquiry scan αλλάζει πολύ αργά ενώ ο ερωτών αλλάζει γρήγορα, θα συναντηθούν τελικά στην ίδια συχνότητα.

Οι συσκευές ανίχνευσης δεν μπορούν να μείνουν σε μια σταθερή συχνότητα, επειδή η συχνότητα που επιλέχτηκε μπορεί να υπόκειται σε παρεμβολή, αλλά μεταπηδούν πολύ αργά σε μια η επόμενη καλύτερη στρατηγική για τη συσκευή έρευνας[inquiry]. Αποκρίνεται στις έρευνες με την αποστολή ενός πακέτου συγχρονισμού μεταπηδήσεως

συχνότητας [Frequency Hop Synchronization (FHS)], το οποίο λέει στη συσκευή έρευνας όλες τις σχετικές πληροφορίες που απαιτούνται για να είναι σε θέση να εγκαταστήσει μια σύνδεση.

Για να εγγυηθούν ότι η συσκευή [inquiry]έρευνας μπορεί να εντοπίσει όλες τις συσκευές μέσα τρόπος ανίχνευσης έρευνας που είναι μέσα στη σειρά, η προδιαγραφή Bluetooth καθορίζει έναν χρόνο έρευνας 10.24 δευτερολέπτων.

Όταν μια συσκευή που ανιχνεύει τις έρευνες λαμβάνει ένα inquiry, περιμένει μια μικρή ψευδοτυχαία χρονική περίοδο, κατόπιν εάν ληφθει μια δεύτερη έρευνα, αυτό διαβιβάζει μια response. Δεν διαβιβάζει αυτήν την απάντηση αμέσως, επειδή αυτό μπορεί να οδηγήσει όλες τις συσκευές σε μια περιοχή να αποκριθούν στην πρώτη έρευνα που στέλνεται, προκαλώντας έναν ανεπιθύμητο υψηλής ισχύος συντονισμένο παλμό της ακτινοβολίας στη ism ζώνη. Η τυχαία καθυστέρηση αποτρέπει αυτήν την συντονισμένη επίδραση.

Operation	Minimum Time (sec)	Average Time (sec)	Maximum Time (sec)
Inquiry	0.00125	3 – 5	10.24 – 30.72
Paging	0.0025	1.28	2.56
Total	0.00375	4.28 – 6.28	12.8 – 33.28

ΣΧΗΜΑ 2-8 Όρια χρόνων των διάφορων διαδικασιών

Οι χρόνοι έρευνας Μια σειρά έρευνας πρέπει να επαναληφθεί τουλάχιστον 256 φορές (διάρκεια 2.56s), προτού να χρησιμοποιηθεί άλλη σειρά. Χαρακτηριστικά, σε ένα χωρίς λάθη περιβάλλον, τρεις σειρές πρέπει να πάρουν τη θέση Αυτό σημαίνει ότι 10.24s θα μπορούσε να παρέλθει εκτός αν ο ερωτών συλλέγει αρκετές απαντήσεις και αποφασίζει να αποβάλει τη διαδικασία. Εντούτοις, κατά τη διάρκεια ενός παραθύρου 1.28s, ένας σκλάβος αποκρίνεται κατά μέσον όρο τέσσερις φορές, αλλά στις διαφορετικές συχνότητες και στους διαφορετικούς χρόνους.

Ο ελάχιστος χρονικός ερευνάς Ο ελάχιστος χρόνος **έρευνας** για μια λειτουργία έρευνας είναι δύο χρονικές υποδοχές (1.25ms).Ο master διαβιβάζει ένα μήνυμα έρευνας στη συχνότητα φ (κ) στην πρώτη στιγμή, και ο slave ανιχνεύει την έρευνα στη συχνότητα

φ(κ) συγχρόνως. Έτσι, ο slave λαμβάνει το μήνυμα έρευνας στο πρώτο slot(υποδοχή). Ο slave θα μπορούσε να αποκριθεί με ένα πακέτο FHS στο μήνυμα έρευνας του κυρίου στο επόμενο slot. Έτσι, δύο οι αυλακώσεις απαιτούνται συνολικά Αυτό είναι ιδιαίτερα απίθανο δεδομένου ότι ο σκλάβος δεν θα ανταποκριθεί μετά την λήψη του πρώτου το μηνύματος έρευνας αλλά μάλλον, περιμένει έναν τυχαίο αριθμό αυλακώσεων Αυτή η τυχαία αξία ποικίλλει μεταξύ 0 και 1023.

Ο μέσος χρόνος έρευνας Όπως δηλώνεται προηγουμένως, 10.24sec θα μπορούσαν να παρέλθουν εκτός αν ο ερωτών λαμβάνει αρκετές απαντήσεις και αποφασίζει να αποβάλει τη διαδικασία. Αυτή η αξία μπορεί να ποικίλει αρκετά, ανάλογα με την ευθυγράμμιση των ρολογιών συσκευών και των αντίστοιχων καταστάσεων τους Αυτό, εντούτοις, δεν είναι επαρκές για να εγγυηθεί ότι όλες οι συσκευές μέσα στη σειρά "θα βρεθούν"! .

ΚΑΤΑΣΤΑΣΕΙΣ ΧΑΜΗΛΗΣ ΙΣΧΥΟΣ

Οι συσκευές Bluetooth που συνδέονται σε ένα piconet μπορούν να τεθούν σε μια από τις 3 διαφορετικές χαμηλής ισχύος καταστάσεις αποκαλούμενες *sniff, τη hold,* και park. Αν και αυτοί αναφέρονται συχνά ως *χαμηλής ισχύος τρόποι,* είναι χρήσιμοι σε διάφορα διαφορετικές εφαρμογές όπως :

- Διευκόλυνση περισσότερων από επτά slaves για να είναι σε ένα piconet
- Δόσιμο χρόνου στον master ώστε να φέρει και άλλους slaves στο piconet του
- Παροχή μέσων για μια συσκευή να συμμετέχει στα πολλαπλάσια piconets (scatternet)
- Συντήρηση της ενέργειας

Οι περισσότερες από τις μεθόδους ενεργειακής συντήρησης σε αυτούς τους χαμηλής ισχύος τρόπους προσανατολίζονται στη μείωση του χρόνου που ο δέκτης μιας συσκευής παραμένει ανοιχτός. Στις υψηλής ισχύος ασύρματες συσκευές, ο πομπός χρειάζεται πολύ περισσότερη ισχύ από το δέκτη. Τα συστήματα όπως το Bluetooth, με εξαιρετικά χαμηλή μετάδοση ισχύος, συχνά επαυξάνουν την τεραστία διοχέτευση τους κατά τη

διάρκεια της λειτουργίας δεκτών. Επιπλέον, αν και μόνο ένας πομπός είναι ανοικτός σε οποιοδήποτε χρόνο κατά τη διάρκεια των κανονικών διαδικασιών Piconet, ένα μεγάλο ποσό ενέργειας χρησιμοποιείται εάν ο δέκτης σε κάθε slave πρέπει να είναι ανοιχτός στην αρχή κάθε χρονικής υποδοχής μετάδοσης master-to-slave. Ο κύριος σκοπός των χαμηλής ισχύος συνδέσεων είναι να αφαιρεθεί εκείνη η απαίτηση.

Για μια point-to-multipoint τοπολογία, ο master πρέπει να φέρει τους slaves στο Piconet του έναν-έναν. Αυτό σημαίνει ότι ο master πρέπει να βγει από το CONNECT και να πάει είτε στην κατάσταση PAGE είτε του INQUIRY. Φυσικά, κατά τη διάρκεια των διαδικασιών page ή inquiry/page, τα υπόλοιπα μέλη του piconet(slaves) δεν θα επικοινωνούν καθόλου, δε θα μπορούν να μιλήσουν ο ένας στον άλλο, και ο master είναι προσωρινά μη διαθέσιμος. Οι slaves μπορούν επίσης να εισαγάγουν μια κατάσταση χαμηλής ισχύος κατά τη διάρκεια του χρόνου που ο master είναι ειδάλλως κατειλημμένος.

Αυτό επιτρέπει το lap-top μας να τοποθετήσει το PDA μας με το οποίο συνδεόμαστε σε hold καθώς εγκαθίσταται μια σύνδεση σε ένα σημείο πρόσβασης του τοπικού LAN, ελαχιστοποιώντας κατά συνέπεια την κατανάλωση ισχύος PDA όταν δεν είναι σε χρήση.

Sniff

Όταν περιλαμβάνεται σε κανονική λειτουργία piconet ο slave πρέπει να ανοίξει το δέκτη του στην έναρξη κάθε άρτιας αριθμημένης χρονικής υποδοχής, όπως καθορίζεται από CLK, για να ελέγχει για τη μετάδοση του master. Η εξαίρεση σε αυτόν τον κανόνα είναι όταν λαμβάνει ένα header πακέτων υποδεικνύοντας τη μετάδοση ενός πακέτου multislot για έναν άλλο slave κατόπιν ο slave μας μπορεί να σταματήσει το δέκτη του κατά τη διάρκεια του πακέτου. Ο *sniff* τρόπος δίνει σε έναν slave μια πιθανότητα να μειώσει τον κύκλο δραστηριότητας του δέκτη του, ενεργοποιώντας τον μόνο σε τακτικά χωρισμένα κατά διαστήματα sniff αποκαλούμενα Tsniff. Κάτω από την κανονική λειτουργία Tsniff piconet = 2 χρονικές υποδοχές(slots), αλλά επειδή η τιμή αποθηκεύεται ως μη προσημασμένος δεκαεξάμπιτος ακέραιος αριθμός, μπορεί να είναι τόσο υψηλό όπως 2_{16} = 65.536 υποδοχές ή περίπου 41 δευτερόλεπτα μεταξύ sniffs. Ο slave κρατά την AM_ADDR του ενώ είναι σε sniff .

Μια δυσκολία με αυτά τα κανονικά sniff χρονικά διαστήματα είναι ότι ο master θα μπορούσε να έχει ένα πακέτο SCO ή ένα πακέτο ACL πιο υψηλής προτεραιότητας για έναν άλλο slave που σχεδιάστηκε για την υποδοχή που ο slave μας σχεδιάζεται να είναι σε sniff. Επομένως, μια άλλη φορά, αποκαλούμενη Nsniff_attempt, είναι ο αριθμός από συνεχόμενες υποδοχές λήψης (στις άρτια αριθμημένες) που ο slave πρέπει για να ελέγξει σε κάθε sniff διάστημα. Εάν ένα πακέτο φθάσει κατά τη διάρκεια αυτής της περιόδου που έχει το AM_ADDR του slave στο header της, κατόπιν ο slave μας θα συνεχίσει να παρακολουθεί για ένα πρόσθετο Nsniff_timeout λήψης υποδοχών ή για τις εναπομείναντες Nsniff_attempt υποδοχές λήψης, οποιοσδήποτε είναι μεγαλύτερος. Όταν ένα πακέτο που απευθύνεται σε έναν ιδιαίτερο slave φθάνει, υπάρχει μεγαλύτερη πιθανότητα ότι το πακέτο για εκείνο τον ίδιο slave θα φθάσει επίσης μέσα σε έναν εύλογα σύντομο χρόνο: επομένως, το N_sniftimeout πρέπει να επιλεχτεί αναλόγως έτσι ώστε ο slave δεν πηγαίνει ¨sleep" προτού να φθάσουν όλα τα πακέτα. Και οι δύο ποσότητες είναι επίσης δεκαεξάμπιτοι ανυπόγραφοι ακέραιοι αριθμοί.

Τέλος, η ποσότητα Dsniff είναι ο αριθμός χρονικών αυλακώσεων έως ότου να συμβεί το πρώτο sniff. Ο sniff τρόπος έχει επιπτώσεις μόνο στα πακέτα ACL, έτσι ο slave πρέπει ακόμα να είναι διαθέσιμος για οποιεσδήποτε συνδέσεις SCO που μπορούν να υπάρξουν με τον master.

Hold

Αντίθετα από το sniff, που είναι περιοδικής φύσης, ο τρόπος Hold είναι μια one-time έξοδος από τις υποχρεώσεις του piconet. Ο slave κρατά την AM_ADDR του αλλά αναστέλλει τα πακέτα ACL για την τιμή *timeout hold* (holdTO), η οποία είναι ένας αριθμός υποδοχών σε hold που εκφράζεται ως δεκαεξάμπιτος unsigned ακέραιος αριθμός, επομένως, μπορεί να διαρκέσει μέχρι περίπου 41 δευτερόλεπτα. Η *hold instant διευκρινίζει* την τιμή CLK όταν αρχίζει η κατάσταση hold. Κατά τη διάρκεια του hold μια συσκευή μπορεί να εκτελέσει διάφορα καθήκοντα Page ή έρευνας, που παρευρίσκονται σε ένα άλλο piconet, ή δεν κάνουν απλά τίποτα και σώζουν ισχύ.

Εάν ένας κύριος πρέπει να βγει από το piconet προσωρινά, κατόπιν μπορεί να

Μια δυσκολία με αυτά τα κανονικά sniff χρονικά διαστήματα είναι ότι ο master θα μπορούσε να έχει ένα πακέτο SCO ή ένα πακέτο ACL πιο υψηλής προτεραιότητας για έναν άλλο slave που σχεδιάστηκε για την υποδοχή που ο slave μας σχεδιάζεται να είναι σε sniff. Επομένως, μια άλλη φορά, αποκαλούμενη Nsniff_attempt, είναι ο αριθμός από συνεχόμενες υποδοχές λήψης (στις άρτια αριθμημένες) που ο slave πρέπει για να ελέγξει σε κάθε sniff διάστημα. Εάν ένα πακέτο φθάσει κατά τη διάρκεια αυτής της περιόδου που έχει το AM_ADDR του slave στο header της, κατόπιν ο slave μας θα συνεχίσει να παρακολουθεί για ένα πρόσθετο Nsniff_timeout λήψης υποδοχών ή για τις εναπομείναντες Nsniff_attempt υποδοχές λήψης, οποιοσδήποτε είναι μεγαλύτερος. Όταν ένα πακέτο που απευθύνεται σε έναν ιδιαίτερο slave φθάνει, υπάρχει μεγαλύτερη πιθανότητα ότι το πακέτο για εκείνο τον ίδιο slave θα φθάσει επίσης μέσα σε έναν εύλογα σύντομο χρόνο: επομένως, το N_sniftimeout πρέπει να επιλεχτεί αναλόγως έτσι ώστε ο slave δεν πηγαίνει ˜sleep" προτού να φθάσουν όλα τα πακέτα. Και οι δύο ποσότητες είναι επίσης δεκαεξάμπιτοι ανυπόγραφοι ακέραιοι αριθμοί.

Τέλος, η ποσότητα Dsniff είναι ο αριθμός χρονικών αυλακώσεων έως ότου να συμβεί το πρώτο sniff. Ο sniff τρόπος έχει επιπτώσεις μόνο στα πακέτα ACL, έτσι ο slave πρέπει ακόμα να είναι διαθέσιμος για οποιεσδήποτε συνδέσεις SCO που μπορούν να υπάρξουν με τον master.

Hold

Αντίθετα από το sniff, που είναι περιοδικής φύσης, ο τρόπος Hold είναι μια one-time έξοδος από τις υποχρεώσεις του piconet. Ο slave κρατά την AM_ADDR του αλλά αναστέλλει τα πακέτα ACL για την τιμή *timeout hold* (holdTO), η οποία είναι ένας αριθμός υποδοχών σε hold που εκφράζεται ως δεκαεξάμπιτος unsigned ακέραιος αριθμός, επομένως, μπορεί να διαρκέσει μέχρι περίπου 41 δευτερόλεπτα. Η *hold instant διευκρινίζει* την τιμή CLK όταν αρχίζει η κατάσταση hold. Κατά τη διάρκεια του hold μια συσκευή μπορεί να εκτελέσει διάφορα καθήκοντα Page ή έρευνας, που παρευρίσκονται σε ένα άλλο piconet, ή δεν κάνουν απλά τίποτα και σώζουν ισχύ.

Εάν ένας κύριος πρέπει να βγει από το piconet προσωρινά, κατόπιν μπορεί να

τοποθετήσει τους όλους slave του στη κατάσταση hold. Αυτό έχει την επίδραση να επιτρέπει τον ίδιο τον Master να μπει σε hold από το χρόνο που ο τελευταίος slave εισάγεται σε hold έως ότου ο πρώτος slave βγει από αυτήν την κατάσταση. Όπως στις sniff παραμέτρους, οι παράμετροι hold ανταλλάσσονται ως πακέτα LMP.

Κατά τη διάρκεια της κανονικής λειτουργίας piconet, ο slave έχει ένα παράθυρο αβεβαιότητας ±10μs πέρα από το οποίο ψάχνει για τον κωδικό πρόσβασης καναλιών από τη μετάδοση ενός master. Ακόμα κι αν εκείνο το ιδιαίτερο πακέτο απευθύνεται σε έναν άλλο slave, όλοι οι slave μπορούν να ξανασυγχρονίζουν τις αντίστοιχες τιμές των CLK τους κάθε φορά που διαβιβάζει ο master ένα (channel access code) κωδικό πρόσβασης καναλιού. Όταν ένας slave επιστρέφει από hold, το παράθυρο αβεβαιότητας θα μπορούσε να είναι πολύ μεγαλύτερο από ±10μs λόγω της κλίσης ρολογιών μεταξύ του master και του slave, έτσι ο slave πρέπει να αυξήσει το χρονικό διάστημα που ο δέκτης του είναι ανοιχτός όταν ψάχνει για την πρώτη μετάδοση master-slave. Ο χρόνος που απαιτείται για το resynchronization μπορεί να μικρύνει εάν ο master χρησιμοποιεί πακέτα μιας υποδοχής χρήσεων για μερικές χρονικές υποδοχές μετά από κάθε επιστροφή slave από το hold. Αυτό θα ασφαλίσει ότι ένα πακέτο διαβιβάζεται πραγματικά στη συχνότητα hop την οποία ο δέκτης ενός επιστροφής slave ακούει.

Park

Ο τρόπος park είναι κατά πολύ ο ισχυρότερος των χαμηλής ισχύος καταστάσεων και δεδομένου αυτού και ο πιο σύνθετος. Σε αντάλλαγμα αυτής της πολυπλοκότητας, ο τρόπος πάρκων παρουσιάζει διάφορα πλεονεκτήματα. Μεταξύ αυτών είναι :

- Η μικρή κατανάλωση ισχύος είναι αποτέλεσμα για τις σταθμευμένες συσκευές.
- Ο master μπορεί να φέρει περισσότερους από επτά slaves στο piconet.
- Ένας slave μπορεί να μπει unparked γρηγορότερα από ότι μπορεί να σελιδοποιηθεί.
- Ένας slave μπορεί να αρχίσει μόνος του την unpark η διαδικασία.

Όταν ένας slave εισάγεται σε park, σταματά AM_ADDR του και λαμβάνει μια οκτάμπιτη *parked member address[σταθμευμένη διεύθυνση μελών* (PM_ADDR)] και μια οκτάμπιτη *διεύθυνση access request address* (AR_ADDR). Το PM_ADDR παίρνει τη θέση του AM_ADDR όταν ο master θέλει να εκδώσει μια εντολή unpark ή άλλη επικοινωνία στο slave, και η AR_ADDR καθορίζει ένα χρονικό παράθυρο κατά τη διάρκεια του οποίου ένας σταθμευμένος slave μπορεί να ζητήσει unparked.

Η PM_ADDR και η AR_ADDR ορίζονται στον slave κατά τη διάρκεια μιας park εντολής LMP που εκδίδεται από τον master. Εάν η PM_ADDR είναι OxOO δίνεται σε έναν slave, κατόπιν θα ανταποκριθεί μόνο στην BD_ADDR του κατά την unparked διαδικασία από τον master, διαφορετικά ο slave θα ανταποκριθεί είτε στη PM_ADDR του είτε στην BD_ADDR του. Κατά συνέπεια δεν υπάρχει κανένα όριο στον αριθμό των slaves που μπορούν να σταθμεύσουν, αν και συχνά σκέφτομαι για το πόσο θα ήταν εφικτό να τοποθετήσουμε 255 συσκευές Bluetooth μέσα σε μια ακτίνα 10 μέτρων. Η επικοινωνία μεταξύ των master και σταθμευμένων slaves ολοκληρώνεται μέσω των πακέτων ραδιοφωνικής μετάδοσης(broadcast) επειδή εκεί δεν υπάρχει AM_ADDR που ορίζεται σε οποιονδήποτε από τους σταθμευμένους slaves. Ένας slave που συμμετέχει σε μια σύνδεση SCO δεν μπορεί να γίνει park.

ΚΕΦΑΛΑΙΟ 3
ΠΑΚΕΤΑ ΜΕΤΑΔΟΣΗΣ

ΕΙΣΑΓΩΓΗ

Το Bluetooth στέλνει τα δεδομένα με ένα σχήμα πακέτων, όπου ένα ψηφιακό μήνυμα είναι σπασμένο σε διάφορα μικρότερα πακέτα και σταλμένο ένα-ένα στον προορισμό. Αντίθετα από το *πρωτόκολλο* (IP) *Διαδικτύου*, όπου τα πακέτα καθοδηγούνται από κόμβο σε κόμβο μεταξύ της πηγής και του προορισμού, τα πακέτα βασικής ζώνης(baseband) Bluetooth στέλνονται άμεσα από την πηγή τους (master or slave) στον προορισμό τους (master or slave). Κάθε πακέτο διαβιβάζεται σε μια νέα hop συχνότητα . Τα πακέτα βασικής ζώνης(baseband) κατασκευάζονται για να εκμεταλλευθούν την διαδικασία *time division duplexing* (TDD) που προβλέπει μια τακτική ανταλλαγή των δεδομένων μεταξύ του master και του slave. Ο master και ένας από τους slaves στο piconet διαβιβάζουν διαδοχικά, έτσι δύο ή περισσότεροι πομποί σημάτων δεν είναι ποτέ συγχρόνως μέσα σε ένα piconet.

Όπου η ακεραιότητα των δεδομένων είναι αρχικής σπουδαιότητας, *η εναλλακτική μετάδοση πακέτου πληροφοριών(packet switching)* χρησιμοποιείται. Αυτό σημαίνει ότι κάθε εισερχόμενο πακέτο ελέγχεται για data bit errors από τον κόμβο προορισμού, και εάν υπάρχουν λάθη, ο προορισμός ζητά από την πηγή να επαναλάβει το πακέτο. Η ρυθμοαπόδοση επηρεάζεται έτσι πολύ από το *ποσοστό λάθους κομματιών* του καναλιού [*bit error rate(*BER)]. Αφ' ετέρου, εάν η χαμηλή λανθάνουσα κατάσταση (μικρή καθυστέρηση) απαιτείται, *η circuit switching (μετατροπή κυκλωμάτων)* υιοθετείται από το piconet. Η σε πραγματικό χρόνο διπλής κατεύθυνσης μετάδοση φωνής εμπίπτει σε αυτήν την κατηγορία. Στα ψηφιοποιημένα πακέτα φωνής ορίζονται συγκεκριμένες χρονικές αυλακώσεις ή υποδοχές (time slots)[Καθόλη την διάρκεια του project θα χρησιμοποιηθούν και οι δυο έννοιες] μετάδοσης, και οι επαναλαμβανόμενες μεταδόσεις δεν επιτρέπονται. Η ρυθμοαπόδοση είναι επομένως απρόσβλητη από την ακεραιότητα καναλιών άντ' αυτού, τα πακέτα φωνής που στέλνονται πέρα από ένα κανάλι με ένα υψηλό BER θα παραγάγουν distortion (διαστρέβλωση) όταν μετατρέπονται σε αναλογικό ήχο.

Το *πρωτόκολλο baseband* αποτελείται από τις βασικές λειτουργίες piconet όπως:

- Συγκέντρωση των πακέτων από τα υψηλότερα στρώματα πρωτοκόλλου και αποστολή τους στο ραδιόφωνο
- Λήψη των bits από το ραδιόBluetooth και συναρμολόγηση των πακέτων για να επεξεργαστούν από τα ψηλότερα στρώματα πρωτοκόλλου
- Γενικός συγχρονισμός piconet
- Επιλογή Frequency hop
- Επεξεργασία ελέγχου καναλιών
- Έλεγχος λάθους
- Whitening δεδομένων
- Βασικές διαδικασίες ασφάλειας

Αυτές οι λειτουργίες εκτελούνται από τον *ελεγκτή συνδέσεων(link controller)*, ο οποίος κάθεται επάνω από το ραδιόφωνο(radio) στη λίστα πρωτοκόλλου Bluetooth. Το piconet ελέγχεται από την εφαρμογή μέσω του *διευθυντή συνδέσεων(link manager)*. Τα δεδομένα περνούν στον ελεγκτή συνδέσεων μέσω του *λογικού πρωτοκόλλου ελέγχου και προσαρμογής συνδέσεων* (L2CAP) και πραγματικού χρόνου διπλής κατεύθυνσης φωνής συνήθως στέλνεται κατευθείαν στον Link controller από την εφαρμογή για να μειώσουμε το latency.

Ένα πακέτο δεδομένων περιέχει τον access code,το header και payload. Ο access code (72-bit) χρησιμοποιείται για να αρχικοποιήσει τον συγχρονισμό στο λεπτομερές σχέδιο κυκλώματος του δέκτη, αλλά επίσης περιέχει διάφορες πληροφορίες όπως την ταυτότητα του Piconet ή την διεύθυνση του δεκτή εξαρτώμενες πάντα από το περιβάλλον της εφαρμογής. Το header κομμάτι (54-bits) περιέχει την διεύθυνση προορισμού, τον τύπο του φορτίου που ακολουθεί, και μερικές πληροφορίες ελέγχου λάθους. Τέλος το payload είναι πεδίο μεταβλητού μήκους που περιέχει το μήνυμα Είναι σημαντικό να

λάβουμε υπόψη ότι μόνο αυτό το μέρος κάθε πακέτου (baseband) ζωνών βάσης περιέχει το πραγματικό μήνυμα που οι εφαρμογές προσπαθούν να ανταλλάξουν. Τα άλλα μέρη του πακέτου (όπως ο the access code and header), αν και απαραίτητα για την κατάλληλη λειτουργία του piconet, είναι μεγάλα, και δεν συμβάλλουν στη ρυθμοαπόδοση δεδομένων του piconet. Για αυτό το λόγο η πραγματική ρυθμοαπόδοση θα είναι πάντα κάτω από 1Mb/s data rate του Bluetooth radio.

Time Division Duplexing (TDD)

Ένα από τα σημαντικότερα κριτήρια σε ένα διπλής κατεύθυνσης σύστημα επικοινωνιών είναι ο καθορισμός του πώς και πότε οι ραδιομονάδες σε κάθε κόμβο μπορούν να ανταλλάξουν τις πληροφορίες. Μια δυνατότητα είναι να εξοπλιστούν οι κόμβοι με έναν πομπό και με έναν δέκτη και να ενεργοποιηθούν ταυτόχρονα σε διαφορετικές συχνότητες. Αυτή η διαδικασία, αποκαλούμενη F*requency division duplexing* (FDD) είναι μια μορφή πλήρους-διπλής μετάδοσης και χρησιμοποιείται στο παραδοσιακό τηλεφωνικό σύστημα κυττάρων. Το πλήρες duplex επιτρέπει στους χρήστες σε κάθε τέλος της συνομιλίας να διακόψει ο ένας τον άλλον, το οποίο θεωρείται από μερικούς ένα πλεονέκτημα. Το FDD μπορεί να είναι κάπως ακριβό επειδή ο πομπός και ο δέκτης πρέπει να λειτουργήσουν ανεξάρτητα, απαιτώντας 2 frequency synthesizers, και μια συσκευή που καλείται *duplexer που* πρέπει να χρησιμοποιηθεί για να συνδυάσει ένα εξερχόμενο διαβιβασθέν σήμα και ένα εισερχόμενο σήμα λήψης με μια ενιαία κεραία.

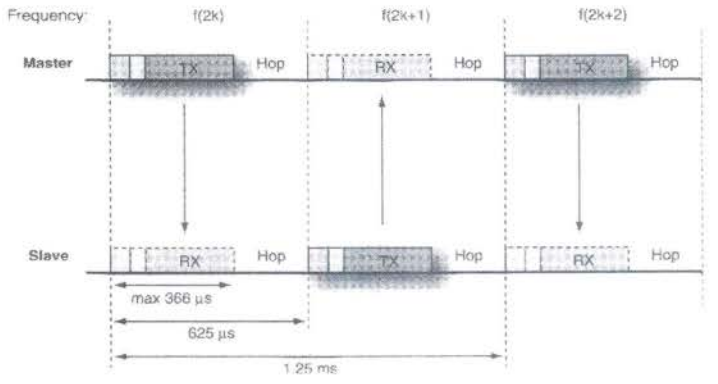
Ένα φτηνότερο και φυσικά μικρότερο σύστημα μπορεί να χτιστεί με τη χρησιμοποίηση μιας διαδικασίας αποκαλούμενης *half duplex,κατά το ήμισυ διπλής*, το οποίο σημαίνει ότι ένας κόμβος διαβιβάζει ενώ ο άλλος κόμβος λαμβάνει και αντίστροφα. Κατά το ήμισυ διπλός είναι φτηνότερος επειδή μόνο ένας frequency synthesizer απαιτείται ανά ραδιομονάδα και είναι μικρότερος επειδή ένας διακόπτης κεραιών αντικαθιστά το ογκώδες duplexer. Το TDD προσδιορίζει ξεχωριστά τις χρονικές υποδοχές (slots) σε κάθε πομπό σε ένα διπλής κατεύθυνσης σύστημα επικοινωνιών έτσι ώστε οι χρήστες να στέλνουν διαδοχικά τα δεδομένα ο ένας στον άλλο. Αυτή είναι η μέθοδος που χρησιμοποιείται για την επικοινωνία μέσα στο Bluetooth piconet. Τα πλεονεκτήματα του TDD περιλαμβάνουν τα εξής:

- Απαιτείται μόνο ένας frequency synthesizer .
- Μια φθηνότερη κεραία αντικαθιστά τον duplexer
- Η γρήγορη μετατροπή TDD μπορεί να μεταμφιέσει ως FDD.

Λειτουργία Single-Slave

Θα αρχίσουμε με την εξέταση του απλούστερου πιθανού Bluetooth piconet, αποτελούμενος από έναν master που επικοινωνεί με έναν slave σε μια από σημείο σε σημείο διαμόρφωση. Ο χρόνος διαιρείται σε αυλακώσεις(slots) που είναι ονομαστικά 625 μs στο μήκος και αριθμημένος με διαδοχικούς ακέραιους αριθμούς. Ο master διαβιβάζει στον slave στις άρτια αριθμημένες χρονικές αυλακώσεις, και ο slave διαβιβάζει στον κύριο στις περιττές αριθμημένες χρονικές αυλακώσεις. Κάθε μετάδοση πραγματοποιείται σε μια νέα hopping συχνότητα, και ένα πλήρες πακέτο δεδομένων αποστέλλεται κάθε φορά που αλλάζει η αυλάκωση(slot). Αυτή η διαδικασία απεικονίζεται στο σχήμα 3-1.

Με τη χρησιμοποίηση αυτής της ιδιαίτερης απόδοσης TDD, και ο master και ο slave έχουν ίση πρόσβαση στο κανάλι, και κάθε ένα είναι έτοιμο να λάβει όταν διαβιβάζει άλλο. Η επικοινωνία προχωρά έτσι κατά τρόπο τακτικό.



ΣΧΗΜΑ 3.1 Επικοινωνία Bluetooth TDD. Ο master μεταδίδει (TX) σε άρτια αριθμημένη υποδοχή

Η αλλαγή μεταξύ της μετάδοσης και λήψης σε κάθε κόμβο Bluetooth είναι τόσο γρήγορη που εμφανίζεται στον ανθρώπινο χρήστη του σαν πλήρες full duplex..

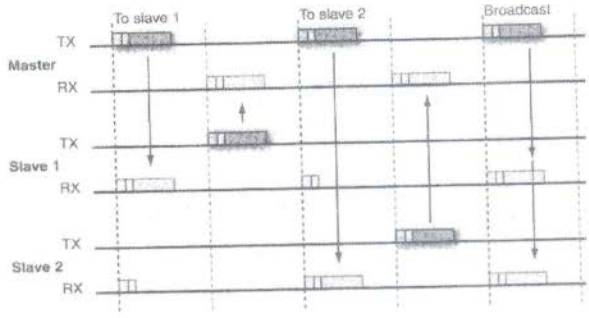
Σε κάθε πακέτο επιτρέπονται μέχρι 366μs για τη μετάδοσή του, εξισώνοντας σε ένα μέγιστο μήκος πακέτων μιας-αυλάκωσης 366 μπιτ. Τα πρόσθετα 259μs χρησιμοποιούνται από το radio στην αλλαγή στην επόμενη συχνότητα στην hop ακολουθία . Κατά τη διάρκεια του χρόνου που απαιτείται για να εκτελέσει ένα hop (μεταπήδηση), καμία επικοινωνία δεν εμφανίζεται στο piconet. Το αποτέλεσμα αυτό, φυσικά, μειώνει τη ρυθμοαπόδοση. Επειδή τα στοιχεία κυκλώματος συγχρονισμού σε κάθε συσκευή Bluetooth είναι ανέξοδα, η παθητική αναμονή και "νευρικότητα" μπορεί να εμφανιστεί μεταξύ των ρολογιών του master και slave ακόμη και εντός των σχετικά μικρών χρονικών περιόδων. Για να προσαρμοστεί αυτό, ένας λαμβάνων κόμβος πρέπει να επιτρέψει ένα παράθυρο των 10μs από κάθε πλευρά του αναμενόμενου χρόνου άφιξης πακέτων για την πραγματική άφιξη να εμφανιστεί.

Λειτουργία Multislave

Όταν το piconet αποτελείται από έναν master και δύο ή περισσότερους slaves, point-to-multipoint σύνδεση, η συνολική ρυθμοαπόδοση πολλαπλασιάζεται μεταξύ των μελών piconet. Άλλη μια φορά, το TDD υιοθετείται (αν και σε μια ελαφρώς πιο σύνθετη μορφή) για να αποτρέψει τα μέλη του piconet από το μπλοκάρισμα του ενός το άλλο από τις ταυτόχρονες μεταδόσεις.

Αυτό παρουσιάζεται στο σχήμα 3-2, όπου ο master διαβιβάζει δεδομένα στις άρτια αριθμημένες χρονικές αυλακώσεις όπως πριν, αλλά ένας slave μπορεί να διαβιβάσει μόνο όταν συγκεκριμένα το header από το πακέτο αποστολής του master έχει την διεύθυνση του στην προηγούμενη χρονική αυλάκωση. Εάν, παραδείγματος χάριν, ο master στείλει ένα πακέτο στο slave 1, ο slave 2 θα κρατήσει το δέκτη ανοιχτό αρκετά ώστε να αποκωδικοποιήσει τον access code κωδικό πρόσβασης πακέτων (που προσδιορίζουν το piconet) και την header επιγραφή (που προσδιορίζει τον προορισμό). Επειδή το πακέτο προορίζεται για το slave 1, ο slave 2 κλείνει το δέκτη του μετά από την αποκωδικοποιήσει του header και περιμένει την αρχή της επόμενης άρτια αριθμημένης χρονικής υποδοχής(slot). Στις περιορισμένου φάσματος ασύρματες συσκευές, ο δέκτης είναι συχνά η πιο πεινασμένη ενεργειακά συσκευή, ακόμα περισσότερο από τον πομπό. Η μέθοδος multislave TDD σχεδιάστηκε για την αποδοτικότητα ισχύος έτσι ώστε να απαιτείται από τους δέκτες των slaves να είναι ενεργοί μόνο όταν χρειάζεται. Τα broadcast πακέτα λαμβάνονται από όλους τους slaves, αλλά κανένας δεν μπορεί να απαντήσει στο επόμενο time slot .

Είναι επίσης προφανές από το σχήμα ότι οι slaves επικοινωνούν μόνο με τον master στο piconet. Εάν δύο slaves θέλουν να ανταλλάξουν τα στοιχεία, μπορούν είτε να περάσουν από τον master είτε να διαμορφώσουν το ανεξάρτητο piconet τους.



ΣΧΗΜΑ 3-2

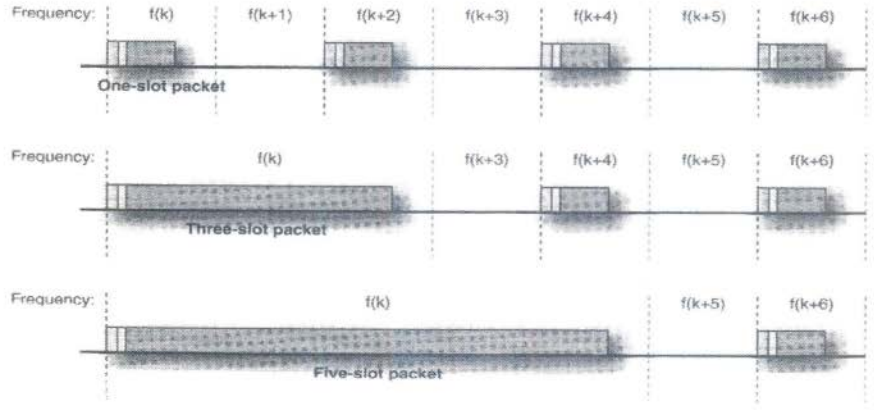
Πακέτα Multislot

Ένα από τα προφανή προβλήματα με ένα πακέτο που περιορίζεται σε 366 μπιτ είναι το σχετικά υψηλό ποσοστό του συνολικού μήκους του που πρέπει να χρησιμοποιηθεί για τον access code and header. Και τα δυο απαιτούν μαζί 126 μπιτ, ή 34 τοις εκατό του συνολικού μήκους πακέτων. Αφηνόμαστε με το ανήσυχο γεγονός ότι μόνο 240 μπιτ ωφέλιμων φορτίων(payload) μπορούν να προσαρμοστούν μέσα σε μια χρονική *625 μs* αυλάκωση, που αντιστοιχεί σε ένα πραγματικό αμφίδρομο ποσοστό στοιχείων μόνο 384 kb/s, ισοδύναμο με 192 kb/s ανά κόμβο σε μια από σημείο σε σημείο διαμόρφωση. Αυτό το ποσοστό δεδομένων μειώνεται περαιτέρω όταν χρησιμοποιείται ο (error control) έλεγχος λάθους, και το ακόμα χαμηλότερο ποσοστό πρέπει να διαιρεθεί μεταξύ όλων των μελών του piconet.

Για τη σημαντική αύξηση ρυθμοαπόδοσης, οι συσκευές Bluetooth μπορούν να διαβιβάσουν multislot πακέτα είτε τρεις είτε πέντε φορές τη διάρκεια των αυλακώσεων. Το σχήμα 3-3 παρουσιάζει τα παραδείγματα της μιας, τριών, και τα πακέτα πέντε χρονικών αυλακώσεων και τον συγχρονισμό τους. Κάθε πακέτο baseband, ανεξάρτητα από το μήκος του, διαβιβάζεται σε μια μία hop frequency. Αυτά τα κανάλια (συχνότητες) περιγράφονται ως *f(k + N)*, όπου *K + ν* αντιπροσωπεύει έναν συγκεκριμένο δείκτη χρονικών αυλακώσεων, ο οποίος είναι για master-to-slave μετάδοση και περιέργως για

την slave-to-master μετάδοση. Όταν η μετάδοση ενός πακέτου multislot ολοκληρώνεται, η hop ακολουθία συνεχίζει στο κανάλι που θα είχε χρησιμοποιήσει εάν δεν είχε εμφανιστεί καμία multislot μετάδοση, έτσι αυτά τα μακρύτερα πακέτα έχουν την ελάχιστη διάσπαση στη λειτουργία piconet. Είτε ο Master είτε slave μπορεί να διαβιβάσει multislot τα πακέτα εάν ο άλλος μπορεί να υποστηρίξει την λήψη τους. Τώρα ο συνολικός αριθμός bit σε ένα ενιαίο πακέτο ζωνών βάσης μπορεί να είναι πολύ είναι υψηλότερος. Εάν ένα πακέτο πέντε-(slot) αυλακώσεων στέλνεται, τέσσερα από τα time slot μπορούν να είναι εντελώς γεμάτα με τα bits, και περίπου 366 *μs* της τελευταίας αυλάκωσης μπορούν να καταληφθούν, κάνοντας ένα συνολικό μήκος 4x625 + 366 = 2.866 μπιτ. (Αυτός ο αριθμός μπορεί να επεκταθεί σε 2.871 μπιτ για να προσαρμόσει το μακρύτερο επιτρεπόμενο πακέτο.) Ο access code και το header απαιτούν ακόμα 126 μπιτ, αλλά αυτά τα γενικά έξοδα απαιτούν τώρα μόνο περίπου 4 τοις εκατό του συνολικού μήκους του πακέτων. Η ρυθμοαπόδοση βελτιώνεται αρκετά.

Τότε γιατί το Bluetooth δε χρησιμοποιεί πάντα πακέτα πέντε-αυλακώσεων; Ο λόγος είναι ότι το τίμημα είναι μεγάλο, όταν ένα μακρύ πακέτο παραλαμβάνεται με λάθη. Σε αυτό το γεγονός το ολόκληρο πακέτο πρέπει να ανακτηθεί, το οποίο απαιτεί άλλες πέντε αυλακώσεις (και μια έκτη αυλάκωση για τον παραλήπτη για να αναγνωρίσει την υποδοχή). Επιπλέον, τα μακριά πακέτα είναι πιθανότερο να αλλοιωθούν από τα κοντά πακέτα. Επομένως, εάν το κανάλι επικοινωνίας είναι επιρρεπές στα λάθη, η ρυθμοαπόδοση μπορεί να είναι υψηλότερη όταν ένα ή 3 πακέτα αυλακώσεων χρησιμοποιούνται άντ' αυτού.



ΣΧΗΜΑ 3-3 Μιας και πολλών χρονικών υποδοχών. Όλα τα πακέτα στέλνονται σε μια μεταπήδηση συχνότητας

ΦΥΣΙΚΕΣ ΣΥΝΔΕΣΕΙΣ

Δύο διαφορετικές φυσικές συνδέσεις μπορούν να καθιερωθούν μεταξύ των συσκευών Bluetooth: *asynchronous connectionless* (ACL) και s*ynchronous connection-oriented σύγχρονες προσανατολισμένες προς τη σύνδεση* συνδέσεις (SCO). Η σύνδεση ACL χρησιμοποιείται για τη μετάδοση δεδομένων, και η σύνδεση SCO χρησιμοποιείται για τη σε πραγματικό χρόνο διπλής κατεύθυνσης φωνή. Σε καθεμία περίπτωση, οι κανόνες μετάδοσης θεσπίζονται έτσι ώστε piconet τα μέλη σχεδόν δεν φράσσουν ποτέ το ένα το άλλο με το να διαβιβάσουν συγχρόνως.

Σύγχρονη σύνδεση (SCO)

Εάν η χαμηλή λανθάνουσα κατάσταση είναι σημαντικότερη από την ακεραιότητα στοιχείων, μια σύνδεση SCO καθιερώνεται μεταξύ του master και του slave. Η λανθάνουσα κατάσταση είναι ο χρόνος μεταξύ της δημιουργίας ενός νέου πακέτου στο διαβιβάζοντας κόμβο και της επιτυχούς υποδοχής της στον κόμβο προορισμού. Η

σύνδεση sco είναι μια circuit switched, από σημείο σε σημείο σύνδεση μεταξύ ενός master και ενός slave. Η λανθάνουσα κατάσταση είναι εγγυημένη για να είναι μια μικρή, σταθερή αξία μέσω δύο μεθόδων:

- τα πακέτα σχεδιάζονται για τη μετάδοση σε συγκεκριμένου χρόνου υποδοχές
- τα πακέτα δεν αναμεταδίδονται ποτέ.

Ένα circuit-switched περιβάλλον απαιτείται για τις σε πραγματικό χρόνο διπλής κατεύθυνσης μεταδόσεις φωνής όπου οι λανθάνουσες καταστάσεις παραπάνω από μερικές δεκάδες των χιλιοστών του δευτερολέπτου μπορούν σημαντικά να εμποδίσουν τη δυνατότητα να επικοινωνήσουν. Ευτυχώς, η αναπαραγωγή φωνής από μια ψηφιοποιημενη ροή bit μπορεί να ανεχτεί ένα αρκετά υψηλό ποσοστό των λαθών bits, έτσι υπό τους περισσότερους όρους η έλλειψη αναμεταδόσεων πακέτων δεν πρέπει να είναι μια σημαντική ζημία στην απόδοση.

Τα πακέτα sco ανταλλάσσονται ανά ζευγάρια, πρώτα από τον master στο slave και έπειτα από το slave στον master, στα διαδοχικά χρονικά slots(αυλακώσεις). Ο slave μπορεί να διαβιβάσει ένα ψηφιοποιημενο πακέτο φωνής στη διατηρημένη αυλάκωσή του ακόμα κι αν ο master δεν διαβιβάζει στην προηγούμενη αυλάκωση, αλλά δεν μπορεί εάν ο master διαβιβάζει ένα πακέτο σε έναν διαφορετικό slave σε εκείνη την αυλάκωση.

Ασύγχρονη χωρίς σύνδεση σύνδεση (ACL)

Η σύνδεση ACL χρησιμοποιείται όπου η ακεραιότητα δεδομένων είναι σημαντικότερη από τη λανθάνουσα κατάσταση. Η εναλλακτική μετάδοση πακέτου πληροφοριών [Packet switching] χρησιμοποιείται στη σύνδεση ACL, όπου όταν πακέτο που παραλαμβάνεται με τα αδιόρθωτα bit errors αναμεταδίδεται συνήθως έως ότου να μην υπάρχει λάθος. Ο μέσος αριθμός αναμεταδόσεων αυξάνεται με τα αυξανόμενα BER καναλιών, έτσι η λανθάνουσα κατάσταση είναι μεταβλητή και μπορεί περιστασιακά να είναι αρκετά μακροχρόνια.

Ένας slave μπορεί να διαβιβάσει ένα πακέτο ACL στον master του μόνο εάν το header από το πακέτο του master είχε την διεύθυνση του στην προηγούμενη χρονική master-to-slave time slot. Εάν ένας slave αποτυγχάνει να αποκωδικοποιήσει ένα πακέτο σε ένα master-to-slave time slot, δεν μπορεί να διαβιβάσει στην επόμενη αυλάκωση. Ένας master μπορεί επίσης να στείλει τα πακέτα broadcast που είναι μηνύματα προοριζόμενα για περισσότερους από έναν slave. Οι ενεργοί slave δεν μπορούν να διαβιβάσουν στο slave-to-master slot μετά από ένα πακέτο broadcast .

Η σύνδεση ACL χρησιμοποιείται επίσης για τη διαβίβαση του ισόχρονου δεδομένων, τα οποία είναι δεδομένα που έχει τα ζητήματα συγχρονισμού που είναι λιγότερο κρίσιμα από τη σε πραγματικό χρόνο διπλής κατεύθυνσης φωνή. Ένα παράδειγμα είναι η μεταφορά ήχου ροής, όπως ένα MP3 αρχείο. Σε αυτήν την κατάσταση γεμίζουν έναν buffer με δεδομένα MP3 προτού να αρχίσει να παίζει, το οποίο επιτρέπει σε μερικές αναμεταδόσεις πακέτων να συμβούν χωρίς τη διακοπή του ήχου. Εντούτοις, εάν ένα ορισμένο πακέτο απαιτεί πάρα πολλές αναμεταδόσεις, μπορεί να ξεπλυθεί, επιτρέποντας στο διαβιβάζοντας κόμβο για να κινηθεί προς το επόμενο πακέτο στο αρχείο.

ΔΙΕΥΘΥΝΣΕΙΣ ΚΑΙ ΟΝΟΜΑΤΑ BLUETOOTH

Η δομή πακέτων ζωνών βάσης Bluetooth θα έχει πολύ περισσότερο νόημα εάν εξετάσουμε αρχικά πώς η εξέταση Bluetooth ολοκληρώνεται. Οι σημαντικές διευθύνσεις είναι η *Bluetooth device address* (BD_ADDR), the *active member address* (AM_ADDR), the *parked member address* (PM_ADDR), and the *access request address* (AR_ADDR). Αυτές οι διευθύνσεις είναι δυαδικοί αριθμοί που αντιπροσωπεύονται συνήθως με δεκαεξαδική μορφή, αλλά μια μονάδα Bluetooth μπορούν να δοθούν σε ένα όνομα plaintext επίσης για την καλύτερη επαφή με μας τους ανθρώπους.

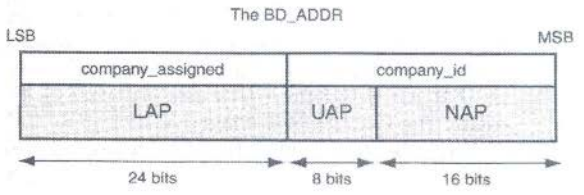
Διεύθυνση συσκευών Bluetooth (BD_ADDR)

BD_ADDR είναι μια διεύθυνση 48-bit που είναι μοναδική σε κάθε συσκευή Bluetooth. Το σχήμα του δίνεται στην 3-4, το οποίο ακολουθεί τα ieee 802 πρότυπα. Το BD_ADDR διαιρείται σε τρεις τομείς, οι οποίοι είναι :

- Lower address part (LAP) που περιέχει 24 bits
- Upper address part (UAP) που περιέχει 8 bits
- Nonsignificant address part (NAP) που περιέχει 16 bits

Το NAP είναι ασήμαντο μόνο δεδομένου ότι δεν χρησιμοποιείται για να καθορίσει τα πράγματα όπως το σύνολο hop καναλιών Bluetooth ή οι διάφοροι access codes, αλλά είναι ακόμα μέρος του BD_ADDR και βοηθάει να γίνει κάθε διεύθυνση μοναδική. Το NAP χρησιμοποιείται επίσης για την ασφάλεια Bluetooth. Τα άλλα δύο πεδία χρησιμοποιούνται για τα στοιχεία όπως ο προσδιορισμός του piconet, η σελιδοποίηση των ιδιαίτερων συσκευών Bluetooth, και η δημιουργία συνόλου καναλιών hop συχνότητας. Μερικά από τα πεδία LAP διατηρημένοι και επομένως δεν μπορούν να οριστούν σε μια συγκεκριμένη συσκευή Bluetooth.

Το UAP και το NAP διαμορφώνουν μαζί μια οντότητα 24-bit αποκαλούμενη *company_id* που ορίζεται από τη ieee 802 ομάδα ως *organizationally unique identifier* (OUI). Το LAP 24-bit, που είναι company_assigned επισυνάπτεται στο company_id να διαμορφώσει το BD_ADDR, έτσι ένα ενιαίο company_id μπορεί να υποστηρίξει πάνω από 16 εκατομμύρια συσκευές Bluetooth. Στην πραγματικότητα, το διάστημα διευθύνσεων Bluetooth 48-bit είναι αρκετά μεγάλο ώστε κάθε πρόσωπο στη γη θα μπορούσε να έχει πάνω από 50.000 Bluetooth συσκευών, κάθε μια με ένα μοναδικό BD_ADDR. Παρά το απέραντο διάστημα διευθύνσεων διαθέσιμο, οι συγκρούσεις διευθύνσεων μπορούν ακόμα να εμφανιστούν πέρα από Bluetooth piconets.



ΣΧΗΜΑ 3-4 Τα πεδία της BD_ADDR

Active Member Address (AM_ADDR)

Ένας master χρειάζεται την ικανότητα να δίνει διευθύνσεις σε κάθε slave σε ένα piconet χωριστά, αλλά θα ήταν ένα χάσιμο του χρόνου μετάδοσης να χρησιμοποιηθούν τα 48-bit BD_ADDR για αυτό το σκοπό. Επειδή υπάρχουν το πολύ-πολύ επτά ενεργοί slave σε ένα piconet, είναι δυνατό να οριστεί σε κάθε slave μια μοναδική διεύθυνση μέσα μόνο σε ένα διάστημα 3-bit. Η AM_ADDR είναι μια διεύθυνση 3-bit που ορίζεται από τον master στους slaves καθώς εισάγονται το piconet. Σε μέχρι επτά ενεργούς slaves μπορούν να οριστούν οι τιμές AM_ADDR από 001 έως 111. Το AM_ADDR με τιμή 000 είναι διατηρημένο για τα broadcast πακέτα από τον master στους πολλαπλάσιους slaves. Το AM_ADDR είναι ο πρώτος τομέας στην επιγραφή πακέτων βασικής ζώνης.

Parked Member Address (PM_ADDR)

Παρόλο που το piconet περιορίζεται σε 7 ενεργούς slaves, ένας τεράστιος αριθμός από parked member slaves μπορούν να είναι στο Piconet. Οι parked slaves είναι συγχρονισμένοι στο χρονισμό μετάδοσης πακέτων του master και στην ακολουθία hop, και "ακούν" περιοδικά για broadcast μεταδόσεις πακέτων από τον master. Όταν ένας ενεργός είναι σε κατάσταση park ο master του ορίζει μια PM_ADDR που την χρησιμοποιεί για να οδηγήσει τον slave σε unpark και να τον κάνει πάλι ενεργό. Η PM_ADDR είναι 8-bit και μέχρι 255 park slaves μπορούν να οριστούν με PM_ADDR τιμές από 0x01 μέχρι 0xFF. Η τιμή 0x00 ορίζεται στους slaves που θα απαντήσουν μόνο στην BD_ADDR τους για τις εντολές unpark από τον master.

Διαμόρφωση πακέτων baseband Bluetooth

Όπως αναφέραμε νωρίτερα, υπάρχουν τρία μέρη σε ένα baseband πακέτο ζωνών βάσης: το access code, το header, και το payload. Δεν περιέχουν όλα τα πακέτα και τα τρία μέρη. Άντ' αυτού, τα πακέτα μπορούν να κατασκευαστούν με τον έναν από τρεις τρόπους:

- κωδικός πρόσβασης μόνο (68 bit)
- κωδικός και επιγραφή πρόσβασης (126 bit)
- κωδικός, επιγραφή, και ωφέλιμο φορτίο πρόσβασης (μέχρι 2.745 bit)

Επειδή το ωφέλιμο φορτίο payload μπορεί να είναι μεταβλητού μήκους, ένα πακέτο baseband ζωνών βάσης περιέχοντας ένα payload έχει επίσης ένα μεταβλητό μήκος με το μέγιστό του να καθορίζεται είτε από 1,3ή 5 slots που χρησιμοποιούνται για την μετάδοση του.

Access Code

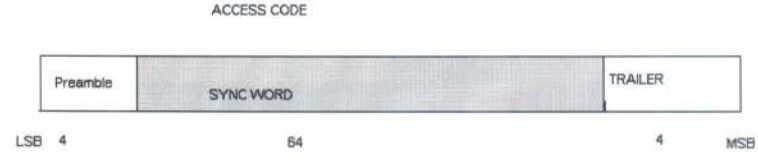
Σχεδόν σε κάθε ασύρματο σύστημα επικοινωνιών πακέτων, το ίδιο το πακέτο αρχίζει με μία ειδική μορφή από bits που είναι γνωστή από το λαμβάνοντα κόμβο. Αυτά τα bits παρέχουν το συγχρονισμό για τη φάση μεταφορέων RF (εάν είναι απαραίτητο) και βοηθούν το λαμβάνοντα κόμβο να βρει και τα όρια κομματιών και λέξης (byte). Κατ' αυτό τον τρόπο, όταν αρχίζουν οι πληροφορίες να έρχονται, τα στοιχεία κυκλώματος συγχρονισμού του δέκτη είναι βαθμονομημένα και έτοιμα να ανιχνεύσουν τα επόμενα bits που έχουν τις τιμές που δεν είναι απαραιτήτως γνωστές εκ των προτέρων.

Όλα τα πακέτα ζωνών βάσης αρχίζουν με έναν *κωδικό πρόσβασης* που παρέχει το bit και το word synchronization. (Φυσικά, ο συγχρονισμός φάσης μεταφορέων δεν είναι απαραίτητος επειδή η μη συνεκτική ανίχνευση κομματιών χρησιμοποιείται) Γενικά, ο κωδικός πρόσβασης

- Μπορεί να χρησιμοποιηθεί από έναν slave για να ξανασυγχρονίσει το CLK του στο CLK των piconet (CLKN του master)
- Παρέχει bit και word synchronization
- Περιλαμβάνει το βασικό πληροφορίες αναγνώρισης του piconet.

Ο κωδικός πρόσβασης αποτελείται από τρία μέρη: the *preamble,* the *sync word,* and the *trailer* όπως φαίνεται στο σχήμα 3-5. Το *preamble,*και το πρώτο bit της sync word συνδυάζονται για να διαμορφώσουν μια ακολουθία 5-bit εναλλάσσοντας 1 και 0 που παρέχουν το συγχρονισμό bit και δίνει στον ανιχνευτή του δέκτη μια πιθανότητα να σετάρει την απόφαση του μεταξύ του 1 και 0 επίπεδα διαφοράς δυναμικού για το μικρότερο πιθανό BER. Παρομοίως το trailer που υπάρχει μόνο όταν ακολουθεί header, ζευγαρώνει με το τελευταίο bit της sync word για άλλη μια ακολουθία 5 bit ώστε να προετοιμάσει τον ανιχνευτή(detector) του δεκτή για σωστή αποκρυπτογράφηση του header .

ΣΧΗΜΑ 3-5 Πεδία του Access code



Επιγραφή Header

Το header, εάν υπάρχει, πάντα αμέσως ακολουθεί τον κωδικό πρόσβασης access code.Το header περιέχει πραγματικές πληροφορίες που δεν είναι αναγκαία γνωστοποιημένες μελλοντικά από τον παραλήπτη. Το πραγματικό πεδίο πληροφοριών είναι μόνο 10 bit μακρύ, αλλά η σωστή υποδοχή της είναι εξαιρετικά σημαντική στην κατάλληλη λειτουργία piconet.

Περιγραφή των επιπέδων Το πακέτο βασικής ζώνης περιέχει 10 bit κατανεμημένα σε πέντε πεδία, μαζί με ένα οκτάμπιτο HEC. Αυτά τα 18 μπιτ κωδικοποιούνται έπειτα με το (3,1) δυαδικό επαναληπτικό κώδικα, που κατασκευάζει συνολικά 54 μπιτ που διαβιβάζονται.

Αυτοί οι τομείς είναι :

AM_ADDR Αυτή η διεύθυνση 3-κομματιών διακρίνει τους ενεργούς slaves στο piconet. Αυτή η διεύθυνση είναι προσωρινή και ορίζεται σε έναν slave κατά τη διάρκεια της διαδικασίας page σελίδων. Ένα πακέτο που στέλνεται από τον master θα έχει το AM_ADDR προορισμού του slave στην επιγραφή. Άλλοι slave στο piconet, σύμφωνα με αυτά καθώς αποκωδικοποιούν μια επιγραφή με AM_ADDR διαφορετικό από δικό τους, μπορούν να κλείσουν το δέκτη τους μέχρι την επόμενη άρτια αριθμημένη χρονική αυλάκωση στην οποία ο master θα στείλει ένα νέο πακέτο . Το AM_ADDR 000 δεν ορίζεται σε κανένα slave άντ' αυτού, αυτή η διεύθυνση χρησιμοποιείται για τα πακέτα broadcast από τον master στους πολλαπλάσιους slaves. (Το πακέτο FHS μπορεί επίσης να έχει AM_ADDR = 000, αλλά δεν είναι ένα πακέτο ραδιοφωνικής μετάδοσης.) Οι slaves που είτε αφήνουν το piconet είτε σταθμεύουν από τον master παραδίδουν την AM_ADDR τους.

TYPE Ο 4-bit type του πεδίου από το πακέτο επιτρέπει σε μέχρι 16 διαφορετικούς τύπους πακέτων να ονομαστούν. Οι τύποι πακέτων είναι διαφορετικοί για τα δεδομένα και τις εφαρμογές σε πραγματικό χρόνο διπλής κατεύθυνσης φωνής. Ο αριθμός των slots αυλακώσεων που καταλαμβάνονται

από το πακέτο συμπεριλαμβάνεται επίσης στον πεδίο TYPE, έτσι ένας χωρίς διεύθυνση slave ξέρει πότε για να αρχίσει να "ακούει" για την επόμενη μετάδοση του master. Οι λεπτομέρειες των τύπων πακέτων θα καλυφθούν στο επόμενο τμήμα.

FLOW Αυτό το bit ελέγχει τη ροή των πακέτων ACL. Παραδείγματος χάριν, εάν ο buffer του δέκτη γεμίζει με τα εισερχόμενα πακέτα, κατόπιν η ροή σταματά (POH = 0) στην επιστροφής του header. Ο άλλος κόμβος μπορεί να στείλει μόνο την ταυτότητα, την ID, POLL,NULL, or SCO πακέτα έως ότου συνεχιστεί η ροή (POH = 1).

ARQN Το bit ARQN λέει την πηγή ότι ένα πακέτο παραλήφθηκε επιτυχώς (ARQN = 1) ή είχε τα λάθη (ARQN = 0) και χρησιμοποιείται στη διαδικασία ARQ.

SEQN Αυτό είναι ένα διαδοχικό bit αρίθμησης για να αποτρέψει τα αντίγραφα πακέτα από την αποδοχή από το λαμβάνοντα κόμβο λόγω ενός αποτυχημένου ACK.

HEC οκτάμπιτη ακολουθία HEC δημιουργείται με το πολυώνυμο γεννητριών που δίνεται από την εξίσωση $G(X)=X_8 + X_7 + X_5 + X_2 + X + 1$, Για να παρέχει την πρόσθετη προστασία από ακούσια αποδοχή ενός πακέτου από ένα άλλο piconet που χρησιμοποιεί τον ίδιο κωδικό πρόσβασηςaccess code, το HEC LFSR φορτώνεται εκ των προτέρων με το BD_ADDR UAP του master κατά τη διάρκεια της κανονικής λειτουργίας piconet. Η αξία HEC υπολογίζεται έπειτα με το συνηθισμένο τρόπο. Το UAP είναι μέρος ταυτότητα μιας συσκευής της company _id, έτσι η πιθανότητα μειώνεται πολύ (αλλά όχι πλήρως) ότι ένα πακέτο από ένα άλλο piconet με το ίδιο CAC(channel access code) θα γίνει αποδεκτό εσφαλμένα.

Payload

Το τρίτο μέρος ενός πακέτου ζωνών βάσης Bluetooth αποτελείται από το payload το όποιο είναι αυτό όπου βρίσκονται οι πληροφορίες χρηστών. Η δομή payload διαφέρει, ανάλογα με εάν το πακέτο είναι ένα FHS, ένα ACL, ή ένας τύπος SCO. Συζητάμε το

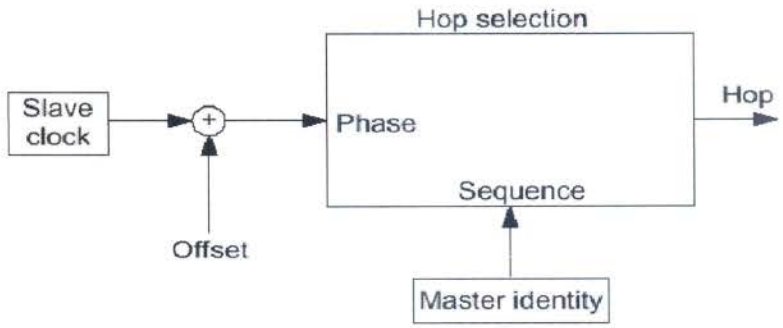
πακέτο FHS σε αυτό το τμήμα, που ακολουθείται από τα πακέτα ACL και SCO στο επόμενο τμήμα.

Συγχρονισμός μέσα στις συσκευές FHSS μάθαμε στο τελευταίο κεφάλαιο ότι για δύο συσκευές για να επικοινωνήσουν τη χρησιμοποιώντας FHSS, πρέπει να συγχρονιστούν κατάλληλα έτσι ώστε αυτές να μεταπηδούν μαζί από το κανάλι στο κανάλι. Αυτό σημαίνει ότι οι συσκευές πρέπει να

- χρησιμοποιούν το ίδιο σύνολο καναλιών.
- χρησιμοποιούν την ίδια hopping ακολουθία μέσα σε εκείνο το σύνολο καναλιών.
- να είναι συγχρονισμένες στο χρόνο μέσα στη hopping ακολουθία.

Όταν οι συσκευές είναι χρόνος που συγχρονίζονται και μεταπηδούν μαζί, θεωρούνται τη χρησιμοποίηση την ίδια hop ακολουθία και φάση. Το πακέτο FHS περιέχει τις πληροφορίες που απαιτούνται για να ικανοποιήσουν τα προηγούμενα κριτήρια. Πριν συζητήσουμε τους τομείς ωφέλιμων φορτίων FHS, θα εξετάσουμε αρχικά το πώς οι συσκευές Bluetooth παράγουν τις hop ακολουθίες τους.

Ενώ ένα μέλος ενός piconet, είτε master είτε slave, η γεννήτρια hop[hop generator] μιας συσκευής Bluetooth έχει ως μια από τις εισαγωγές του τα (LSB) λιγότερα σημαντικά 28 μπιτ του BD_ADDR του κυρίου, τα οποία καθορίζουν την HOP ακολουθία που χρησιμοποιείται από τη συσκευή. Η φάση hop καθορίζεται από τα σημαντικότερα 27 μπιτ(MSB) του CLK, που δημιουργούνται με το συνδυασμό του CLKN της μονάδας και ενός όφσετ. Το LSB των κομματιών CLK που χρησιμοποιούνται για τη φάση hop που αλλάζει κάθε 625 μs, με συνέπεια ένα βαθμό της τάξης 1.600 hop ανά δεύτερο. Φυσικά , επειδή CLK = CLKN για τον κύριο, το όφσετ του είναι μηδέν. Η έξοδος της hop generator είναι η τιμή που στέλνεται στον frequency synthesizer της ραδιομοναδας του . Ο σκοπός, έπειτα, είναι για κάθε μέλος σε ένα piconet να έχουν τις ίδιες τιμές εισόδου στους hop generator τους για κάθε στιγμή εγκαίρως έτσι ώστε να μεταπηδούν από συχνότητα σε συχνότητα. Με αλλά λόγια χρησιμοποιούν την ίδια συχνότητα και φάση.



ΣΧΗΜΑ 3-6 Επιλογή hop

Το πακέτο FHS το πακέτο FHS είναι ο τρόπος με τον οποίο ο κύριος στέλνει hopping συχνότητάς του τις πληροφορίες σε έναν slave κατά τη διάρκεια της διαδικασίας page. Το πακέτο FHS στέλνεται επίσης από τις συσκευές που απαντούν σε μια έρευνα. Αυτό το πακέτο αποτελείται από 144 bit δεδομένα του χρηστή και ενός δεκαεξάμπιτου FCS(frame check sequence) που όλα προστατεύονται από το ποσοστό 2/3 FEC(forward error correction) για ένα συνολικό payload 240 bit. Ο code, το header, και το payload συνδυάζονται να κάνουν 366 μπιτ, γεμίζοντας εντελώς μια ενιαία χρονική υποδοχή.

Οι τομείς στοιχείων του ωφέλιμου φορτίου FHS περιγράφονται στον ακόλουθο κατάλογο:

Parity bits Αυτοί είναι τα ίδια με τα πρώτα 34 μπιτ στο sync word της μονάδας που στέλνει το πακέτο FHS.

LAP Αυτό είναι η LAP της BD_ADDR της συσκευής που στέλνει το πακέτο FHS. Το sync word του αποστολέα μπορεί να αναδημιουργηθεί εύκολα από τη χρησιμοποίηση αυτών των πρώτων δύο πεδίων FHS.

Scan repetition [επανάληψη ανίχνευσης (SR)] Αυτό δείχνει το χρονικό διάστημα μεταξύ δύο διαδοχικά παράθυρα page scan.

Scan period [*περίοδος ανίχνευσης* (SP)] Αυτό είναι το χρονικό διάστημα στο οποίο ο υποχρεωτικός τρόπος scan page θα χρησιμοποιηθεί από τη συσκευή αφότου ανταποκρίνεται στην έρευνα.

NAP Αυτό είναι το NAP του BD_ADDR της συσκευής που στέλνει το πακέτο FHS.

Class of device Το επίπεδο κατηγορίας προσδιορίζει τη σημαντικότερη λειτουργία της συσκευής που στέλνει το πακέτο FHS. Οι κατηγορίες περιλαμβάνουν τις υπηρεσίες όπως δικτύωση, απόδοση, σύλληψη, μεταφορά αντικειμένου, ήχος, τηλεφωνία, και πληροφορία.

AM_ADDR Αυτή είναι ενεργού μέλους διεύθυνση που ορίζεται από τον master στον slave κατά την διάρκεια της διαδικασίας page. Το πεδίο ορίζεται στην τιμή 000 όταν το FHS συνδέεται με μια απάντηση σε ένα inquiry.

CLK 27-2 Αυτά είναι τα σημαντικότερα 26 bit του CLKN της συσκευής που στέλνει το FHS πακέτο. Επειδή τα δυο LSB δεν περιλαμβάνονται η λύση απ αυτό το πεδίο είναι 2 χρονικές υποδοχές.CLK_{1-0} μπορούμε να υποθέσουμε ότι είναι 00 όταν ο master στέλνει ένα FHS πακέτο σε έναν slave κατά την διαδικασία page επειδή αυτή η μετάδοση συμβαίνει στην αρχή κάθε άρτιας χρονικής υποδοχής.

PAGE SCAN MODE. Αυτό πληροφορεί τον δέκτη για τον τύπο του page scanning που ο αποστολέας του FHS πακέτου χρησιμοποιεί σε διαφορετικούς χρόνους από ότι στην υποχρεωτική page scan κατάσταση που απαιτείται .

ΠΑΚΕΤΑ ΣΤΙΣ ΦΥΣΙΚΕΣ ΣΥΝΔΕΣΕΙΣ

Υπάρχουν 2 τύποι φυσικών συνδέσεων που το Bluetooth υποστηριζει, το ACL και τα SCO, και έχουν διαφορετικό latency, ARQ καθώς και διαφορετική δομή πακετων. Αυτες οι δυο συνδέσεις συμπεριφέρονται διαφορετικά από τα μέλη ενός piconet.

ACL για δεδομένα

Τα δεδομένα χρηστών συνήθως μεταφέρονται χρησιμοποιώντας πακέτα ACL. Αυτά περιέχουν εντολές και απαντήσεις που συνεργάζονται με τον έλεγχο του piconet. Ορίζονται 7 τύποι πακετων,6 από αυτούς έχουν CRC κώδικα για αυτό το λόγο υιοθετούν ARQ για την αξιοπιστία στην επικοινωνία.

Τα πακέτα ACL έχουν ένα προσδιοριστικό τύπο τριών-χαρακτήρων που αποτελείται από δύο γράμματα και έναν αριθμό. Ο πρώτος χαρακτήρας είναι πάντα D, το οποίο

σημαίνει *τα δεδομένα.* Ο δεύτερος χαρακτήρας μπορεί να είναι είτε ένα Η για *την υψηλή ταχύτητα* είτε Μ για *τη μέση ταχύτητα* , και ο τελευταίος χαρακτήρας μπορεί να είναι ένα 1 ,2, ή 3, το οποίο προσδιορίζουν τον αριθμό χρονικών αυλακώσεων που χρησιμοποιούνται από το πακέτο. Το πακέτο είναι υψηλής ταχύτητας εάν δεν έχει κανένα FEC, και είναι μέση ταχύτητα εάν ο μικρότερος κώδικας Hamming εφαρμόζεται στο payload. Για παράδειγμα, το DM3 είναι δεδομένο, με μια μέση ταχύτητα, και πακέτο ACL τριών-αυλακώσεων. Παρατηρήστε ότι τα payloads πακέτων ACL δεν χρησιμοποιούν ποτέ το (3,1) δυαδικό κώδικα διορθώσεων επαναληπτικού λάθους εκείνος ο κώδικας προστατεύει μόνο το header των πακέτων βασικής ζώνης.

Ένα ειδικό πακέτο ACL, αποκαλούμενο *AUXl,* χρησιμοποιείται κατά το μεταφορά των ακατέργαστων στοιχείων μεταξύ δύο συσκευών Bluetooth. Το ωφέλιμο φορτίο αυτού του πακέτου μιας-υποδοχής(slot) έχει ένα οκτάμπιτο header αλλά κανένα FCS. Κανένα ARQ δεν είναι δυνατό, και η ποιότητα συνδέσεων δεν μπορεί να εξασφαλιστεί με αυτά τα πακέτα. Το AUX1 πακέτο χρησιμοποιείται σπάνια για να μεταφέρει δεδομένα, αλλά μπορεί να είναι πρακτικό κατά δοκιμή των BER δια μέσου του καναλιού.

Η ρυθμοαπόδοση οποιαδήποτε από τα πακέτα ACL μπορεί να υπολογιστεί με έναν απλό τρόπο, τουλάχιστον σε ένα χωρίς λάθη κανάλι. Κατ' αρχάς, το ακατέργαστο ποσοστό δεδομένων Bluetooth είναι 1 bit/ms, έτσι οποιοδήποτε έχει διάρκεια εκφράζεται σε μικροδευτερόλεπτα, και περιέχει εκείνο τον ίδιο αριθμό σε bit. Υποθέτουμε ότι το piconet έχει τη μια κύρια επικοινωνία με έναν slave (από σημείο σε σημείο). Εάν υπάρχουν πολλαπλάσιοι σκλάβοι, κατόπιν η συνολική ρυθμοαπόδοση πρέπει να διαιρεθεί μεταξύ τους.

Το πρώτο βήμα στους υπολογισμούς μας απαιτεί τι θα καλέσουμε *χρόνος κύκλου Tcycle,* που ορίζεται ως ο χρόνος μεταξύ της έναρξης δύο διαδοχικών πακέτων ACL από τον ίδιο κόμβο. Παραδείγματος χάριν, εάν ένας master και ένας slave και οι δύο ανταλλάσσουν DH1 τα πακέτα, κατόπιν κάθε ένας διαβιβάζει ένα πακέτο κάθε 1.250 μs, *αυτό το διάστημα είναι χρόνος κύκλου.* Έπειτα πρέπει να καθοριστεί ο *χρόνος δεδομένων,* το οποίο είναι το χρονικό διάστημα κατά τη διάρκεια ενός κύκλου στον οποίο δεδομένα στέλνονται. Συνεχίζοντας το παράδειγμά μας, ένα DH1 πακέτο έχει payload 240-bit, συμπεριλαμβανομένης ενός οκτάμπιτου header και δεκαεξάμπιτο FCS. Αφαιρώντας αυτά τα bit από το payload αφήνουν 216 μπιτ δεδομένων χρηστών, που

διαβιβάζονται για μία περίοδο 216 μs. Η ρυθμοαπόδοση είναι απλά η αναλογία Tdata στον Tcycle σε Mb/s. Για ανταλλαγή πακέτων DH1, έπειτα, κάθε χρήστης έχει ρυθμοαπόδοση του 216/1.250 = 0.1728 Mb/s, ή 172,8 kb/s.

Το προηγούμενο παράδειγμα υπέθεσε ότι ο master και slave και οι δύο χρησιμοποιούν τον ίδιο τύπου πακέτου για την ανταλλαγή δεδομένων τους σε αυτό που καλείται *συμμετρικό κανάλι.* Υπάρχουν πολλές καταστάσεις, όπως η μεταφορά αρχείων, στην οποία ένας κόμβος θα διαβιβάσει τα στοιχεία ως τρία ή πέντε υποδοχών πακέτα, αλλά ο άλλος κόμβος θα επιστρέψει μόνο μια υποδοχή null ή ίσως poll (εάν ο κόμβος είναι ο Master) πακέτο που περιέχει τις πληροφορίες ACK/NAK πληροφορίες στο header, ή ίσως DH1 ή DM1 πακέτο εάν ένα μικρό ποσό δεδομένων πρόκειται να επιστραφεί επίσης. Αυτό το *ασυμμετρικό κανάλι* έχει μια *μπροστινή κατεύθυνση* για τα μακριά πακέτα και μια *αντίστροφη κατεύθυνση* για τα επιστροφής πακέτα μιας χρονικής υποδοχής . Είναι εύκολο να συμπεράνουμε ότι η ρυθμοαπόδοση στο συμμετρικό κανάλι είναι υψηλότερη από όσο θα ήταν εάν το αντίστροφο κανάλι περιείχε επίσης multislot πακέτα για συμμετρική επικοινωνία.

Σύμφωνα με τον σχήμα 3-7, η χαμηλότερη μέγιστη ρυθμοαπόδοση έρχεται με τη χρησιμοποίηση DM1 των πακέτων, όπου ένα πολύ μεγάλο ποσοστό του χρόνου αφιερώνεται στα γενικά έξοδα. Κατά συνέπεια, η μέγιστη ρυθμοαπόδοση είναι μόνο περίπου 10 τοις εκατό του ακατέργαστου ποσοστού μετάδοσης 1Mb/s προς όλες τις κατευθύνσεις . Σε άλλη περίπτωση, ένα ασυμμετρικό κανάλι που χρησιμοποιεί DH5 τα πακέτα οδηγεί στη μέγιστη ρυθμοαπόδοση περισσότερων από 700 kb/s, ή περίπου 13 χρόνους γρηγορότερα από έναν τηλεφωνικό 56 kb/s modem. Εάν επιλέγαμε να στείλουμε πέντε πακέτα αυλακώσεων και στις δύο κατευθύνσεις, το ποσοστό στοιχείων θα μειωνόταν σε 433,9 Kbps!

Η επιλογή των συμμετρικών ή ασυμμετρικών συνδέσεων επιτρέπει στα σενάρια χρηστών μας για να λάβει υπόψη τη βελτίωση στο ποσοστό στοιχείων σε μια κατεύθυνση της ασυμμετρικής σύνδεσης (παραδείγματος χάριν, PDA μας που θα φυλλομετρήσει τον Ιστό μέσω ενός κεντρικού υπολογιστή θα απαιτήσει περισσότερο εύρος ζώνης μεταφορτώνοντας τις σελίδες από θα απαιτήσει για μας να διευκρινίσει την επόμενη σύνδεση για να φυλλομετρήσει.). Ο πίνακας 3-7 επεξηγεί τα μέγιστα ποσοστά

στοιχείων με όλους τους τύπους πακέτων και στις συμμετρικές και ασυμμετρικές συνδέσεις.

ACL Packet Type	Payload Header (Bytes)	User Payload (Bytes)	FEC	CRC	Symmetric Max Data Rate (Kbps)	Asymmetric Max Data Rate (Kbps)	
						Forward	Reverse
DM1	1	0 – 17	2/3	Yes	108.8	108.8	108.8
DH1	1	0 – 27	0	Yes	172.8	172.8	172.8
DM3	2	0 – 120	2/3	Yes	258.1	387.2	54.4
DH3	2	0 – 180	0	Yes	390.4	585.6	86.4
DM5	2	0 – 224	2/3	Yes	286.7	477.8	36.3
DH5	2	0 – 338	0	Yes	433.9	723.2	57.6

ΣΧΗΜΑ 3-7. Μέγιστες ροές δεδομένων για τα ACL πακέτα Bluetooth

SCO ΓΙΑ ΜΕΤΑΔΟΣΗ ΦΩΝΗΣ

Τα δεδομένα χρηστών που αποτελούνται από ψηφιοποιημένη σε πραγματικό χρόνο διπλής κατεύθυνσης φωνή μεταφέρονται χρησιμοποιώντας τα πακέτα SCO. Τρεις τύποι πακέτων SCO έχουν καθοριστεί, μαζί με έναν τέταρτο τύπο που συνδυάζει το SCO και τα δεδομένα ACL μέσα στον ίδιο τομέα ωφέλιμων φορτίων. Μια σύνδεση SCO είναι συμμετρική μεταξύ ενός master και ενός slave, έτσι οι υποδοχές είναι προκαθορισμένες για να υποστηρίξουν ένα 64 kb/s ψηφιοποιημένο ρεύμα φωνής σε κάθε κατεύθυνση. Το Bluetooth στέλνει τη ψηφιοποιημένη φωνή κατά τρόπο παρόμοιο με αυτόν που χρησιμοποιείται στο DECT (για τους ευρωπαίους Digital European Cordless Telephone και για τους μη ευρωπαίους σημαίνει Digital Enhanced Cordless Telephone.) Κάθε πακέτο SCO βασικής ζώνης περιέχει μερικά bit της φωνής, και επειδή το ακατέργαστο ποσοστό δεδομένων Bluetooth είναι 1 Mb/s, το σχετικά αργό 64 kb/s ψηφιοποιημενη ροή φωνής μπορεί να σταλεί σε περιοδικές σύντομες εκρήξεις, αφήνοντας την αφθονία του χρόνου να αφουγκραστεί ένα πακέτο επιστροφής SCO από την άλλη μεριά της σύνδεσης. Οι συσκευές Bluetooth ανταλλάσσουν ζευγάρια πακέτων μιας-υποδοχής στο ποσοστό των 800/sec.

Το μέρος του payload ενός πακέτου SCO έχει μόνο έναν τομέα σε αυτό, που αποτελείται από 240 bit των ψηφιοποιημένων δεδομένων φωνής, με ή χωρίς διόρθωση λάθους. Αυτά τα πακέτα δεν περιέχουν ένα payload header, ούτε FCS. Κατά συνέπεια, τα πακέτα SCO δεν αναμεταδίδονται ποτέ, και ούτε ARQ υπάρχει. Α. Δεδομένου ότι το BER αυξάνεται, κατόπιν, η σύνδεση SCO θα αρχίσει να πάσχει από το διαστρεβλωμένο ήχο.

Όπως τα αντίστοιχα ACL τους, τα πακέτα SCO έχουν επίσης έναν τρεις προσδιοριστικούς χαρακτήρες που αποτελείται από δύο γράμματα που ακολουθούνται από έναν αριθμό. Δυστυχώς, μερικές από τα γράμματα και τους αριθμούς είναι τα ίδια με τα πακέτα ACL, αλλά η έννοιά τους είναι απολύτως διαφορετική. Οι πρώτοι δύο χαρακτήρες πακέτων SCO είναι πάντα *HV,* το οποίο σημαίνει *την υψηλής ποιότητας φωνή(high-quality voice).* Ο τελευταίος χαρακτήρας μπορεί να είναι ένα 1, 2, ή 3, το οποίο προσδιορίζει τον τύπο διόρθωσης λάθους στο payload. Το ωφέλιμο φορτίο ενός HV1 πακέτου έχει το (3,1) δυαδικό επαναληπτικό κώδικα, το HV2 ωφέλιμο φορτίο περιέχει το (15.10) μικρότερο κώδικα Hamming, και το HV3 ωφέλιμο φορτίο δεν έχει καμία ικανότητα διορθώσεων λάθους. Ο ευκολότερος τρόπος να κρατηθεί αυτό είναι να συνειδητοποιηθεί ότι το ψηφίο είναι ο αριθμητής στο ποσοστό κώδικα FEC δηλαδή HV1 χρησιμοποιεί το ποσοστό 1/3, HV2 ποσοστό 2/3 χρήσεων, και HV3 ποσοστό 3/3 χρήσεων (δηλαδή κανένα) FEC.

Η αναλογική ροή φωνής δειγματοληπτείται στα 64 kb/s και τα δεδομένα στέλνονται στον ελεγκτή συνδέσεων για την κωδικοποίηση σε πακέτα HV. Αυτοί οι όλοι έχουν τα ίδια μεγέθη payloads 240 bit (30 bytes), αλλά το ποσό ψηφιοποιημενης φωνής που περιλαμβάνεται σε καθεμία διαφέρει λόγω FEC.

Ένα ειδικό πακέτο SCO αποκαλούμενο *data / voice* (DV) χρησιμοποιείται όταν είναι απαραίτητο να περιληφθούν μερικά δεδομένα εκτός από τη ψηφιοποιημενη φωνή σε μια από τις χρονικές υποδοχές SCO, παραδείγματος χάριν, μερικές εντολές ελέγχου συνδέσεων και οι απαντήσεις μπορούν να είναι προσαρτημένες κατ' αυτό τον τρόπο εάν επιδιώκεται. Το πακέτο DV περιέχει 80 μπιτ payload της ψηφιοποιημενης φωνής χωρίς FEC, μαζί με οκτάμπιτο header, μέχρι και72 μπιτ των δεδομένων ACL, και ένα δεκαεξάμπιτο FCS που υπολογίζεται για τα στοιχεία ACL μόνο. Μόνο το μέρος ACL του πακέτου υπόκειται σε ARQ, έτσι εάν μια αναμετάδοση απαιτείται, κατόπιν τα παλαιά

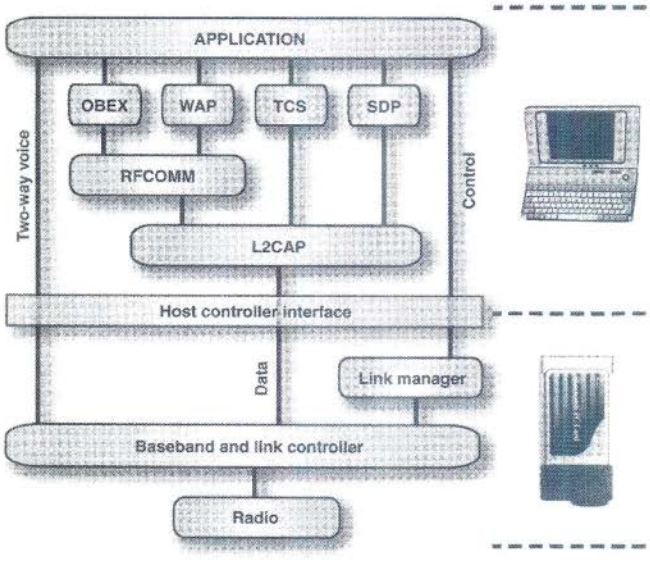
δεδομένα είναι συνδεμένα με ένα επόμενο πακέτο DV με τις νέες πληροφορίες φωνής ή τοποθετημένο μέσα σε ένα καθαρό πακέτο ACL σε μια χρονική μη-SCO υποδοχή.

Η σύνδεση μπορεί να ρυθμιστεί μέσω των εντολών που στέλνονται στο ωφέλιμο φορτίο ενός DV ή DM1 πακέτου, καθένα από τα όποια αντικαθιστά το πακέτο HV1 που προγραμματίζεται για μια ιδιαίτερη χρονική αυλάκωση. Οι σύντομες εντολές ως τμήμα ενός πακέτου DV δεν θα διακόψουν τη ροή φωνής, αλλά οι πιο μακροχρόνιες εντολές που απαιτούν ένα πακέτο DMI θα διακόψουν τον ήχο για 80 bit (1,25ms) .

Για μια σύνδεση SCO με HV2 τα πακέτα,2 διαδοχικές χρονικές υποδοχές για κάθε τέσσερις χρησιμοποιούνται για την ανταλλαγή πακέτων SCO. Εάν HV3 τα πακέτα χρησιμοποιούνται άντ' αυτού, κατόπιν δύο διαδοχικές χρονικές υποδοχες από κάθε έξι χρησιμοποιούνται. Επομένως, μέχρι δύο διπλής κατεύθυνσης συνδέσεις φωνής μπορεί να υποστηριχθεί με HV2 τα πακέτα, και μέχρι τρεις μπορεί να υπάρξει όταν τα HV3 χρησιμοποιούνται , προτού το Bluetooth piconet να είσαι πλήρως κορεσμένο. Αυτές οι πολλαπλάσιες συνδέσεις φωνής μπορούν να υπάρξουν μεταξύ ενός master και ενός slave ή μεταξύ master και πολλαπλάσιων slave. Φυσικά, ο master στο piconet πρέπει να είναι από τη μία πλευρά σε κάθε ένα από αυτά τα κανάλια φωνής.

Για τη λειτουργία scatternet, μόνο μια συσκευή μπορεί να υποστηρίξει μια HV3 σύνδεση σε κάθε ένα από δύο piconets. Επειδή τα διαφορετικά piconets δεν είναι συγχρονισμένα, ένας χρήστης πρέπει να είναι εκτός, για τουλάχιστον 3 συνεχόμενες χρονικές υποδοχές ώστε να έχει την ικανότητα να ανταλλάξει 2 SCO πακέτα στο διαφορετικό piconet. Γι'αυτό το λόγο δεν είναι δυνατό να ανταλλαχθούν HV1 ή HV2 πακέτα.

ΚΕΦΑΛΑΙΟ 4
ΑΡΧΙΤΕΚΤΟΝΙΚΗ BLUETOOTH



ΣΧΗΜΑ 4.1 Η ΣΤΟΙΒΑ ΠΡΩΤΟΚΟΛΛΟΥ BLUETOOTH

Για τα πρώτα δυο επίπεδα της στοίβας έχουμε μιλήσει σε προηγούμενες ενότητες. Πρέπον θα ήταν όμως να κάνουμε μια σχετική αναφορά σε αυτά προτού συνεχίσουμε την περιγραφή μας σε καινούργια μονοπάτια.

ΕΠΙΠΕΔΟ ΡΑΔΙΟΖΕΥΞΗΣ

Όπως έχουμε αναφέρει σε αυτό το επίπεδο δημιουργούνται οι φυσικές συνδέσεις μεταξύ των συσκευων. Λειτουργεί στη μη αδειοδοτημένη ζώνη ISMστα 2.4 GHz και χρησιμοποιεί την τεχνολογία FHSS me 1600 hops/sec.Η διαμόρφωση είναι GFSK.

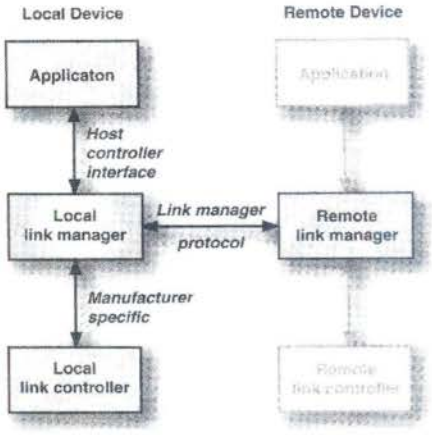
BASEBAND

Εδώ ουσιαστικά γίνεται ο έλεγχος στο επίπεδο των ραδιοζευξης. Εδώ καθορίζεται η ακολουθία hop της συχνότητας, γίνεται κρυπτογράφηση κατώτερου επιπέδου για την ασφάλεια των ζεύξεων και διαχειρίζεται τα πακέτα δεδομένων με τον LC(link controller)[περισσότερα στοιχεία στο κεφ 3]

LINK MANAGER

Μέχρι τώρα έχουμε μελετήσει τα μέρη της λίστας πρωτοκόλλου Bluetooth που είναι κυρίως υλικό όπως το επίπεδο της ραδιόζευξης και ο μηχανισμός καταστάσεων με την μορφή του *ελεγκτής συνδέσεων*(LC). Καθώς κινούμαστε ποιο ψηλά στη λίστα πρωτοκόλλου Bluetooth παρατηρούμε τη μετάβαση στρωμάτων βαθμιαία από το υλικό σε firmware, και έπειτα, καθώς κινούμαστε προς τον host, στις εφαρμογές λογισμικού.

Ο *διευθυντής* (LM) *συνδέσεων* κατοικεί μεταξύ του στρώματος *host controller interface* (HCI) (εάν υπάρχει) και του LC κατωτέρω μέσα στη λίστα πρωτοκόλλου Bluetooth (σχήμα 4-1). Το LM είναι αμφισβητήσιμα το χαμηλότερο στρώμα στη λίστα πρωτοκόλλου που αρχίζει να εκθέτει μερικά χαρακτηριστικά λογισμικού. Όπως ανακαλύπτουμε οι κατασκευαστές της ενότητας του radio Bluetooth και της βασικής ζώνης ICs τοποθετούν συνήθως το LM firmware, είτε φυσικά στο τσιπ ζωνών βάσης είτε σε μια χωριστή μονάδα μνήμης.



ΣΧΗΜΑ 4-2 Ο τοπικος LM επικοινωνει με τον host

Το LM επικοινωνεί με τρεις διαφορετικές οντότητες κατά τη διάρκεια μιας συνεδρίασης Bluetooth: με τον τοπικό host μέσω HCI, του τοπικού LC, και του μακρινού LM, όπως φαίνεται στο σχήμα 4-2. Το τοπικό LM υπάρχει συνήθως στην μονάδα σαν ένα κομμάτι μια πλήρους υλοποίησης Bluetooth host-μονάδα, και το μακρινό LM ορίζεται ως το LM στην άλλη άκρη μιας σύνδεσης επικοινωνίας Bluetooth Για παράδειγμα, το Host μπορεί να κατευθύνει το τοπικό LM για να συνδεθεί με μια άλλη συσκευή, οπότε σ'αυτή την περίπτωση ο τοπικός LM εργάζεται με τον τοπικό LC για να πραγματοποιήσει το απαραίτητο page. Όταν το page είναι επιτυχές, το τοπικό LM αρχίζει με το μακρινό LM για να οργανώσει και να διαμορφώσει τη σύνδεση για να την προετοιμάσει για την ανταλλαγή στοιχείων χρηστών. Αυτή η πορεία επικοινωνίας απεικονίζεται όπως άμεσα συνδέοντας τα δύο LMs στο σχήμα 4-2, αλλά, φυσικά, επικοινωνούν πραγματικά μέσω των αντίστοιχων Bluetooth LC και με τις ραδιοζεύξεις. Η προδιαγραφή Bluetooth παρουσιάζει μια πολύ δομημένη μέθοδο για τις επικοινωνίες LM-με-LM, αλλά η μέθοδος που χρησιμοποιείται από το τοπικό LM για να αλληλεπιδράσει με την τοπική λίστα πρωτοκόλλου μπορεί να είναι συγκεκριμένη για κάθε κατασκευαστή συσκευών Bluetooth εάν δεν χρησιμοποιείται HCI.

Σε αυτό το κεφάλαιο, θα περιγράψουμε τους διάφορους στόχους που το LM εκτελεί και ενισχύουμε τις περιγραφές με μερικά παραδείγματα.

LINK MANAGER PROTOCOL

Τα πακέτα που εναλλάσσονται μεταξύ των LMs λαμβάνουν γενικά τη μορφή μιας *εντολής (command)* και *μιας απάντησης (response)* εάν το άλλο LM καλείται να εισαχθεί σε έναν ιδιαίτερο τρόπο λειτουργίας, ή ένα *αίτημα (request)* και *μια απάντηση (response)* εάν πληροφορίες χρειάζονται από τους άλλους LM . Πληροφορίες που προσφέρονται εθελοντικά στο άλλο LM συνήθως δεν απαιτούν καμία απάντηση. Αυτές οι *Link Manager Protocol* διαδικασίες (LMP) είναι αρκετά στοιχειώδης και περιλαμβάνουν συχνά μόνο μια μοναδική λειτουργία της σύνδεσης, όπως η είσοδος στην κατάσταση hold.

Τα μηνύματα χρήσεων LMP μέσα σε ένα πακέτο DM1 (ή σε μερικές περιπτώσεις ένα DV) περιέχουν τη διαμόρφωση και τις πληροφορίες σύνδεσης, τη διαχείριση piconet, και οδηγίες ασφάλειας. Αυτά τα μηνύματα καλούνται *μονάδες δεδομένων πρωτοκόλλου [protocol data units]* (PDUs). Επειδή τα μηνύματα χτίζονται σε ένα πακέτο Bluetooth, προορίζονται για το LM στην άλλη μεριά της σύνδεσης. Αυτά τα ειδικά φορτία (payloads) DM1, ή η ισοδύναμη μερίδα δεδομένων ενός φορτίου DV, "συλλαμβάνονται" από τον προορισμό LM και δεν περνούν μακρύτερα επάνω στη λίστα πρωτοκόλλου. Όπως συνήθως, η προδιαγραφή Bluetooth λέει *τι* ο LM πρέπει να κάνει, αλλά όχι *πώς* να το κάνει.

Τα πακέτα LMP έχουν μια πιο υψηλή προτεραιότητα από τα δεδομένα χρηστών μεταξύ δύο συσκευών, έτσι ενώ ανταλλάσσονται PDUs, τα υψηλότερα στρώματα στη λίστα πρωτοκόλλου μπορούν να μην δουν τίποτα για αρκετές χρονικές υποδοχές (slots). Επιπλέον, τα πακέτα LMP μπορούν επίσης να διαλύσουν μια σύνδεση SCO εάν δεν υπάρχει καμία αχρησιμοποίητη υποδοχή(slot) ACL διαθέσιμη επειδή μερικά PDUs έχουν έναν πιο μακρύ πεδίο δεδομένων από ότι το πακέτο DV μπορεί να υποστηρίξει. Σε αυτές τις περιπτώσεις, ένα ζευγάρι πακέτων SCO θα εγκαταλειφθεί και θα αντικατασταθεί από ένα DM1 LMP PDU και της απάντησή του. (Καταπληκτική επιτυχία, τρεις συντμήσεις σε μια σειρά. Αυτό σημαίνει Bluetooth ομιλία)

Το LM στηρίζεται στο LC και στην υλοποίηση του της διόρθωσης λάθους, ανίχνευση λάθους, και ARQ για την αξιόπιστη μετάδοση του PDU.Αυτό σημαίνει ότι το ίδιο το LM δεν έχει καμία διαδικασία για την υποδοχή ενός PDU, και υποθέτει ότι κάθε PDU θα φθάσει τελικά στον προορισμού ελεύθερο από λάθη. Εντούτοις, όπως με οποιοδήποτε

πακέτο ACL στο *ασύγχρονο* κανάλι (UA) *χρηστών*, η μέγιστη λανθάνουσα κατάσταση δεν μπορεί να διευκρινιστεί επειδή οι κακές συνθήκες καναλιών μπορούν να οδηγήσουν σε πολλές αναμεταδόσεις των πακέτων που αλλοιώθηκαν κατά τη διάρκεια της υποδοχής. Επίσης, το LC ενός master μπορεί εύλογα να εγγυηθεί ότι η επικοινωνία θα πραγματοποιηθεί με έναν συγκεκριμένο slave μόνο μία φορά κάθε T_{poll} (εξ ορισμού 40) slots. Συνεπώς, τα link management tasks (καθήκοντα διαχείρισης της σύνδεσης) θα μπορούσαν να απαιτήσουν έναν σημαντικό χρόνο να ολοκληρώσουν. Για να αποτρέψει τις άπειρες περιόδους περιμένοντας , ο χρόνος μεταξύ της λήψης βασικής ζώνης PDU και της αποστολής μιας απάντησης πρέπει να είναι λιγότερο από 30 δευτερόλεπτα, η οποία είναι η αξία διαλείμματος απάντησης LMP. Εάν αυτό ο επιτυγχάνεται, η συσκευή υποθέτει ότι το επηρεασθέν PDU ολοκληρώθηκε ανεπιτυχώς.

Γενική περίοδος συνδέσεων

Έχουμε μελετήσει ήδη τις διαδικασίες έρευνας και page, όπου οι συσκευές βρίσκουν η μια την άλλη και συνδέονται. Μετά από αυτήν την αρχική σύνδεση, το LM εκτελεί τα διάφορα καθήκοντα διαμόρφωσης συνδέσεων και έπειτα παρατηρεί τα δεδομένα που ανταλλάσσονται, ψάχνοντας οποιαδήποτε πακέτα LMP και παρεμποδίζοντας τα για επεξεργασία. Τέλος, όταν η ανταλλαγή στοιχείων είναι πλήρης, ο LM μπορεί να εκτελέσει την αποσύνδεση.

Όπως αναμένεται, το LM διαδραματίζει το μέγιστο ρόλο του μεταξύ του χρόνου που η διαδικασία page είναι επιτυχής και όταν αρχίζουν οι συσκευές να ανταλλάσσουν δεδομένα χρηστών. Η διαδικασία διαμόρφωσης συνδέσεων μπορεί συχνά να περιλάβει διάφορες ανταλλαγές LMP PDU μεταξύ του master και του slave LM. Μερικές αφίξεις PDU απαιτούν εφαρμογή και ίσως επίσης ο χρήστης να ειδοποιηθεί και να κάνει κάποια ανταπόκριση, ενώ άλλες μπορούν να αντιμετωπιστούν από το ίδιο τον LM ή ίσως από κάποιο άλλο λογισμικό/firmware υψηλότερο στη λίστα πρωτοκόλλου. .

Γενικά, οι πτυχές που αντιμετωπίζονται από το LM εμπίπτουν σε τρεις κατηγορίες:

Διαμόρφωση και πληροφορίες συνδέσεων : όταν η διαδικασία page είναι επιτυχής και ο master και ο slave συνδέονται με το piconet, πρέπει να ανακαλύψουν τα χαρακτηριστικά γνωρίσματα συνδέσεων (παραδείγματος χάριν, υποστήριξη για πακέτα

multislot και RSSI received signal strength indication) είναι διαθέσιμα στην άλλη συσκευή. Τα πακέτα LMP PDU υπάρχουν επίσης για τη ρύθμιση QoS, τον έλεγχο ισχύος, και άλλες λειτουργίες διαμόρφωσης κατά τη διάρκεια οποτεδήποτε η σύνδεση είναι ενεργή.

Διαχείριση Piconet : Περιλαμβάνει την ένωση και την αποσύνδεση των slaves, τη χρησιμοποίηση αλλαγής master-slave , την εγκατάσταση των συνδέσεων SCO, και το χειρισμό των sniff, hold, και park καταστάσεων χαμηλής ισχύος.

Η διαχείριση ασφάλειας : Το LMP χειρίζεται επίσης τις περισσότερες από τις εφαρμογές που συνδέονται με την επικύρωση και την κρυπτογράφηση της σύνδεσης Bluetooth .

Μόλις καθιερωθεί το κανάλι ACL και διαμορφωθεί, οι εφαρμογές μπορούν τελικά να αρχίσουν την εργασία και να αρχίσουν να ανταλλάσσουν δεδομένα. Εάν τα πακέτα SCO πρόκειται να ανταλλαχθούν, κατόπιν ο LM πρέπει να χρησιμοποιήσει τα πακέτα LMP για να σετάρει το κανάλι SCO. Όπως συζητήσαμε στο προηγούμενο κεφάλαιο, οι LM θα συμφωνήσουν σχετικά με τη μέθοδο κωδικοποίησης φωνής χρησιμοποιούμενη, και είτε HV1, HV2, είτε HV3 πακέτα θα ανταλλαχθούν όπως επίσης και ο χρονισμός τους. Προκειμένου να μειωθεί η λανθάνουσα κατάσταση, η σε πραγματικό χρόνο διπλής κατεύθυνσης φωνή διαβιβάζεται συνήθως στα χαμηλότερα στρώματα πρωτοκόλλου Bluetooth άμεσα από την εφαρμογή

Logical Link Control and Adaptation Protocol (L2CAP)

Εάν οι χρήστες ανταλλάσσουν δεδομένα ACL, κατόπιν το *πρωτόκολλο προσαρμογής ελέγχου συνδέσεων Logical Link Control and Adaptation Protocol* (L2CAP) διαδραματίζει έναν σημαντικό ρόλο στην παρακολούθηση της ανταλλαγής. Το L2CAP είναι ένας μέσος διαχειριστής, που ενεργεί ως σύνδεσμος μεταξύ της εφαρμογής και του (link controller)ελεγκτή συνδέσεων Bluetooth. Στην πραγματικότητα, διάφορες εφαρμογές μπορούν να επικοινωνήσουν πέρα από μια σύνδεση Bluetooth RF, και το

L2CAP έχει την ευθύνη να διατηρεί την τάξη στις ροές δεδομένων. Θα δούμε πώς αυτό γίνεται έπειτα.

Τώρα που έχουμε μπει στο Βασίλειο της λίστας πρωτοκόλλου Bluetooth όπως εμφανίζεται στον host ως τμήμα ενός πακέτου λογισμικού, είναι σημαντικό να υπενθυμίσουμε κάποια στοιχεία. Κατ' αρχάς, για τις υλοποιήσεις λογισμικού, η προδιαγραφή Bluetooth επιτρέπει συνήθως μεγάλη ευελιξία στους κατασκευαστές όσο αναφορά την ανάπτυξη του κώδικά τους, ειδικά για την επικοινωνία μεταξύ των διάφορων επιπέδων της λίστας πρωτοκόλλου σε έναν host. Πράγματι, ο κώδικας είναι η πηγή υπεηφάνειας (και προστασίας πνευματικής ιδιοκτησίας) για πολλούς υπεύθυνους για την ανάπτυξη. Ως έχει, θα ήταν αδύνατο να διευθυνσιοδοτηθεί κάθε προσέγγιση υλοποίησης εδώ. Επίσης, τα πιο υψηλά επίπεδα της λίστας πρωτοκόλλου γίνονται όλο και περισσότερο σύνθετα επειδή μπορούν να εμφανιστούν να είναι εφαρμογές από μόνα τους. .

Στην προδιαγραφή Bluetooth, το στρώμα L2CAP περιγράφεται σαν να μην υπήρχε καμία master-slave σχέση μεταξύ των μελών piconet. Πράγματι, οι λέξεις "master" και "slave" δεν βρίσκονται οπουδήποτε στο κεφάλαιο L2CAP της προδιαγραφής. Δεν υιοθετούμε αυτήν την μέθοδο εδώ, εν τούτοις, επειδή ο τρόπος που μερικές λειτουργίες L2CAP ολοκληρώνονται εξαρτάται από εάν η συσκευή είναι master ή slave. Εντούτοις, λάβετε υπόψη ότι ο στόχος L2CAP είναι να κάνει τη master-slave σχέση άσχετη και να αντιμετωπιστούν οι συσκευές επικοινωνίας ως ισότιμες κάθε φορά που είναι δυνατόν.

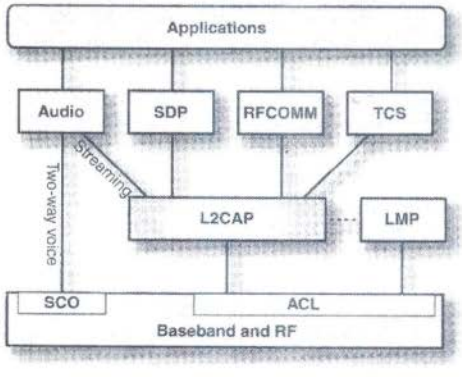
Logical Link Control and Adaptation Protocol (L2CAP) for Data

Το L2CAP είναι μια υπομονάδα λογισμικού που κανονικά κατοικεί στον host και παρέχει σύνδεση-προσανατολισμός (master σε έναν slave και slave σε master) και χωρίς σύνδεση (υπονοούμενος ότι είναι από έναν κύριο στους πολλαπλάσιους slaves) υπηρεσίες δεδομένων. Αυτό σημαίνει ότι ο L2CAP δεν παρέχει σε πραγματικό χρόνο διπλής κατεύθυνσης τη δυνατότητα φωνής (SCO). Μπορεί, εντούτοις, να επικοινωνήσει με το LM για τη βοήθεια οργάνωσης καναλιών. Ο κύριος σκοπός του L2CAP είναι να ενεργήσει ως αγωγός(κανάλι μεταφοράς) για τα δεδομένα όσον αφορά τη σύνδεση ACL μεταξύ των εφαρμογών βασικής ζώνης(baseband) Bluetooth και host.

Όπως ο LM,ο L2CAP στηρίζεται στη διαδικασία ανταλλαγής πακέτων βασικής ζώνης για την ακεραιότητα των δεδομένων μέσω ARQ(automatic repeat request) και ενδεχομένως, FEC(forward error correction) επίσης. Επομένως, κανένα AUX1 πακέτο δεν επιτρέπεται για L2CAP επικοινωνία επειδή δεν έχουν CRC(cyclic redundancy check) υλοποίηση και συνεπώς, καμία ARQ ικανότητα.

Δύο μορφές δεδομένων χρηστών μπορούν να ανταλλαχθούν μέσω των υπηρεσιών του L2CAP. Το ένα, αποκαλούμενος *το user asynchronous* (UA), τοποθετεί την αξιοπιστία πάνω από όλα και απαιτεί από τα πακέτα να αναμεταδίδονται μέχρι να φτάσουν επιτυχώς. Η UA υπηρεσία είναι αναγκαία κατά τη μεταφορά των αρχείων δεδομένων από μια συσκευή σε άλλη. Η άλλη μορφή ανταλλαγής δεδομένων καλείται *user isochronous* (UI), στον οποίο η ακεραιότητα δεδομένων είναι σημαντική, αλλά περιστασιακά μπορεί να επηρεαστεί από απαιτήσεις latency . Ένα παράδειγμα βρίσκεται στη μονόδρομη σε πραγματικό χρόνο ακουστική ή βίντεο (πολυμέσα) ροή, στην οποία ένας buffer στη λήψη δεν πρέπει να επιτραπεί να αδειάσει . Ένα κακό πακέτο που δεν μπορεί να μεταφερθεί επιτυχώς μετά από ορισμένες προσπάθειες "ξεπλένεται", και το σύστημα συνεχίζει στο επόμενο πακέτο στη ροή δεδομένων.

Σχήμα 4.3 Το L2CAP πρέπει να παρακολουθεί διάφορες εφαρμογές από πάνω του Η πραγματικού χρόνου διπλής κατεύθυνσης φωνή παρακάμπτει τον L2CAP



Λειτουργίες L2CAP

Το σχήμα 4-3 παρουσιάζει λίγο περισσότερη λεπτομέρεια για το πώς τακτοποιείται το L2CAP μέσα στη λίστα πρωτοκόλλου Bluetooth. Οι εφαρμογές των host λειτουργούν μέσω διάφορων διαφορετικών εξαρτώμενων πυρήνων λογισμικού Bluetooth, οι οποίοι επικοινωνούν στη συνέχεια με το L2CAP με τον τρόπο της πολυπλεξίας. Οι σε πραγματικό χρόνο διπλής κατεύθυνσης εφαρμογές φωνής παρακάμπτουν το L2CAP και χρησιμοποιούν μια σύνδεση SCO για τη μεταφορά τους, αλλά ο ήχος που ρέει μπορεί να χρησιμοποιήσει το κανάλι UI μέσω L2CAP αντ' αυτού. Επίσης, L2CAP μπορεί να επικοινωνήσει με το LM του, εάν είναι απαραίτητο, για την οργάνωση καναλιών ACL και άλλους στόχους.

Η φιλοσοφία πίσω από την ανάπτυξη L2CAP περιέλαβε τις απαιτήσεις της απλότητας και των χαμηλού κόστους . Οι συσκευές που έχουν λίγη μνήμη και χαμηλή ταχύτητα υπολογισμού δεν πρέπει να "καταπιεστούν" από το L2CAP όσο αναφορά τη δαπάνη άλλων διαδικασιών, και το πρωτόκολλο δεν πρέπει να καταναλώνει ένα υπερβολικό ποσό ισχύος. Επιπλέον, L2CAP σχεδιάστηκε για την εφαρμογή σε έναν μεγάλο αριθμό διαφορετικών μονάδων όπως οι προσωπικοί υπολογιστές, *οι προσωπικοί ψηφιακοί βοηθοί* (PDAs), τα ασύρματα και κυψελοειδή τηλέφωνα, και τα παιχνίδια αλληλεπίδρασης.

Οι λειτουργίες του L2CAP μπορούν να διαιρεθούν σε τέσσερις κατηγορίες : πολυπλεξία πρωτοκόλλου, κατάτμηση πακέτων και επανασυναρμολόγηση, ποιότητα της υπηρεσίας (QoS), και group management . Αυτοί μπορούν να καθοριστούν ως εξής:

Protocol multiplexing(πολυπλεξία) Θα παρατηρήσατε από το σχήμα 4-3 που, αντίθετα από τα χαμηλότερα στρώματα πρωτοκόλλου, L2CAP πρέπει να επικοινωνήσει με διάφορα διαφορετικά στρώματα επάνω από αυτό. Η επικοινωνία είναι διπλής κατεύθυνσης δηλαδή το πρωτόκολλο παίρνει τα πακέτα από αυτά τα υψηλότερα στρώματα και τα μετατρέπει σε payload ACL Bluetooth-μεγέθους, και παίρνει τα payloads από τον ελεγκτή συνδέσεων LC και τα κατευθύνει στο σωστό υψηλότερο στρώμα. Με άλλα λόγια, L2CAP παρέχει την πολυπλεξία πρωτοκόλλου με έναν τρόπο

που είναι προφανής στα υψηλότερα πρωτόκολλα. Το L2CAP υλοποιεί την πολυπλεξία πρωτοκόλλου με την καθιέρωση εικονικών καναλιών μεταξύ των συσκευών που περιλαμβάνουν έναν πεδίο προορισμού μέσα σε κάθε πακέτο L2CAP.

Segmentation and reassembly(τμηματοποίηση και επανασυναρμολόγηση) Τα πακέτα που χρησιμοποιούνται από το πρωτόκολλο ζωνών βάσης Bluetooth είναι μικρά από τα περισσότερα πρότυπα, που τα payloads χρηστών περιορίζονται σε 339 bytes το πολύ. Ένα υψηλότερου επιπέδου πρωτόκολλο δεν εμποδίζεται από ένα κανάλι επικοινωνίας που έχει τα προβλήματα αξιοπιστίας της ραδιοζεύξης, έτσι το μέγεθος *της μέγιστης μονάδας μετάδοσής του* (MTU) είναι συχνά σημαντικά μεγαλύτερο, μερικές φορές όσο και 64K Bytes. Αυτά τα μεγάλα πακέτα πρέπει να αποτελούνται από διάφορα πακέτα ζωνών βάσης Bluetooth για τη μετάδοση, και τα εισερχόμενα πακέτα βασικής ζώνης λαμβάνονται από τον L2CAP και συναρμολογούνται ξανά στα μεγάλα κομμάτια δεδομένων που το υψηλότερο επίπεδο αναμένει να λάβει. Αυτή η διαδικασία είναι επίσης διαφανής στο υψηλότερο στρώμα πρωτοκόλλου.

QoS Το L2CAP μπορούν να εφαρμόσει ένα επίπεδο QoS για κάθε protocol που αυτό περιλαμβάνει τέτοια αντικείμενα όπως τις απαιτήσεις εύρους ζώνης, πόσο γρήγορα τα διαδοχικά πακέτα μπορούν να φθάσουν, μέγιστη λανθάνουσα κατάσταση, και απόκλιση καθυστέρησης. Το QoS προκαθορίζει κάτι που καλείτε *best effort[καλύτερη προσπάθεια],* η οποία είναι ένας άλλος τρόπος ότι θα κάνει το καλύτερο που μπορεί κάτω από τις περιστάσεις.

Group management Πολλά υψηλότερα πρωτόκολλα στον host απαιτούν την ικανότητα να διαχειρίζονται μια ομάδα διευθύνσεων. Το Bluetooth LM διαχειρίζεται μια ομάδα αποκαλούμενη *piconet,* που αποτελείται και από τους ενεργούς και σταθμευμένους slaves. Το L2CAP παίρνει αυτήν την έννοια ένα βήμα περαιτέρω και επιτρέπει την σχεδίαση των group πρωτοκόλλων μέσα σε ένα Piconet.Ένα παράδειγμα θα ήταν να στείλουμε ένα αρχείο mp3 για πραγματικού χρόνου για να το ακούσουν 2 η 3 slaves μέσα σε ένα 7-slave piconet

HCI

Μια από τις πιο κοινές φυσικές υλοποιήσεις Bluetooth είναι υπό μορφή κάρτας ή υπομονάδας που συνδέονται με έναν υπολογιστή host. Όταν διαμορφώνεται με αυτόν τον τρόπο, ο host πρέπει να έχει ένα τρόπο επικοινωνίας με την μονάδα, να περνά εντολές σε αυτή, και να εξασφαλίζει αποτελέσματα. Ο host απαιτεί επίσης μια μέθοδο για να στέλνει στη μονάδα πακέτα δεδομένων για διαβίβαση και για την αποδοχή πακέτων δεδομένων της μονάδας που έχουν παραληφθεί από μια άλλη συσκευή Bluetooth. Η προδιαγραφή Bluetooth περιλαμβάνει μια οντότητα αποκαλούμενη *host controller interface [διεπαφή ελεγκτών οικοδεσποτών]* (HCI) που παρέχει τέτοια επικοινωνία μεταξύ του Host και της μονάδας. Μέσα στη λίστα πρωτοκόλλου Bluetooth, η μονάδα περιέχει συνήθως το ραδιόφωνο, τον ελεγκτή συνδέσεων LC, και το διευθυντή συνδέσεων LM, και το υπόλοιπο της λίστας πρωτοκόλλου από το L2CAP και πάνω ανήκει στον bluetooth- host. Το HCI παρέχει έτσι την επικοινωνία μεταξύ της εφαρμογής και του LM για τη διαχείριση του piconet, το διπλής κατεύθυνσης μεταφοράς πακέτων, και τη μεταφορά πακέτων δεδομένων χρηστών μεταξύ του host και της μονάδας (βλ. το σχέδιο 4-1).

Η υλοποίηση HCI σε ένα σχέδιο Bluetooth δεν απαιτείται για την πιστοποίηση, αλλά είναι σίγουρα μια καλή ιδέα εάν μια μονάδα σχεδιάζεται ώστε να έχει τη συμβατότητα με μια ευρεία ποικιλία των host. Αφ' ετέρου, εάν το Bluetooth είναι μέρος ενός ανεξάρτητου σχεδίου, όπως ένα ραδιοελεγχόμενο παιχνίδι, έπειτα το HCI μπορεί να μην απαιτηθεί καθόλου. Άντ' αυτού, η ραδιοζεύξη Bluetooth και (ίσως) το chipset του ελεγκτή βασικής ζώνης θα επικοινωνήσουν πιθανότατα άμεσα με έναν μικροελεγκτή στον οποίο η λειτουργία της μονάδας θα έχει προγραμματιστεί.

Λειτουργία διεπαφών ελεγκτών οικοδεσποτών (HCI)

Επειδή ο σκοπός του HCI είναι να επικοινωνήσει μεταξύ του host και της μοναδας Bluetooth, πρέπει να λάβει μέτρα για οποιαδήποτε επικοινωνία που μπορεί να απαιτηθεί μεταξύ αυτών των δύο οντοτήτων. Αυτό περιλαμβάνει τον έλεγχο, τα στοιχεία, και τη διπλής κατεύθυνσης σε πραγματικό χρόνο φωνή. Ο HCI σετάρει απλά το πρωτόκολλο για τέτοια επικοινωνία, αλλά ο πραγματικός φυσικός δίαυλος στο οποίο η επικοινωνία πραγματοποιείται μεταξύ του host και της μονάδας Bluetooth μπορεί να είναι μέσα από ένα *universal serial bus* (USB), a *Personal Computer Memory Card International Association* (PCMCIA) ή συμπαγή κάρτα λάμψης, RS- 232 σειριακές επικοινωνίες, ή *universal asynchronous receiver / transmitter*(UART). Η πλήρης υλοποίηση του HCI, έπειτα, απαιτεί τέσσερις πρόσθετες οντότητες στη λίστα πρωτοκόλλου Bluetooth: ένας οδηγός λογισμικού HCI στον host, ένας οδηγός φυσικού διαύλου στον host, ένας οδηγός φυσικού διαύλου στην μονάδα Bluetooth, και HCI firmware στην επίσης στην μονάδα. Ο στόχος του HCI είναι να εξασφαλιστεί ότι ο συγκεκριμένος φυσικός οδηγός που χρησιμοποιείται είναι άσχετος με την επικοινωνία μεταξύ του οδηγού HCI του host και του firmware *host controller*(HC) της μονάδας. Υπό αυτήν τη μορφή, η αλλαγή του μηχανισμού μεταφορών από, για παράδειγμα, USB σε RS- 232 δεν απαιτεί καμία αλλαγή σε HCI και ως εκ τούτου καμία αλλαγή στο σωρό λογισμικού οικοδεσποτών ή firmware της ενότητας.

Επειδή το HCI βρίσκεται και στον host και στην μονάδα bluetooth, είναι σημαντικό να γίνει μια διάκριση μεταξύ των δύο έτσι μπορούν να συζητηθούν χωριστά. Υπό αυτήν τη μορφή, σύμφωνα με την προδιαγραφή Bluetooth και θα αναφέρουμε την οντότητα host ως *οδηγός HCI* και την οντότητα μονάδα ως είτε HC είτε ως *firmware HCI.* Δεν είναι ειρωνικό ότι, αντί ενός καλωδίου που συνδέει τους δύο host για μια συνδεμένη με καλώδιο σύνδεση, έχουμε δύο καλώδια (ή τις συνδέσεις διαύλων) που συνδέουν τους hosts με τις αντίστοιχες μονάδες Bluetooth τους για μια ασύρματη σύνδεση;

RFCOMM

RFCOMM (ένα όνομα που προέρχεται από μια ραδιοσυχνότητα [RF]-προσαρμοσμένη εξομοίωση των σειριακών ports COM σε ένα PC) μιμείται την 9pin RS232 σειριακή επικοινωνία μέσω από ενός καναλιού L2CAP. Στην απλή γλώσσα, αυτό είναι το πρωτόκολλο καλώδιο-αντικατάστασης. RFCOMM επιτρέπει την εξομοίωση RS- 232 ελέγχου και τα σήματα δεδομένων μέσα από το Bluetooth baseband, και παρέχει επίσης τις ικανότητες μεταφορών για upper-level τις υπηρεσίες που ειδάλλως θα χρησιμοποιούσαν μια σειριακή σύνδεση ως μηχανισμό μεταφορών τους.

Είναι βασισμένο στο πρότυπο TS 07.10 για εξομοίωση λογισμικού της διεπαφής υλικού RS232. Το TS 07.10 περιλαμβάνει τη δυνατότητα για πολυπλεξία για αρκετές εξομοιώσεις σειριακών ports επάνω σε μια σύνδεση δεδομένων χρησιμοποιώντας ένα different Data Link Connection Identifierς συνδέσεων στοιχείων (DLCI) για κάθε port. Εντούτοις, κάθε συνεδρίαση TS 07.10 μπορεί να συνδεθεί μέσω ενός καναλιού L2CAP και έτσι μπορεί να επικοινωνήσει μόνο με μια συσκευή Μια κύρια συσκευή πρέπει να έχει χωριστά τις συνεδρίες RFCOMM που τρέχουν για κάθε slave που απαιτεί μια σύνδεση σειριακής port. Αυτό το προηγούμενο πρωτόκολλο, TS 07,10, καθορίστηκε από το ευρωπαϊκό ίδρυμα προτύπων τηλεπικοινωνιών (ETSI), πρώτιστα για τη χρήση με τα φορητά τηλέφωνα GSM.

OBEX

Αντικείμενο-ή αυτά που καλούμε δεδομένα- ανταλλάσσεται χαρακτηριστικά μεταξύ δύο συσκευές που χρησιμοποιούν ένα μοντέλο πελατών/server υπολογιστών. (Δηλαδή οι λειτουργίες μιας συσκευής ως κεντρικός υπολογιστής και "εξυπηρετούν" τα αντικείμενα δεδομένων σε άλλη, πελάτης, συσκευή.) Το Bluetooth έχει υιοθετήσει το πρωτόκολλο ανταλλαγής αντικειμένου (OBEX) που είχε καθοριστεί αρχικά από την υπέρυθρη ένωση στοιχείων (IrDA) για να διευκολύνει την ανταλλαγή των αντικειμένων στοιχείων μεταξύ των διαφορετικών συσκευών.

Το πρωτόκολλο OBEX όχι μόνο επιτρέπει την ανταλλαγή στοιχείων μεταξύ δύο συσκευών, αλλά και καθορίζει ένα φάκελο-ενταγμένο σε λίστα αντικείμενο, το οποίο μπορεί να χρησιμοποιηθεί για να κοιτάξει το περιεχόμενο των φακέλων που κατοικεί σε

μια μακρινή συσκευή. Αυτό το πρωτόκολλο ενισχύεται περαιτέρω από την υιοθέτηση Bluetooth των ικανοποιημένων σχημάτων vCard, vCalendar, vMessage, και vNote, τα οποία είναι ανοικτά πρότυπα που χρησιμοποιούνται για να ανταλλάξουν τις επιχειρησιακές κάρτες, τις προσωπικές ημερολογιακές καταχωρήσεις, τα μηνύματα, και τις σημειώσεις.

PPP

Το από σημείο σε σημείο πρωτόκολλο (PPP), που αναπτυσσόμενο από την Internet Engineering Task Force (IETF), καθορίζει πώς τα Internet Protocol (IP) δεδομένα διαβιβάζονται μέσω των σειριακών από σημείο σε σημείο συνδέσεις. Αυτό το πρωτόκολλο υιοθετείται χαρακτηριστικά στις dial-up Internet συνδέσεις , ή κατά πρόσβαση ενός δρομολογητή δικτύων μέσω μια αφιερωμένη γραμμή.

Στον κόσμο Bluetooth, το PPP τρέχει μέσω του πρωτοκόλλου RFCOMM για να εγκαταστήσει τις από σημείο σε σημείο συνδέσεις μεταξύ των συσκευών Bluetooth. Το πρωτόκολλο PPP χρησιμοποιημένο στην πρόσβαση του τοπικού LAN, Dial-Up Networking, and Fax profiles.

Το PPP αποτελείται ο ίδιος από τρία κύρια συστατικά, δύο από τα οποία είναι πρωτόκολλα σε αυτά . Αυτά τα τρία συστατικά του PPP είναι:

- Ενθυλάκωση
- Πρωτόκολλο ελέγχου συνδέσεων (LCP)
- Πρωτόκολλα ελέγχου δικτύων (NCPS)

TCS Binary

Το Telephony Control Protocol Specification Binary δυαδικό προδιαγραφών πρωτοκόλλου ελέγχου τηλεφωνίας (TCS δυαδικό, αποκαλούμενος επίσης TCSBIN),

είναι βασισμένο στο International Telecommunication Union-Telecommunication standardization Sector (ITU-T) Q.931 πρότυπο για τον έλεγχο κλήσης τηλεφωνίας. Περιλαμβάνει ένα εύρος εντολών σήματος από το group management στην εισερχόμενη ανακοίνωση κλήσης, καθώς επίσης και την ακουστικές καθιερώσεις και τη λήξη σύνδεσης. Χρησιμοποιείται και στα ασύρματα σχεδιαγράμματα τηλεφωνίας και ενδοσυνεννοήσεων.

SDP

Το Service Discovery Protocol πρωτόκολλο ανακαλύψεων υπηρεσιών διαφέρει από όλα τα άλλα στρώματα επάνω από το L2CAP δεδομένου ότι είναι κεντροθετημένο. Δεν έχει ως σκοπό να αλληλεπιδράσει με ένα υπάρχον υψηλότερο πρωτόκολλο στρώματος, αλλά άντ' αυτού εξετάζει μια συγκεκριμένη απαίτηση της λειτουργίας Bluetooth:
να ανακαλύψει ποιες υπηρεσίες είναι διαθέσιμες σε μια συνδεδεμένη συσκευή .Το SDP δρα όπως μια βάση δεδομένων υπηρεσιών Η τοπική εφαρμογή είναι αρμόδια για την εγγραφή των διαθέσιμων υπηρεσιών στη βάση δεδομένων και την ενημέρωση των αρχείων. Οι μακρινές συσκευές μπορούν έπειτα να ρωτήσουν τη βάση δεδομένων για να ανακαλύψουν ποιες υπηρεσίες είναι διαθέσιμες και πώς να συνδέθουν με αυτές Οι λεπτομέρειες της ανακάλυψης υπηρεσιών μπορούν να είναι σύνθετες, αλλά κάθε σχεδιάγραμμα περιγράφει ακριβώς ποιες πληροφορίες πρέπει να καταχωρηθούν με το SDP βασισμένο στην υλοποιηση της εφαρμογής.

WAP

Το ασύρματο πρωτόκολλο εφαρμογής (WAP) χρησιμοποιείται για να εφαρμόσει τις υπηρεσίες Διαδικτύου στα ψηφιακά κυψελοειδή τηλέφωνα και άλλες μικρές ασύρματες συσκευές. Εάν κατέχετε ένα κινητό που επιτρέπει την σύνδεση με internet (συνήθως αποκαλούμενο web phone), γνωρίζετε ότι το WAP είναι το πρωτόκολλο πίσω από το web τηλέφωνο να φυλλομετρά τον Ιστό και να ανακτεί το ηλεκτρονικό ταχυδρομείο και άλλες πληροφορίες βασισμένες στο Internet.

Ανά προδιαγραφές, οι πληροφορίες που στέλνονται στις wap συσκευές πρέπει να παραδοθούν σαν κείμενο, ¨no-frills"' διαμόρφωση που προσαρμόζεται για τις μικρές οθόνες κοινές στις ασύρματες συσκευές. Οι ισόχωροι που προσαρμόζονται για WAP δημιουργούνται με WML (WAP Markup Language), μια έκδοση WAPfriendly του κώδικα HTML.

Κανονικές ιστοσελίδας σημειώσεων αναπτύσσονται με έναν τύπο προγραμματισμού του κώδικα αποκαλούμενο γλώσσα σήμανσης υπερκειμένων (HTML). Η έκδοση του HTML που χρησιμοποιείται για να αναπτύξει wap-φιλικές ιστοσελίδες καλείται WAP Markup Language .

Το WAP, όπως το Bluetooth, έχει μοναδική λίστα πρωτοκόλλου. Τα πρωτόκολλα μοναδικά σε WAP περιλαμβάνουν το ασύρματο περιβάλλον εφαρμογής (WAE, συζήτησε έπειτα), το ασύρματο πρωτόκολλο συνόδου (WSP), το ασύρματο πρωτόκολλο συναλλαγής (WTP), την ασύρματη ασφάλεια στρώματος μεταφορών (WTLS), και το ασύρματο πρωτόκολλο διαγραμμάτων δεδομένων (WDP). Μια καθαρή συσκευή WAP θα χρησιμοποιούσε όλα αυτά τα πρωτόκολλα, καθώς επίσης και UDP/IP και άλλα κοινά πρωτόκολλα.

Όλα τα bluetooth- τηλέφωνα και PDAs που κατασκευάζονται για τη συνδετικότητα Διαδικτύου ενσωματώνουν WAP.

PROFILES

Η λειτουργία που υποτίθεται ότι εκπληρώνει μια Bluetooth συσκευή είναι βασισμένη πάνω στο μοντέλο χρήσης , που είναι ένα πραγματικό μοντέλο που ο κάθε πελάτης αναμένει από αυτή τη συσκευή(τα μοντέλα περιγράφονται παρακάτω). Συνοπτικά τα μοντέλα είναι:

- 3 σε 1 τηλέφωνο
- headset
- internet bridge
- Data access point
- Object push

- File transfer
- Automatic synchronization

Αλλά μοντέλα χρήσης έχουν προστεθεί σαν τις ικανότητες του Bluetooth που ταιριάζουν σε αλλά πεδία όπου μια ασύρματη σύνδεση θα ήταν ένα λογικό μέσω για επικοινωνία Μεταξύ αυτών είναι:

- Human interface device(HID)
- Διανομή Audio/video
- Απομακρυσμένος έλεγχος Audio/video
- Basic printing
- Basic imaging
- Hardcopy cable replacement
- Personal area network(PAN)
- Operating a phone via an in-car device

Αυτά όλα τα μοντέλα χρήσης δεν αποτελούν μέρος της προδιαγραφής Bluetooth. Αντιθέτως ένα σετ από προφίλ έχε καθιερωθεί που δίνουν στις συσκευές την προσωπικότητα τους. Θέλουμε η συσκευή να είναι HS(headset)? Χρησιμοποιούμε το HS προφιλ. Ένα ποντίκι? Χρησιμοποιούμε το HID profile.
Ο σκοπός ύπαρξης ενός Bluetooth profil είναι:

1. Μειώνει των αριθμό επιλογών και ορίζει τις παραμέτρους σύμφωνα με τα πρωτόκολλα
2. Ορίζει την σειρά με την οποία οι διαδικασίες συνδυάζονται
3. Παρέχει κοινή εμπειρία χρηστή σε συσκευές διαφορετικών κατασκευαστών

ΓΕΝΙΚΑ ΠΡΟΦΙΛ

Τα πρώτα δύο profile Bluetooth καλούνται γενικά , επειδή είναι απαραίτητα σε όλες τις μορφές επικοινωνίας Bluetooth. Αντίθετα από μερικά profile που είναι περισσότερο δεμένα σε συγκεκριμένα μοντέλα χρήσης , τα γενικά σχεδιαγράμματα αναμένονται να υλοποιηθούν από όλες τις συμβατές συσκευές Bluetooth.

Γενικό profile πρόσβασης (GAP)

Το GAP καθορίζει τις γενικές διαδικασίες σχετικές με την ανακάλυψη, τη διαχείριση συνδέσεων, και τη χρήση των επιπέδων ασφάλειας για τις Bluetooth- συσκευές. Επίσης καθορισμένο στο προφίλ είναι οι απαιτήσεις τυποποιήσεις για μερικές από τις παραμέτρους όπου ο χρήστης μπορεί να έχει πρόσβαση. Αυτό το προφίλ πρέπει να περιληφθεί με όλες τις Bluetooth συσκευές που δεν απαιτούν την προσαρμογή σε οποιοδήποτε προφίλ, ή εάν η συσκευή πρόκειται να εκτελέσει μια συνηθισμένη εφαρμογή. Εάν η bluetooth συσκευή προσαρμοστεί σε ένα άλλο profile, τοτε τα τροποποιημένα τμηματα του GAP θα λιστοποιηθουν σε εκείνο το profile.

Ένα μεγάλο μέρος του GAP ειναι αφιερώμενο στον καθορισμό των όρων που χρησιμοποιούνται ως τμήμα του λεξιλογίου Bluetooth, συμπεριλαμβανομένων εκείνων των όρων που υιοθετούνται στο επίπεδο διεπαφης *με τον χρήστη user interface*(UI). Παραδείγματος χάριν, το α-συμβαλλόμενο μέρος ορίζεται ως η συσκευή σελιδοποίησης όταν καθιερώνεται η σύνδεση ή ο ιδρυτής μιας διαδικασίας σε μια ήδη-καθιερωμένη σύνδεση. Το β-συμβαλλόμενο μέρος είναι η σελιδοποιημένος συσκευή ή ο αποδέκτης της διαδικασίας. Ακόμα κι αν οι δύο συσκευές δεν έχουν καμία λειτουργία από κοινού και δεν μπορούν ενδεχομένως να λειτουργήσουν μαζί (όπως το HS και ο εκτυπωτής), πρέπει αυτές να είναι ικανές να συνδεθούν τουλάχιστον μέσω μιας σύνδεσης Bluetooth και να ανακαλύψουν την ασυμβατότητα τους. Ο προσεκτικός καθορισμός και η χρήση των διάφορων όρων UI πρέπει να μειώσουν την πιθανότητα ότι ένα κακώς γραπτό εγχειρίδιο οδηγίας θα εισαγάγει την αγορά.

Οι βασικές αρχές σχεδιαγράμματος GAP είναι :

- Δήλωση των αναγκών για τον καθορισμό και τη χρήση των ονομάτων, τιμών, και σχέδια κωδικοποίησης
- Καθορίζει τις γενικές διαδικασίες για την ανακάλυψη της ταυτότητα, το όνομα, και τις βασικές ικανότητες μιας άλλης ανακαλύψιμης bluetooth- συσκευής
- Καθορίζει τις γενικές διαδικασίες σύνδεσης
- Περιγράφει τις γενικές διαδικασίες που χρησιμοποιούνται περιγράφοντας για την εγκατάσταση μιας σύνδεσης σε μια άλλη συνδέσιμη bluetooth- συσκευή

Επιπλέον το GAP καθορίζει διάφορες λειτουργικές καταστάσεις των Bluetooth συσκευων. Αυτες καθορίζουν την ικανότητα ανακάλυψης συσκευών, την ικανότητα σύνδεσης και paring modes της συσκευης. Ποιο αναλυτικά :

Οι τρόποι ανακαλύψεων Το GAP καθορίζει τρεις διαφορετικούς τρόπους για την ανακάλυψη συσκευών: *γενικός ανακαλύψιμοι* (συνεχώς διαθέσιμος σε άλλες συσκευές), *περιορισμένοι ανακαλύψιμος* (διαθέσιμος μόνο για μια περιορισμένη χρονική περίοδο ή υπό συγκεκριμένων όρων), και *nondiscoverable* (μη διαθέσιμος σε άλλες συσκευές).
Οι τρόποι συνδετικότητας Το GAP καθορίζει τις πολιτικές για την καθιέρωση των επικοινωνιών συσκευών, χρησιμοποιώντας του ενός από δύο τρόπους: *connectable* (θα αποκριθεί στη σελιδοποίηση) ή *nonconnectable* (δεν θα αποκριθεί στη σελιδοποίηση).
Τρόπος ένωσης Είναι μια διαδικασία έναρξης όπου δύο συσκευές καθιερώνουν ένα κοινό κλειδί συνδέσεων για την επόμενη πιστοποίηση, υπάρχουν δύο διαφορετικοί τρόποι ένωσης, *ένωση* (δέχεται την ένωση) ή (δεν δέχεται την ένωση).

Service Discovery Application Profile (SDAP)

Η προδιαγραφή Bluetooth περιλαμβάνει περιεκτικά μέσα για μια συσκευή που ψάχνει για τις υπηρεσίες που είναι διαθέσιμες σε μια άλλη συσκευή. Το SDAP λειτουργεί μέσω του sdp, το οποίο παρέχει την ικανότητα για μια άλλη συσκευή να ανακαλυφθεί, ποιες υπηρεσίες είναι διαθέσιμες και να καθορίσει τα χαρακτηριστικά αυτών των υπηρεσιών. Το πρωτόκολλο είναι βασισμένο στο κλασικό πρότυπο client/server, όπου ο πελάτης θέλει να έχει πρόσβαση στις υπηρεσίες που παρέχονται στον κεντρικό υπολογιστή. Ο

πελάτης ρωτά τον κεντρικό υπολογιστή υπό μορφή αιτημάτων, και ο κεντρικός υπολογιστής ανταποκρίνεται στα αιτήματα με πληροφορίες.

Τα περισσότερα σχεδιαγράμματα Bluetooth έχουν ένα σχετικά στενό SDP πεδίο, όπως η ανάκτηση των πληροφοριών που απαιτούνται για να οργανώσουν μια υπηρεσία μεταφοράς ή σενάριο χρήσης . Το SDP αρχίζει συχνά αυτόματα σε αυτές τις περιπτώσεις, και οι απαραίτητες πληροφορίες ανακτώνται χωρίς αλληλεπίδραση χρηστών. Αντίθετα, το SDAP προορίζεται να αρχίσει από έναν ανθρώπινο χρήστη και επιτρέπει την εκτενή έρευνα για τις υπηρεσίες σε μια συσκευή πελατών. Ένα παράδειγμα θα ήταν να είχαμε πρόσβαση σε έναν κατάλογο καρτών βιβλιοθηκών ή ένα σύνολο οικονομικών βάσεων δεδομένων.

Η επισκόπηση SDP Το SDP μπορεί να χρησιμοποιηθεί για να έχει πρόσβαση σε μια συγκεκριμένη συσκευή (όπως μια ψηφιακή φωτογραφική μηχανή) και να ανακτήσει τις ικανότητές της ή για να έχει πρόσβαση σε μια συγκεκριμένη εφαρμογή (όπως η εργασία τυπωμένων υλών) και να βρει τις συσκευές που υποστηρίζουν εκείνη την εφαρμογή. Ο προηγούμενος στόχος απαιτεί μια συσκευή και μια σύνδεση ACL για να ανακτήσει τις επιθυμητές πληροφορίες, και ο τελευταίος περιλαμβάνει τη σύνδεση με και την ανάκτηση των πληροφοριών από διάφορες συσκευές που ανακαλύπτονται μέσω μιας έρευνας.

Το SDP υποστηρίζει τα εξής:

- Φυλλομέτρημα για τις υπηρεσίες σε μια ιδιαίτερη συσκευή
- Έρευνα για και ανακάλυψη των υπηρεσιών που εδρεύουν επάνω στις επιθυμητές ιδιότητες
- Επαυξητικά ψάχνοντας την λίστα υπηρεσιών μιας συσκευής για να περιορίσει το ποσό των δεδομένων που θα ανταλλαχθεί

Η ανακάλυψη υπηρεσιών που χρησιμοποιεί SDAP το SDAP διευκρινίζει τις λειτουργίες που εκτελούνται και από τις δύο συσκευές που συμμετέχουν στην ανακάλυψη των υπηρεσιών. Ο πρώτη είναι η *τοπική συσκευή* (LocDev), η οποία είναι η συσκευή που κινεί τη διαδικασία ανακαλύψεων υπηρεσιών και περιέχει και SDAP και τα

τμήματα πελατών από SDP. Η δεύτερη είναι η *μακρινή συσκευή* (RemDev) που αποκρίνεται στις υπηρεσίες ερευνών της LocDev μέσω του κεντρικού(server) υπολογιστή της SDP.Ανάλογα με το περιβαλλον, η LocDev και η RemDev μπορούν τελικά να ανταλλάξουν τους ρόλους ή να υποθέσουν διαφορετικούς ρόλους, ανάλογα με τις ανάγκες και τις ικανότητές τους. Εντούτοις, για να είναι κατάλληλη ως LocDev, η συσκευή πρέπει να έχει ένα UI αποτελέσματα για την είσοδο των υπηρεσιών απαιτήσεων και ίσως της επιστροφής των αναζητήσεων υπηρεσιών.

Φυσικά, ενώπιον των υπηρεσιών μπορεί να αναζητηθεί ή να φυλλομετρηθεί, το LocDev και το RemDev πρέπει πρώτα να δημιουργήσουν μια σύνδεση ACL και να ολοκληρώσουν οποιεσδήποτε απαραίτητες πιστοποίηση και κρυπτογράφηση. Εντούτοις, καμία υπόθεση δεν γίνεται ως προς το εάν η LocDev ή η RemDev είναι ο master στο piconet, και το profile δεν απαιτεί την επικύρωση ή την κρυπτογράφηση για τη χρήση του αυτός μέχρι την ιδιαίτερη υλοποίηση.

ΤΑ ΥΠΟΛΟΙΠΑ PROFILE

ΒΑΣΙΣΜΕΝΑ ΣΕ ΣΕΙΡΙΑΚΗΣ ΘΥΡΑΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

- Serial porrt profile
- Dial-up Networking(DUN)
- LAN access
- FAX
- Headset(HS)
- Hands free(HF)
- Video conferencing

ΒΑΣΙΣΜΕΝΑ ΣΤΗΝ ΑΝΤΑΛΛΑΓΗ ΑΝΤΙΚΕΙΜΕΝΩΝ

- Object Push
- File Transfer
- Synchronization

- Basic Printing
- Basic Imaging

ΠΡΟΦΙΛ ΤΗΛΕΦΩΝΙΑΣ

- Coldless Telephny
- Intercom

AUDIO/VIDEO ΠΡΟΦΙΛ

- Advanced audio Distribution
- Video Distribution

ΔΙΑΦΟΡΑ ΠΡΟΦΙΛ

- Audio/Video Remote Control
- Human Interface Device
- Hardcopy Cable Replacement
- Personal Area Networking (PAN)
- Common ISDN Access

ΣΧΗΜΑ 4-4. Απαιτησεις επιπεδων του bluetooth stack απο τα profil

Profile	Lower Layers	L2CAP	SDP	RFCOMM	PPP	OBEX	TCS-Bin
Service Discovery Application	X	X	X				
Cordless Telephony	X	X	X				X
Intercom	X	X	X				X
Serial Port	X	X	X	X			
Headset	X	X	X	X			
Dial-up Networking	X	X	X	X			
FAX	X	X	X	X			
LAN Access	X	X	X	X	X		
Generic Object Exchange	X	X	X			X	
Object Push	X	X	X			X	
File Transfer	X	X	X			X	
Synchronization	X	X	X			X	

ΚΕΦΑΛΑΙΟ 5
ΑΣΦΑΛΕΙΑ

ΕΙΣΑΓΩΓΗ

Επειδή το Bluetooth είναι ένα ασύρματο σύστημα επικοινωνιών υπάρχει μια βέβαιη πιθανότητα ότι οι μεταδόσεις της θα μπορούσαν να παρεμποδιστούν σκόπιμα ή να φραχτούν, ή ψεύτικες πληροφορίες να περάσουν στα μέλη του piconet. Για να παρέχει την προστασία χρήσης για το piconet, το σύστημα πρέπει να καθιερώσει την ασφάλεια σε διάφορα επίπεδα πρωτοκόλλου. Αντίθετα από πολλά πρωτόκολλα δικτύων που αφήνουν το ζήτημα της ασφάλειας μέχρι τις συνημμένες υπομονάδες λογισμικού, το Bluetooth προσφέρει τα ενσωματωμένα μέτρα ασφάλειας στο επίπεδο συνδέσεων.

Σαν ένα ad hoc δίκτυο, οι συσκευές Bluetooth υπόκεινται στις ανάγκες ασφάλειας πέρα από αυτό που απαιτείται κανονικά για τα ενσύρματα είτε για τα συγκεντρωμένα ασύρματα δίκτυα. Οι ενσύρματες συνδέσεις παράγουν ακτινοβολία όταν στέλνονται οι πληροφορίες από τη μια άκρη στην άλλη, αλλά η απόσταση είναι χαρακτηριστικά πολύ σύντομη. Κατά συνέπεια, υπάρχει συνήθως περισσότερη έμφαση στην διαβεβαίωση ότι οι χρήστες έχουν πιστοποιηθεί κατάλληλα απ'ό,τι στην παρεμπόδιση της μακρινής αναχαίτισης των δεδομένων. Τα συγκεντρωμένα ασύρματα δίκτυα, όπως το 802.11, λειτουργούν γενικά με μια κεντρική βάση δεδομένων των οντοτήτων ασφάλειας όπως οι κωδικοί πρόσβασης και τα κλειδιά. Φυσικά, εάν αυτή η βάση δεδομένων εκθέτονταν, οι συνέπειες θα μπορούσαν να ήταν καταστρεπτικές, αλλά η προστασία μιας ενιαίας βάσης δεδομένων είναι γενικά ευκολότερη από τη φρούρηση διαφορετικών βάσεων δεδομένων που διανέμονται σε ένα ειδικό δίκτυο(ad hoc).

Οι απειλές στα διανεμημένα δίκτυα μπορούν να διαιρεθούν κατά προσέγγιση σε 3 κατηγορίες που αυτές είναι:

Αποκάλυψη πληροφοριών Διαρροή των πληροφοριών από το σύστημα σε έναν που δεν έχει την έγκριση για να έχει πρόσβαση στις πληροφορίες.

Ακεραιότητα δεδομένων Σκόπιμη αλλαγή των πληροφοριών για να παραπλανηθεί ο παραλήπτης.

Άρνηση των υπηρεσιών (DoS) Μπλοκάροντας την είσοδο σε μια υπηρεσία, καθιστώντας το μη διαθέσιμο ή να περιορίσει τη διαθεσιμότητά του σε εξουσιοδοτημένους χρήστες.

Επειδή τα ειδικά δίκτυα δεν έχουν καμία συγκεντρωμένη υποδομή, τα ζητήματα ασφάλειας πρέπει να διανεμηθούν επίσης. Υπάρχουν μερικές συγκεκριμένες εξαιρέσεις σε αυτόν τον κανόνα, όπως ένα σημείο πρόσβασης Διαδικτύου που μπορεί να αρχίσει την ασφάλεια από μια κεντρική βάση δεδομένων για κάθε συνδεδεμένο χρήστη, αλλά ως επί το πλείστον οι συσκευές Bluetooth που συνδέονται η μια με την άλλη θα εφαρμόσουν την ασφάλεια χωρίς την επέμβαση οποιουδήποτε τρίτου manager.

Επισκόπηση της ασφάλειας Bluetooth

Η ασφάλεια μέσα στο Bluetooth καλύπτει τρεις σημαντικές περιοχές: επικύρωση, έγκριση(εξουσιοδότηση), και κρυπτογράφηση. Η διαδικασία *της [authentication] επικύρωσης* αποδεικνύει την ταυτότητα ενός μέλους piconet σε άλλο. Τα αποτελέσματα της εξουσιοδότησης χρησιμοποιείται για τον καθορισμό *της έγκρισης* ενός πελάτη για να έχει πρόσβαση στις διάφορες υπηρεσίες σε έναν server. Η διαδικασία *της κρυπτογράφησης* χρησιμοποιείται για να κωδικοποιήσει τις πληροφορίες που ανταλλάσσονται μεταξύ των συσκευών έτσι ώστε οι μη αδειοδοτημένοι (ακόμη και άλλα μέλη του ίδιου piconet) δεν μπορούν να διαβάσουν το περιεχόμενό του. Αυτές οι τρεις διαδικασίες ασφάλειας εφαρμόζονται μέσα σε διάφορα στρώματα της λίστας πρωτοκόλλου του Bluetooth. Παραδείγματος χάριν, ο ελεγκτής συνδέσεων έχει την ικανότητα παραγωγής τυχαίων αριθμών και περιλαμβάνει τις μεθόδους για τα κλειδιά ασφάλειας και τις μαθηματικές διαδικασίες για την εξουσιοδότηση και την κρυπτογράφηση. Το LM περιλαμβάνει διάφορες εντολές για το χειρισμό των ζητημάτων ασφάλειας, και το L2CAP μπορεί να κινήσει τις διαδικασίες ασφάλειας όταν γίνεται μια προσπάθεια σύνδεσης καναλιών. Το HCI χειρίζεται την ασφάλεια επικοινωνίας μεταξύ

του host και της μονάδας Bluetooth, και διάφορα υψηλότερα πρωτόκολλα περιγράφουν τις συγκεκριμένες απαιτήσεις για την εφαρμογή τους.

ΕΠΙΠΕΔΑ ΑΣΦΑΛΕΙΑΣ

Το *generic access profile* (GAP) διευκρινίζει πώς η ασφάλεια Bluetooth οργανώνεται. Η ασφάλεια αρχίζει όταν αποφασίσει ένας χρήστης πώς μια συσκευή θα εφαρμόσει τις επιλογές της ανακάλυψης και του connectability. Οι διαφορετικοί συνδυασμοί αυτών των ικανοτήτων μπορούν να διαιρεθούν σε τρεις γενικές κατηγορίες:

- **Silent** Η συσκευή δεν θα μπει ποτέ στις καταστάσεις PAGE SCAN ή INQUIRY SCAN , και έτσι δεν θα δεχτεί οποιεσδήποτε συνδέσεις. Η συσκευή ελέγχει απλά την κυκλοφορία Bluetooth.
- **Private** Η συσκευή θα μπει περιοδικά στο κράτος PAGE SCAN, αλλά δεν θα μπαίνει ποτέ στο INQUIRY SCAN, έτσι η συσκευή δεν μπορεί να ανακαλυφθεί. Οι συνδέσεις θα γίνονται αποδεκτές εάν η BD_ADDR της συσκευής είναι γνωστή από τον ενδεχόμενο κύριο κατά τη διάρκεια του PAGE.
- **Public** Η συσκευή εισάγεται περιοδικά και στην INQUIRY and PAGE SCAN, έτσι ώστε να μπορεί να ανακαλυφθεί και να συνδεθεί.

Το GAP αναφέρεται στις καταστάσεις discoverability της συσκευής, το connectability, και (pairing) ένωσης στο περιβάλλον είτε είναι σεταρισμενα για τη σιωπηλή, ιδιωτική, ή δημόσια δυνατότητα πρόσβασης.

Τα επίπεδα ασφάλειας καθορίζονται για πολλά διαφορετικά σενάρια που περιλαμβάνουν τις δημόσιες ή ιδιωτικές συσκευές και τις υπηρεσίες που παρέχουν. Το GAP καθορίζει τρεις διαφορετικούς τρόπους ασφάλειας που μια συσκευή μπορεί να εφαρμόσει. Είναι :

- **Mode 1 (nonsecure)** Μια συσκευή δεν θα ξεκινήσει κανένα μέτρο ασφάλειας, έτσι η επικοινωνία πραγματοποιείται χωρίς την πιστοποίηση ή κρυπτογράφηση.
- **Mode 2 (service-level enforced security)** Δύο συσκευές μπορεί να εγκαταστήσουν μια σύνδεση ACL με τρόπο nonsecure. Οι διαδικασίες ασφάλειας κινούνται όταν ενα καναλι L2CAP υποβάλλει αίτημα
- **Mode 3 (link-level enforced security)** Διαδικασίες ασφάλειας ξεκινούν όταν καθιερώνεται μια σύνδεση ACL.

Μια συσκευή που χρησιμοποιεί το επίπεδο ασφάλειας mode 2 θα κινήσει τις διαδικασίες ασφάλειας όταν παραλαμβάνεται ένα L2CAP_ConnectReq που συνδέεται με ένα κανάλι που απαιτεί την ασφάλεια. Τα μέτρα ασφάλειας ολοκληρώνονται προτού να επιστραφεί L2CAP_ConnectRsp. Οι απαιτήσεις ασφάλειας αυτού του καναλιού θα μπορούσαν να περιλάβουν την πιστοποίηση, έγκριση, και ίσως την κρυπτογράφηση, και τα διαφορετικά κανάλια μπορούν να έχουν διαφορετικές απαιτήσεις ασφάλειας. Για τον mode 3, οι διαδικασίες ασφάλειας κινούνται όταν λαμβάνεται το LMP_hostconnection_req και ολοκληρώνονται προτού να σταλεί το LMP_setup_complete.

Ο τρόπος 2 είναι πιθανώς ο πιο εύκαμπτος τρόπος να εφαρμοστεί η ασφάλεια σε μια συσκευή Bluetooth. Παραδείγματος χάριν, ένας πελάτης θα μπορούσε να συνδεθεί με έναν server με μια σύνδεση ACL,ακολουθούμενη από ένα κανάλι L2CAP, για να φυλλομετρήσει τις υπηρεσίες χωρίς την ανάγκη για ασφάλεια. Όταν μια προσπάθεια γίνεται για να έχουμε πρόσβαση σε μια υπηρεσία, κατόπιν η πιστοποίηση, που ακολουθήθηκε από έναν έλεγχο έγκρισης, θα μπορούσε να απαιτηθεί προτού να χορηγηθεί η πρόσβαση.

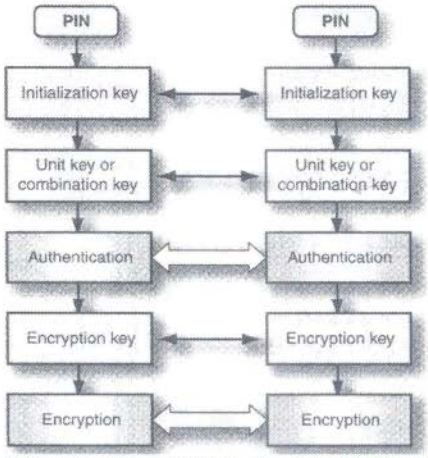
Περίληψη των διαδικασιών ασφάλειας Bluetooth

Το πρόβλημα ασφάλειας απαιτεί γενικά την ικανότητα μιας συσκευής να ελέγξει την ταυτότητα μιας άλλης συσκευής (πιστοποίηση) με έναν τρόπο που δεν παρέχει οποιεσδήποτε χρήσιμες πληροφορίες σε έναν τρίτο, ούτε επιτρέπει μια πρόσβαση τρίτων μέσω αναρμόδιας πιστοποίησης. Επιπλέον, τα δεδομένα κρυπτογράφησης θα

μπορούσαν να είναι πιθανά, πάλι όμως χωρίς την παροχή πληροφοριών σε έναν τρίτο που θα βοηθούσε να σπάσει τον κώδικα κρυπτογράφησης.

Η φιλοσοφία πίσω από την ασφάλεια Bluetooth είναι να χτίσει μια αλυσίδα γεγονότων, τα οποία να μην παρέχουν τις σημαντικές πληροφορίες σε έναν τρίτο(ωτακουστή), αλλά όλα να εμφανιστούν σε μια συγκεκριμένη ακολουθία για την ασφάλεια που οργανώνεται επιτυχώς. Το ακόλουθο παράδειγμα ισχύει για την από σημείο σε σημείο ασφάλεια, όπου ένας MASTER επικοινωνεί με έναν μόνο SLAVE. Οι συσκευές αρχίζουν με έναν κοινό *προσωπικό αριθμό αναγνώρισης* (PIN), αποκαλούμενη επίσης *passkey* Bluetooth, επάνω στο οποίο "χτίζονται" διάφορα 128-bit κλειδιά . Το PIN χρησιμοποιείται για να δημιουργήσει ένα *κλειδί έναρξης*, και αυτό το κλειδί στη συνέχεια χρησιμοποιείται για να δημιουργήσει ένα *κλειδί συνδέσεων*, το οποίο μπορεί να είναι ένα unit key (για τις συσκευές με τους περιορισμένους πόρους) ή ένα combination key (για τις περισσότερες συσκευές). Το κλειδί συνδέσεων γίνεται μέρος της διαδικασίας πιστοποίησης. Εάν η κρυπτογράφηση είναι επιθυμητή, το κλειδί συνδέσεων χρησιμοποιείται για να παραγάγει ακόμα ένα κλειδί αποκαλούμενο *κλειδί κρυπτογράφησης*.

Το σχήμα 5-1 παρουσιάζει την ακολουθία γεγονότων που οδηγούν στα ενδεχόμενη δημιουργία του κλειδιού κρυπτογράφησης. Κατά τη διάρκεια της δημιουργίας του κλειδιού και της πιστοποίησης, οι συσκευές διαβιβάζουν τυχαίους αριθμούς η μια στην άλλη που δεν παρέχουν καμία πληροφορία σε έναν ωτακουστή. Κατά την διάρκεια που και οι δύο συσκευές αρχίζουν με το ίδιο PIN, θα παραγάγουν κανονικά το ίδιο κλειδί έναρξης, το κλειδί πιστοποίησης (σύνδεση), και το κλειδί κρυπτογράφησης.



ΣΧΗΜΑ 5.1 Για να εντείνουμε την ασφάλεια, οι συσκευές Bluetooth χρησιμοποιούν μια αλυσίδα γεγονότων για να δημιουργήσουν διάφορα κλειδιά χρησιμοποιούμενα από την πιστοποίηση και την κρυπτογράφηση. Κάθε νέο κλειδί εξαρτάται από την τιμή του προηγούμενου κλειδιού

ΠΙΣΤΟΠΟΙΗΣΗ

Η πιστοποίηση είναι η διαδικασία της γνωστοποίησης ταυτότητας της συσκευής στο άλλο άκρο μιας σύνδεσης. Ο *ελεγκτής* ρωτά τον *ενάγοντα* και ελέγχει την απάντησή του εάν είναι σωστή, και τότε η επικύρωση είναι επιτυχής. Φυσικά, οποιοσδήποτε μπορεί σε απόσταση ακοής να λάβει τις κωδικοποιημένες λέξεις, έτσι σε αυτήν την κατάσταση η ασφάλεια βεβαιώνεται μόνο για μια one-time επικύρωση.

ΕΞΟΥΣΙΟΔΟΤΗΣΗ

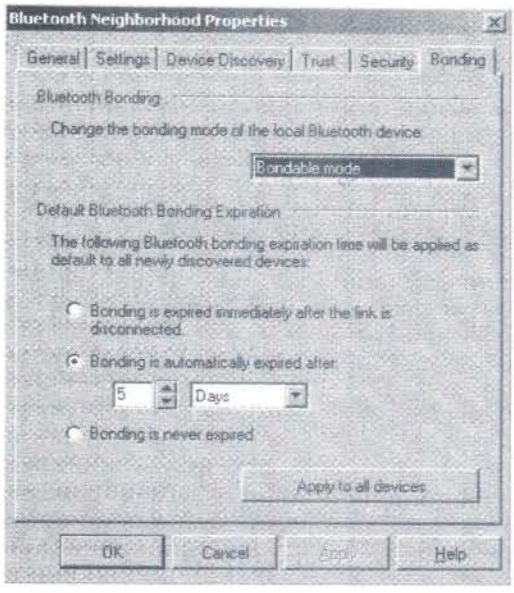
Σε ένα χαρακτηριστικό σενάριο πελατών εξυπηρετητών, ο πελάτης συνδέετε με τον server και απαιτεί χρήση των υπηρεσιών του όπως είναι οι πληροφορίες αρχείων ή η πρόσβαση στο Διαδικτύου. Σε αυτό το σενάριο, ο server παίρνει το ρόλο του ελεγκτή και ο πελάτης του ενάγοντος. Μόλις πιστοποιηθεί επιτυχώς ο πελάτης στον server, παραχωρείται πρόσβαση στις υπηρεσίες που εδρεύουν στο επίπεδο έγκρισής του. Η έγκριση μπορεί να εφαρμοστεί με διάφορους τρόπους:

- Η πρόσβαση χορηγείται σε όλες τις υπηρεσίες.
- Η πρόσβαση χορηγείται σε ένα υποσύνολο των υπηρεσιών.
- Η πρόσβαση χορηγείται σε μερικές υπηρεσίες όταν η επικύρωση είναι επιτυχής, αλλά η περαιτέρω πρόσβαση απαιτεί την πρόσθετη επικύρωση βασισμένη σε κάποιο χρήστη που εισάγεται στη συσκευή πελατών.

Το τελευταίο υλοποιείται συνήθως στο στρώμα εφαρμογής και περιλαμβάνει τη μεσολάβηση μιας *εξωτερικής οντότητας ελέγχου ασφάλειας [external security control entity* (ESCE)]. Αυτός είναι συνήθως ανθρώπινος χειριστής που αποφασίζει πώς να συνεχίσει με ένα σχετικό με την ασφάλεια θέμα. Εν πάση περιπτώσει, η έγκριση μπορεί να εφαρμοστεί από έναν διευθυντή ασφάλειας που αλληλεπιδρά με διάφορα στρώματα πρωτοκόλλου επάνω από HCI

PAIRING, BONDING, TRUST

Οι έννοιες της ένωσης, της σύνδεσης, και της εμπιστοσύνης είναι μερικές φορές θολωμένες στις διάφορες δημοσιεύσεις για την ασφάλεια Bluetooth. Αυτό οφείλεται συχνά στο γεγονός ότι οι μέθοδοι ασφάλειας διαφέρουν, ανάλογα με την κατάσταση και τους τύπους συσκευών που λειτουργούν.



ΣΧΗΜΑ 5-2

Pairing Δύο συσκευές γίνονται *ζευγάρι* όταν αρχίζουν με το ίδιο PIN και παράγουν το ίδιο κλειδί συνδέσεων, και χρησιμοποιούν έπειτα αυτό το κλειδί για την πιστοποίηση τουλάχιστον της παρούσας συνόδου επικοινωνίας. Η συνεδρία μπορεί να υπάρξει για τη ζωή μιας σύνδεσης L2CAP (για τον τρόπο 2 ασφάλειας) ή τη ζωή της σύνδεσης ACL (για τον τρόπο 3 ασφάλειας). Η ένωση μπορεί να εμφανιστεί μέσω μιας αυτόματης διαδικασίας επικύρωσης εάν και οι δύο συσκευές έχουν ήδη το ίδιο αποθηκευμένο PIN από το οποίο μπορούν να αντλήσουν τα ίδια κλειδιά συνδέσεων για την πιστοποίηση. Εναλλακτικά, καθεμία ή και οι δύο εφαρμογές μπορούν να ρωτήσουν τους αντίστοιχους χρήστες τους για τη χειρωνακτική είσοδο του PIN.

Bonding Μόλις ζευγαρωθούν οι συσκευές μπορούν είτε να αποθηκεύσουν τα κλειδιά συνδέσεών τους για τη χρήση σε επόμενες πιστοποιήσεις είτε να τα απορρίψουν και να επαναλάβουν τη διαδικασία ένωσης κάθε φορά που συνδέονται. Εάν τα κλειδιά συνδέσεων αποθηκεύονται, κατόπιν οι συσκευές bonded, επιτρέπουν τις μελλοντικές πιστοποιήσεις που θα εμφανιστούν να χρησιμοποιήσουν τα ίδια κλειδιά συνδέσεων και χωρίς απαίτηση του χρήστη να εισαγάγει το PIN πάλι. Το σχήμα 5-2 παρουσιάζει τις

bonding επιλογές που περιλαμβάνονται με μια εμπορική εφαρμογή λογισμικού. Η σύνδεση μπορεί να λήξει αμέσως αφότου αποσυνδέεται (μη bonded), ή λήγει μετά από ένα ορισμένο χρονικό διάστημα (προσωρινά δεσμευμένο), ή ποτέ (μόνιμα συνδεμένο). Όταν το bonding λήγει, οι συσκευές πρέπει να περάσουν από τη διαδικασία pairing πάλι.

Η απόφαση εάν πρέπει να γίνουν bond οι συσκευές είναι βασισμένη στο σχετικό ρίσκο της αποθήκευσης του κλειδιού συνδέσεων ενάντια στην επανάληψη του pairing κάθε φορά που συνδέονται οι συσκευές. Όταν οι συσκευές εκτελούν το pairing, υπάρχει μια πιθανή τρωτή περίοδος όταν χρησιμοποιούνται τα PINs για να διαμορφώσουν τα αρχικά κλειδιά, κατά την διάρκεια της οποίας στέλνεται ένας τυχαίος αριθμός μέσω του αέρα από μια συσκευή σε άλλη. Ένας τρίτος θα μπορούσε να παρεμποδίσει τον τυχαίο αριθμό, να υποθέσει το pin, και έπειτα ενδεχομένως να αντλήσει ένα από τα κλειδιά συνδέσεων. Ένα PIN είναι συχνά πολύ μικρότερο από το 128-bit κλειδί συνδέσεων και μπορεί να βρεθεί ευκολότερα.

Αφ' ετέρου, η αποθήκευση ενός κλειδιού συνδέσεων, είτε στον host είτε στην ίδια τη Bluetooth μονάδα, έχει τους κινδύνους του εάν ο host και η μονάδα Bluetooth δεν ασφαλίζονται με φυσικό τρόπο κατά τη μη χρησιμοποίηση τους. Ένας εισβολέας με την πρόσβαση στον host ή την μονάδα μπορεί να είναι σε θέση να "κατεβάσει" τα αποθηκευμένα κλειδιά συνδέσεων και να τα χρησιμοποιήσει για αναρμόδια πιστοποίηση ή την αποκρυπτογράφηση των αρχείων.

Trust Η έννοια *της εμπιστοσύνης* ισχύει για την έγκριση μιας συσκευής για να προσεγγιστούν ορισμένες υπηρεσίες σε μια άλλη συσκευή. Μια συσκευή εμπιστοσύνης πιστοποιείται προηγουμένως και, βασισμένη σε εκείνη την πιστοποίηση, έχει την έγκριση για να έχει πρόσβαση στις διάφορες υπηρεσίες. Μια untrusted συσκευή μπορεί να πιστοποιηθεί, αλλά η περαιτέρω δράση απαιτεί την επέμβαση των χρηστών με έναν κωδικό πρόσβασης, προτού να χορηγηθεί η έγκριση στις υπηρεσίες πρόσβασης. Η επέμβαση των χρηστών δεν καθιερώνει απαραιτήτως την εμπιστοσύνη, έτσι ένας άλλος κωδικός πρόσβασης μπορεί να απαιτηθεί κάθε φορά που η υπηρεσία πρέπει ν προσπελαστεί.

Ένα εμπορικό πακέτο λογισμικού Bluetooth μπορεί να είναι μια απλή προσέγγιση που δίνει στο χρήστη την επιλογή να δέχεται όλες τις συνδέσεις (που εμπιστεύονται τη

καθεμία), να απορρίπτει όλες τις συνδέσεις (που δεν εμπιστεύονται καμία), ή να κληθεί να δεχτούν ή να απορρίψουν κάθε εισερχόμενη σύνδεση καθώς φθάνει (επιλέγοντας ποιων να εμπιστευθούν). Αυτή η ιδιαίτερη εφαρμογή της εμπιστοσύνης είναι σφαιρικής φύσης, που ισχύει για τις εισερχόμενες συνδέσεις παρά στην πρόσβαση στις συγκεκριμένες υπηρεσίες.

Κρυπτογράφηση

Από μια σκοπιά της ασφάλειας, μια από τις σημαντικότερες ανεπάρκειες της ασύρματης επικοινωνίας είναι το γεγονός ότι οι μεταδόσεις της μπορούν να ακουστούν πέρα από τις σχετικά μεγάλες αποστάσεις μακριά από την απλή πορεία οπτικής επαφής μεταξύ των σημείων τέλους. Πράγματι, ένα από τα χαρακτηριστικά των περισσότερων ad-hoc ασύρματων συσκευών είναι η χρήση μη κατευθυντικών κεραιών τους έτσι ώστε τα σήματά τους μπορούν να παραληφθούν από άλλες συσκευές, ανεξάρτητα από πού βρίσκονται η μια σχετικά με την άλλη. Αποστέλλοντας τις πληροφορίες σε όλες οι κατευθύνσεις διευκολύνουν την υποκλοπή τους, ώστε τα ευαίσθητα δεδομένα πρέπει να κρυπτογραφηθούν για να αποτρέψουν την αναρμόδια χρήση τους.

Η κρυπτογράφηση γίνεται με την αλλαγή του μηνύματος *(σαφές κείμενο)* σε αυτό που μοιάζει με μια τυχαία ακολουθία κομματιών *(cipher κείμενο)* πριν από τη μετάδοση. Οι εξουσιοδοτημένοι χρήστες είναι σε θέση να αλλάξουν το cipher κείμενο πίσω στο σαφές κείμενο ως εισαγωγή σε μια κρυπτογράφηση. Η cipher διαδικασία χρησιμοποιεί ένα *κλειδί κρυπτογράφησης* μαζί με το σαφές κείμενο ως εισαγωγή σε έναν αλγόριθμο κρυπτογράφησης, από τον οποίο προκύπτει το cipher κείμενο. Στον προορισμό, το cipher κείμενο και ένα *κλειδί αποκρυπτογράφησης* χρησιμοποιούνται σε έναν άλλο αλγόριθμο για να αναδημιουργήσουν το σαφές κείμενο. Συνήθως, οι αλγόριθμοι δημοσιοποιούνται, όπως συμβαίνει με ciphers Bluetooth. Η δύναμη της κρυπτογράφησης είναι στον αλγόριθμο και στο κλειδί μαζί, και όχι μόνο στον ίδιο τον αλγόριθμο

Οι κρυπτογραφικοί αλγόριθμοι μπορούν να είναι είτε συμμετρικοί είτε ασυμμετρικοί. Ένας *συμμετρικός αλγόριθμος* χρησιμοποιεί τον ίδιο αλγόριθμο για την κρυπτογράφηση και την αποκρυπτογράφηση. Και οι δύο άκρες της σύνδεσης χρησιμοποιούν επίσης το ίδιο κλειδί, έτσι το σύστημα είναι αρκετά απλό. Ο κίνδυνος, φυσικά, είναι ότι εάν το

κλειδί εκθέτεται η ασφάλεια χάνεται. Αυτός ο κίνδυνος αυξάνεται αναλογικά προς τον αριθμό των συσκευών που κατέχουν το κλειδί. Το Bluetooth χρησιμοποιεί έναν συμμετρικό αλγόριθμο κρυπτογράφησης/αποκρυπτογράφησης.

Ο *ασυμμετρικός αλγόριθμος* είναι βασισμένος σε μια μαθηματική έννοια που επιτρέπει ένα κλειδί να χρησιμοποιηθεί για την κρυπτογράφηση μόνο, και άλλο κλειδί απαιτείται για την αποκρυπτογράφηση. Τα κλειδιά είναι ανεξάρτητα το ένα από το άλλο, έτσι ξέροντας το ένα δεν θα παράσχει οποιεσδήποτε πληροφορίες για την "εξαγωγή" του άλλου. Αυτός ο αλγόριθμος προσαρμόζεται στη *δημόσια βασική* μέθοδο *συστήματος κρυπτογραφίας[public key cryptography]*, στην οποία ένα από τα κλειδιά, αποκαλούμενο *δημόσιο κλειδί,* δίνεται σε καθεμία που το θέλει. Αυτό το κλειδί μπορεί να χρησιμοποιηθεί για να δημιουργήσει το cipher κείμενο από το σαφές κείμενο, αλλά είναι άχρηστο για την αντιστροφή της διαδικασίας. Μόνο το *ιδιωτικό κλειδί* μπορεί να κάνει αυτό, και εκείνο το κλειδί κρατιέται προσεκτικά μυστικό.

Το κύριο πλεονέκτημα της δημόσιας βασικής μεθόδου συστήματος κρυπτογραφίας είναι ότι το κλειδί αποκρυπτογράφησης (ιδανικά) κρατιέται μόνο σε μια θέση, έτσι είναι δυσκολότερο να παραχωρηθεί απ'ό,τι στη συμμετρική μέθοδο, όπου το κλειδί κρυπτογράφησης/αποκρυπτογράφησης κατέχεται και από τους δύο χρήστες της σύνδεσης. Επιπλέον, αντίθετα από το συμμετρικό αλγόριθμο, δεν υπάρχει καμία απαίτηση να συζητηθεί ή να μεταφερθεί το κλειδί κρυπτογράφησης από μια συσκευή σε άλλη, στην διάρκεια του οποίου μια "παραχώρηση" του κλειδιού μπορούσε να συμβεί. Το κύριο μειονέκτημα στο δημόσιο βασικό σύστημα είναι η κρυπτογράφησή του και η ταχύτητα αποκρυπτογράφησης, που είναι περίπου 1.000 φορές πιο αργή από την χρησιμοποίηση ενός συμμετρικού αλγόριθμου. Λόγω αυτού, πραγματικοί στόχοι κρυπτογράφησης ολοκληρώνονται συχνά με τη χρησιμοποίηση του δημόσιου κλειδιού του συστήματος για να διανείμει με ασφάλεια τα συμμετρικά κλειδιά στα συμμετέχοντα συμβαλλόμενα μέρη, τα οποία χρησιμοποιούνται έπειτα για μια ενιαία συνεδρία επικοινωνίας και απορρίπτονται έπειτα. Το Bluetooth δεν έχει κανένα ενσωματωμένο δημόσιο κλειδί κρυπτογράφησης , αλλά κάποιο μπορεί βεβαίως να εφαρμοστεί στο επίπεδο εφαρμογής.

Frequency Hopping and Whitening as Encryption Measures Επειδή το Bluetooth ενσωματώνει συνήθως το hopping συχνότητας και τους αλγόριθμους δεδομένων Whitening, μπορεί κανένα από αυτά να παράσχει την απαιτούμενη προστασία ; Η απάντηση είναι όχι. Ένας υποκλοπέας θα χρησιμοποιήσει ένα εύκολα αποκτηθέν Bluetooth chipset ως βάση για τον δέκτη και τον επεξεργαστή παρεμπόδισης. Η ακολουθία hop είναι γνωστή επειδή οι τιμές BD_ADDR και CLKN του master στέλνονται μέσω αέρα ως τμήμα του πακέτου FHS κατά τη διάρκεια του page, και όταν αυτές οι τιμές τοποθετηθούν στη γεννήτρια hop του ωτακουστή, η συσκευή θα μεταπηδά μαζί με το υπόλοιπο του piconet. Απλές firmware τροποποιήσεις μπορούν να το επιτρέψουν να λάβει σε όλες τις υποδοχές, με αυτόν τον τρόπο παρεμποδίζοντας κάθε μετάδοση.

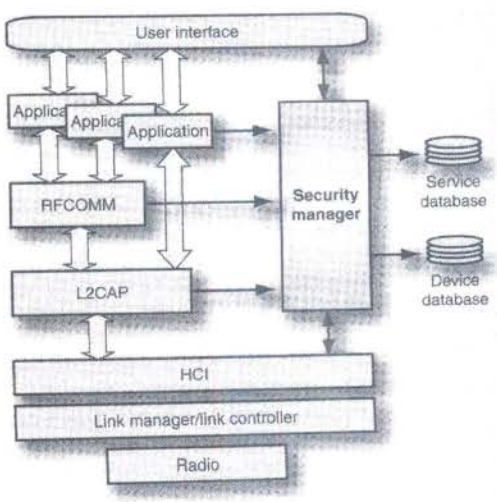
Για παρόμοιους λόγους, οι whitening και dewhitening αλγόριθμοι των δεδομένων δεν ενισχύουν την ασφάλεια .Και οι δύο αλγόριθμοι είναι μέρος του κάθε Bluetooth-κατάλληλου chipset, και η dewhitening διαδικασία πραγματοποιείται αυτόματα σε κάθε λαμβανόμενο πακέτο. Η μόνη λογική αξία κρυπτογράφησης έμφυτη στη hopping συχνότητας και τη λεύκανση στοιχείων είναι προστασία από τον περιστασιακό κρυφακούγοντας χρησιμοποιώντας εξοπλισμό nonBluetooth.

Διαχείριση ασφάλειας

Εάν οποιοδήποτε μέρος της ασφάλειας bluetooth είναι να πραγματοποιηθεί αυτόματα, ένας διευθυντής ασφάλειας πρέπει να είναι μέρος του πακέτου λογισμικού host. Επιπλέον, για τη μέγιστη ευελιξία, η πιστοποίηση και η εξουσιοδότηση θα έπρεπε να εμφανιστούν μετά από το καθορισμό του επίπεδου ασφαλείας της απαιτούμενης υπηρεσίας, έτσι τα μέτρα ασφαλείας πρέπει να εφαρμοστούν αφότου καθιερώνεται η σύνδεση ACL. Αυτό υπονοεί ότι ο mode 2 (σύνδεση-ισόπεδη επιβεβλημένη ασφάλεια) πραγματοποιείται. Φυσικά, μια άλλη επικύρωση θα μπορούσε να εμφανιστεί με την αρχική καθιέρωση της σύνδεσης ACL, αλλά σε πολλές περιπτώσεις εκείνη η επικύρωση θα ήταν περιττή.

Το σχήμα 5-3 παρουσιάζει τον διευθυντή ασφάλειας που κατοικεί σε έναν host Bluetooth επικοινωνώντας με L2CAP και με το LM μέσω του HCI.Ένα τυπικό σενάριο ασφάλειας μοιάζει με αυτό:

1. Ένα αίτημα σύνδεσης από μια άλλη συσκευή φτάνει στο επίπεδο L2CAP.
2. Ο L2CAP ζητά αποτίμηση από το διευθυντή ασφάλειας.
3. Ο διευθυντής ασφάλειας ανατρέχει την απαιτούμενη υπηρεσία στη βάση δεδομένων για τις πληροφορίες ασφάλειας.
4. Ο διευθυντής ασφάλειας ανατρέχει το BD_ADDR της συσκευής αίτησης μέσα στη βάση δεδομένων για τις εγκρίσεις πρόσβασης.
5. Ο διευθυντής ασφάλειας αρχίζει την απαραίτητη πιστοποίηση και (εάν αν χρειάζεται) διαδικασίες κρυπτογράφησης με το LM μέσω HCI.
6. Εάν όλος είναι καλά, κατόπιν το LM δίνει μια ευνοϊκή απάντηση μέσω HC!.
7. L2CAP τελειώνει τη διαδικασία οργάνωσης σύνδεσης.



ΣΧΗΜΑ 5-3

Η αρχιτεκτονική διευθυντών ασφάλειας στο σχήμα 5-3 θα μπορούσε να χρησιμοποιηθεί για να εφαρμόσει τον τρόπο 3 (σύνδεση-ισόπεδη) ασφάλεια επίσης. Μια

πιθανή σύγκρουση εμφανίζεται όταν αποθηκεύονται τα κλειδιά συνδέσεων σε δύο διαφορετικές θέσεις: στην μονάδα Bluetooth για ενισχυμένο link level security και στον host για την service-level ενισχυμένη ασφάλεια. Προκειμένου να αποτραπεί η αδικαιολόγητη εμπιστοσύνη χορήγηση στις συσκευές τα κλειδιά συνδέσεων των οποίων αποθηκεύονται στην ενότητα, ο διευθυντής ασφάλειας μπορεί να αφαιρέσει αυτά τα κλειδιά, αφαιρώντας κατά συνέπεια τη σύνδεση μεταξύ των συσκευών, με τη χρησιμοποίηση των εντολών HCI.

ΚΕΦΑΛΑΙΟ 6
ΜΟΝΤΕΛΑ ΧΡΗΣΗΣ

Επισκόπηση των εφαρμογών Bluetooth

Δεδομένου ότι η έννοια Bluetooth άρχισε να παίρνει μορφή στα μέσα της δεκαετίας του '90, τα διάφορα πρότυπα χρήσης δημιουργήθηκαν ως πιθανές εφαρμογές ενός περιορισμένου φάσματος ψηφιακού ασύρματου συστήματος με data rates από περίπου 100 έως 500 kilobits ανά δευτερόλεπτο *(kb/s)*. Θα εξετάσουμε κάθε ένα από αυτά τα αρχικά πρότυπα, τα οποία απελευθερώθηκαν ταυτόχρονα με την προδιαγραφή 1.0A

Τρία - σε - ένα τηλέφωνο

Το τηλεφωνικό σύστημα άρχισε ως σύνολο σταθερών καλωδίων που συνδέουν τα τηλέφωνα στις σταθερές θέσεις μέσω ενός διακόπτη κεντρικών γραφείων. Σήμερα αυτό το δίκτυο των τηλεφώνων και των καλωδίων καλείται *Plain Old Telephone Service* (POTS). Χωρίς την ενίσχυση της ασύρματης ευκινησίας, κάνοντας ένα τηλεφώνημα σήμανε ότι ένας χρήστης έπρεπε να βρει ένα τηλέφωνο αρχικά, και να καλέσει έπειτα ένα άλλο τηλέφωνο στο οποίο το επιθυμητό πρόσωπο μπορεί η δε μπορεί να είναι φυσικά παρών.

Με την εμφάνιση του κυψελοειδούς τηλεφώνου, οι χρήστες θα μπορούσαν να φέρουν τα τηλέφωνά μαζί τους. Αυτό πρόσφερε δύο ευδιάκριτα πλεονεκτήματα (τουλάχιστον θεωρητικά): Ένα τηλέφωνο είναι πάντα διαθέσιμο για να δημιουργηθεί μια κλήση, και μια άλλη ομάδα ατόμων μπορεί να πραγματοποιήσει μια κλήση στο κινητό τηλέφωνο και έχει μια υψηλή πιθανότητα να επικοινωνήσει με το επιθυμητό πρόσωπο. Φυσικά, η σημαντική κυψελοειδής υποδομή πρέπει να είναι παρούσα, και η χρήση εκείνης της υποδομής πρέπει να είναι ο καταλληλότερος και οικονομικά αποδοτικός τρόπος να τοποθετηθεί μια κλήση ώστε το σύστημα να υπερισχύσει. Στην πραγματικότητα τα κυψελοειδή τηλέφωνα μπορούν να είναι ακριβά και να παραγάγουν τη διάστικτη(ανομοιόμορφη) κάλυψη, έτσι τα περισσότερα σπίτια και επιχειρήσεις

χρησιμοποιούν ακόμα POTS. Ακόμα κι έτσι, ένα ασύρματο τηλέφωνο που συνδέεται με POTS μπορεί να επιτρέψει την περιπλάνηση σε όλο το σπίτι ή το γραφείο.

Το Bluetooth 3-σε-1 τηλέφωνο(σχήμα 6-1) προβλέπει ένα τηλέφωνο που μπορεί να λειτουργήσει με το (μη- Bluetooth) κυψελοειδές σύστημα, ως ασύρματο τηλέφωνο μέσω μιας σύνδεσης Bluetooth με έναν κοντινό σταθμό βάσεων που συνδέεται με POTS ή ως walkie-talkie σε άλλο 3-σε-1 τηλέφωνο. Θα υπήρχε μια ¨κινητική" μεταφορά μεταξύ των κυψελοειδών και ασύρματων τηλεφωνικών συνδέσεων καθώς ο χρήστης κινείται από μέρος σε μέρος. Επιπλέον, αυτή η διαμόρφωση θα μπορούσε να επιτρέψει την ανάθεση ενός ενιαίου προσωπικού τηλεφωνικού αριθμού και για τις τρεις χρήσεις.

Λάβετε υπόψη, εντούτοις, ότι οι συσκευές Bluetooth μπορούν να λειτουργήσουν σε επίπεδα ισχύος μέχρι 100 μ W, επιτρέποντας σε αυτές να επικοινωνήσουν σε αποστάσεις μεγαλύτερες από 10 μέτρα. Επίσης, όταν χωρίζονται οι χρήστες από τους τοίχους ή άλλα εμπόδια, μπορεί ακόμα να είναι καταλληλότερο να χρησιμοποιηθούν οι ασύρματες συσκευές από να μιλήσει μέσω του εμποδίου.

ΣΧΗΜΑ 6.1 Το 3 σε 1 τηλέφωνο μοντέλο χρήσης

Ακουστικά και μικρόφωνο κεφαλής(headset)

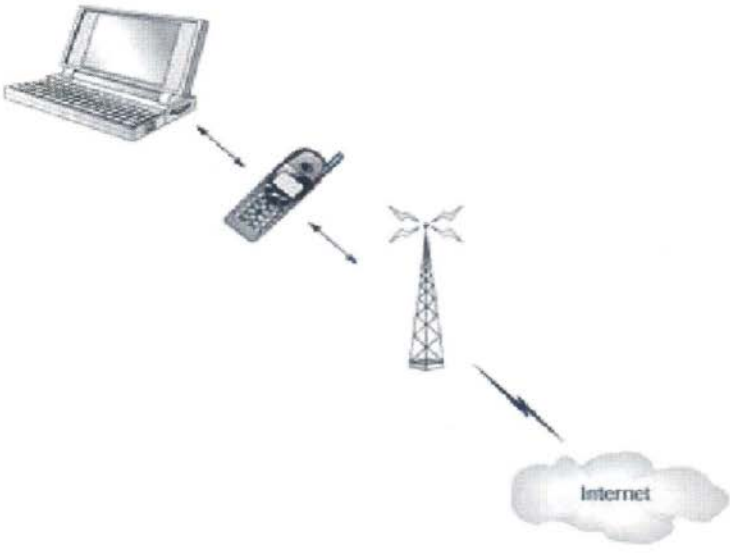
Ένα ελαφρύ headset με μια ασύρματη σύνδεση με τη συσκευή εξυπηρέτησης της μπορεί να αποδειχθεί η μεγαλύτερη αγορά για τις συσκευές Bluetooth. Πολλοί χρήστες έχουν πραγματοποιήσει ήδη την ευκολία της σύνδεσης ενός συνδεμένου με καλώδιο headset με το τηλέφωνο, ελευθερώνοντας και τα δύο χέρια.

Καθώς τα διάφορα κράτη και οι τοπικές κυβερνήσεις κινούνται για να περιορίσουν την τηλεφωνική χρήση κυττάρων οδηγώντας, το Bluetooth headset θα γίνει μια ουσιαστική συσκευή για παραγωγή των κλήσεων από ένα αυτοκίνητο. Το τηλέφωνο κυττάρων παραμένει κρυμμένο μακριά στον χαρτοφύλακα, και με ένα μικρό, ελαφρύ headset μπορεί να έχουν πρόσβαση στο τηλέφωνο μέσω των εντολών φωνής ενώ και τα δύο χέρια καταλαμβάνονται με τον έλεγχο του οχήματος. Με τις εκατοντάδες των εκατομμυρίων των κυψελοειδών μικροτηλεφώνων σε χρήση, τα περισσότερα από τα οποία φέρονται τελικά σε ένα όχημα, είναι προφανές ότι εάν το Bluetooth μπορεί να γίνει η κυρίαρχη ασύρματη σύνδεση headset με headset, η δυνατότητα πωλήσεων θα είναι απέραντη.

Φυσικά, το headset Bluetooth δεν θα περιοριστεί στις συνδέσεις με ένα κυψελοειδές τηλέφωνο, αλλά άντ' αυτού θα μπορούσε αυτόματα να συνδέθει με οποιαδήποτε συμβατή συσκευή μέσα στο βεληνεκές της που είναι ικανή για ακουστική επικοινωνία.

Γέφυρα Διαδικτύου

Μια αρκετά κοινή μέθοδος για πρόσβαση στο Διαδίκτυο είναι ένας συνδεδεμένος υπολογιστής lap-top μέσω του καλωδίου με ένα κυψελοειδές τηλέφωνο, το οποίο στη συνέχεια χρησιμοποιείται για να καλέσει τον αριθμό διεπιλογών *φορέων παροχής υπηρεσιών Διαδικτύου* (ISP). Το πρότυπο χρήσης γεφυρών Διαδίκτυου με Bluetooth αντικαθιστά απλά το καλώδιο με μια ασύρματη σύνδεση, όπως φαίνεται στο σχήμα 6-2. Η σύνδεση πρέπει να είναι σε θέση να "περάσει" τις εντολές σύνδεση και αποσύνδεση (AT) στο τηλέφωνο καθώς επίσης και παρέχει τη διπλής κατεύθυνσης κυκλοφορία δεδομένων μεταξύ του τηλεφώνου και του lap-top.



ΣΧΗΜΑ 6.2 Το μοντέλο χρήσης για σύνδεση με Internet μέσω κινητού τηλεφώνου

Σημείο πρόσβασης στοιχείων (Data Access Point)

Διευρύνοντας ελαφρώς στην έννοια της γέφυρας Διαδικτύου, ένα σημείο πρόσβασης δεδομένων Bluetooth επιτρέπει έναν υπολογιστή να συνδέσει με μια υπηρεσία δεδομένων, όπως το τοπικό LAN, μέσω μιας ασύρματης σύνδεσης. Το ίδιο το τοπικό LAN θα μπορούσε να έχει οποιαδήποτε διαμόρφωση, ενσύρματη ή ασύρματη, και όλες οι υπηρεσίες του τοπικού LAN θα ήταν διαθέσιμες στον υπολογιστή σαν να συνδέθηκε μέσω καλωδίου. Αυτή η μέθοδος πρόσβασης θα προλάμβανε την ανάγκη να τρέχουν τα καλώδια του τοπικού LAN εκτενώς μέσω ενός κτηρίου, καθιστώντας το ιδιαίτερα κατάλληλο για τα telemarketers ή τις ομάδες πωλήσεων να έχουν πρόσβαση στις βάσεις δεδομένων και τους εκτυπωτές.

Ώθηση αντικειμένου και μεταφορά αρχείων

Τα πρότυπα χρήσης μεταφοράς ώθησης και αρχείων αντικειμένου Bluetooth χτίστηκαν επάνω σε παρόμοιες λειτουργίες που χρησιμοποιούν υπέρυθρες ακτίνες που είναι διαθέσιμες *στις προσωπικές ψηφιακές βοηθητικές* συσκευές (PDA) για αρκετά έτη. Μετά από μια απλή διαδικασία σύνδεσης, οι χρήστες είναι σε θέση να μεταφέρουν τις πληροφορίες, όπως οι επιχειρησιακές κάρτες, τα τηλεφωνικά στοιχεία, ή τα μεγαλύτερα αρχεία μεταξύ τους. Αυτές οι διαδικασίες λαμβάνουν τη μορφή *ώθησης*, όπου ο ιδρυτής στέλνει ένα αρχείο, ή ανακτά ένα αρχείο. Οι διαδικασίες ώθησης και ανάκτησης μπορούν να συνδυαστούν, παραδείγματος χάριν, σε μια ανταλλαγή business card.

Επειδή το Bluetooth δεν περιορίζεται στο *line-of sight* (LOS), η διαδικασία μεταφοράς αρχείων επιτρέπει την κατάλληλη διαλογική σύσκεψη. Αυτή η ικανότητα ήδη υπάρχει σε πολλές συνδεμένες με καλώδιο εφαρμογές του τοπικού LAN, όπου ένα αρχείο μπορεί να ανοίξει από διάφορους χρήστες, και οποιαδήποτε τροποποίηση που γίνεται θα εμφανίζεται σε όλες τις οθόνες.

Αυτόματος συγχρονισμός

Πολύ έχουν δοκιμάσει την απογοήτευση να χειριστούν διάφορα αντίγραφα από αυτό που είναι υποτιθέμενο για να είναι το ίδιο αρχείο στις διαφορετικές μηχανές. Ο τηλεφωνικός PDA κατάλογός σας περιέχει τους ίδιους αριθμούς με εκείνους που αποθηκεύονται στο τηλέφωνο κυττάρων σας; Εάν όλες οι συσκευές που διατηρούν τα αντίγραφα των αρχείων είναι εξοπλισμένες με Bluetooth, μπορούν, όταν είναι στην επιτρεπτή απόσταση, να συνδεθούν και να ενημερώνουν αυτόματα τα αρχεία τους στην πιο πρόσφατη έκδοση.

Παραδείγματος χάριν, υποθέστε ότι θέλετε να συγχρονίσετε τα αρχεία στον υπολογιστή σας γραφείων και σπιτιών. Ενώ στο γραφείο, το PDA σας μπορεί να εγκαταστήσει μια σύνδεση Bluetooth και να αντιγράψει τα νέα ή ενημερωμένα αρχεία υπολογιστών γραφείου στη μνήμη του. Όταν το PDA λαμβάνεται κατ' οίκον, μπορεί

αυτόματα να συνδεθεί με τον εγχώριο υπολογιστή και να ενημερώσει τα αρχεία του (σχήμα 6-3). Επιπλέον, η διαδικασία μπορεί να αντιστραφεί όταν επιστρέφεται το PDA στο γραφείο.

Σχήμα 6-3 Αυτόματος συγχρονισμός

Άλλες χρήσεις για Bluetooth

Τα πρότυπα χρήσης που συζητήθηκαν νωρίτερα αναπτύχθηκαν όταν ήταν ακόμα το Bluetooth στις αρχές. Δεδομένου ότι η τεχνολογία Bluetooth ωριμάζει, άλλες εφαρμογές που είναι απολύτως νέες ή οι παραλλαγές αυτών των προτύπων χρήσης θα αρχίσουν να εμφανίζονται .

ΚΕΦΑΛΑΙΟ 7
ΣΥΓΚΡΙΣΗ ΜΕ ΑΛΛΑ ΑΣΥΡΜΑΤΑ ΠΡΟΤΥΠΑ

Το Bluetooth δεν είναι η μόνη ασύρματη λύση συνδετικότητας διαθέσιμη σήμερα. Υπάρχουν διάφορες άλλες τεχνολογίες που ωθούνται για τις ασύρματες συνδέσεις και τη δικτύωση. Μερικές από αυτές τις τεχνολογίες είναι άμεσοι ανταγωνιστές με το Bluetooth. Μερικές είναι αρκετά διαφορετικές (και εξυπηρετούν τις αρκετά διαφορετικές εφαρμογές) ώστε να συνυπάρξουν με Bluetooth, και ακόμη και για να συμπληρώσουν τις εφαρμογές Bluetooth. Παρακάτω θα παραθέσουμε λίγα στοιχεία για τις άλλες ασύρματες επικοινωνίες, τα πλεονεκτήματα τους, όπως επίσης και μια σύγκριση με την τεχνολογία Bluetooth.

IRDA

Η ποιο αμεσότερα ανταγωνιστική τεχνολογία σε Bluetooth είναι η *υπέρυθρη* (IR). Η Infrared Data Association (IrDA) έχει καθιερώσει πρότυπα για τις υπέρυθρες συνδέσεις (αποκαλούμενες πρότυπα IrDA) που έχουν υιοθετηθεί από περισσότερες από 160 διαφορετικές επιχειρήσεις και χρησιμοποιούνται ευρέως σήμερα. Εάν έχετε ένα PalmPilot ή άλλο PDA, πιθανότατα έχετε χρησιμοποιήσει την πόρτα IR της που συνδέει και synch με το PC σας, ή με τα στοιχεία επιχειρησιακών καρτών ακτινών σε και από ένα άλλο PDA. Στην πραγματικότητα, η ικανότητα IR μπορεί να βρεθεί σε περισσότερες από 150 εκατομμύριο συσκευές υπολογισμού, με τις πωλήσεις τέτοιων συσκευών που αυξάνονται σε ένα 40% ετήσιο ποσοστό.

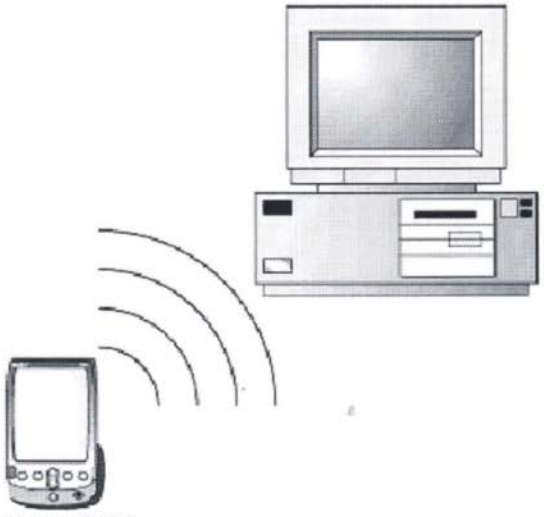
Πώς λειτουργεί το IrDA

IrDA χρησιμοποιεί υπέρυθρο φως - *όχι ραδιοκύματα* - για να μεταδώσει τα σήματα δεδομένων από μια συσκευή σε άλλη. Δεδομένου ότι το φως δεν μπορεί να περάσει μέσω των στερεών αντικειμένων, οι συσκευές που συνδέουν μέσω IrDA πρέπει να είναι άμεσα ορατές η μια από την άλλη . Ένας περαιτέρω περιορισμός είναι ότι η απόσταση είναι

περιορισμένη και η γωνία επαφής είναι σχετικά στενή και για οποιαδήποτε σήματα πέρα από 1 μέτρο και έξω από έναν κώνο 30-μοιρων δεν θα παραληφθούν.

Αυτοί οι τεχνικοί περιορισμοί περιορίζουν λίγο πολύ το IrDA στις άμεσες ένα προς ένα συνδέσεις, όπως φαίνεται στο σχήμα 7-1. (Δεν μπορείτε να χρησιμοποιήσετε IrDA για να συνδέσετε τις πολλαπλάσιες συσκευές σε οποιοδήποτε είδος δικτύου.)

Οι χαρακτηριστικές χρήσεις IrDA είναι να συνδεθούν δύο PDAs, να συνδεθούν ένα PDA με ένα PC, ή για να συνδεθούν άλλες σταθερές περιφερειακές μονάδες με ένα PC . Η κίνηση μιας συσκευής είναι πιθανό να διακόψει την υπέρυθρη σύνδεση.



ΣΧΗΜΑ 7-1 Το πρότυπο IRDA

Παρά αυτούς τους περιορισμούς, το IrDA έχει διάφορα πλεονεκτήματα. Κατ' αρχάς, είναι γρήγορο. Τυποποιημένο IrDA διαβιβάζει τα στοιχεία σε μια μέγιστη ρυθμοαπόδοση 4Mbps, ενώ τα νέα *γρήγορα υπέρυθρα* πρότυπα *Fast Infrared*(του FIR) καθορίζουν ένα ποσοστό μεταφοράς 16Mbps. Η μέγιστη ρυθμοαπόδοση 1Mbps του Bluetooth χλομιάζει στη σύγκριση.

Δεύτερον, οι ίδιοι οι περιορισμοί της τεχνολογίας (οπτική επαφή, απόσταση, και γωνία) κάνουν το IrDA έναν πολύ ασφαλή τρόπο να διαβιβαστούν τα δεδομένα. Εκτός αν είστε κοντά στον κώνο, δεν μπορείτε να πάρετε τα υπέρυθρα σήματα καθόλου. Και, επειδή τα σήματα δεν είναι ραδιοκύματα, η παρέμβαση από άλλες συσκευές είναι ένα αμφισβητήσιμο σημείο. (Επιπλέον, IrDA δεν απαιτεί κανέναν κανονισμό της FCC.)
Ποια είδη συσκευών χρησιμοποιούν μια σύνδεση IrDA; Ο κατάλογος είναι μακρύς και αυξανόμενος:

- Προσωπικοί ψηφιακοί βοηθοί (PDAs)
- Φορητός, σημειωματάριο, και υπολογιστές γραφείου
- Εκτυπωτές
- Modems
- Ψηφιακές φωτογραφικές μηχανές
- Scanners
- Copiers
- fax
- Ρολόγια
- Hands-free εξαρτήσεις αυτοκινήτων
- Ιατρικός και βιομηχανικός εξοπλισμός

Πλεονεκτήματα IrDA

Το IrDA είναι μια ιδανική ασύρματη αντικατάσταση τεχνολογία-τόσο μακροχρόνια όπως οι δύο συσκευές τοποθετούνται κοντά από κοινού. Είναι επίσης η καλύτερη τεχνολογία για να διαβιβάσει τα ασφαλή στοιχεία.
Εδώ έπειτα, είναι τα κύρια πλεονεκτήματα IrDA:

- Γρήγορο (4Mbps)
- Ανέξοδο ($2 ή λιγότεροι ανά συσκευή)
- Μικρή κατανάλωση ισχύος
- Ασφάλεια
- Μη ευαίσθητο στην παρεμβολή RF
- Ευρέως χρησιμοποιημένο

Μειονεκτήματα του IrDA

Το IrDA δεν είναι μια καλή τεχνολογία για την τοπική δικτύωση περιοχής. Η ταχύτητα δεν είναι σχεδόν τόσο γρήγορη όσο Ethernet ή το 802.11 , και οι περιορισμοί σύνδεσης είναι πάρα πολύ μεγάλοι. Δεν είναι επίσης καλό για δημόσιες ad hoc συνδέσεις στο οποίο Bluetooth υπερέχει. Περιορίζεται λίγο πολύ στις περιορισμένου φάσματος από σημείο σε σημείο συνδέσεις, όπως η αντικατάσταση των καλωδίων μεταξύ ενός PC και των περιφερειακών μονάδων του.

Τα κύρια μειονεκτήματα IrDA, έπειτα, είναι:

- Περιορισμένη απόσταση (3 πόδια)
- Περιορισμένη γωνία σύνδεσης (30 βαθμοί)

Πώς συγκρίνεται με το Bluetooth

Και IrDA και Bluetooth μπορούν να χρησιμοποιηθούν για να αντικαταστήσουν τα καλώδια μεταξύ του υπολογισμού και συσκευές επικοινωνιών. Το IrDA το κάνει γρηγορότερα, αλλά Bluetooth το κάνει με περισσότερη ευελιξία και απόσταση. Δεδομένου ότι το ποσοστό μετάδοσης 1Mbps Bluetooth είναι αρκετά γρήγορο για τους εκτυπωτές, τα scanner , τα πληκτρολόγια, τα ποντίκια, και τα όμοια τους (λίγο πολύ όλα εκτός από τα βίντεο χρειάζονται ακόμα το καλώδιο μεταξύ του PC σας και της οθόνης), η προστιθέμενη IrDA ταχύτητα δεν αντισταθμίζει τα μειονεκτήματα τοποθέτησής της. Στην αγορά καλώδιο-αντικατάστασης, Bluetooth είναι ο πιθανός νικητής.

Από την άποψη της σύνδεσης μιας συσκευής υπολογισμού με το συνδεμένο με καλώδιο τοπικό LAN, (σύντομα θα είναι 16Mbps) η ταχύτητα IrDA's 4Mbps του δίνει ένα χαρακτηρισμένο πλεονέκτημα πέρα από τη σύνδεση 1Mbps Bluetooth. Ενώ το Bluetooth είναι επαρκές για τα αρχεία εκτύπωσης και άλλες περιστασιακές εφαρμογές, η πλήρης σύνδεση του τοπικού LAN σε 1Mbps είναι ακριβώς πάρα πολύ αργή. Το IRDA ισοφαρίζει το Bluetooth.

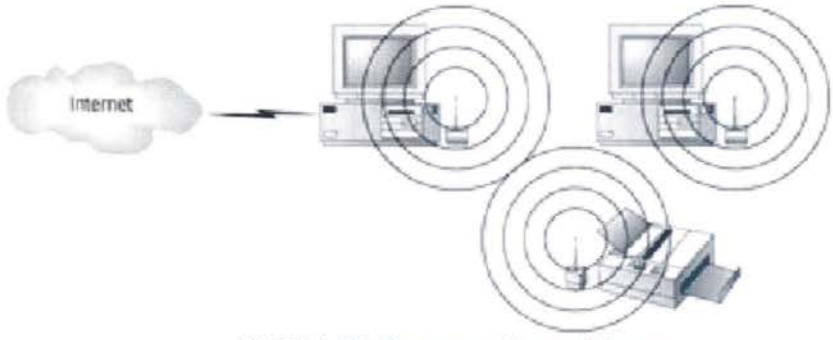
Όταν είναι να δημιουργηθούν ad-hoc δημόσιες συνδέσεις-τέτοιες όπως η αποστολή και λήψη του ηλεκτρονικού ταχυδρομείου περπατώντας μέσω ενός αερολιμένα το Bluetooth είναι ο σαφής νικητής. Δεν μπορείτε απλά να κάνετε αυτό με τη σημερινή υπέρυθρη τεχνολογία οι περιορισμοί σειράς και γωνίας είναι απαγορευτικοί.

Οι ειδικές *ιδιωτικές* συνδέσεις, εντούτοις, είναι ένα διαφορετικό πράγμα. Εάν χρησιμοποιείτε μια πιστωτική κάρτα ή άλλη συσκευή στις πληροφορίες πληρωμής ακτινών σε έναν κατάλογο μετρητών υψηλής τεχνολογίας στο τοπικό λιανικό κατάστημά σας, και IrDA και Bluetooth θα κάνουν την εργασία επαρκώς. Στην πραγματικότητα, η ασφαλέστερη τεχνολογία IrDA's να του δώσει ένα μικρό πλεονέκτημα πέρα από τη ραδιοφωνική αναμετάδοση RF Bluetooth.

Κατόπιν αυτών είναι πιθανό παρά τις καλύτερες προσπάθειες της υπέρυθρης ένωσης στοιχείων το Bluetooth θα αντικαταστήσει το IR για την πλειοψηφία των σχετικών εφαρμογών, ειδικά εκείνοι που περιλαμβάνουν την αντικατάσταση καλωδίων.

HomeRF

Το HomeRF είναι μια ασύρματη τεχνολογία δικτύωσης που σχεδιάζεται ρητώς για τη χρήση στα δίκτυα σπιτιών και μικρών επιχειρήσεων. Όπως το Bluetooth,έτσι και το HomeRF χρησιμοποιεί την 2.4GHz RF-ως εκ τούτου το όνομά του (RF στο σπίτι). Το HomeRF αναπτύχθηκε από την ομάδα εργασίας HomeRF, μια ομάδα επιχειρήσεων που οδηγήθηκε από την Proxim, η οποία κατέχεται εν μέρει από την Intel, η οποία είναι επίσης μέλος υποστηρικτών της Bluetooth SIG. (Αυτό είναι μόνο ένα παράδειγμα του τοποθέτησης των πολλαπλάσιων στοιχημάτων από μερικούς από τους κορυφαίους κατασκευαστές υλικού.) Αλλά μέλη της ομάδας εργασίας περιλαμβάνουν τα Cayman systems, Compaq, Motorola, και την Intel όλοι από τους οποίους έχουν αυτήν την περίοδο τα προϊόντα δικτύωσης HomeRF στην αγορά.



ΣΧΗΜΑ 7-2. Ενα τυπικο homerf δίκτυο

Πλεονεκτήματα HomeRF

Ο σκοπός που δημιουργήθηκε το HomeRF ήταν τα ασύρματα εγχώρια δίκτυα. Για το τυπικό χρηστή το HomeRF είναι εύκολο να εγκατασταθεί και να διαμορφωθεί, λειτουργεί σύμφωνα με το περιβάλλον του σπιτιού, και είναι σχετικά ανέξοδο (όταν συγκρίνεται με 802.11).

Εδώ είναι τα κύρια πλεονεκτήματα HomeRF:

- Γρήγορο (10Mbps με SWAP 2.0, μονο 1- 2Mbps με την SWAP 1.0)
- Λιγότερο ακριβός από άλλες ασύρματες εναλλακτικές λύσεις δικτύωσης
- Εύκολο να εγκατασταθεί
- Δεν απαιτεί κανένα αφιερωμένο σημείο πρόσβασης
- Επιτρέπει μέχρι 127 συσκευές ανά δίκτυο
- Επιτρέπει τα πολλαπλάσια δίκτυα στην ίδια φυσική θέση
- Το Hopping συχνότητας μειώνει τις παρεμβολές με το σπίτι και τα ηλεκτρονικά

Μειονεκτήματα HomeRF

Ενώ HomeRF είναι καλό για το σπίτι, δεν είναι αρκετά χρήσιμο όταν χρησιμοποιείται σε ένα μεγαλύτερο γραφείο ή σε ένα εταιρικό περιβάλλον. Δεν είναι επίσης καλοταιριασμένο στις απλές εφαρμογές αντικατάστασης καλωδίου ή στους τύπους των από σημείο σε σημείο ad-hoc συνδέσεων που το Bluetooth υπερέχει.

Ως εκ τούτου, εδώ είναι τα κύρια μειονεκτήματα του HomeRF:

- Περιορισμένη απόσταση (75-125 πόδια) όταν συγκρίνεται με 802.11
- Δύσκολο να ενσωματώθει στα υπάρχοντα συνδεμένα με καλώδιο δίκτυα
- Λιγότερο σταθερό από 802.11 ή τις Ethernet-βασισμένες συνδέσεις δικτύων
- Μεγάλη κατανάλωση ισχύος (μη κατάλληλη για τη φορητή χρήση)

Πώς το HomeRF συγκρίνεται με το Bluetooth

Το HomeRF είναι μια καλή τεχνολογία για τα μικρά δίκτυα χαμηλών-φορτίων. Δεν είναι μια καλή τεχνολογία για τα μεγαλύτερα δίκτυα ή τα δίκτυα που είναι εξαπλωμένα έξω στα μεγαλύτερα διαστήματα, ούτε σχεδιάστηκε για τις φορητές συσκευές ή τις Ad-hoc συνδέσεις. Αυτό μεταφράζεται οτι είναι ένας τύπος ειρηνικής συνύπαρξης μεταξύ του HomeRF και των τεχνολογιών Bluetooth. Μπορείτε να χρησιμοποιήσετε Bluetooth για να αντικαταστήσετε τα καλώδια μεταξύ των περιφερειακών μονάδων σας και του PC σας, κατόπιν χρήση HomeRF για να συνδέσετε PCs σας το ένα με το άλλο σε ένα μικρό εγχώριο δίκτυο. Επειδή και οι δύο τεχνολογίες χρησιμοποιούν hopping συχνότητας, δεν πρέπει να παρεμποδίσουν η μια την άλλη από καμιά άποψη. . Δεδομένου ότι είναι αυστηρά "σεταρετέ το και αφήστε το", δεν ανταγωνίζεται με το Bluetooth σε οποιαδήποτε άλλο περιβάλλον.

IEEE 802.11b/WI-FI

Η Wireless Ethernet Compatibility Alliance(WECA) έχει αγκαλιάσει μια γερή ασύρματη τεχνολογία δικτύωσης βασισμένη σε μια προδιαγραφή που αναπτύσσεται από το ίδρυμα ηλεκτρονικών και ηλεκτρολόγων μηχανικών (IEEE). Η IEEE 802.11b προδιαγραφή είναι στον πυρήνα μιας τεχνολογίας που έχει λέγεται *το WI-FI*, για *το Wireless Fidelity*. Το WI-FI στοχεύει στα εταιρικά δίκτυα, δεδομένου ότι είναι περισσότερο δαπανηρό και υψηλότερης απόδοσης τεχνολογία είτε απο το Bluetooth είτε το κάπως ανταγωνίσιμο HomeRF.

Η WECA υποστηρίζεται από ποικίλους κατασκευαστές υλικού συμπεριλαμβανομένου την 3Com, Apple, Cabletron, Compaq, Lucent, και Nokia- πολλές από τις οποίες είναι επίσης μέλη του Bluetooth SIG.

Πώς λειτουργεί το 802.11

Όπως Bluetooth και HomeRF, 802.11 χρησιμοποιούν τη ραδιοφωνική μετάδοση σημάτων RF στη ζώνη 2.4GHz RF. Αντίθετα από Bluetooth και HomeRF, που και τα 2 χρησιμοποιούν την τεχνολογία FHSS, το 802.11 χρησιμοποιεί την DSSS (direct sequence spread spectrum). Η διαφορά μεταξύ FHSS και DSSS είναι ότι τα σήματα FHSS μεταπηδούν μέσα σε 79 διαφορετικές συχνότητες που χωρίζονται σε διαστήματα των 1MHz, τα σήματα DSSS καθορίζονται μέσα σε ένα κανάλι 17MHz (τρία των οποίων είναι διαθέσιμος στη ζώνη 2.4GHz), αλλά καλύπτονται με πολύ κατασκευασμένο "θόρυβο" για να μειώσουν την παρέμβαση και να βελτιώσουν την ασφάλεια. Η πρόσθετη ασφάλεια παρέχεται από το πρότυπα κρυπτογράφησης Wireless Equivalent Privacy (WEP), τα οποία χρησιμοποιούν την 128-bit τεχνολογία κρυπτογράφησης.
Ένα αποτέλεσμα της χρησιμοποίησης DSSS αντί FHSS είναι ότι 802.11 είναι γρήγορο, που φτάνει μέχρι 11Mbps μετάδοσης δεδομένων. Από αυτή την άποψη, το 802.11 είναι αποδεκτό υποκατάστατο Ethernet, το οποίο έχει τις παρόμοιες ταχύτητες μετάδοσης. Το μειονέκτημα της χρησιμοποίησης DSSS είναι ότι το 802.11 είναι πιο ευαίσθητο στην παρέμβαση από άλλες συσκευές που χρησιμοποιούν τη 2.4GHz ζώνη, ειδικά οι τύποι συσκευών που βρίσκονται χαρακτηριστικά σε περιβάλλον σπιτιού-ασύρματα τηλέφωνα σπιτιών, πόρτες γκαράζ, φούρνοι μικροκυμάτων, και όμοια τους.

Ένα 802.11 δίκτυο απαιτεί τη χρήση υλικού σημείου πρόσβασης (σταθμός βάσεων), η οποία μπορεί να προσθέσει στο κόστος του δικτύου. (Οι σταθμοί βάσεων κοστίζουν οπουδήποτε από $250 σε περισσότερο από $1200.) Ένα σημείο πρόσβασης είναι η μονάδα δεκτών/πομπών αποστολής σημάτων όπου οι μακρινές συσκευές έχουν πρόσβαση για να συνδέσουν με το δίκτυο.

Πλεονεκτήματα 802.11

Το 802.11/Wi-FI είναι καλό ως ασύρματο δίκτυο για τα εταιρικά και για τα περιβάλλοντα πανεπιστημιουπόλεων. Είναι γρήγορο, γερό, και απολύτως συμβατό με τα υπάρχοντα δίκτυα Ethernet.

Τα κύρια πλεονεκτήματα, έπειτα, του 802.11/WI-FI περιλαμβάνουν:

- Γρήγορο (11Mbps)
- Γερο και αξιόπιστες συνδέσεις
- Καλύπτει μεγάλη απόσταση (300 πόδια ή και περισσότερο)
- Εύκολα ενσωματώνεται στα υπάρχοντα δίκτυα Ethernet

Μειονεκτήματα 802.11

Όσο καλό είναι το 802.11 στο γραφείο, αλλο τόσο δεν είναι κατάλληλο σε ένα περιβάλλον σπιτιού. Το κόστος του είναι αρκετά υψηλό, είναι πάρα πολύ σύνθετο, και επιπλέον είναι πάρα πολύ ευαίσθητο στην παρέμβαση από άλλες συσκευές του σπίτι. Αυτά τα μειονεκτήματα δεν αποκλείουν το 802.11 για χρήση στο σπίτι- γεγονός είναι ότι μερικές επιχειρήσεις ωθούν ενεργά το WI-FI για σπίτι-μόνο, τουλάχιστον αυτήν την περίοδο, τοποθετούν 802.11 σε ανταγωνιστικά μειονεκτική θέση στα σχεδιασμένα προϊόντα HomeRF.

Ένα άλλο σημαντικό ζήτημα που έχει επιπτώσεις στην υιοθέτηση 802.11 είναι ότι αυτή η τεχνολογία έχει βασανιστεί, στο παρελθόν, από τα ζητήματα συμβατότητας. Φαίνεται ότι οι διαφορετικοί κατασκευαστές διάβασαν τις προδιαγραφές με διαφορετικούς τρόπους, έτσι ώστε μια 802.11 κάρτα δικτύων από έναν κατασκευαστή να μην λειτουργήσει σε ένα 802.11 δίκτυο που χτίστηκε από άλλο κατασκευαστή. Στην πραγματικότητα, αυτό το ζήτημα συμβατότητας ήταν πίσω από το σχηματισμό WECA και την καθιέρωση των προτύπων WI-FI. Ακριβώς όπως οι συσκευές Bluetooth δοκιμάζονται από την Bluetooth SIG για τη συμμόρφωση με την προδιαγραφή Bluetooth, η WECA εξετάζει τώρα το 802.11 τις συσκευές για τη διαλειτουργικότητα και οι συσκευές που περνούν τη δοκιμή WECA μπορούν να φέρουν την ετικέτα WI-FI.

Τα αρχικά μειονεκτήματα του 802.11/Wi-Fi είναι:

- Υψηλό κόστος
- Απαιτεί φυσικά σημεία πρόσβασης
- Δύσκολος να διαμορφώσει και να διατηρήσει
- Καμία υποστήριξη φωνής ή τηλεφωνίας
- Πιθανά ζητήματα συμβατότητας μεταξύ των συσκευών από τους διαφορετικούς κατασκευαστές

	Bluetooth	HomeRF	IEEE802.11b/ Wi-Fi	IrDA
Technology	RF	RF	RF	Infrared
Primary Use	Cable replacement and ad hoc device-to-device connections	Home or small office LANs	Corporate or campus LANs	Cable replacement and ad hoc device-to-device connections (narrow angle)
Maximum speed	1Mbps	10Mbps	11Mbps	4Mbps
Range	30 feet	150 feet	300 feet	3 feet
Connects through walls	Yes	Yes	Yes	No
Connection angle	360 degrees	360 degrees	360 degrees	30 degrees
Data support?	Yes	Yes	Yes	Yes
Native voice/telephony support?	Yes	Yes	No	Yes
	Bluetooth	**HomeRF**	**IEEE802.11b/ Wi-Fi**	**IrDA**
Frequency sharing	FHSS	FHSS	DSSS	
Requires separate access points (base stations)?	No	No	Yes	No
Susceptibility to RF interference	Medium	Medium	High	None
Power requirements	Low	High	High	Low
Manufacturing cost per device	$15 now; dropping to $5	$70–$120	$100–$300	$2

ΣΧΗΜΑ 7-3 Συνοπτικός πίνακας δυνατοτήτων του κάθε συστήματος

ΑΠΟΤΕΛΕΣΜΑΤΑ

- Το Bluetooth χρησιμοποιείται καλύτερα ως τεχνολογία αντικατάστασης καλωδίου, και για να καθιερώσει και τις ιδιωτικές και δημόσιες ad hoc επικοινωνίες μεταξύ δύο ή περισσότερων συσκευών (μέσα σε μια σειρά 30-ποδιών). Δεν έχει τη απόσταση ή το εύρος ζώνης για τις ασύρματες εφαρμογές του τοπικού LAN.

- Το IrDA χρησιμοποιείται καλύτερα ως τεχνολογία αντικατάστασης καλωδίων όπου στενή οπτική επαφή και εγγύτητα μεταξύ των συσκευών υπάρχει. Δεν έχει την απόσταση ή το εύρος ζώνης για τις ασύρματες εφαρμογές του τοπικού LAN, το εύρος γωνίας που απαιτείται για τις ad hoc συνδέσεις, ή την ικανότητα φωνής που απαιτείται για τις εγχώριες εφαρμογές.
- Το HomeRF χρησιμοποιείται καλύτερα στις εφαρμογές εγχώριας δικτύωσης, που έχει ως σκοπό να φέρει τα σήματα φωνής και δεδομένων με την ελάχιστη παρέμβαση. Δεν έχει την απόσταση ή την ευρωστία απαραίτητη για τις εταιρικές εφαρμογές του τοπικού LAN.
- 802.11 χρησιμοποιείται καλύτερα στις εφαρμογές του εταιρικού και τοπικού LAN πανεπιστημιουπόλεων. Δεν έχει αυτήν την περίοδο την επαρκή προστασία παρέμβασης ή την ικανότητα φωνής για τις εγχώριες εφαρμογές.

Για τις τεχνολογίες, εάν τα πράγματα συνεχιστούν τον τρέχων αγώνα τους, είναι πιθανό ότι το Bluetooth θα αντικαταστήσει το IrDA και για την αντικατάσταση καλωδίων και για τις ad hoc συνδέσεις. Οι δυνάμεις του Bluetooth (και η ογκώδης υποστήριξη βιομηχανίας) είναι, ειλικρινά, συντριπτικές, ειδικά όταν βρίσκονται αντιμέτωπες με τους έμφυτους περιορισμούς οπτικής επαφής των υπέρυθρων ακτινών.

Επιπλέον, εάν το 802.11/WI-FI μπορεί να γίνει ευκολότερο στη χρήση (και ελαφρώς χαμηλότερα να διατιμηθεί), είναι περισσότερο πιθανό ότι το WI-FI θα γίνει το de facto πρότυπο για όλη την ασύρματη δικτύωση-ακόμα και στο σπίτι. Εξετάζοντας τον ένα η τον άλλο τρόπο, είναι απίθανο ότι το HomeRF θα κάνει τις επιδρομές του στο εταιρικό περιβάλλον. Εάν είναι να προκύψει μόνο ένα πρότυπο, θα είναι πιθανό να είναι το WI-FI.

Αυτό αφήνει το Bluetooth (για τις περιορισμένου φάσματος και από σημείο σε σημείο συνδέσεις) και το 802.11/WI-FI (για τα ασύρματα δίκτυα) ως πιθανούς επιζώντες οποιωνδήποτε ασύρματων πολέμων τεχνολογίας. Με πολλές από τις ίδιες επιχειρήσεις που υποστηρίζουν και τα δύο πρότυπα, αναμείνετε να δείτε μελλοντικές συσκευές Bluetooth και WI-FI τροποποιημένες και συναλλασσόμενες στην αγορά που θα πωλούνται για την καλύτερη συνύπαρξη, κάθε μια θα στρέφεται σε διαφορετικούς τύπους καταναλωτικών εφαρμογών.

ΚΕΦΑΛΑΙΟ 8
ΜΕΛΛΟΝ-ΣΥΜΠΕΡΑΣΜΑΤΑ

ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΥΞΗΣΕΙΣ

Ποιες όμως θα είναι στο μέλλον οι αυξήσεις στη βασική λειτουργία του Bluetooth; Βεβαίως, νέα profile θα εισαχθούν καθώς συλλαμβάνονται, δημιουργούνται, και εγκρίνονται. Αυτά θα απελευθερωθούν κατά τη διάρκεια του χρόνου υπό μορφή αναπροσαρμογών στην προδιαγραφή ύπαρξης. Επιπλέον, τα σύνολα κρίσιμων τυπογραφικών λαθών θα δημοσιευθούν ως επιφάνεια προβλημάτων. Εντούτοις, οι περισσότεροι υπεύθυνοι για την ανάπτυξη της λειτουργίας του Bluetooth έχουν βρει την προδιαγραφή 1.1 να είναι σταθερή, αν και στις 5 Νοεμβρίου του 2003 εξέδωσαν την προδιαγραφή 1.2 η οποία είναι συμβατή με την 1.1 αλλά οπωσδήποτε θα φέρει κάποιες μικροαλλαγές.

Δεδομένου ότι το Bluetooth ωριμάζει και οι ικανότητες και οι περιορισμοί του είναι δοκιμασμένες σε πραγματικές εφαρμογές, η προσοχή θα γυρίσει αμετάβλητα στο πώς η απόδοσή της μπορεί να βελτιωθεί. Εδώ είναι μερικές από τις δυνατότητες για τις μελλοντικές αυξήσεις στη λειτουργία του Bluetooth, με έμφαση στα χαμηλότερα επίπεδα πρωτοκόλλου :

1. Για τις γρηγορότερες ροές δεδομένων μερικοί θα υποστήριζαν ότι το Bluetooth πρέπει να αυξήσει το ποσοστό δεδομένων για να είναι ανταγωνιστικό. Άλλοι υποστηρίζουν ότι η παρόν ταχύτητα δεδομένων είναι αρκετά γρήγορη για τον προοριζόμενο σκοπό του. Αυτό είναι ένας τομέας έντονης συζήτησης, αλλά είναι σημαντικό να συνειδητοποιηθεί ότι η γρηγορότερη μετάδοση δεδομένων φέρνει και τις αντίστοιχες τιμωρίες υπό μορφή πιο σύντομης απόστασης, μεγαλύτερης κατανάλωσης ισχύος, ή/και μεγαλύτερου κόστους. Στο χαρακτηριστικό ποσοστό δεδομένων (400 kb/s), 100 σελίδες του τυπωμένου κειμένου μπορούν να έχει μεταφερθεί σε περίπου 10 δευτερόλεπτα και μια 600 kB υψηλής ευκρίνειας ψηφιακή φωτογραφία σε περίπου 12 δευτερόλεπτα. Είναι οι υψηλότερες ταχύτητες στοιχείων άξιες τέτοιων "τιμωριών" ; Για να απαντηθεί αυτή την ερώτηση, η ομάδα εργασίας Radio2 έχει διαμορφωθεί

μέσα στη ομάδα ενδιαφέροντος Bluetooth SIG για να ερευνήσει τις υψηλότερες ροές δεδομένων.

2. *Προσαρμοστικό hopping συχνότητας* (*Adaptive frequency hopping* AFH) Το AFH μπορεί να μειώσει την απώλεια πακέτων εάν εφαρμόζεται κατάλληλα. Πολλοί θεωρούν ότι AFH θα γίνει τελικά μέρος της προδιαγραφής Bluetooth.
3. Η αποθήκευση και η ικανότητα μεταβίβασης με παρούσα μορφή της, Bluetooth δεν έχει κανένα επίσημο μέσο για τη σειρά της με την αναμετάδοση των μηνυμάτων μέσω των τρίτων. Φυσικά, το χαρακτηριστικό γνώρισμα μπορεί να εφαρμοστεί στα υψηλότερα πρωτόκολλα, αλλά αυτό μπορεί να είναι δυσκίνητο. Η τοποθέτηση μιας αποθήκευσης και μεταβίβασης ικανότητας στην προδιαγραφή θα παράσχει τις ενσωματωμένες εντολές που μπορούν να χρησιμοποιηθούν ώστε να καθορίζουν τον προορισμό και, εάν είναι απαραίτητο, τη διαδρομή που ένα πακέτο πρέπει να πάρει μέσω των ενδιάμεσων κόμβων Bluetooth. Τα πλεονεκτήματα περιλαμβάνουν μια αποτελεσματική απόσταση που περιορίζεται μόνο από τη διαθεσιμότητα συσκευών κατά μήκος της διαδρομής και διαβιβάζουν χαμηλότερα τη δύναμη για την επίτευξη των πιο στενών κόμβων. Τα μειονεκτήματα περιλαμβάνουν τη χαμηλότερη αξιοπιστία, την αυξανόμενη παρέμβαση από τις πολλαπλάσιες μεταδόσεις, τη μειωμένη ρυθμοαπόδοση, και την υψηλότερη πολυπλοκότητα κόμβων.
4. Οι έξυπνες κεραίες εάν η ικανοποιητική ικανότητα επεξεργασίας σήματος αναπτύσσεται για να ελέγξει μια ηλεκτρονικά πηδαλιουχούμενη κεραία σειράς, κατόπιν η δυνατότητα υπάρχουν για να αυξήσουν πολύ την απόδοση με την κατεύθυνση του κύριου λοβού της κεραίας προς τον επιθυμητό κόμβο. . Κατά συνέπεια, το C/I(carrier to interference ratio) θα βελτιώσει εμφανώς, ενδεχομένως να επιτρέψει τις μειώσεις της μετάδοσης ισχύος. Επίσης, η παρέμβαση σε άλλους χρήστες θα μειωθεί περαιτέρω από άχρηστους στόχους στην κατεύθυνσή τους. Η χαμηλή ισχύς μετάδοση κατεύθυνση- ακτινών θα μπορούσε ενδεχομένως να μειώσει και τη σειρά της ευπάθειας να κρυφακούσει και τη απόσταση της ευαισθησίας στο μπλοκάρισμα. Τα μειονεκτήματα,

φυσικά, είναι το κόστος, η πολυπλοκότητα, και οι απαιτήσεις δύναμης μιας τέτοιας εφαρμογής.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Προφανώς το Bluetooth έχει επιβιώσει από τον ασύρματο πόλεμο. Το Bluetooth σε συνδυασμό με το WI/FI μπορούν να προσφέρουν τα πάντα όσο αναφορά ένα ασύρματο δίκτυο. Επιπλέον το Bluetooth δεν προοριζόταν να γίνει τεχνολογία ασύρματων LAN.Το 802.11b/Wi-Fi και το homeRF είναι τα 2 πρότυπα που δημιουργήθηκαν για αυτήν τη δουλειά. Σχεδιάστηκε ώστε να αντικαθιστά καλώδια(το οποίο το κάνει καλά)και να κάνει συνδέσεις ad hoc από σημείο σε σημείο(το οποίο επίσης κάνει καλά). Αναδιαμφισβήτητα είναι ένα πρότυπο που θα κυριαρχήσει στην αγορά αφού υπάρχουν πολλές μεγάλες εταιρίες που το στηρίζουν και επεκτείνεται σε όλο και πιο πολλές εφαρμογές. Είναι εύκολο στη χρήση, φθηνό για τη δουλεία που προορίζεται, μπορεί να τα βγάλει επάξια εις πέρας. Δεν έχει τίποτα να φοβηθεί.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] www.Bluetooth.org

[2] www.Bluetooth.com

[3] "Bluetooth application developer's : the short range interconnect solution" by Dave Kammer, Gordon Mcnutt, Brian Senese, Jennifer 2002

[4] "Bluetooth operation and use" by Robert Morrow 2002

[5] "Discovering Bluetooth" by Michael Miller 2001

[6] Bluetooth specification 1.1

[7] Bluetooth profiles 1.1

[8] "The mathematical Theryof Communication" Bell System Technical, Journal by shannon

[9] Magnus Sommansson, Ericsson "Test Systems Validation Guideline", Version 0.8, 2000