Debreceni Egyetem
Informatikai Kar

Vezetéknélküli hálózatok biztonsági kérdései

Készítette:
Papp Szilárd
Programozó Matematikus Szak

Témavezető:
Dr. Krausz Tamás
Információ Technológia Tanszék

TARTALOM

1. BEVEZETÉS

Régebben a számítógép csak számítógép, a telefon pedig csak telefon volt. Napjainkban ez a megkülönböztetés már sokkal nehezebb, és az elkövetkező öt évben valószínűleg értelmét is fogja veszíteni. A vezeték vagy drót nélküli (wireless) technológiák és az internetes telefonálás fejlődésének köszönhetően a mai személyi számítógépek hordozhatóbbak, mint valaha, és még a saját számítógépünkről is kezdeményezhetünk telefonhívást. Eközben a mobiltelefonokba, elektronikus személyi titkárokba (PDA, Personal Digital Assistant), és vezeték nélküli levelezőeszközökbe belekerültek az asztali számítógép jellemvonásai, szolgáltatásai, és processzorteljesítménye.

Ezeknek a fejlesztéseknek számos előnye van. A vezeték nélküli megoldások nagyobb mobilitást és kényelmet nyújtanak otthonra és könnyebb internet-hozzáférést otthonunkon kívül. Pillanatnyilag a vezeték nélküliség néhány nyilvános hozzáférési pontra (hotspot) korlátozódik, de idővel ugyanazt a vezeték nélküli internet-hozzáférést lehet majd élvezni a számítógépen, mint a mobiltelefonokon.

No persze, ahogy mostanra már nyilván kitaláltuk, az új műszaki megoldások jó tulajdonságait össze kell vetni az esetleges biztonsági hátrányokkal. A hátrányok, különösen a vezeték nélküli rendszerek esetében bizony jelentősek. A problémák közül még a szerényebb, ha valaki az internetkapcsolatunkra csatlakozva szabadon töltöget és ingyen böngészik – a lista csúnyábbik végén olyan tolvajok és bűnözök találhatók, akik személyes adatokat lopnak. A mobiltelefonok kézi számítógéppé alakulásuk közben áldozatul esnek a PC-ket gyötrő kártevőknek (már léteznek mobiltelefon-vírusok), és a számítógép telefonhoz közeledésének (VoIP) is megvannak a maga hátrányai, amelyek közül néhánynak biztonsági következményei is vannak.

Szakdolgozatom célja a vezeték nélküli számítógép-hálózatok különböző megoldásainak és ezek biztonsággal kapcsolatos kérdéseinek bemutatása.

Mivel a vezeték nélkül kommunikáló eszközök száma rohamosan növekszik, és ezzel együtt a levegőben terjedő információ mennyiség is, a vezeték nélküli hálózatok egyre inkább

célponttá válnak a támadók szemében. Hiszen egy nem megfelelően védett WLAN esetében sokkal könnyebb az információk megszerzése, mint vezetékes társából, mert a támadó elég, ha csak az antennák hatósugarában van. Be kell látnunk, hogy az eszközök megfelelő biztonsági beállítása roppant fontos, mert egy cég informatikai infrastruktúrájának működése és biztonsága élet-halál kérdése a mai világban. Persze feltörhetetlen, kijátszhatatlan védelem soha sem létezik, de mindent meg kell tennünk, hogy ez a lehető legnehezebb legyen. Ezt a legújabb technikák és eszközök hálózatunkba való integrálásával érhetjük el.

2. HOGYAN MŰKÖDIK A VEZETÉK NÉLKÜLI HÁLÓZAT ?

Manapság számos háztartásban előfordul, hogy egynél több, közös internetkapcsolatot használó számítógép van. Egyre több az otthoni hálózat, amelynek számítógépei között megengedett a fájlcsere, valamint az internethasználaton való osztozkodás. Ezekben az otthoni hálózatokban a számítógépek vagy kábellel, vagy vezeték nélkül csatlakoznak egymáshoz. A vezeték nélküli hálózatokat azért szeretjük, mert nem fut kábel minden számítógéphez a házban, és a családtagok egyszerre is használhatják az Internetet akár a fürdőszobából, akár a nappaliból, az otthoni irodából vagy akár még a kertből is (a hozzáférési pont jelerősségétől függően).

Egy alapszintű vezeték nélküli kapcsolathoz két összetevőre van szükség: egy vezeték nélküli kártyára vagy lapkára a számítógépben, illetve egy hozzáférési pontra (AP, access point), amit néha vezeték nélküli útválasztónak (wireless router) is hívnak. A mai hordozható számítógépek többsége beépítve tartalmazza a vezeték nélküli elérés lehetőségét, ha pedig régebbi laptopunk van, vásárolhatunk egy kártyát, ami biztosítja ezt a képességet.

A hozzáférési pont többféle módon is csatlakozhat az Internetre: telefonos betárcsázással, DSL modemen vagy kábelmodemen keresztül. Egy hozzáférési ponthoz több számítógép is csatlakozhat rádiós kapcsolaton keresztül.

A mai otthoni vezeték nélküli kapcsolatoknak egy szabványrendszer, az úgynevezett Wi-Fi az alapja, ami a „wireless fidelity” rövidítése („vezeték nélküli hűség”, a Hi-Fi alapján).

A WiFi szabványt az Institute of Electrical and Electronics Engineers (IEEE) gondozza – ez a szervezet vizsgálja felül a műszaki szabványokat, hogy biztosítsa a különböző vállalatok által gyártott termékek problémamentes együttműködését. A Wi-Fi több szabványt is tartalmaz, amelyek a 802.11 kód alá tartoznak, a vezeték nélküli hálózati szabványokat kidolgozó munkacsoport azonosítója után.

2.1 A vezeték nélküli kapcsolatról

Ahogy a bevezetőben is említettem, vezeték nélküli kapcsolat többféle módon is létesíthető két vagy több eszköz között. A felsorolt technológiák alapja azonban közös, mind valamilyen *rádiófrekvencia* felhasználásával továbbítják és fogadják az adatokat. Az egyetlen kivétel az infravörös adatátvitel, mely esetében bizonyos hullámhosszú fény segítségével jön létre a kapcsolat. A Bluetooth 2,4 GigaHertz-es (gigahertz: GHz), a WiFi pedig 2,4 / 5 GHz -es rádiófrekvenciát használ az adatátvitelhez. Ezek a paraméterek alapvetően meghatározzák a technológia felhasználásának lehetőségeit: az infravörös kapcsolat csak két egymást tökéletesen "látó" készülék esetén működik, mivel egy irányban terjedő fényről van szó. A Bluetooth és a WiFi segítségével azonban képesek vagyunk egymást fizikailag nem "látó" készülékek között is kapcsolatot teremteni, mivel a rádióhullámok áthatolnak a szilárd anyagokon is, bár ekkor erősségük, hatótávolságuk jócskán lecsökkenhet.

A továbbiakban a vezeték nélküli kapcsolaton ezért WiFi minősített, WLAN kapcsolatot értek.

A vezeték nélküli kapcsolatra képes eszközök valamely gyártó által készített rádióadót/vevőt tartalmaznak, amellyel képesek adatokat küldeni és fogadni. Szerencsére ezzel nem kell sokat foglalkoznunk, az operációs rendszer elfedi előlünk a részleteket: a szokásos meghajtó progam telepítése után elvileg már használhatjuk is WiFi eszközünket.

2.2 A vezeték nélküli hálózat lehetőségei

A vezeték nélküli hálózatok lehetőségei *szinte korlátlanok*, sorra jelennek meg hétköznapi eszközök, amelyek rendelkeznek WiFi kapcsolat-teremtési képességgel (telefonok, asztali PC-k, notebook-ok, egyéb szórakoztató elektronikai eszközök és természetesen PDA-k). Vezeték nélküli eszközök használatával megszabadulhatunk az idegesítő kábelrengetegtől, kényelmesebb,

rendezettebb környezetet teremtve magunk körül. A WiFi lehetőségeit elsősorban az internet elérésében élvezhetjük. Itt kell szót ejteni az ún. *Hotspot* -okról, azaz "vezeték nélküli internet elérési pontokról". Ezek száma napról napra rohamosan növekszik, találkozhatunk velük éttermekben, szállodákban, kávézókban, oktatási intézményekben, céges székházakban, de akár közterületeken is. Ezt a szolgáltatást ingyen vagy fizetés ellenében vehetjük igénybe, szolgáltatótól függően.

Ennek az új technológiának illetve a hotspot-ok segítségével hozzáférhetünk adatainkhoz, email-einkhez, kedvenc internetes oldalainkhoz, különféle multimédiás anyagainkhoz, sőt még céges adatbázisunkhoz is, kényelmesen és bárhol, ahol ilyen jellegű kapcsolatot tudunk teremteni. Cégünknél, ha például egy megbeszélésre tartunk irodánkból a tárgyalóba, megszakítás nélkül kapcsolatban maradhat a PDA-nk vagy notebookunk és azonnal kezdhetjük prezentációnkat anélkül, hogy megvárakoztatnánk ügyfeleinket.

2.3 A sávszélesség kérdése

A vezeték nélküli hálózat szokásos felhasználása azonban rendszerint az internet megosztás a vezeték nélküli kliens eszközök számára. Egy DSL kapcsolat néhányszáz KiloBit/másodperc sávszélességét ennél jóval több kliens között oszthatjuk meg, és tekintve az internet illetve email használatunk "löketszerű" szokásait (letöltjük az oldalt, emailt, majd egy darabig olvasgatjuk, azaz nem generálunk folyamatos hálózati forgalmat, nem terheljük a hálózatot: nem foglaljuk a sávszélességet), a hálózat egyetlen felhasználója sem fog jelentős lassulást tapasztalni a kommunikációban, tehát mindenki boldogan internetezhet. Ebből következtethetünk arra, hogy az Acces Point -ok dinamikusan kezelik, hogy kinek mennyi sávszélességet biztosítanak éppen, az aktuális kívánalmaknak megfelelően. Ezek a hálózati eszközök, az Access Point -ok, tehát pontosan úgy viselkednek, mint vezetékes társaik, a különbség csak annyi, hogy itt nem kell a kábelekkel vesződnünk és sokkal mobilabbak vagyunk.

2.4 Vezeték nélküli hálózattípusok

A vezetékes hálózatokhoz hasonlóan a vezeték nélküli hálózatok is különböző típusokba sorolhatók az adatátvitel távolsága szerint.

2.4.1 WWAN-ok (nagy kiterjedésű vezeték nélküli hálózatok)

A WWAN technológiák lehetővé teszik a távoli nyilvános és magán hálózatokon történő vezeték nélküli kommunikációt. Ezek az összeköttetések nagy földrajzi távolságokra terjedhetnek ki, például városokra vagy országokra, vezeték nélküli szolgáltatók több antennaállomása vagy műholdas rendszere segítségével. A jelenlegi WWAN technológiák második generációs (2G) rendszerekként ismertek. A legfontosabb 2G rendszerek közé a GSM (Global System for Mobile Communications), a CDPD (Cellular Digital Packet Data) és a CDMA (Code Division Multiple Access) tartozik. Hamarosan komolyabb erőfeszítések történnek a második generációs hálózatok – melyek némelyike korlátozott barangolási képességekkel rendelkezik és inkompatibilis egymással – átalakítására harmadik generációs (3G) technológiákká, melyek globális szabványokat követnek, és világméretű barangolási képességekkel rendelkeznek. Az ITU aktívan támogatja egy globális 3G szabvány kifejlesztését.

2.4.2 WMAN-ok (nagyvárosi vezeték nélküli hálózatok)

A WMAN technológiák lehetővé teszik egy nagyváros különböző pontjai közötti vezeték nélküli kapcsolatokat (például több irodaház között egy városban vagy egy egyetem területén) az optikai kábel vagy rézvezeték, valamint a bérelt vonalak magas költsége nélkül. A WMAN hálózatok ezen kívül tartalékrendszerként szolgálhatnak vezetékes hálózatok mellett, ha a vezetékes hálózatok elsődleges bérelt vonalai használhatatlanná válnak. A WMAN hálózatok rádióhullámokat vagy infravörös fényt használnak adatátvitelre. Egyre keresettebbek a szélessávú vezeték nélküli hálózatok, melyek nagy sebességű internet-hozzáférést biztosítanak. Bár különböző technológiák léteznek, például az MMDS (multichannel multipoint distribution service, többcsatornás többpontos elosztó szolgáltatás) és az LMDS (local multipoint distribution services, helyi többpontos elosztó szolgáltatás), az IEEE 802.16 szélessávú vezeték nélküli

hozzáférési szabványokon dolgozó munkacsoportja még mindig fejleszti ezeknek a technológiáknak a szabványait.

2.4.3 WLAN-ok (helyi vezeték nélküli hálózatok)

A WLAN technológiák segítségével a felhasználók vezeték nélkül köthetők össze helyi hálózatban (például egy vállalati vagy egyetemi épületben vagy egy nyilvános helyen, például repülőtéren). A WLAN-ok ideiglenes irodákban vagy más helyeken használhatók, ahol kiterjedt kábelezés nem oldható meg, vagy egy meglévő LAN-t kell kiegészíteni, hogy a felhasználók különböző időpontokban különböző helyeken dolgozhassanak egy épületben. A WLAN-ok kétféleképpen működhetnek. Az infrastrukturális WLAN-okban a vezeték nélküli állomások (rádiós hálózati kártyával vagy külső modemmel rendelkező eszközök) vezeték nélküli hálózat-elérési pontokhoz csatlakoznak, melyek hidakként működnek az állomások és a meglévő gerinchálózat között. Az egyenrangú (ad hoc) WLAN-okban kis helyen (pl. egy konferenciateremben) számos felhasználó képes ideiglenes hálózatot kialakítani hozzáférési pontok nélkül, ha nincs szükségük hálózati erőforrásokra.

1997-ben az IEEE elfogadta a WLAN-okra vonatkozó 802.11 szabványt, amely 1 és 2 Megabit/másodperc (Mbit/s) közötti átviteli sebességet határoz meg. A 802.11b, amely egyre inkább domináns helyzetre tesz szert a szabványok között, 11 Mbit/s sebességet tesz lehetővé 2,4 gigahertzes (GHz) frekvenciasávban. Egy másik új szabvány a 802.11a, amely 54 Mbit/s maximális adatátviteli sebességet tesz lehetővé 5 GHz-es frekvenciasávban.

2.4.4 WPAN-ok (vezeték nélküli személyes hálózatok)

A WPAN technológiák segítségével a felhasználók személyes működési környezetükben (POS) használt eszközei (pl. személyi digitális asszisztensek, mobiltelefonok és laptopok) ad hoc vezeték nélküli kommunikációra képesek. A POS betűszó a személy legfeljebb 10 méteres környezetét jelöli. Jelenleg a Bluetooth és az infravörös fény a WPAN két legfontosabb technológiája. A Bluetooth egy kábelhelyettesítő technológia, ami rádióhullámokat használ legfeljebb 10 méteres távolságban történő adatátvitelre. A Bluetooth adatok falon, zseben és aktatáskán keresztül is átvihetők. A Bluetooth technológia fejlesztését a Bluetooth SIG (Special

Interest Group) végzi, amely 1999-ben adta közre a Bluetooth 1.0-s verziójának specifikációját. Alternatív lehetőégként, nagyon kis távolságon belül (egy méter vagy kevesebb) a felhasználók infravörös kapcsolatot is használhatnak.

A WPAN technológiák fejlesztésének szabványosítására az IEEE megalakította a 802.15 munkacsoportot. Ez a munkacsoport fejleszti a WPAN szabványt a Bluetooth 1.0-s verziójú specifikációja alapján. A szabványtervezet elsődleges célkitűzése a kis komplexitás, a kis áramfelvétel, az együttműködési képesség és a 802.11 hálózatokkal való együttélés.

3. VEZETÉKES ÉS VEZETÉK NÉLKÜLI HÁLÓZATOK

A vezetékes hálózatokat már jó harminc éve használjuk, a "vezeték nélküliség" viszont csak néhány éve került be a köztudatba, kecsegtető lehetőségei azonban rendkívüli ütemben növelik ismertségét és alkalmazását. Ma már rengeteg olyan termék van, amellyel olcsón kiépíthetjük akár otthoni vezeték nélküli hálózatunkat is, tehát ez a technológia már nem csak a nagy cégek, kormányzati és oktatási intézmények sajátja, hanem bárki által elérhető!

A vezetékes hálózat hátránya a vezeték nélkülivel szemben, hogy ha kapcsolódni akarunk hozzá, mindenképpen valamilyen kábeles összeköttetés kell létrehoznunk, ami igen csak korlátozza a mozgásunkat, vagy mai divatos kifejezéssel élve a mobilitásunkat. Vezeték nélküli hálózat esetében azonban nincs szükségünk kábelekre, készülékeink hatósugarán belül bárhol kapcsolatot létesíthetünk más eszközökkel. Kompromisszumot pedig igazán nem kell kötnünk WiFi hálózat használata esetén a vezetékes hálózatokhoz képest, kizárólag a maximum átviteli sebességet tekintve.

3.1 Vezetékes hálózatunk bővítése

Visszatérve a WLAN hálózatunk összeállításához, meg kell említeni azt a szokványos esetet, amikor vezetékes hálózatunk már ki van építve, az internetcsatlakozásunk eleve megosztott egy vezetékes router segítségével, és egy vagy több asztali gépünk csatlakozik hozzá, azonban szeretnénk vezeték nélküli képességgel is bővíteni ezt a már meglévő és beállított hálózatot. Ebben az esetben csupán egy Access Point-ra van szükségünk, az előbb felvázolt Gateway (átjáró) jellegű eszközhöz képest, amely kevesebb szolgáltatást nyújt ugyan, de azokra nincs is szükségünk és egyben olcsóbb is, mint az említett mindent-egybe készülék. A megvásárolt

Access Point segítségével hálózatunkat tehát kiegészíthetjük, felruházhatjuk vezeték nélküli képességgel, azaz olyan eszközt iktatunk be a hálózatba, amely lehetőséget ad vezeték nélküli eszközeinknek, hogy a már meglévő hálózatunkhoz csatlakozzanak, kábelrengeteg nélkül. Nincs más dolgunk, mint ezt az eszközt rádugni a vezetékes routerünk egyik LAN portjára, bekonfigurálni és a dolog már működik is.

4. VEZETÉK NÉLKÜLI SZABVÁNYOK

4.1 IEEE Szabványok

A jelen fejezetben három IEEE-szabványt mutatok be, a 802.11b, 802.11g, 802.11a. A b, g és a szabványok az adatátvitel alapvető kérdéseivel foglalkoznak. A b, g és a jelű szabványok több dologban is eltérnek: a kapacitásban (mennyi adatot képesek átvinni adott idő alatt), az áthidalt távolságban (milyen messzire képesek továbbítani a jelet), a használt rádióhullámok tartományában, illetve hogy miként kezelik az interferenciát. (A rádióhullámú jeleket zavarja a tereptárgyak – falak, födémek, természeti képződmények, például hegyek – által okozott interferencia, de ugyanígy ütközhetnek a más készülékek, például mikrohullámú sütők gerjesztette elektromágneses mezővel is.)

A legszélesebb körben elfogadott szabvány a 802.11b, ami azt jelenti, hogy a megvásárolt vezeték nélküli berendezések és nyilvános hozzáférési pontok (amelyek például kávézókban találhatók) többsége használja vagy támogatja ezt a szabványt. A 802.11b maximális kapacitása másodpercenként 11 megabit, és körülbelül 50 méter távolságot képes áthidalni.

Az újabb szabványok még nagyobb sebességet nyújtanak – másodpercenként 54 megabitet –, és mostanra már talán át is vették a 11 megabites eszközöktől a vezető helyet. Szinte naponta jelennek meg új termékek, amelyek közül néhány többféle szabványt is támogat, és a hálózati követelményektől függően váltani is tud köztük. A szabvány kiválasztásakor különféle kompromisszumokat kell kötni. A 802.11a hatótávolsága például feleakkora, mint a többié, de az 5 GHz körüli sávban működik, ami kevésbé zsúfolt, és kevésbé hajlamos a mágneses interferenciára. A 802.11b-nek és g-nek nagyobb a sebessége, és rengeteg fogyasztói Wi-Fi eszköz és vezeték nélküli hálózat támogatja. Ezekben azonban érezhető interferenciát okozhatnak a vezeték nélküli telefonok és mikrohullámú sütők. A három Wi-Fi szabványt az 1. táblázat foglalja össze.

Szabvány	Legnagyobb sebesség	Hatótávolság	Terméktámogatás	Frekvencia
802.11b	11 Mb/mp	30-50 m	Széleskörű támogatás a vezeték nélküli eszközökben	2,4 GHz
802.11g	54 Mb/mp	30-50 m	Egyre támogatottabb. Összeegyeztethető a 802.11b szabvánnyal (de csak 11 Mb/mp sebességen)	2,4 GHz
802.11a	54 Mb/mp	10-25 m	Új technológia, jelenleg a legkevésbé támogatott. Nem működik együtt a 802.11b vagy g szabványokkal	5 GHz

1. táblázat Vezeték nélküli hálózati szabványok

Tegyük fel elhatároztuk magunkat, hogy kiépítjük otthonunk vagy cégünk vezeték nélküli hálózatát engedve a kor követelményeinek és persze kényelmünknek. Első körben minden bizonnyal meglepetésként ér bennünket a kapható eszközök hatalmas választéka, itt aztán nem lesz egyszerű a választás! Hirtelen különböző számokkal, betűkkel és ezek különböző kombinációival találjuk szemben magunkat, ami rendszerint jól elbizonytalanítja a vásárlót, legalábbis ha nincs megfelelően felkészülve.

A vezeték nélküli hálózatok az évek során több szabvánnyal is gazdagodtak. A mai ***hivatalos szabványok*** (az adatátviteli képességet, sávszélességet tekintve) az *IEEE 802.11b, 802.11a,* és *802.11g*. Az IEEE (Institute of Electrical and Electronics Engineers) a nemzetközi szabványügyi szövetség, a 802.11 a WiFi szabványrendszert a B, A és G betűk pedig a konkrét szabványt jelzik. Lássuk ezeket a szabványokat kicsit bővebben.

4.1.1 802.11b

Ez a szabvány a 2,4 GHz -es nyílt frekvenciatartományt használja, ahogy mikrohullámú sütőnk, vezeték nélkül telefonunk és egyéb hétköznapi vezeték nélküli eszközeink is. Ennek megfelelően a különböző eszközök rádióhullámai interferálhatnak, magyarul zavarhatják egymást. A továbblépést az alap 802.11-nél is alkalmazott direkt szekvenciális CDMA kódjainak kicserélésével érték el.

Sávszélességét tekintve *11Mbit/másodperc* (megabit: Mbit) *elméleti maximum adatátviteli sebességre* képes, ami *a gyakorlatban 4-6Mbit*-et jelent. Ez jóval gyorsabb, mint például DSL

kapcsolatunk sebessége, azaz bőven elegendő több kliens egyidejű internet kiszolgálására, komolyabb adatforgalom esetén (zenehallgatás, filmnézés, fájlmásolás stb.) azonban már kevés lehet. Előnye viszont, hogy manapság már nagyon elterjedt és nagyon olcsó, ezért találkozunk vele a legtöbb elektronikai eszközben (telefonokban, PDA-kban stb). Hatótávolsága 30-50 méter épületben, 1 km épületen kívül az Access Point-ra történő tiszta rálátás esetén.

4.1.2 802.11a

A 802.11a szabvány szinte egyszerre jelent meg a 802.11b -vel, amelytől azonban több aspektusban is eltér. Legfontosabb, hogy az *5GHz -es tartományban üzemel*, tehát szokásos eszközeink, amelyek rádiófrekvenciás hullámokat bocsátanak ki, nem zavarják az adatforgalmunkat. A megemelt frekvenciából adódóan sávszélessége is növekedett, *maximum 54Mbit/másodperc* (a gyakorlatban 21-22Mbit), viszont a nagyobb frekvenciájú rádióhullámok tulajdonságainak köszönhetően (könnyebben elakadnak a különböző tárgyakban, falakon) *hatótávolsága kisebb*, mindössze 10-25 méter épületen belül. Ezt ellensúlyozza, hogy az 5GHz-es tartományban több, egymást nem átfedő "csatornát" vehetünk akár egyszerre is igénybe, azaz növelhetjük konkrét sávszélességünket, lehetővé téve, hogy egyszerre több felhasználó nyugodtan nézhessen filmet (streaming) vagy másolhasson nagy fájlokat anélkül, hogy jelentős sebességcsökkenést érzékelne. Ez az igen korszerű ortogonális frekvenciatartománybeli multiplexálás (Orthogonal Frequency Division Multiplexing, OFDM)

4.1.3 802.11g

A "legfrissebb" hivatalos IEEE vezeték nélküli szabvány, ugyanabban a tartományban üzemel, mint a 802.11b, azonban *megnövelt, 54Mbit/másodperc sávszélességgel rendelkezik*, ami gyakorlatilag 15-20Mbit-et jelent a valóságban, tehát az *A* változattal azonos képességű. Hatótávolsága viszont a *B* változatéval megegyező, épületen belül 30-50 méter. Ez a szabvány visszafelé kompatibilis a *B* változattal, azaz egy *G* -s eszköz képes kommunikálni egy *B* -s Access Point-tal illetve egy *B* -s eszköz is egy *G* -s Access Point-tal.

4.1.4 802.11n

A 802.11n két legfontosabb előnye a gyorsabb adatátvitel (akár 120Mbps valós körülmények között is) és a jelenleg elérhetőnél akár másfélszer nagyobb lefedettség. További előny, hogy a több antennának köszönhetően képes összeilleszteni a jeltöredékeket, így számos olyan ponton is vezeték nélküli kapcsolat biztosítható, ahol eddig eltűnt a jel.
A legfontosabb változtatás a 40 MHz-es csatorna implementálása. Az eredeti terveket módosítva az új verzió képes a korábbi 2,4 GHz-es sávot használó eszközöket kezelni úgy, hogy két 20 MHz-es frekvenciát használ egymás mellett. Az új szabvány szerint a rendszer folyamatosan figyeli, vannak-e a környezetében olyan régebbi eszközök, melyek nem képesek kezelni a szélesebb sávszélességet. Ha talál ilyet, a 802.11n eszköz leszabályozza önmagát, és csak az egyik 20 MHz-es sávon küldi az adatokat. Minderre úgy képes, hogy a 802.11n MIMO technológiájának köszönhetően továbbra is 802.11n sebességet biztosít.
A másik jelentős változás szerint a 802.11n eszköz az adatküldés előtt ellenőrzi, hogy mindkét csatorna szabad-e. A harmadik fejlesztésnek köszönhetően a Bluetooth képes eszközök jelezhetik, hogy nem kívánnak 40 MHz-es módban adatot fogadni. Természetesen a Bluetooth-képes eszköznek egyben WLAN felülettel is kell rendelkeznie a jelzés küldésére – ilyen például az Apple iPhone.
Az új szabványnak megfelelően az 5 GHz-es sávon kommunikáló IEEE 802.11a eszközök is képesek kihasználni a teljes 40 MHz-es csatornát.
Bár a végleges szabvány egy lépéssel közelebb került az elfogadáshoz, még számos tennivaló vár a bizottságra. A 2.0 verzió elfogadása márciusra várható, a legújabb, véglegesítésre szánt 3.0 verzió pedig májusra várható. Amint a 3.0 tervezetet az IEEE tagok 75 százaléka elfogadja, a szabvány megindul a hivatalos véglegesítés útján.

4.2 Optikai megoldások

4.2.1 A lézeres adatátvitel

A lézeres átvitelt alkalmazó adó- vevő párokat pont-pont közötti adatátvitelre használhatjuk. A kommunikáció teljesen digitális, a lézerfény irányított energiakoncentrációja nagyobb távolság (néhány km) áthidalását teszi lehetővé. Az illetéktelen lehallgatás, illetve külső zavarás ellen viszonylag védett. Az időjárási viszonyok azonban befolyásolják fény terjedését, így az eső, a köd, a légköri szennyeződések sajnos zavarként jelentkeznek. Felhasználható lokális hálózatok, telefonközpontok összekötésére. A megvalósított adatátviteli sebesség jelenleg 2 és 155 Mbps között van. Hosszabb (3,5 km) távolságok áthidalására, de rövid távolsága esetén (300-400 m) elérhető akár 1,5 Gbps átviteli sebesség is. A technológia folyamatos fejlődést mutat ezért várható, hogy egyre nagyobb távolságokra és egyre nagyobb adatátviteli sebességre lesz képes a közeljövőben.

4.2.2 IRDA

A számítástechnikában már régen felmerült az igény, hogy a számítógépek egyszerűen tudjanak egymással alkalmi kommunikációt kialakítani. Egy kézenfekvő megoldást kínál a háztartási szórakoztató berendezések távirányítóinál már régóta alkalmazott infravörös fény. A kilencvenes évek elején el is készültek az első ilyen berendezések, de szabványok nélkül ezek csak saját típustársaikkal tudtak kommunikálni. Ekkor alakult meg az IrDA csoportosulás és szabványosította az infravörös kapcsolatokat több különböző rétegben. Lássuk, hogy is néz ez ki.

IrDA DATA

Ez az ága az IrDA szabványnak a régebbi, ez szolgál tényleges adatátvitelre 9,6 kbit/sec-től egészen 4 Mbit/sec-ig. Az IrDA átvitel 1 méter távolságig kell, hogy működjön (létezik alacsony fogyasztású változat is, ahol ez csak 20 cm), kétirányú adatkapcsolatot biztosít és CRC

kódolással védi az adatokat. A fizikai rétegre az IrLAP (Link Access Protokol) épít, ami biztosítja a hibajavítást valamint a környezetben lévő készülékek felismerését. A következő réteg az IrLMP (Link Management Protocol) ami biztosítja, hogy egy fizikai IrDA kapcsolaton keresztül több logikai kapcsolat is működhessen illetve lehetőséget biztosít, hogy a partnerek megvalósított protokolljait és szolgáltatásait feltérképezzük. Ez a 3 (fizikai, IrLAP, IrLMP) réteg kötelező, a további protokollok már opcionálisak.

A 4. rétegben IAS (Information Access Service) információt nyújt a megvalósított protokollokról míg a Tiny TP (Transfer Protokol) az adatok átvitelét szabályozza, szükség szerint felszabdalva és összerakva az átviendő adatmennyiséget.

Az 5. rétegben találhatóak a leglényegesebb protokollok, alapjában véve ezek határozzák meg, az elérhető szolgáltatásokat.

IrCOMM: soros és párhuzamos port emuláció (ezt használják az IrDA-t támogató mobiltelefonok)

IrOBEX: objektumokat (fájlokat) lehet cserélni vele, például a Palm sorozat gépei a névjegyek infravörös cseréjekor egy vCard típusú fájlt küldenek át IrOBEX szabvány szerint.

IrTran-P: képek elküldéséhez, ezt támogatják például a Casio digitális fényképezőgépei és a Nokia 9110 és a Sharp WinCE palmtopjai.

IrMC: mobil telefonok kezelése, a telefonkönyv, a telefonban lévő naptár, hívás vezérlés és magának a hangnak az átvitelét specifikálja.

IrLAN: LAN hozzáférés IrDA-n keresztül.

Kicsit kilóg a sorból az IrDA Lite, ami egyszerűbb eszközöknek egy olyan megvalósítási lehetőségek kínál, ami kompatibilis a teljes IrDA protokoll csomaggal, de egyszerűbben megvalósítható.

IrDA CONTROL

Az IrDA control nagyobb hatótávolságú de lassabb berendezésekhez készült, tipikusan billentyűzetekhez, egerekhez, távirányítókhoz és játékvezérlőkhöz. A remények szerint ez a szabvány a számítógépeken kívül a tévéknél, játékkonzoloknál, webtévéknél is el fog terjedni. Itt kétirányú 75 kb/sec átvitel a követelmény, minimum 5 m hatótávolsággal, amit egyszerre 8 különböző berendezés is használhat.

IrDA átvitel rétegei

A kommunikáció az IrDA 1.0 ajánlás szerint a 9.6kbps - 115kbps sebességtartományra korlátozódik (SIR). Az újabb IrDA ajánlás már 4Mbps maximális sebességet tartalmaz (FIR), és kidolgozás alatt van az a 16Mbps (VFIR) maximális átviteli sebességű eszközök IrDA specifikációja is. Létezik egy 576kbps/1.152Mbps szinkron átviteli mód is. Az IrDA protokoll - hasonlóan az ISO/OSI modellhez - rétegekre tagolódik, melyek egy része szükséges az átvitelhez, míg a többi az átviteli feladattól függően választható. IrTran-P IrObex IrLan IrCom

<table>
<tr><td>IrTran-P</td><td>IrObex</td><td>IrLan</td><td>IrCom</td><td>IrMC</td></tr>
<tr><td>LM-IAS</td><td colspan="4">Tiny Transport Protocol - Tiny TP</td></tr>
<tr><td colspan="5">Ir Link Mgmt - MUX - IrLMP</td></tr>
<tr><td colspan="5">Ir Link Access Protocol - IrLAP</td></tr>
<tr><td>Async Serial-IR 9600-115.2kb/s (SIR)</td><td>Sync Serial-IR 0.576 és 1.152Mb/s (MIR)</td><td>Sync 4PPM 9.6kb/s-4Mb/s (FIR)</td><td colspan="2">Sync 16PPM 9.6kbps-16Mb/s (VFIR)</td></tr>
</table>

2. táblázat Az IRDA rétegei

Szükséges rétegek:

PHY (phisical layer)

Az optikai karakterisztika, és a kódolás leírása. Tipikusan 1 méteres hatótávolság és 15 fokos nyílásszögű kónusz jellemzi, de a fejlesztések ezt befolyásolhatják. Rálátás szükséges a

kommunikációhoz, de annak minőségét befolyásolhatja az interferencia más Ir eszközökkel, fluoreszcens fényforrással, napfénnyel vagy holdsugárral. A minimális hatótávolságot az alacsony energiafogyasztású eszközök esetében 0.2m-ben határozták meg. Irodai környezetben a gyártók tipikusan 2-2.5m-ig specifikálják az eszközök hatótávolságát. A hatótávolság növelésénél figyelembe kell venni a szem biztonságára vonatkozó IEC és CENELEC emissziós ajánlásait.

IrLAP (Link Access protokol)

Alapszintű megbízható pont-pont közti half-duplex kapcsolatot létesít, melyben nincs ütközés-detektálás.

LM (Link Management Protocol)

A protokoll többszörözi a szolgáltatásokat és alkalmazásokat az IrLAP kapcsolaton. Szorosan kapcsolódik az IAS-hoz.

IAS (Information Access Service)

Az eszköz számára elérhető szolgáltatások és alkalmazások tára.

Opcionális rétegek:

TTP (Tiny Transport Protocol)

Csatornánkénti átvitelvezérlés az egyenletes adatátvitelhez. IrDA Lite - 9.6kbps átviteli sebességű redukált kódkészletű protokoll.

IrOBEX (Object Exchange protocol)

Egyszerű fáj- és adatobjektum-átvitel.

IrCOMM

Soros és párhuzamos port emuláció.

IrLAN

Hálózati hozzáférést biztosít.

IrTran-P

Digitális kamerák és egyéb képfelvevők valamint fotónyomtatók protokollja képek átviteléhez.

IrMC

Mobil kommunikációs eszközök (telefon stb.) protokollja, mely leírja, hogy hogyan vihetők át olyan információk mint határidőnapló bejegyzések, telefonszámok, címek, üzenetek.

4.3 Bluetooth

Néhány évvel ezelőtt merült fel az Ericsson fejlesztői körében, hogy egy valóban kis költségű, kis fogyasztású kábelt helyettesítő rádiós eszközre szükség lehetne. Lehetséges használatát felvázolták különféle szituációkban és ennek nyomán sorra került a megvalósíthatóság vizsgálata is, mind technikailag, mind pedig gazdasági szempontokból.

Egy ilyen eszköz alapot szolgáltathat arra, hogy a hordozható, népszerű szóhasználattal a mobil eszközök kommunikálhassanak egymással, "ad hoc" összekapcsolási lehetőséget teremthet egy újszerű, personal area network létrehozására, ami hasonló előnyöket nyújthat, mint az irodai-munkahelyi környezetben a LAN, a local area network. A Bluetooth cégek konzorciuma által kidolgozott technikai specifikáció megvalósíthatóvá teszi ezt a víziót: javított, 1.1-es változata

2001 tavaszán került közzétételre, és mintegy 1500 oldal terjedelemben minden technikai részletkérdésre igyekszik választ adni.

Az utolsó 10 év fejlődése a mikroelektronika és különösen a VLSI technológia területén széles körben elterjedtté tette a számítógépes és távközlési erőforrásokat, korábban elképzelhetetlen teljesítményű feldolgozó egységek és hatalmas tároló területek, memóriák kerültek beépítésre mindennapi eszközeinkbe.

A tömegfogyasztásra szánt PC-k, laptopok, személyes célú, kézbe fogható és állandóan kéznél lévő eszközök, mobil, és vezeték nélküli telefonok (cellular and cordless phones) személyi digitális asszisztens (PDA) eszközök és ezek kiegészítői és perifériái sikerét az egyre csökkenő méretek és a mérséklődő árak alapozták meg. Az adat és információtovábbítás ezek között az eszközök között a mai napig leginkább kábelek közvetítésével oldható meg. Egy új, univerzális célú rádiós kapcsolati eszköz körvonalazásával lehetőség nyílik vezetékek nélküli kommunikációra, kis távolságra és esetenként, a felmerülő igény és szükség szerinti mértékben összekapcsolva a beépített rádiók hatókörében elérhető eszközöket.

Mint már megszokhattuk, egy-egy új információs-kommunikációs technika megjelenésével minimálisan egy tucatnyi új fogalmat is meg kell tanulnunk, legalább nagy vonalakban el kell igazodnunk jelentésükben. Az alábbiakban a kis távolságú, vezeték nélküli adatátvitel egyre többfelé használt új fogalomkészletéből mutatunk be kulcsfogalmakat, a rendszer működésének kereteit vázolva.

4.3.1 Fő jellemzők

A Bluetooth koncepció alapján kidolgozott első, kis méretű, kis fogyasztású és remélhetőleg olcsó eszközök (BlueMoon, BlueCore, Blueberry stb. fantázianevű chipek) lehetőséget nyújtanak arra is, hogy már meglévő eszközökbe utólag kerüljenek beépítésre, és így ezek az új típusú kommunikációs hálózat ill. lehetőségek részesei legyenek. Ilyen eszközök lehetnek, - amelyekben az új chipeknek helyet kell szorítani - a fent említetteken túl még a modemek, printerek,

projektorok, kamarák, de lehetnek egészen új típusú eszközök is, amelyek igényelnek ilyen kis távolságú, univerzális rádiós kapcsolatokat.

A Bluetooth eszköz lehetőséget kínál mindennek mindennel való összekapcsolására, mégpedig olyan módon is, hogy a használónak semmilyen akciót nem kell kezdeményeznie.

A koncepció egyik sarokpontja, hangsúlyos elképzelése az ad hoc kapcsolatépítés, az alkalomszerű összekapcsolhatóság (ad hoc connectivity).

A jelenleg használatos rádiótelefon rendszerek (mobil telefonok) az un. cellular rádió architektúrát használják. Ez azt jelenti, hogy a mobil hálózat egy vezetékekkel összekapcsolt gerincen, infrastruktúrán alapszik. Ezt az infrastruktúrát olyan alap vagy bázisállomások képezik, amelyek meghatározott stratégiai pontokon vannak kiépítve és elhelyezésükkel biztosítják egy adott terület "lefedettségét". A használók a kis teljesítményű kézi, mobil készülékeikkel, pontosabban ezek rádió adó-vevőivel ezeket a gerinchálózati pontokat, bázisállomásokat érik el, és ezeken, mint kapukon lépnek be a hálózatba.

A használatos protokoll olyan, hogy a vezérlő funkciókat a bázisállomások végzik: a csatornák kiosztását, lefoglalását a kapcsolat felépítését és bontását, a lehetséges interferenciák minimális szintre szorítását mind a bázisállomás végzi.

Ez a fajta "szereposztás" jellemzi a leginkább elterjedt mobil telefon rendszereket, így a GSM (Global System for Mobil Communications) a D-AMPS, IS-95 rendszereket is. Ilyen elveken működnek a privát célú rádió rendszerek is, mint pl. a WLAN, amely a 802.11 szabványon alapul, a HIPERLAN I és II. a DECT (Digital Enhanced Cordless Telecommuniations) valamint a Personal Handyphon System (PHS) is.

Az igazi ad hoc hálózati kapcsolatok kiépítésére alkalmas rendszerben nincs különbség a vezérlő vagy bázis állomás és a terminál között. Az ad hoc kapcsolat felépítése a felek közötti kommunikáción alapszik. Mivel nincsenek bázisállomások, nincs vezetékes kapcsolat sem közöttük. Nincs olyan központi vezérlő egység, amely számon tartaná vagy irányítaná a

kapcsolatok felépítését és megszűnését, nincs lehetőség a kapcsolatok központi koordinálására sem, így nincs lehetőség központi beavatkozásra, vagy operátori tevékenységre sem.

Az a szituáció, vagy forgatókönyv, ami a Bluetooth kidolgozói előtt lebegett, (5.) nagyszámú, (esetenként egy-egy helyszínen nyolc-tíz résztvevőből álló) egymás mellett létező rádiós kapcsolatból állhat, amelyek egy időben léteznek, mindenféle koordináció vagy irányítás nélkül. Ugyanakkor a tipikus szituáció az, hogy az ilyen nem koordinált autonóm, ad hoc módon felépülő hálózatok egy-egy helyszínen átfedik egymást.

Az ad hoc rádiós környezetnek számos következménye van, amelyek követelményként is megfogalmazhatók néhány területen. Így a használt rádió spektrum területén, a kapcsolat felvételére használható eszközök felderítése és aktivizálása kérdésében, a kapcsolatok felépítésekor, a többszörös, többszereplős hozzáférés kialakításában, a csatorna lefoglalásában és ennek kontrolálásában, a különféle sebesség igényű átvitel elsőbbségének eldöntésében (prioritization) az egyes résztvevők által okozott zavarok, interferenciák kezelésében, valamint az eszközök fogyasztásának optimális beállításában. Ezek mind olyan technikai részletkérdések, amelyekre a Bluetooth specifikáció részletes válaszokat kínál.

Hagyományosan ad hoc jellegű rádió rendszereket, mint amilyenek a jól ismert walky-talky rendszerek, már jó ideje használnak a katonai gyakorlatban, a rendőrség, a tűzoltók munkájában, katasztrófa elhárító teamek munkájában valamint ipari tevékenységek közben is. A Bluetooth rendszer azonban az első olyan széles körben hozzáférhető kereskedelmi rendszer, amely az ad hoc rádió rendszerek előnyeit a legszélesebb közönség számára teszi elérhetővé.

A rádiós spektrummal szemben alapvető követelmény, hogy lehetőleg globális méretekben, szabadon hozzáférhető legyen a legszélesebb közönség számára. A Bluetooth első használói között olyan utazó üzletemberek lesznek, akik bárhol vannak, szeretnének eszközeikkel kapcsolatokat teremteni.

Olyan rádiós sáv, amely nem igényel külön engedélyeket a használathoz az un. ISM sáv. Ezt a sávot eredetileg ipari tudományos és orvosi kísérletekhez tartották fenn, (innen az elnevezése is, Industrial, Scientific and Medical band) ma azonban már a legtöbb országban szabadon

hozzáférhető a kereskedelmi célú használatra. Az Egyesült Államokban a sáv használata az FCC 15. számú szabályozása alá esik, és terjedelme a 2400 MHz-től 2483,5 MHz-ig terjed. Európában a használatot az ETS-3003218 szabályozza. A sáv terjedelme nem teljesen egységes, Franciaországban és Spanyolországban valamivel szűkebb, a legtöbb európai országban megegyezik az amerikai sáv terjedelmével. Japánban a sáv még szélesebb, egészen a 2.5 GHz-ig terjed. A szabályozás leglényegesebb pontja, hogy előírják a legnagyobb kisugározható teljesítményt, és ez korlátozza az üzemeltethető adó-vevők hatótávolságát.

A szabad használat következtében a sávban a legkülönfélébb célú eszközök üzemelhetnek. Mivel nem lehetséges a koordináció a csatornák használatában, lényeges kérdéssé lép elő az állomások egymást zavaró hatása, az interferencia. Mivel azonban elég széles, több mint 80 MHz terjedelmű sávról van szó, ebben a széles sávban mindig lehet olyan szegmenseket találni az adott helyszínen, ahol alacsony az interferencia. Az interferencia megelőzésének hatékony módszere az un. szórt spektrumú üzemmód használata. Ez a technika nemrég még kizárólag katonai alkalmazásokban volt használatos. Ez az üzemmód lehetőséget nyújt a csatorna többszörös hozzáférésének megoldására is. A Bluetooth kommunikáció céljaira 79 darab, egyenként 1 Mhz széles un. hop frekvenciát, vagy ugrási frekvenciát határoztak meg, minden egyes frekvenciát 625 microsekundum időre lehet igénybe venni (időrés). Nagyszámú, véletlenszerű frekvencia kiosztási sémát definiáltak, ezeket a szekvenciákat az un. master állomás határozza meg, és a rádió adás-vétel egy-egy ilyen ugrási séma alapján történik. A többi állomás, amelyek slave üzemmódban dolgoznak, ezekhez az időbeli ütemezésekhez és frekvencia kiosztásokhoz igazodnak.

Az olcsó hardver előállításának igényét, valamint a kommunikáció robusztusságát szem előtt tartva jól ismert és egyszerű hardverrel megvalósítható modulációs módot választottak, ez pedig az FSK, a frekvencia moduláció. Az 1-es logikai szintet az éppen használt rádiós frekvenciától való pozitív eltérés képviseli, a logikai 0 szintet pedig a negatív eltérés.

A teljes frekvencia spektrum, a definiált adási szekvenciákkal, (frequency hop sheme , FHS) az átviteli kapacitást maximum 79 MB/s értékben engedné meg. Egy-egy helyszínen a résztvevők számára és az éppen folyó kommunikáció idejére egy master állomás vezérlete alatt többnyire

egyetlen, az adási frekvenciákkal meghatározott csatorna áll rendelkezésre, ez pedig 1 Mb/s átviteli kapacitást képvisel. Különböző, egyéb megfontolások alapján az mondható el, hogy egy helyszínen nem lehetséges az elméleti átviteli kapacitás elérése, de bizonyos körülmények között az átviteli kapacitás jelentősen meghaladhatja az egyetlen csatornára megadott maximális 1 Mb/s értéket.

Egy adási hop-szekvenciával azonosított csatornát piconetnet nevezik. A piconet résztvevői között egy master és több slave állomás lehet. Egy helyszínen több, egymástól függetlenül működő piconet is létezhet egy időben, ha ezek kommunikációja átfedi egymást, akkor scatternetről beszélünk.

A Bluetooth rendszerben a kommunikáció csomag alapon zajlik. Minden egyes időrésben egyetlen csomag adható. A csomagokat különféle azonosítók jellemzik, de egyetlen csatornán minden csomag hordozza a master állomás azonosítóját. A csomagok tartalmaznak hibavédelmet szolgáló kódolást is, mégpedig külön a csomag fejlécére, ez a header error check (HEC) és külön az adatrészre is. Ez utóbbi lehet CRC típusú vagy az un. forward error correction módszer alapján végzett kódolás (FEC) ill. hibavédelem.

Négyféle vezérlő csomagtípust definiáltak:

ID csomagok: csak a csatorna hozzáférést engedélyező access kódot tartalmazza. Csak jelzésre szolgál.
NULL csomag: a csatorna hozzáférést engedélyező access kódot és csomag fejlécet tartalmaz.
POLL csomag: a master küldi ki, hogy a slave állomást válaszra bírja.
FHS csomag: az adási frekvenciák szinkronizálására használatos. Idő adatokat és azonosítókat tartalmaz.
12 csomag típus szolgál a tényleges, szinkron és aszinkron típusú kommunikáció lebonyolítására. A szinkron típusú kommunikációban elsősorban a digitalizált hang (beszéd) továbbítása zajlik, és két állomás virtuális kapcsolatán alapul, un. kapcsolat-orientált kommunikáció. (SCO, syncronous connection-oriented link)
Az aszinkron kommunikációs módban az adatok továbbítása zajlik, és ez a mód nem tételezi fel a

két állomás virtuális kapcsolatát. (ACL, asyncron connectionless link). A kommunikáció a master és az elérhető összes slave állomás között zajlik.

4.3.2 A kommunikáció felépítésének problémái

A kapcsolat felépítése egy ad hoc hálózatban nem egyszerű feladat: az a kérdés, hogy hogyan találják meg egymást az állomások, és hogyan tudnak kapcsolatot építeni?

A Bluetooth specifikációban három eljárás-elemet ajánlanak a fenti problémák kezelésére: ezek a scan a page és az inquery eljárás. A nem aktív résztvevő alvó állapotban (idle mode) van, hogy takarékoskodjon az energiafogyasztással.

Időről időre azonban "felébred", hogy tesztelje, nem akar-e egy másik egység kapcsolatot létesíteni vele. A scan módhoz külön hop-frekvencia szekvenciát határoztak meg, a scennelő állomás - az, amelyik a kapcsolatfelvételt kezdeményezi - ezeken végiglépve sugározza az azonosítóját tartalmazó csomagokat. Ha egy "felébredő" egység valamelyik frekvencián meghallja az access kódot, és válaszol, akkor kicserélik a kapcsolat felépítéséhez szükséges információkat, a kezdeményező állomás, amely scennelte a frekvenciákat, masterként fog dolgozni, és megadja a kommunikációban használatos ugrási frekvencia sorozatot (FHS) és az időzítéshez szükséges információkat, majd felépítik a kapcsolatot, létrejön egy piconet. A korábban alvó, idle módban lévő állomás slaveként vesz részt a kommunikációban.

Vannak természetesen bonyolultabb helyzetek is és ennek megfelelően más algoritmusok, amelyek alapján egymásra találhatnak a rádiós "hallótávolságon" belül található állomások. Pl. ha már korábban volt kommunikáció az állomások között, akkor rendelkeznek információval arról, hogy a csomagok küldéséhez szükséges időzítést milyen mértékben kell módosítani az új helyzethez. Az előző kommunikáció óta eltelt idő hosszától függően ez az információ azonban egyre kevésbé lesz pontos, ill. használható.

A rendszer egyik érdekes tervezési problémája a frekvenciaugrásokat előállító egység. Különféle megfontolásokból ezt a feladatot nem lehet előre meghatározott és tárolt táblázatok segítségével megoldani.

Minden egyes Bluetooth egységben egy külön hardver látja el a feladatot. Ezt úgy lehet elképzelni, mint egy zárt, fekete dobozt, amibe az egység hardware azonosítója és óraimpulzusok adják a bemenetet, és a kimeneten megjelennek a kommunikációhoz használható frekvenciák egy kvázi-véletlenszerű sorrendben. Ezek a frekvenciák együtt, a generált időbeli egymásutánban adják ki a használatos csatornát.

A hop frekvencia sorozatokat a következők jellemzik:

- Függenek az egység azonosítójától, kezdő időpontjuk, ill. fázisuk igazodik a generáló egység órájához.
- Ugyanaz a frekvencia ciklus 23 órás időszakon belül nem térhet vissza.
- 32 egymást követő frekvenciaugrás mintegy 64 MHz spektrumot, ill. frekvencia távolságot fog át.
- Átlagosan minden egyes frekvenciának azonos az esélye, hogy bekerüljön a "látogatandó" szekvenciába.
- Az ugró frekvenciák száma igen nagy.
- Ha változik az órajel vagy az egység azonosítója, a generált ugrási frekvencia sorrend is azonnal változik.

4.3.3 Takarékos fogyasztás, biztonság

Ugyancsak külön problémakört jelent a Bluetooth rendszer áramfogyasztásának megtervezése, ill. a működés során az optimális fogyasztás beállítása és vezérlése. Mivel a rendszer egyik lényeges jellemzője a kis fogyasztás, minden egység tartalmaz teljesítményvezérlési lehetőséget, amely segítségével a körülményeknek megfelelően optimálisan lehet beállítani a rádióadó teljesítményét. Az "alvó" módban, amikor az egység időről időre belehallgat valamelyik frekvenciába, a fogyasztás a normál üzemi fogyasztás 1 százaléka körül van.

Létezik egy különösen kis fogyasztású, un. shiff mód is, amikor az inaktív egység csak nagy időintervallumokban hallgat bele a csatornába. A fogyasztás csökkentésének egyik módja, hogy az egység csak akkor adja az adatcsomagot, amikor az már készen áll, és amikor a kapcsolat fenntartásához szükséges információ átvitelére van szükség, akkor csak egy rövid un. null csomagot küld.

A rádióadó egység teljesítményének vezérlése (amelynek lehetőségét minden Bluetooth egységbe kötelezően beépítik, az un. vett jelszint indikátor - RSSI - alapján) a terjedési veszteségek, valamint a frekvenciaterjedés sajátos, lassú elhalkulásaiból (slow fading) adódó veszteségek kiegyenlítésére szolgál. Mivel nincs koordináció az egyes egységek között, semmi sem akadályozza meg, hogy egy egység ne tudjon kísérletet tenni arra, hogy túlságosan megemelt teljesítményszinttel a versenytársait kiszorítsa.

A Bluetooth rendszer rádiócsatornákon dolgozik. Ilyen környezetben fokozott szerepet kapnak az információátvitel biztonsági kérdései. A rendszerben többféle szintű biztonsági eljárás szolgálja az illetéktelen használat és a lehallgatás megakadályozását. A jogosult felhasználó azonosításának, az autentikációnak, valamint az adatok titkosításának és visszakódolásának különféle eljárásait alkalmazzák. Az eljárások különböző szintjei ill. az alkalmazott algoritmusok erőssége függ az átviendő információ jellegétől. Az adatkezelés egyik központi eleme egy 128 bit hosszúságú un. kapcsolati kulcs (link key), amit a hardver tárol, és a user semmilyen módon nem tud hozzáférni.

Mindent összevetve maga a rendszer a kommunikáció alsó szintjén azonban csak korlátozott eszközöket nyújt a biztonságos kommunikáció megvalósítására. A szoftverek felsőbb szintjén, az alkalmazásokban kell az esetleg felmerülő pótlólagos biztonsági igényeket kielégíteni.

Szólni kell még a Bluetooth egység és a befogadó, host egység kapcsolatáról. A legtöbb esetben itt standard adatátviteli protokollokkal leírható környezetről van szó. A Bluetooth specifikáció a host interface kezelésére többféle protokollt kínál fel, ilyen pl. az un. L2CAP, Logical Link Control and Adaptation Protocol. Ennek elsődleges feladata a host rendszer felől átvett más jellegű, hosszabb csomagok lebontása és újra felépítése a Bluetooth rendszer számára. Az RFCOMM elnevezésű protokoll feladata a hagyományosan soros kommunikációnak ismert adatáramlás kezelése, míg a TCS a telefon rendszer felé teremt kapcsolatot (Telephon Control Specification). Ugyanígy vannak protokollok, amelyek kapcsolatot teremtenek a hagyományos hálózati, Internet alapú protokollokkal, így a TCP/IP-vel, a PPP-vel, ill. a mobil telefóniába bevezetett WAP protokollal is.
A Bluetooth rendszer saját céljait szolgálja az un. SDP, Service Discovery Protocol, elsősorban az a feladata, hogy segítségével egy kommunikációt indító egység felderítse, hogy partnerei milyen szolgáltatásokra képesek, és ezek a szolgáltatások milyen paraméterekkel jellemezhetőek (pl. nyomtatók, fax rendszerek, stb. jellemzői).

Hogy ne kelljen az egész Bluetooth rendszert minden alkalommal, minden egyes egységbe teljes egészében implementálni, un. profilokat határoztak meg. A profilok a különféle alkalmazásokhoz igazodnak. Pl. egy printerbe kerülő Bluetooth egységnek nem kell tartalmaznia olyan szoftver komponenseket, amelyek a hangátvitel kezelésére szolgálnak (hacsak nincs valami különleges feladata az ilyen hang kezelő alrésznek az adott printer esetében). A profilokkal így csökkentett méretű rendszer takarékosan tud bánni a memóriával és a számítási erőforrással, olyan esetekben, amikor az alkalmazás esetleg az egész rendszernek csak nagyon kis méretű részét használja.

4.3.4 Versenyben lévő, hasonló célokat szolgáló, hasonló igényekre reflektáló technikák

A Bluetooth egy a kis hatótávolságú rádiós rendszerek között, amelyek sokcélú, adatátviteli kapcsolatot létesíthetnek a személyes használatú, legtöbbször mobil eszközök között.

Infravörös fényt használ az IRDA rendszer. Az infravörös fényt használó megoldások már jelentős múltra tekinthetnek vissza az egyéni otthonokban. Jól ismert a tv készülék vagy a videó rögzítő távvezérlésére szolgáló infravörös kezelő egysége. Újabb változatában nemcsak egyirányú vezérlésre szolgál, hanem kétirányú adatátvitelre is, pl. laptop számítógép és nyomtató között, laptop és PC között. Ugyancsak ismertek a leggyakoribb kezelő egységek, az egér és a billentyűzett vezeték nélküli kapcsolódásának megoldására. Mobil telefonba is építenek ilyen egységet.
Jellemzője, hogy csak pont-pont összeköttetés valósítható meg vele. Esetenként zavaró lehet, hogy a csatorna irány érzékeny, ami azt jelenti, hogy a kisugárzott infravörös fény csak bizonyos kitüntetett irányokban terjed.
Ez a tulajdonság zavaró lehet, pl. fülhallgató csatlakoztatásánál, ha az adatátvitel időnként elhalkul, vagy megszűnik.

Wireless LAN: célja, hogy épületekben, telephelyen kiváltsák vele a kábelezést, helyettesítsék a lokális hálózat kábeleinek kiépítését. Amerikában jelentős mértékben elterjedt, újabban nálunk is kínálnak ilyen eszközöket hálózat építéshez.
Az IEEE 802.11 szabványra alapul, jelentősen drágább, mint a hagyományos vezetékes hálózat ill. a Bluetooth lesz, vagy lehet. A másik jellemzője, hogy alapvetően nem kicsi és mozgatható, hordozható, "mobil" eszközökhöz tervezték.

HomeRF: ugyancsak a 2.4.GHz ISM sávot használja, ugyancsak "ad hoc" hálózat kiépítése a cél,
Technikai különbségek: a hop frekvencia itt 8 Hz, míg a Bluetooth -nál 1600 Hz.
Csak adatátvitelre szolgál. Hang átvitelt (telefon) nem terveztek hozzá.

DECT Digital Enhanced Cordless Telephony, mint a neve is mutatja, elsősorban a telefon szolgálatokhoz igazított technika, hasonlóan rövid távú rádiós csatornákon dolgozik. Fixen telepített interfaceket alkalmaz a hagyományos telefonvonali csatlakozáshoz, az ISDN valamint a mobil, GSM telefonrendszerekhez. Lehetőség van a hatótávolság kiterjesztésére, un. átjátszó vagy relay állomás közbeiktatásával. Szabványosítása 1994 körül kezdődött az európai ETSI égisze alatt, elterjedése azonban egyelőre korlátozottnak tűnik. (Az Ericsson pl. forgalmaz már DECT rádiós kapcsolatokkal felszerelt mobil készülékeket).

4.3.5 A használat körvonalai

A Bluetooth rendszer számára az ISM rádiósávok szabályozásakor kialakított un. teljesítmény osztályok használata az irányadó, és így a rendszer, az összekapcsolódó egységekből álló piconet hatótávolsága, kommunikációs köre 10 - 100 méter átmérőjű terület. Az ilyen méretű térre, legalábbis az alsó határain joggal alkalmazható a Personal Area Network , a személyes területű hálózat új fogalma. A fogalmat ugyan a Local Area Network mintájára alkották, kommunikációs vonzatai mégis eltérnek ettől. A kommunikációkutatással társadalomtudományi nézőpontokból foglalkozók számra a kommunikáló emberek, kis csoportok terét, fizikai közegét jelentik ezek a térbeli viszonyok. Kultúrához kötötten is, de szituációról szituációra is más és más a két ill. többszemélyes beszélgetés tere, sajátos törvényeknek engedelmeskedik, pl. a normális hangerővel folytatott beszéd, a köznapi kommunikációs terekben mindig meglévő, kísérő, nemverbális kommunikációs csatornák.

A mérnökök és a szilícium lapkák szoftvereit tervezők most ezekbe a kommunikációs mikro terekbe lépnek be, ezeket a finom személyközi viszonyokat kezdik "hálózatosítani". Valami olyasmit kell ez alatt elgondolnunk, hogy egy ilyen térben - legyen az egy lakószoba privát tere vagy valamilyen nyilvános vagy félig nyilvános tér (buszmegálló, mozi előtere, könyvtár vagy konferenciaterem, stb.) nemcsak a megszokott, természetes emberi kommunikáció útján kerülhetünk kapcsolatba az ugyanott tartózkodó embertársainkkal, hanem a nálunk és náluk lévő

elektronikus eszközeinkkel is. Mégpedig úgy, hogy ezek már öntevékenyen felderítik a partnerek jelenlétét, sőt felépítik a kicsiny, személyes aurájú hálózatot, és bizonyos információkat tőlünk függetlenül is kicserélnek egymással. Ha mindez megvan, akkor mi is próbálkozhatunk ismerkedéssel vagy privát reflexiók küldözgetésével. Vannak persze egyszerűbb és egyértelműbb feladatok és szituációk, amikor a vezeték nélküli kapcsolatok jó szolgálatot tehetnek. Pl. egy többszereplős konferencia helyszínen fordítást, tolmácsolást, kis csoportos értelmezést, kommentálást tehetnek lehetővé.

A tervezők abból indultak ki, hogy néhány esetben célszerű a kisméretű, hordozható eszközeinket, számítógépeket és mobil telefonokat összekötni nagyobb és helyhez kötött társaikkal. Azt mondják, hogy nem akarnak mást, csak megkönnyíteni ezt a feladatot. Ne kelljen kábeleket cipelni, ne kelljen ügyelni a helyes csatlakozásokra, és ne kelljen belegabalyodni a már működésre bírt, összekábelezett együttesekbe.

Innentől kezdve azonban a technikai logika önálló életre kel. Ha már megtervezésre kerül egy kis hatótávolságú rádiós összekapcsoló eszköz, amolyan kommunikációs mindenes, akkor az legyen kitalálva a ma elérhető technika felső szintjén, lehetőleg úgy, hogy az eljövendő években (évtizedben?) is használható legyen. Legyen olcsó, kicsiny méretű, kis fogyasztású, mindenhová beépíthető, lehetőleg ismerje a ma használatos legtöbb adatátviteli módot, ne kerüljön zavarba, ha hangot, beszédet, zenét kell közvetítenie. Ha meg már ilyen sokcélú eszközt sikerült körvonalazni, akkor elindulhat a fantázia is, és különféle víziók nyomán új eszközök, új használati területek is születhetnek. Minél többféle ötlet kerül elő, annál több eszközt lehet gyártani, eladni és ez lehet a folyamatot erősítő hatású pozitív visszacsatolás. Közben az emberi kommunikáció ősi, intim területei, helyszínei és szituációi is megváltoznak azáltal, hogy a technika észrevétlenül bekapcsolja, belefűzi a globális kommunikáció virtuális tereibe.

Azt, hogy a lehetőségekből és a technikai tervekből mi valósul meg, egyelőre nehéz előre körvonalazni.
Minden esetre az előrejelzések nem fukarkodnak a szép jövő felvillantásában:
A Bluetooth chipeket 2002 végére 100 millió eszközbe építik be. 2005 végére 1 milliárd darab készülhet, ez mintegy 5 milliárd dollár hasznot jelent. Bármennyire igaz, hogy az itt szóban forgó

területeken kockázatos jósolni akár egy fél évre is, a fenti számok mégis olyan impozánsak, hogy az érdekelt cégek úgy vélhetik, érdemes kockáztatni, ill. belevágni. Annál is inkább, mert ezeken a területeken állandóan és megújulva szükség van technikai fogantatású víziókra, értelmes jövőképekre, reménykeltő elképzelésekre, a technika lehetőségeit kézzel fogható termékekbe kényszerítő koncepciókra. Lehet, hogy a Bluetooth esetében is ilyennel állunk szemben, lehet, hogy többel, és a széles közönség megtalálja benne egyfajta igényeinek, kommunikációs mintáinak szolgálatát.

4.3.6 Használati minták, az első alkalmazási példák

A Bluetooth által megcélzott szűk hatókörű rádiós összekötetést más úton is realizálni lehetne. Felvetődhet a kérdés: miért nem építenek mobil telefont a PC-be, laptop-ba? Kétféle ellenérvet is fel szoktak hozni erre, az egyik szerint a használati minták nem támogatják az ilyen készülék hibridet. Egy laptop, hordozható számítógép használata, a rajta való munka nagyobb része jelentősen különbözik a telefonálástól. A két eszköz az Internetre való csatlakozáskor kapcsolódik, vagy kapcsolódhat össze. A másik érv inkább a potenciális fogyasztók pénztárcájára hivatkozik: egy ilyen eszköz túlságosan drága lenne, ahhoz, hogy nagyobb tömegű igényt elégítsen ki.

Mindamellett vannak olyan próbálkozások, hogy összeházasítsák a mobil telefont és a személyes noteszgépet, leginkább úgy, hogy a telefonban helyet szorítanak a személyes címtárnak vagy az előjegyzési naptárnak.

Az Internet felé való nyitásra a mobiltelefonok tervezői részéről már eddig is láttunk próbálkozásokat, pl. lehet erre a WAP, amely egyszerűsített internetkezelést nyújt, vagy a közeljövő gyors adatátviteli megoldása, a GPRS, amely ennek a törekvésnek a leginkább emlegetett és reményteli útja.

Az alább felsorolandó jellemzőivel nagyon jól illeszkedik a mobil, ill. hordozható eszközök széles köréhez:

- Más rádiós megoldásokhoz viszonyítva kis költségű
- Nagyon kis fogyasztású, ami a telepes táplálású, hordozható gépek esetében elsődleges szempont
- Kicsiny méretű, és remény van a jövőben a méretek további csökkenésére
- Különféle hálózatokhoz való csatlakozást biztosít, a csatlakozási pontok különféle gyártóktól származhatnak
- Nagyon sokféle eszközt támogat
- the best "last 10 meters " technology

4.4 Wibree

A Nokia egy rövid hatótávolságú, vezeték nélküli technológiát fejlesztett ki. A Wibree hatékonyabb mint a Bluetooth, kevesebb energiát fogyaszt.

A bemutatott rövid hatótávolságú, vezeték nélküli adatátviteli technológia, a Wibree a Nokia Research Center vezetője, Bob Ianucci szerint tízszer kevesebb energiát fogyaszt, mint a Bluetooth. A Nokia immár öt éve fejleszti a Wibree technológiát, mely most tisztul le, és a cég jelenleg folytatja a szabványosítási eljárást, hogy új technológiájuk mielőbb elterjedhessen és megjelenjen a többi gyártó kínálatában is.

A Wibree rádióchipek sokkal kisebbek, mint a Bluetooth lapkák, így sokkal kisebb eszközökbe is be lehet építeni őket. Az új technológia adatátviteli sebessége 1 Mbps, ami egyharmada a Bluetooth 2.0 sebességének, hatótávolsága 30 láb, vagyis 9,1 méter (a Bluetooth hatótávolsága 10 méter).

4.5 NFC (Near Field Communication)

A Near Field Communication (NFC) technológia biztonságos vezeték nélküli adatátvitelt tesz lehetővé alig néhány centiméteres hatókörön belül. Például egy terminál és a közvetlen közelébe helyezett mobiltelefon között. A szóba jöhető alkalmazási területek lehetnek a telefonnal való fizetés, beléptetési jogosultság igazolása, jegyvásárlás rendezvényekre, ahol a mobiltelefon a fizetés után belépőjegyként is szolgálhat. A mobiltelefon szolgáltatókon kívül - amelyek nagy üzleti lehetőséget látnak a fizetőrendszerek kiépítésében - a hitelkártya társaságok is érdeklődnek a technológia iránt. Mindez előrevetíti, hogy a mobiltelefon funkciói hamarosan kiegészülnek a készpénzes és kártyás fizetés lehetőségeivel. Napjainkban dinamikusan terjednek az érintkezés nélküli szolgáltatások, ezt támasztják alá a közelmúlt bejelentései is, többek között a kontaktus nélküli készpénz-helyettesítő kártyák és terminálok tervezett bevezetése Londonban, valamint a GSM Association erőfeszítései az NFC szabványosítására. A világszerte végzett tesztek alapján a fogyasztók kedvelik, hogy az NFC-nek köszönhetően mobiltelefonjukról egyszerűen és gyorsan tudnak fizetni, információt cserélni és egyéb szolgáltatásokat igénybe venni.

A rendszer által használt rádiótechnikás azonosítóchipek (RFID) frekvenciája, ami 13,65 MHz. A chipek passzív és aktív működésűek, vagyis csak a leolvasókészülék közelében kapcsolnak be. A működésükhöz 2,5-3 volt feszültség szükséges és az adatokat 400 Kbit/s-os sebességgel veszik át a mobiltelefonokról. A kifejlesztett hálózat számos szabványt támogat, köztük van például az ISO 14443A/MIFARE, a FeliCa, valamint az UART, az SPI és a már jól bevált USB 2.0 is.

4.6 HOME RF

1997-ben több mint 85 gyártó, beleértve a Compaqot, Ericssont, HP-t, IBM-et, Microsof-tot, Intelt, közreműködésével jött létre a HomeRF munkacsoport, melynek célja egy otthoni vezeték nélküli hálózat kialakítása volt, amely hang és adat egyidejű továbbítására alkalmas. A HomeRF hálózat kétféle módon működhet, vagy menedzselt otthoni hálózatként, vagy peer-to-peer ad hoc hálózatként. Menedzselt hálózat esetén a hálózatot a CP (Connec-tion Point) kontrolálja, amely átjáróként működik az eszközök és az Internet, valamint a PSTN hálózat között.

Leggyakoribb felhasználási lehetőségei:

- Mobil kijelzők, melyek akár egy PC kiegészítőjeként, vagy Internet böngészőként is üzemelhetnek.

- Tartalom megosztás az otthoni hálózatban található számítástechnikai eszközök között lehetővé téve adatmentést, nyomtatást és többjátékos módban futtatható játékok használatát.

Jelenleg két változatban érhető el: az 1.0 maximális sebessége 1,6 Mb/s, a továbbfej-lesztett 2.0-ás megoldás a hagyományos Ethernetnek megfelelő 10 Mb/s-os sebességet nyújt.

A Home Radio Frequency specifikáció a Bluetooth-szal és a 802.11-gyel konkuráló vezeték nélküli hálózati szabvány, mely a 2,4 GHz-es frekvenciát használja egy lakáson belüli hálózati kapcsolat kiépítésére.

Mind a HomeRF, mind az IEEE 802.11b szabvány megengedi, hogy az otthoni hálózatokban minden eszköz egyetlen rádiófrekvenciás internetcsatlakozást használjon, beleértve az asztali és a mobil gépeket is. A fő különbség a két szabvány között az, ahogyan az adatcsomagokat továbbítják. Míg az IEEE 802.11b egyetlen "kövér" csatornát használ, addig a HomeRF frekvenciaugrásos elven működik, jobban takarékoskodva a sávszélességgel.

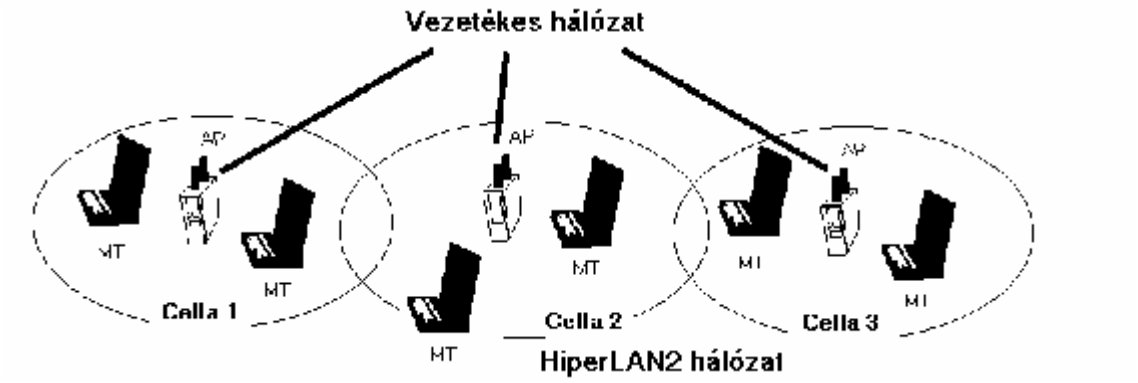
A felügyelő konzorcium 2003-as felbomlása azonban a HomeRF pályafutásának végét jelenti.

4.7 HYPERLAN/2

Mobil számítógépek használatakor mindig felmerül, hogy milyen jó is lenne, ha menet közben is tudnánk online adatokat kezelni. Erre már megindultak a fejlesztések, GSM rádiótelefonokkal lehet 9,6 kps-től egészen 43,2 kbps-ig vonalkapcsoltan illetve csomagkapcsoltan a GPRS segítségével az ígéretek szerint akár 100 kbps sebességgel is kommunikálni, de az ember ennél többre vágyik.

Egy vezeték nélküli hálózat általában fixen telepített hozzáférési pontokból és mobil hálózati eszközökből áll. A hozzáférési pontok kapcsolódnak a vezetékes hálózatra és továbbítják a mobil készülékek felé az adatforgalmat. Nagyobb hálózat esetén egy helyen több hozzáférési pont is elérhető lehet, ilyenkor a mobil egység választja ki a számára legmegfelelőbb hozzáférési pontot a térerő és egyéb paraméterek alapján. Mozgás közben a változó körülményeknek megfelelően át lehet jelentkezni egy másik hozzáférési pontra, ilyenkor előfordulhat, hogy néhány adatcsomag elveszik, azonban ezt az IP protokoll gond nélkül lekezeli.

A HiperLAN2 hálózat celluláris felépítésű. Az egyes cellák forgalmát egy-egy bázisállomás vezérli, melyeket AP-nak (Access Point, Hozzáférési Pont) nevezünk. A hálózati szolgáltatást igénybe vevő összes felhasználó a cellák valamelyikében foglal helyet, de természetesen a felhasználók mozoghatnak a cellák között (handover). Az egy cellához tartozó felhasználók száma korlátozott. A felhasználók a legközelebbi AP-hoz egy rádiós interfésszel rendelkező MT (Mobile Terminal, Mobil Terminál) segítségével csatlakoznak. Alapértelmezés szerint az adatok a cellákban két irányban haladhatnak: egy MT-től az AP-hoz, ill. az AP-tól az MT-hez. Az előbbi irányt uplink, utóbbit downlink iránynak hívjuk. A cellák az 5GHz-es frekvenciatartomány egy-egy jól meghatározott 25MHz széles szeletét használják. Az AP-k vezetékeken keresztül kapcsolóeszközökhöz, ill. egyéb hálózatokhoz csatlakozhatnak. (1. ábra)



3. ábra Egy HiperLAN2 hálózat

A HyperLAN/2 az 5GHz-es frekvenciasávban üzemel, ahol az egyes berendezések automatikusan választanak maguknak frekvenciát a rádiós környezetükhöz igazodva. A jelek kódolására az OFDM modulációt alkalmazzák, ami különösen épületeken belül, erős reflexió esetén hatékony. Az alkalmazott kódolástól és a hibajavítástól függően 6 Mbps-tól egészen 54 Mbps-ig terjednek az átviteli sebességek, amik közül a berendezések mindig az adott vételi viszonyoknak legmegfelelőbbet választják ki. A zavarok csökkentése, az egyszerűbb elektronikai megvalósítás és a mobil egységek elem élettartamának növelése érdekében az adás erősségét szabályozzák és csak a szükséges energiát sugározzák ki. Egy állomás adáskörzete irodai környezetben 30 méter, míg szabad térben elérheti a 150 métert is.

Egy csatorna forgalmát mindig a hozzáférési pont vezérli, kijelölve az egyes mozgó készülékekhez hozzárendelt időréseket. A rendszer érdekessége, hogy ugyan azon a frekvencián történik az adás és a vétel, időben elválasztva, így a mai tipikusan aszimmetrikus internetes forgalomnál is jól kihasználja a rendelkezésre álló sávszélességet. További előny, hogy nagy forgalomnál a vezérelt csatornakiosztás hatékonyabb mint a hagyományos Ethernet ütközéses algoritmusa.

A használat szempontjából a HyperLAN szabvány úgy lett kialakít hogy bármely létező hálózat részeként üzemelhet, így használható Ethernet, ATM vagy akár a 3. Generációs mobil hálózatok hordozójaként is.

Ugyan a hozzáférési pontok kis hatósugara miatt nem várható folyamatos 54 Mbps-os lefedettség azonban ma sokan úgy látják, hogy a repülőtereken, üzletközpontokban, szállodákban és az olyan helyeken, ahol tömeges igény van rá el fognak terjedni a vezeték nélküli hálózatok.

4.8 WIMAX

Az IEEE 802.16 csoportja a pont-multipont összeköttetést adó szélessávú vezeték nélküli technológiákkal foglalkozik. Nem a ma használatos vezeték nélküli hálózatok (WLAN) felváltására hozták létre, hanem a kiegészítésükre. Ez nagymértékben kiterjeszti majd a jelenlegi vezeték nélküli IP-hálózatok (Wi-Fi) alkalmazási körét, a védett ill. szabad frekvenciasávokban történő üzemeltethetőségnek, a közvetlen rálátást nem igénylő egyedülálló átviteli jellemzőknek és a garantált szolgáltatási minőséget biztosító technológiának köszönhetően.
A WiMAX révén városnyi területeket is össze lehet majd kötni, vagyis mindenhová eljuthat majd a szélessávú internethozzáférés. Míg a 802.16-os szabvány (a WiMAX) akár 50 kilométeres körzetben is adhat hálózati hozzáférést, a WiFi (WLAN szabvány) csak 100 méteres körzetet képes elláthatni. Ezzel a technológiával bázisállomásonként 280 Mbit/s-re emelhető az adatátviteli sebesség, azaz 70 megabit/másodperces lehet az osztható sávszélesség; ez körülbelül 60 üzleti T1-es vonalnak vagy nagyjából 1000 otthoni, 1 megabit/másodperces ADSL-vonalnak felelhet meg. Ennek a technológiának az a további - és igen nagy - erénye, hogy nem kell hozzá közvetlen rálátás az átjátszókra, s ezzel voltaképpen többet ígér minden ma használatos szélessávú, vezeték nélküli kapcsolatnál, mivel a végpontokban nem kell majd kültéri antenna.
A WiMax hálózatok legfeljebb 70 Mbit/s sebességű adatátvitelre képesek. Szakértők szerint a WiMax mind a DSL (Digital Subscriber Lines), mind pedig a kábelnetes megoldásoknál olcsóbb lehet, hiszen esetében nem kell kábeleket lefektetni, a vezeték nélküli infrastruktúra kiépítése pedig rendkívül olcsó.

A WiMAX-nak igen jó tulajdonsága, hogy nem a túlzsúfolt 2,4 GHz sávot használja - mint a WiFi, BlueTooth és vezeték nélküli telefonok -, hanem az 1,75 - 3,5 - 5, –11 körülit. Ez szintén szabad (ingyenes) spektrum, vagyis a használata nem kerül milliárdokba, mint a W-CDMA

tartományokéi. A WiMAX a városi és vidéki területeken egyaránt telepíthető, ott is szélessávú internetkapcsolatot tesz elérhetővé, ahol a DSL technológiai nem vezethető be.

A Wimax (IEEE 802.16), a Wifi továbbfejlesztett változata. A Wifi főleg belső térre van optimalizálva, míg a Wimax szabvány létrehozásával a nagy távolságok áthidalása volt a cél. Egyetlen központi egységet rácsatlakoztatva egy megfelelő sávszélességű bérelt vonali internetre, több száz felhasználó szolgálható ki akár 40 km-es körzeten belül ADSL sebességgel. A Wimax teljes egészében kompatibilis a Wifi rendszerekkel, vagyis alkalmas arra is, hogy összeköttetést biztosítson az egymástól távol levő Wifi hálózatok között.

Felmerülhet a kérdés: Megfelelő út a Wifi/Wimax lenne?

Ezeknek a rendszereknek nagy erénye az ingyenes frekvenciatartomány, hiszen így nem szükséges fizetni a koncessziós díjakat. A Wimax szabvánnyal a nagy távolságok áthidalása sem akadály. Az átjátszó állomásokat mindkét rendszer esetén ki kell építeni. A nagy gyártók is látnak benne fantáziát, hiszen dollár milliárdokat fektettek a fejlesztésekbe. Telefonálásra is alkalmas a hálózat, hiszen két egymással - az internet segítségével - összekapcsolt eszközzel, hang alapú kapcsolat is létesíthető kis költségek mellett, bár ehhez minkét eszköznek ugyanabban a pillanatban online kell lenni. Sok minden szól tehát a Wifi mellett.

Egy dolog azonban a technológia ellen szól, és pont ez teszi a mai nap eldönthetetlenné a kérdést. Azzal, hogy a Wifi/Wimax az ingyenes frekvenciatartományban működik, ki van téve azoknak az interferencia zavaroknak, amelyeket az ugyanebben a sávban működő más berendezések (távirányító, vezeték nélküli telefon, stb.) okoznak. Addig, amíg a 3G esetén - cserébe a nagy összegű frekvenciadíjért - az adott tartományban más nem működhet, erre a Wimax, de főleg a Wifi esetén nincs garancia. Problémát okoz továbbá szintén főként a Wifi rendszereknél, hogy a különböző tereptárgyak jelentős mértékben rontják a rendszer átviteli képességet. Mindez azt jelenti, hogy a szolgáltatók nem tudják garantálni a kapcsolat minőségét, amely feltételt egy európai színvonalú vállalat csak jelentős megkötésekkel vállal fel. Az pedig, hogy magánszemélyek építsenek ki egymásba kapcsolt Wifi egységekkel hálózatot, és hozzáférhetővé tegyék bárki számára számos akadályba ütközik. További nehézséget jelentenek a rendszer

biztonsági problémái is. A hagyományos hálózatok is lehallgathatóak, de ahhoz komoly eszközök és fizikai beavatkozás szükséges. A Wifi hálózat - noha forgalma egyre jobb megoldásokkal titkosítva van - a hatósugarában elérhető eszközökkel kommunikálni tud, tehát ha nem megfelelően van a rendszer konfigurálva, akkor a szomszéd irodában ugyanúgy hozzáférhetnek az adatainkhoz, mint mi magunk. Könnyen megmaradhat tehát a technológia a belső magánhálózatok, rendezvények, egyetemek, repülőterek viszonylag korlátozott szintjén vagy olyan területeken, ahol nem érdemes - a valószínűsíthetően kevés potenciális megrendelő miatt - 3G átjátszókat kiépíteni.

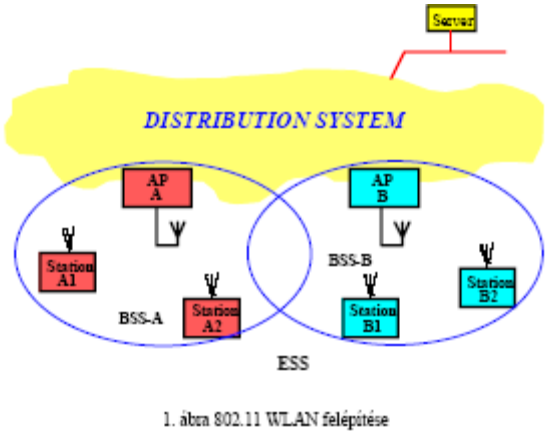
5. VEZETÉK NÉLKÜLI KAPCSOLAT LÉTESÍTÉSE

5.1 A 802.11 félépítése

5.1.1 Az architektúra elemei

A 802.11 WLAN-ok a cellás elvre épülnek, ahol a rendszert cellákra osztják. Minden cellát (**Basic Service Set, BSS**, a 802.11 terminológiában) egy bázisállomás vezérel (**Access Point**, **AP**). Habár egy WLAN állhat egyetlen cellából egyetlen Apvel (ahogy azt majd a későbbiekben látni fogjuk), a legtöbb esetben több cella alkot egy hálózatot és az AP-ket egy elosztó hálózat köti össze (**Distribution System, DS**).

Ez a gerinchálózat tipikusan lehet egy Ethernet hálózat, de akár vezeték nélküli is. Az összekapcsolt WLAN, mely cellákból és a hozzájuk tartozó AP-kből áll, valamint az elosztó hálózatból együtt alkotja egy 802.11 hálózatot alkot a felsőbb OSI rétegek számára és a szabványbeli elnevezése: **Extended Service Set** (**ESS**). Az 3. ábrán a 802.11 WLAN felépítése látható.



1. ábra 802.11 WLAN felépítése

4. ábra 802.11 WLAN felépítése

A szabvány definiálja még a **Portal** fogalmát. A Portál a 802.11 és egy másik 802 LAN összekapcsolására szolgáló eszköz. Ez a koncepció valójában a “fordító bridge” funkcionalitásai

egy részének absztrakt leírását jelenti. Habár a szabvány nem rögzíti, de a gyakorlati megvalósításokban az AP és a Portál ugyanaz a fizikai entitás.

5.1.2 Az elosztó rendszer megvalósításának lehetőségei

Gyűrű*:*

A gyűrű topológia esetén szükség van adat fizikai címzésére az egyik csatlakozási ponttól a következőig. A rádió és az optikai jelek küldhetők ugyan irányítottan, de ez nem lehet megoldás WLAN elosztó rendszere esetén, ha feltételezzük azt, hogy a csatlakozó hozzáférési pontok helyzete változhat (dinamikusan változó környezet esetén a BSS-ek hozzáférési pontja változhat), ezért adatcsomagnak tartalmazniuk kell a következő hozzáférési pont címét. Néhány gyűrű struktúrájú elosztó rendszeren alapuló optikai WLAN is kifejlesztettek, azokat a vállalatokat célozva meg, amelyeknek már van token-ring alapú hálózata.

A gyűrű struktúrában azt szabályozzák, hogy ki küldhet információt. Speciális adatcsomagot használnak, amiket token-nek hívnak, ez adja meg a jogot az adat küldésre. Az adat csomagot az egyik csomópont küldi tovább a következőnek a kiindulási ponttól a cél csomópontig. A csomópontnak csak akkor küldhet adatot, ha a token nála van. A token megszerzése esetén kicseréli az adatcsomagjával a tokent és azt küldi tovább a következő csomópontnak, amely a csomag fejrészében beállítja a következő csomópont címét ez a folyamat ismétlődik, amíg a címzett meg nem kapja az üzenetet.

Egy új csomópont kapcsolódása esetén újra kell konfigurálni a gyűrűt. Meg kell állapítani, hogy mely csomópont előzi meg az új csomópontot és melyik követi azt. A token elvesztése esetén tokent visszaállító protokollt indítanak.

Busz*:*

Ez a legdemokratikusabb topológia, minden csomópont azonos. Ha több csomópont kísérli meg az átviteli közeg használatát azonos időben ütközés jön létre.

A közeg-hozzáférés szabályozására történhet logikai token átvitelével és vivő érzékeléssel.

Logikai gyűrű*:*

Az átvitel fizikailag olyan, mintha buszon történne, de egy logikai gyűrűt is definiálnak. A működési mechanizmusa megegyezik a gyűrű struktúráéval.

Csillag*:*

A busz alapú hálózati topológia ellentéte. A központi állomás “mester” vezérli az információ cserét. A többi állomás “szolgák” csak a mester állomásnak küldhetnek, vagy a mester állomástól fogadhatnak adatokat. A mester állomás periodikusan lekérdezi az aktív szolga állomásokat és csak a megcímzett állomás küldhet adatot a mester állomásnak. Ez az eljárás azokban a hálózatokban alkalmazható, ahol az információáramlás kiegyenlített.

Az elosztó rendszer konkrét megvalósítását a szabvány nem definiálja, csak az általa nyújtott szolgáltatásokat. Az elosztó rendszer kiterjesztett hálózati szolgáltatásokat nyújt a hozzákapcsolódó BSS-ek és LAN integrációkon keresztül és tetszőleges bonyolultságú vezeték nélküli hálózat kialakítását teszi lehetővé.

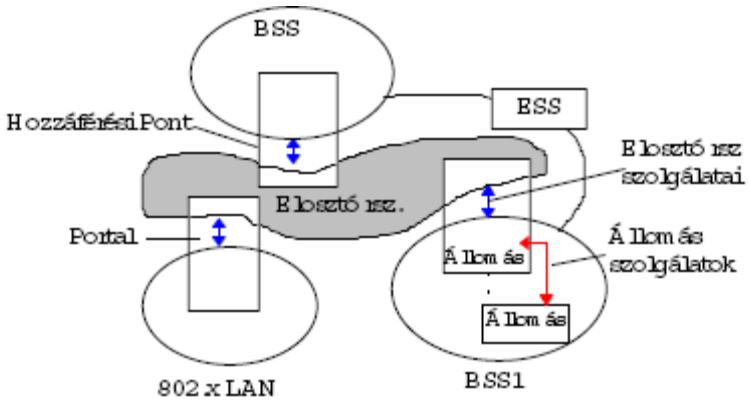
A szabvány logikailag elkülöníti a BSS-en belül használt átviteli közeget az elosztó rendszer átviteli közegétől, ez a kulcsa az architektúra rugalmasságának, ugyanis az elosztó rendszer függetlenül definiálható bármelyik fizikai megvalósítás jellegzetességeitől, ezért a közeghozzáférést szabályzó réteg fölött elhelyezkedő réteg számára úgy tűnik, mintha a különálló BSS-ek egyetlen független BSS-et alkotnának.

A szabvány ezt nevezi kiterjesztett szolgálati összeillesztésnek (ESS). Az állomások az ESS-en belül kommunikálhatnak és a mobil állomások az ESS-en belül mozoghatnak a BSS-ek között.

A BSS-ek elhelyezkedésére a szabvány nem tesz megkötéseket. A BSS-ek területei részlegesen átlapolhatják egymást folyamatos lefedést biztosítva, de ennek az ellenkezője is igaz lehet, azaz a lefedettségi területük határai nem érnek össze. Egy fizikai helyen több különböző szervezet, vagy vállalat által létesített vezeték nélküli LAN hálózat is működhet, illetve infrastruktúra hálózaton belül adhoc hálózat is kialakítható.

5.1.3 A logikai szolgálatok interfészei

A 802.11-es szabvány lehetőséget ad arra, hogy az elosztó rendszernek nem kell azonosnak lennie egy már meglévő vezetékes LAN hálózattal, hanem azt többféle technológia is megvalósíthatja. A szabvány azt sem köti ki, hogy az elosztó rendszer adatkapcsolati, vagy hálózati réteg alapú legyen. Az architektúra általánossága abból adódik, hogy a szabvány alkotók között több csoport képviseltette az érdekeit. A szabvány emiatt explicit módon nem definiálja az elosztó rendszert, helyette inkább az architektúra komponensek közötti szolgálatokat határozza meg.



5. ábra A teljes 802.11 Architektúra.

A szolgálatokat az állomás és elosztó rendszer szolgálatokra lehet bontani.

Az állomás szolgálatok

• Azonosítás: A cellán belüli szolgálat, amely lehetővé teszi az átviteli közeghez való hozzáférést. Az átviteli közeghez való kapcsolódás céljából az állomásnak meg kell határoznia azonosságát. A vezetékes LAN hálózatokban a fizikai hálózathoz hozzáférés szabályozható, ez azonban nem tételezhető fel a WLAN hálózatokban. A szolgáltatás kapcsolat szintű hozzáférést tesz lehetővé, vagyis egyszerűen a vezeték nélküli hálózat felépítéséhez használt, vezetékes LAN hálózatok

hozzáférésével azonos szabályozást tesz lehetővé. Az architektúrák lehetnek nyitottak, amikor bármilyen, a szabványnak megfelelő eszköz hozzáférhet az átviteli közeghez, és osztott kulcsúak.

• Az állomásnak az átviteli közeghez való hozzáférésének megszűntetése.

• Titkosítás: Az adatbiztonság megköveteli, hogy bizonyos kereteket csak a címzett olvashassa. A vezetékes LAN hálózatokban az figyelheti a forgalmat, aki a hálózathoz kapcsolódik, míg a WLAN hálózatoknál bárki, akinek a szabványnak megfelelő rádiós interfésze van.

• Az állomás hozzárendelése egy hozzáférési ponthoz Mielőtt egy állomás adatot küldhetne egy hozzáférési ponton keresztül először szükség van arra, hogy hozzáférési ponthoz legyen rendelve, hogy az elosztó rendszer számára ismert legyen, hogy egy terminál melyik cellába tartozik.

• Egy meglévő BSS - terminál összerendelést megszüntetése.

Az elosztó rendszer szolgálatai

• MSDU adatcsomagok szállítása az elosztórendszeren belül az BSS – terminál összerendelő szolgálat információinak felhasználásával.

• Integráció: MSDU adategységek szállítása az elosztórendszer és a vezetékes hálózat között a “Portal” logikai ponton keresztül.

• Az állomás számára a hozzáférési pontok közötti mozgást lehetővé tevő szolgálat. *Logikai címtartományok*

A szabvány lehetővé teszi, hogy a cellák átviteli közege, az elosztó rendszer átviteli közege és az integrált vezetékes LAN hálózat számára, hogy átviteli közegeik eltérőek legyenek, valamint különböző címtartományokat használjanak. A szabvány csak a BSS-ek átviteli közegének címtartományát specifikálja, az IEEE 48 bites címtartományának használatával, ami megfelel a 802-es szabvány családban alkalmazottal.

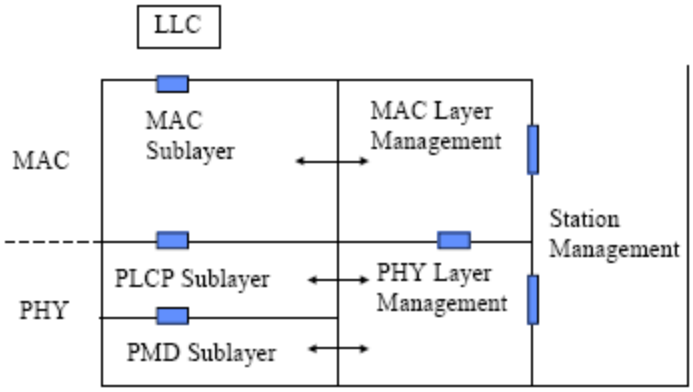
A legtöbb esetben a vezetékes LAN hálózat és a 802.11 közeg hozzáférési réteg címtartománya megegyezik. Az architektúra azonban azt is lehetővé teszi, hogy mindhárom címtartomány különböző legyen, például amikor az elosztó rendszer hálózati címzést használ a vezeték nélküli átviteli közeg címtartománya és az elosztó rendszer címtartománya eltérő lesz.

Az, hogy az architektúra több logikai átviteli közeget és címtartományt kezelhet lehetővé teszi számára, hogy független legyen az elosztó rendszertől és közöttük a kapcsolat tisztán interfész jellegű legyen.

5.2 Az IEEE 802.11 rétegek leírása

5.2.1 802.11 referencia model

Mint minden 802.x protokoll, a 802.11 protokoll a MAC és a Fizikai réteget fedi le.



6. ábra 802.11 referencia modell - protokoll entitások

MAC Entitás

• Alap közeghozzáférés

• fragmentáció

• titkosítás

MAC Layer Management Entity

• szinkronizálás

• teljesítmény menedzsment

• roaming (cellaváltás)

• MAC MIB (Management Information Base) fenntartás

Physical Layer Convergence Protocol (PLCP)

• PHY-specifikus, közös PHY SAP-ot biztosít, azaz a MAC kereteket (MPDU) fizikai csomagokká alakítja oda és vissza.

• Clear Channel Assessment jelet biztosít (vivőérzékelés)

Physical Medium Dependent Sublayer (PMD)

• moduláció és kódolás

PHY Layer Management

• csatornahangolás – link adaptáció

• PHY MIB fenntartás

Station Management

• a MAC és a PHY menedzsmenttel működik együtt, illetve az együttműködésüket hangolja össze

A MAC rétegek által ellátott tipikus szabványos funkcionalitásokon túl a 802.11 MAC további funkciókat is ellát, melyeket tipikusan felsőbb rétegek szoktak ellátni, pl. fragmentáció, csomag újraadás, nyugtázás.

Jelenleg a szabvány egyetlen MAC-et definiál, ami 3 PHY-vel tud együttműködni, melyek 1 vagy 2 Mbps-os átvitelt biztosítanak.

• Frekvenciaugratásos szórt spektrumú (Frequency Hopping Spread Spectrum, FHSS) a 2.4 GHz sávban,

• Direkt szekvenciális szórt spektrumú (Direct Sequence Spread Spectrum, DSSS) a 2.4 GHz sávban és

• InfraRed (Diffuse Infrared, DFIR) Direkt szekvenciális, frekvencia-ugratásos (915 MHz, **2.4 GHz**, 5.2 GHz), Infra (850-900 nm).

Bár eredetileg az adatkapcsolati réteg feladata nem korlátozódik pusztán a közeghozzáférés szabályozására (MAC), mivel ő felelős többek között a csomagok tördeléséért és visszaállításáért, valamit azért is, hogy elrejtse a fizikai réteg sokféleségét a felhasználó (hálózati réteg) elől, mégis a MAC funkció az, ami a legnagyobb kihívást jelenti és ami jelentősen hozzájárul az egész WLAN rendszer minősítéséhez. Az LLC funkciót viszont különösebb nehézség nélkül meg lehet

oldani (a 802.11 családban függetlenül attól, hogy vezetékes LAN-ról vagy vezeték nélküliről van szó, ugyanazt az LLC-t használják). Ezért az adatkapcsolati réteg kapcsán mi is a MAC-re koncentrálunk.

5.2.2 A MAC réteg

A 802.11 MAC rétege kétféle közeghozzáférési módszert definiál:
Elosztott: Distributed Coordination Function (DFC), ahol a mobil terminálok ugyanazt az egyszerű szabályt alkalmazzák a rádiócsatorna megszerzésére, mindenféle központi „döntőbíró" nélkül, és
Központosított: Point Coordination Function (PCF), ahol a terminálok kérései alapján az AP dönt a rádiócsatorna kiosztásáról, és a döntésének megfelelően adja meg a jogot az egyes mobil állomásoknak az adásra.

5.2.2.1 Elosztott vezérlésen alapuló közeg-hozzáférési eljárás, Distributed Coordination Function (DCF)

Keretek közötti idők (Inter Frame Spaces)
A szabvány négy féle IFS-t definiál, melyek különböző prioritások biztosításához használhatók.
• SIFS - Short Inter Frame Space, egyedi dialógushoz tartozó átvitelek elválasztására szolgál. (pl. Fragment-Ack), és ez a legkisebb IFS. Adott időpillanatban legfeljebb egy állomás adhat, ezért neki prioritása van a többiekkel szemben. Ez az érték fix minden PHY-re és úgy határozzák meg, hogy az adó állomás képes legyen visszakapcsolni vételi módba a bejövő csomag dekódolásához. 802.11-nél FH esetén ez az érték 28 μs, DSSS-nél 10μs.
• PIFS - Point Coordination IFS, az AP használja (vagy a Point Coordinator, ahogy ebben az esetben hívják) a többi állomás előtti közeghez való hozzáférésre. Ez az érték a SIFS plusz egy Slot Time (FHSS: 50μs, DSSS: 20μs), azaz 78 μs, illetve 30μs.

• DIFS - Distributed IFS, az új átvitelt kezdeményezni akaró állomás használja, PIFS plusz egy slot time.

• EIFS - Extended IFS, egy hosszabb IFS, amit az az állomás használ, amelyik olyan csomagot vett, amit nem tud értelmezni. Ez arra szolgál hogy megvédje az állomást (amelyik nem tudta értelmezni a Virtual Carrier Sense-re vonatkozó időtartam információt) a mostani dialógus későbbi csomagjaival való ütközéstől.

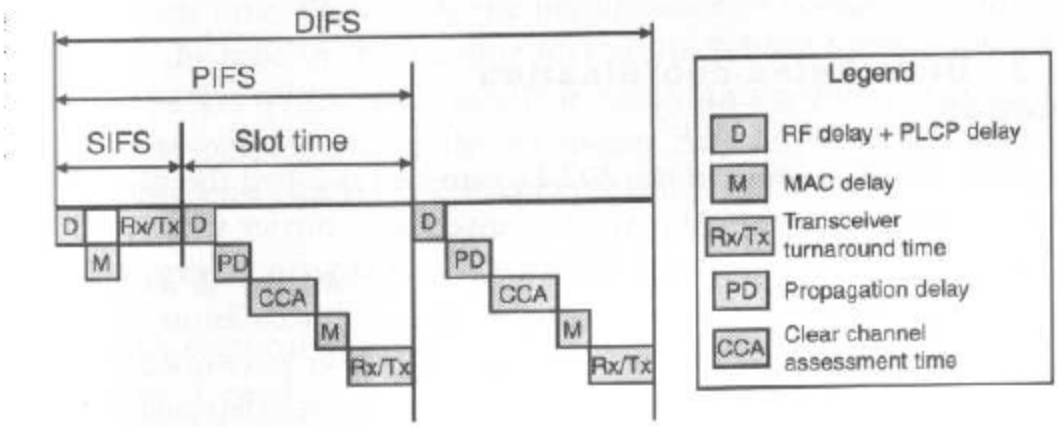


Table 4.5
Interframe Space Specifications

Interframe Space	DSSS	FHSS	DFIR
SIFS	10 µs	28 µs	7 µs
PIFS	30 µs	78 µs	15 µs
DIFS	50 µs	128 µs	23 µs
Slot time	20 µs	50 µs	8 µs

7. ábra Keretek közötti idők

Az alap közeghozzáférési módszer: CSMA/CA

Az alap közeghozzáférési módszer a **Distributed Coordination Function** alapvetően CarrierSense Multiple Access megoldásra épül Collision Avoidance mechanizmussal kiegészítve.(**CSMA/CA**). A CSMA protokollok jól ismertek az iparban, ilyen pl. az Ethernet, ami CSMA/CD módszer használ (CD, Collision Detection).

A CSMA protokollok a következőképpen működnek: Az adni kívánó állomás figyeli a közeget. Ha a közeg foglalt (másik állomás ad) akkor elhalasztja az adását egy későbbi időpontra. Ha a közeget szabadnak érzékelte, akkor megkezdheti az adását.

Ezen típusú protokollok akkor hatékonyak, ha a közeg nem túlságosan terhelt, mivel ilyenkor minimális késleltetéssel adhatnak az állomások. Ugyanakkor előfordulhat, hogy több állomás egyidejűleg szabadnak érzékeli a közeget és egyszerre kezd adni, ami ütközéshez vezet. Az ütközési helyzeteket fel kell tudni ismerni és így a MAC réteg újraadhatja a csomagot és nem a felsőbb rétegeknek kell ezzel foglakozni, ami jelentős késleltetést okozna. Ethernet esetén az ütközést az adóállomás ismeri fel és ezután egy ún. újraadási fázisba megy át, ami az **exponential random backoff** algoritmust használja.

Ez a megoldás vezetékes LAN-oknál nagyon jó, de WLAN-oknál nem célszerű alkalmazni a következők miatt:

1. Collision Detection eljárás megvalósítása Full Duplex rádiós képességeket igényelnek, ami jelentősen növelné az árakat.

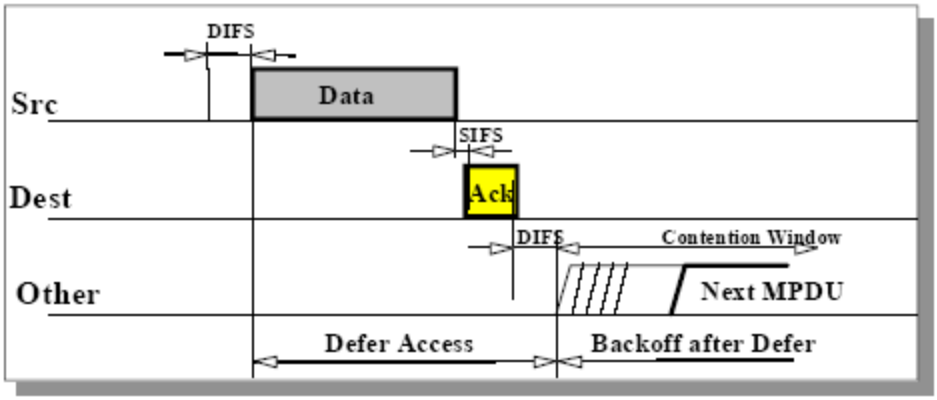
2. Vezeték nélküli környezetben nem tételezhetjük fel, hogy minden állomás hallja a többit (ami a Collision Detection alapja, és az a tény, hogy egy állomás szabadnak érzékelte a közeget, nem jelenti azt, hogy az a vevőnél csakugyan szabad is. Ezen problémák lekűzdésére a 802.11 Collision Avoidance (CA) eljárást alkalmaz Positive Acknowledge-tel kiegészítve a következő módon:

1. Az adni kívánó állomás érzékeli a közeget. Ha foglalt, akkor elhalasztja az adását.

Ha szabad egy előre definiált ideig (Distributed Inter Frame Space, DIFS), akkor az állomás adhat.

2. A vevőállomás ellenőrzi a vett csomag CRC-jét és nyugtát küld (acknowledgment packet, ACK, MAC nyugta). A nyugta vétele jelzi az adónak, hogy nem történt ütközés. Ha az adó nem kapott nyugtát újra küldi a csomagot

amíg nyugtát nem kap vagy el nem dobja adott számú próbálkozás után. A SIFS azért kisebb, mint a DIFS, hogy a harmadik állomás ne kezdhessen el adni a nyugta elküldése előtt. (Az egynél több célcímű csomagokra, pl. multicast, nincs nyugta).



8. ábra Az ütközés elkerülés alapelve

Exponenciális Backoff Algoritmus

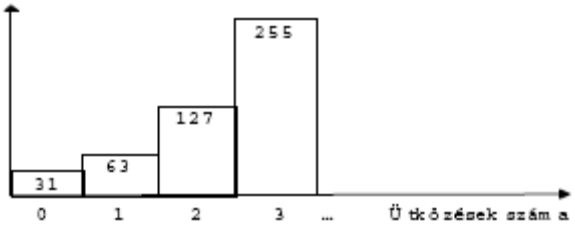
A Backoff jól ismert módszer egyazon közeghez hozzáférni szándékozó állomások közötti verseny feloldására. Az eljárás során minden állomás egy véletlen számot generál *n* és 0 között és a generált számnyi időrést (slot) vár mielőtt a közeghez fordulna.

A **Slot Time**-ot oly módon definiálták, hogy egy állomás mindig képes legyen annak megállapítására, hogy egy másik állomás hozzáfért a közeghez az előző slot kezdetekor. Ez felére csökkenti az ütközés valószínűségét.

Az exponenciális Backoff azt jelenti, hogy valahányszor egy állomás egy időrést választ és az ütközik, akkor a véletlen szám generálás felső határát exponenciális eloszlás szerint sorsolja.

Backoff_Time=INT(CW*RANDOM())*Slot_Time

A kifejezésben szereplő CW (Contention Window) a verseny ablak mérete. A verseny ablak mérete nem állandó, kezdetben 31 résidőnyi, ha egy terminál ütközést szenved egy adott csomag adásánál, akkor az ablak méret nő, az állomás menedzsment információs adatbázisában szereplő maximális értékig. A RANDOM() egy véletlen számot generáló függvény nulla és egy között.



9. ábra A verseny ablak méretének változása

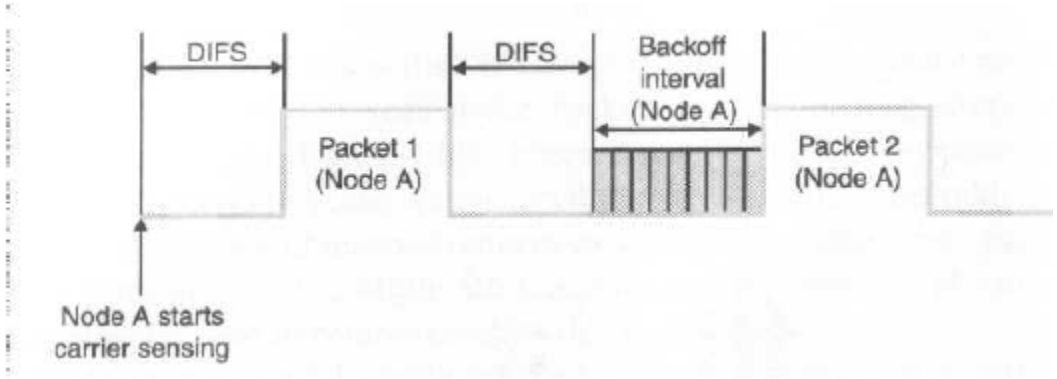
A 802.11 szabvány által definiált **Exponential Backoff algoritmust** az alábbi esetekben kell végrehajtani:

• Amikor az első átvitel előtt az állomás figyeli a közeget és azt foglaltnak találja

• Minden újraadás után, és

• Minden sikeres átvitel után (multipacket transmission során, 9. ábra). Ezzel fair módon járunk el a többi állomással szemben. Esélyt adunk, hogy ők is adáshoz jussanak.

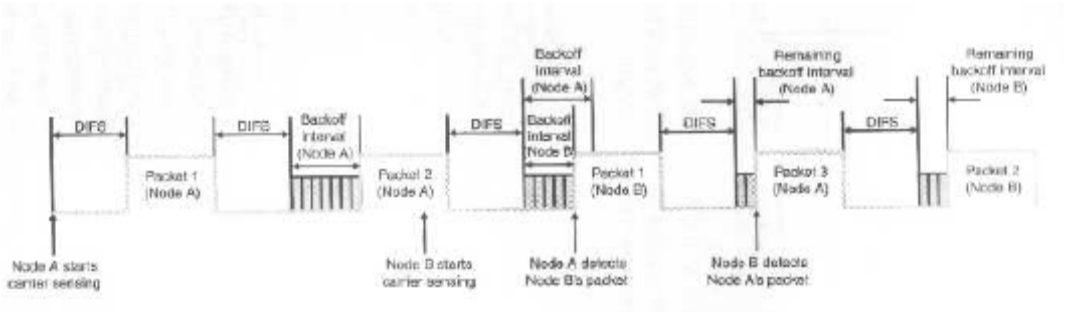
Az egyetlen eset, amikor nem használandó ez az eljárás, ha az állomás adni kíván és előtte DIFS ideig szabadnak érzékelte a közeget (7. ábra).



10. ábra Multipacket transmission szemléltetése

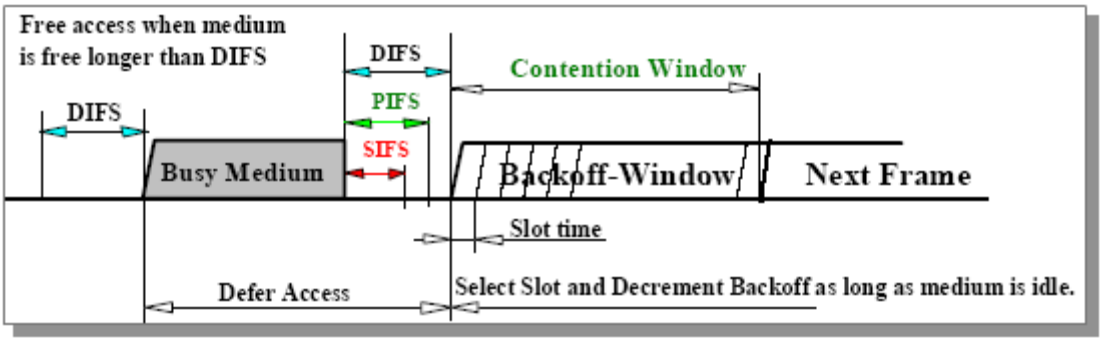
A hozzáférés tiltási fázis a vivőérzékelésen alapul. Ezt a fizikai rétegben Clear Channel Assessment-nek (CCA) hívják. Ezt egészíti ki a *Virtual Carrier Sense.*

A késleltetési idő csökkentése akkor kezdődhet meg, ha a médium DIFS ideig szabad. Ha eltelik egy résidőnyi idő és egyetlen terminál sem kezdte meg adását, akkor csökkenthető a késleltetési idő értéke eggyel, ezután ismét a közeg figyelése következik. Ez a folyamat egészen addig tart, míg a médiumon átvitelt nem érzékelnek. Egy terminál akkor adhat, ha a késleltetési ideje nullára csökken. Amennyiben a közegen átvitelt tapasztalnak a terminálok a késleltetési idő csökkentése befejeződik a következő DIFS idejű üresnek érzékelésig.



11. ábra Közeghozzáférés működésének szemléltetése

Az 11. ábra az IFS idők „erejét” mutatja. PIFS kisebb, mint DIFS, hogy a PCF „erősebb” legyen, mint a DCF. Fontos, hogy ha nem érkezik közvetlenül a csomag adása után SIFS idővel a nyugta, akkor újra kell adni a csomagot.

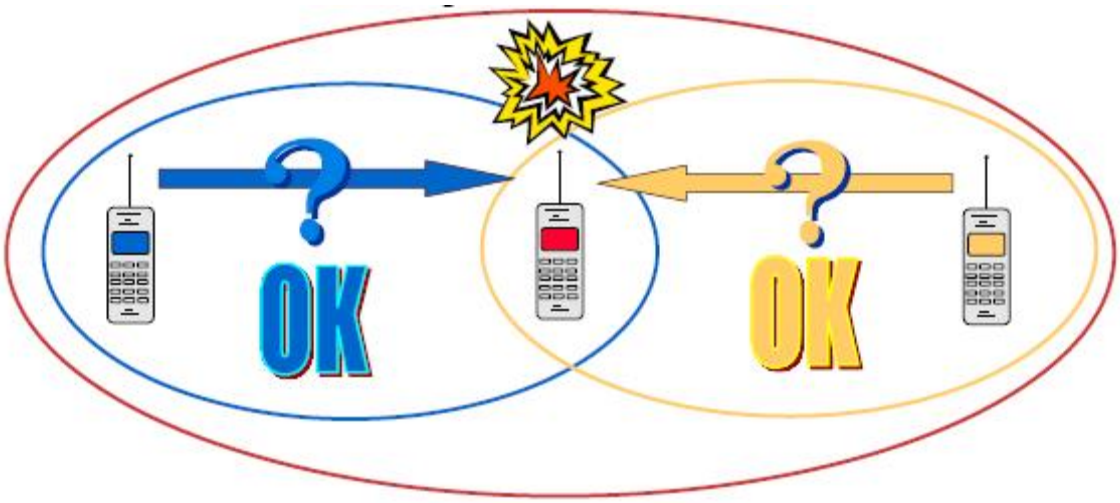


12. ábra A hozzáférési mechanizmus és résidők szemléltetése

A rejtett terminál probléma

Ez a krimikbe illő kifejezés egy nagyon fontos jelenséget takar, melyet a 12. ábra szemléltet. A három különböző színű mobil telefon három felhasználót jelképez.

Minden telefon körül a saját színével látható a rádiós lefedési területe, azaz az a terület, amelyen belül az adását venni lehet. Először a SÁRGA terminál akar csomagot küldeni a PIROS-nak, ezért először belehallgat a rádiócsatornába, hogy az nem foglalt-e. Mivel üresnek találja, ezért elkezdi az adását. Mindeközben a KÉK felhasználó is csomagot szeretne továbbítani a PIROS terminálnak, ezért ő is belehallgat a rádiócsatornába. Mivel a SÁRGA telefon hatósugara nem éri el a KÉK terminált (azaz a SÁRGA telefon rejtve marad a KÉK elől), ezért a KÉK üresnek érzékeli a rádiócsatornát, és bátran adni kezd. Ennek eredményeképpen a PIROS telefonnál összeütköznek a csomagok.



13. ábra Rejtett terminál probléma szemléltetése

Virtual Carrier Sense

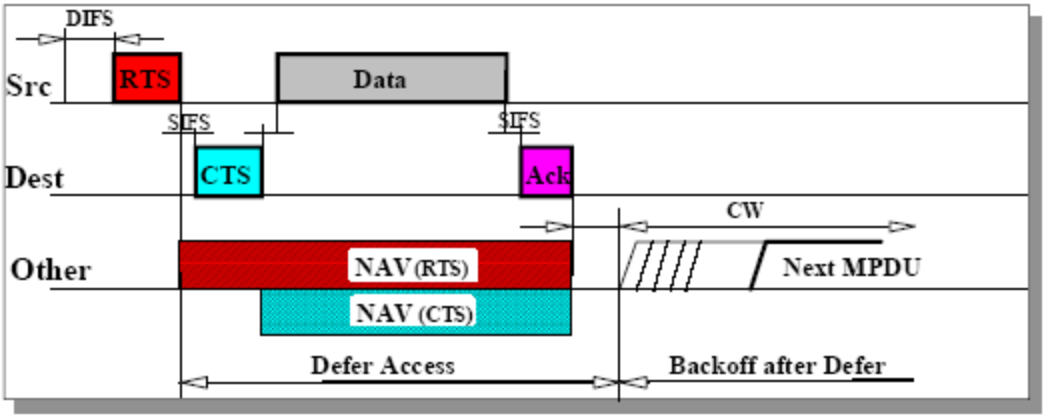
Annak érdekében, hogy csökkentsük az egymás nem hallásából adódó ütközések számát a szabvány definiálja a Virtual Carrier Sense eljárást. Az adni kívánó állomás először egy rövid vezérlő csomagot küld (**RTS,** Request ToSend), ami tartalmazza a forrást, a célt, a következő tranzakció időtartamát, azaz a csomagot és a hozzá tartozó nyugtát. A cél válaszol (ha szabad a

közeg) egy vezérlő csomaggal (**CTS,** Clear to Send), ami ugyanezeket az időtartam információkat tartalmazza.

Valamennyi állomás, amelyik vette az RTS-t és/vagy a CTS-t, beállítja a **Virtual Carrier Sense** indikátorát (**NAV**, **Network Allocation Vector**), az adott időtartamra és ezt az információt használja a fizikai vivő érzékeléssel együtt a közeg figyelésére. Ez a megoldás csökkenti az ütközések valószínűségét a vevő oldalon egy olyan állomással szemben, ami rejtett az adó előtt az RTS idejére, mivel az állomás meghallja a CTS-t és a tranzakció idejére nem próbál a közeghez férni.

Az RTS-beli időtartam információ megvédi az adó környezetét is az ütközéstől az ACK idejére (azon állomásoktól, melyek a nyugtázó állomás hatókörén kívül vannak.). Meg kell jegyezni továbbá, hogy az RTS és CTS rövid csomagok ezért az ütközési overhead is csökken, mivel ezeket gyorsabban lehet érzékelni mint a hosszú csomagok esetében és az újraadás is hamarabb történhet. Ez abban az esetben igaz, ha az RTS lényegesen rövidebb a csomagnál, ezért a szabvány definiálja az **RTS Threshold** változót. Csak az ennél hosszabb csomagokra alkalmazható az RTS/CTS eljárás.

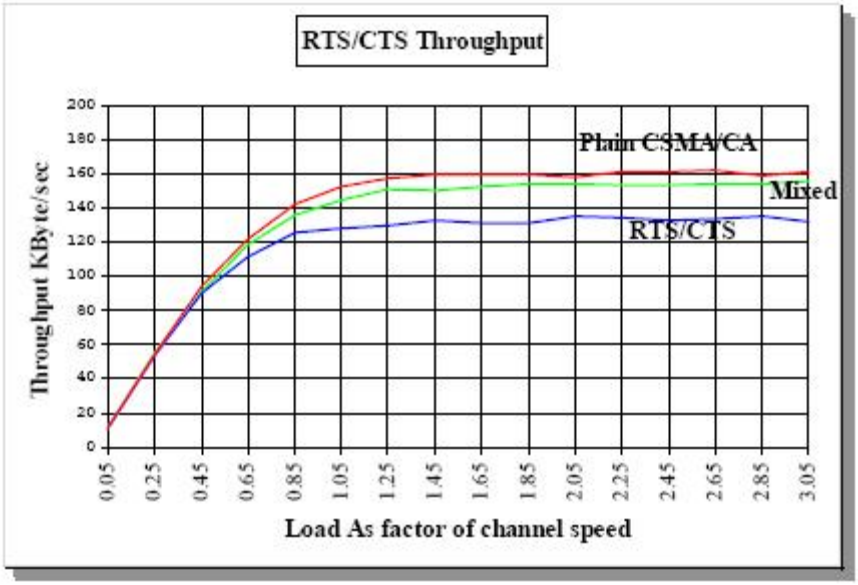
A 13. ábra az A és B állomások közötti tranzakciót mutatja és a szomszédjaik NAV beállítását.



14. ábra Rejtett terminál probléma feloldása virtuális vivőérzékeléssel

A NAV State a fizikai vivő érzékeléssel kombinálva jelzi a közeg foglaltságát.

Az RTS vezérlő keretek átvitele után előfordulhat, hogy nem érkezik rá nyugta. Ennek oka lehet az, hogy ütközött egy másik RTS vezérlő kerettel, vagy adat kerettel esetleg interferáló jelekkel az RTS, CTS vezérlő keretek időtartama alatt. Ebben az esetben a keretet újra kell adni a véletlen késleltetési időt generáló algoritmus alkalmazásával megnövelt ablakmérettel. Akkor is a véletlen késleltetési időt generáló alkalmazására van szükség, ha egy adatkeretre nem érkezik nyugta.

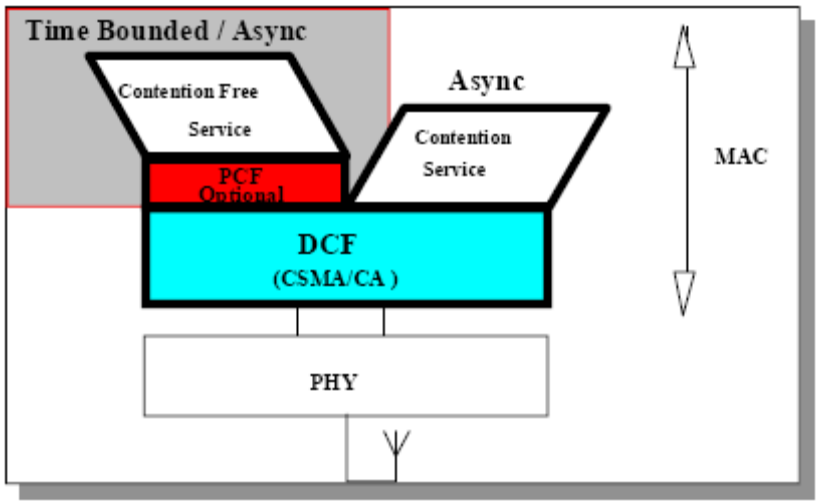


15. ábra RTS/CTS overhead hatása

A fenti ábrán az RTS/CTS overhed látható a hagyományos CSMA/CA-hoz viszonyítva. Ugyanakkor ne felejtsük el, hogy RTS/CTS nélkül a rejtett terminál problémát nem lehetne kezelni.

5.2.2.2 Központosított vezérlésen alapuló közeg-hozzáférési eljárás, Point Coordination Function (PCF)

Az időkorlátos szolgáltatások, pl. video vagy beszédátvitel magasabb prioritást igényelnek, mint a sima adatátvitel. Ezt teszi lehetővé a PCF az AP-k által használt kisebb IFS, a PIFS idő segítségével. A magasabb prioritás révén az AP polling kéréseket küld az állomásoknak az adatátvitelért, így vezérli a közeghozzáférést.
Azért, hogy a többi állomás is hozzáférhessen a közeghez az AP-nek elég időt kell hagynia a DCF-nek két PCF periódus között.

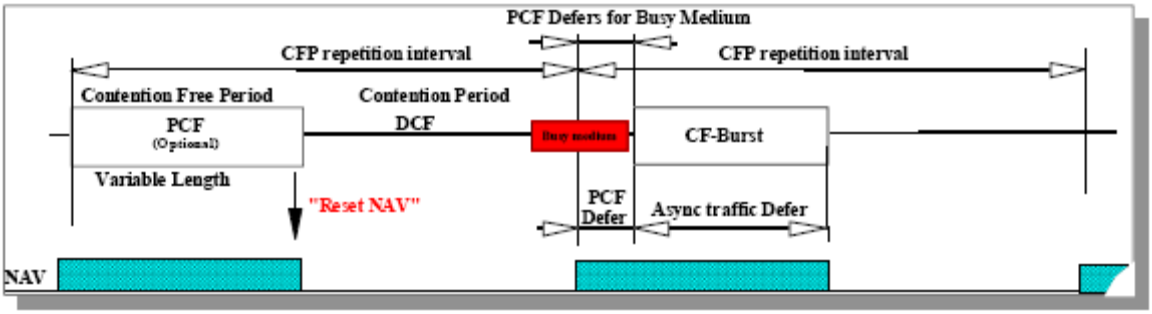


16. ábra PCF elhelyezkedése a protokoll struktúrában

A PCF opcionális közeg-hozzáférési eljárás, amely csak infrastruktúra konfigurációkban alkalmazható. Az alap közeg-hozzáférési eljárás felett működik azzal a céllal, hogy versenymentes keretátvitelt biztosítson és egyben megoldást jelent a prioritátos terminálok időszakos lekérdezésére is. Az eljárás működéséhez szükséges, hogy implementálva legyen a hozzáférési pontban, amely eldönti az egyes terminálok adási jogát. A hozzáférési pont magához veszi a közeg vezérlését a versenymentes periódus kezdetén és megtartja azt egészen a végéig.
A nem lekérdezhető állomásokkal nem alakul ki verseny sem a következő két okból kifolyólag:

A keretek között rövidebb idejű adási szüneteket használnak (SIFS), mint amit felfedezne az állomásokban meglévő alap hozzáférési eljárás (DIFS), ezért a terminálok nem csökkentik az adás késleltetési idejüket.

Mindegyik terminál követi a hozzáférési pont által diktált szabályt és beállítja a várható hálózat foglalási időt tartalmazó változóját minden egyes versenymentes periódus kezdetén annak teljes időtartamára (CPFMaxDuration). A keretek információt hordoznak arra vonatkozóan, hogy mennyi ideig tart a keret átvitele és az azt követő nyugta megérkezése. Amikor egy állomás érvényes keretet vesz a keret időtartam mezője alapján felülírja a hálózatfoglalás időtartamát jelző változóját, ha az nagyobb a változóban szereplő értéknél



17. A versenymentes és versengéses időszak változása

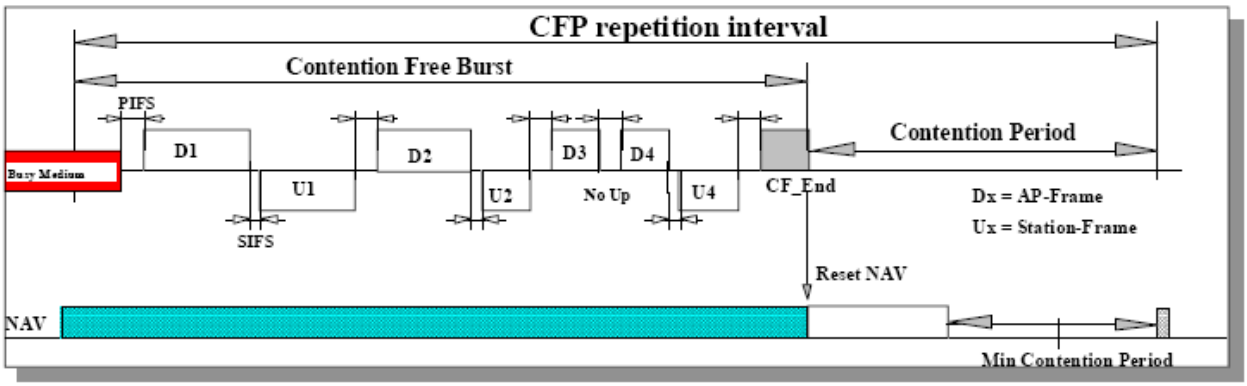
A lekérdezett állomásoknak meg van a választási lehetősége, hogy válaszoljon a lekérdezésére (CF-POLL). A lekérdezés folyamatát végző központi állomás minden lekérdezhető állomásnak megadja az átvitel jogát ciklikus multiplexeléssel. A mester állomásként működő hozzáférési pont és a lekérdezett állomás nem cserélnek RTS/CTS kereteket a versenymentes periódusban. A lekérdezett állomás egyetlen adatcsomagot adhat a bármelyik címre vonatkozóan, amit a mester állomás továbbít majd. A versenymentes és versengéses periódusok egymást felváltva követik.

Egy keret újraadásának igényének felmerülésekor, azaz ha egy keretre nem érkezik nyugta a terminálótól, a mester állomás újraadhatja azt PIFS idő után a versenymentes periódusban.

A keretek nyugtázása megvalósítható a versenymentes periódusban is. A mester állomás az adat és az előző keretre vonatkozó nyugta (ACK) összefogásával. Ezzel elkerülhető az elkülönült ACK vezérlő keretek átviteléből adódó többlet fejrész

átvitele, habár a nem lekérdezhető állomások, vagy a nem lekérdezett, de lekérdezhető állomások küldhetnek nyugtát a versenymentes periódus alatt az alaphozzáférés nyugtázási eljárását használva.

A központosított hozzáférési eljárás a következő módon valósul meg. A mester állomás figyeli a médiumot annak megállapítása céljából, hogy szabad, vagy sem. Amikor szabadnak érzékeli egy PIFS ideig ad egy irányító-vezérlő keretet (beacon), ami a lekérdezéshez szükséges információkat viszi. Ezután a mester állomás DATA, CF-POLL, DATA+CF-POLL keretet ad, vagy kiadhatja a CF-END keretet közvetlenül a beacon után SIFS időtartam kivárása után, ha nincs tárolt átviendő keret, vagy nincs olyan terminál, amit le kellene kérdezni. A CF-END törli a NAV változót.



18. ábra PCF börszt felépítése

5.2.2.3 Fragmentáció és visszaállítás (Reassembly)

Egy tipikus LAN protokoll néhány száz bájtos csomagokat használ (a leghosszabb Ethernet csomag 1518 bájtos lehet). Ugyanakkor vezeték nélküli környezetben célszerűbb a rövidebb csomagok használata az alábbi okokból kifolyólag:

• A rádiós linken a csomag méretével nő a csomag meghibásodásának valószínűsége a magas bithibaarány miatt.

• Csomag meghibásodása esetén (ütközés vagy zaj) minél kisebb a csomag annál kisebb az újraküldési overhead.

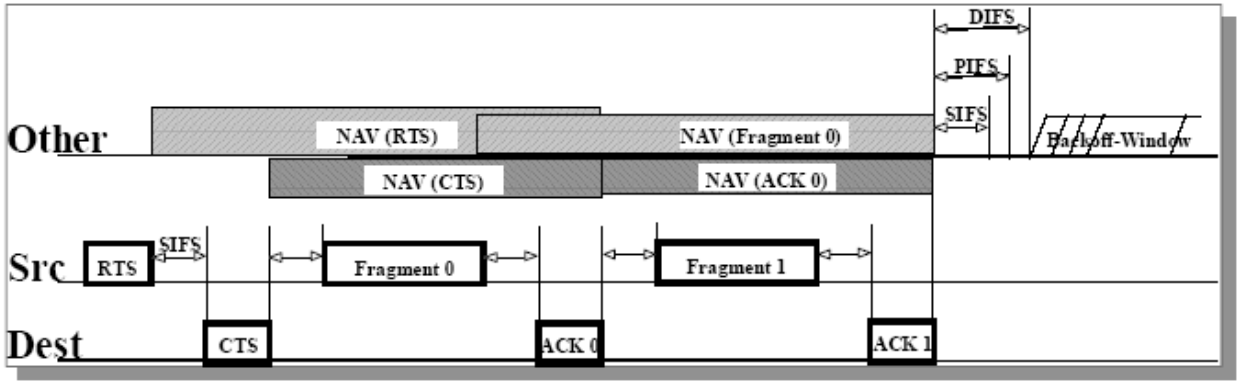
• Frekvenciaugratásos rendszerben a közeget periodikusan megszakítják (jelen esetben 20 ms-onként), ezért a kisebb csomag esetén kisebb eséllyel kell elhalasztani a csomagot.

Azonban nem érdemes egy új protokollt bevezetni, ami nem képes a hosszú csomagok kezelésére, ezért a problémát a fragmentáció/visszaállítás módszerével oldották meg a MAC rétegben. Az eljárás egy egyszerű Send-and-Wait algoritmus, ahol az adó állomás nem küldhet új fragmentet amíg az alábbiak egyike meg nem történik:

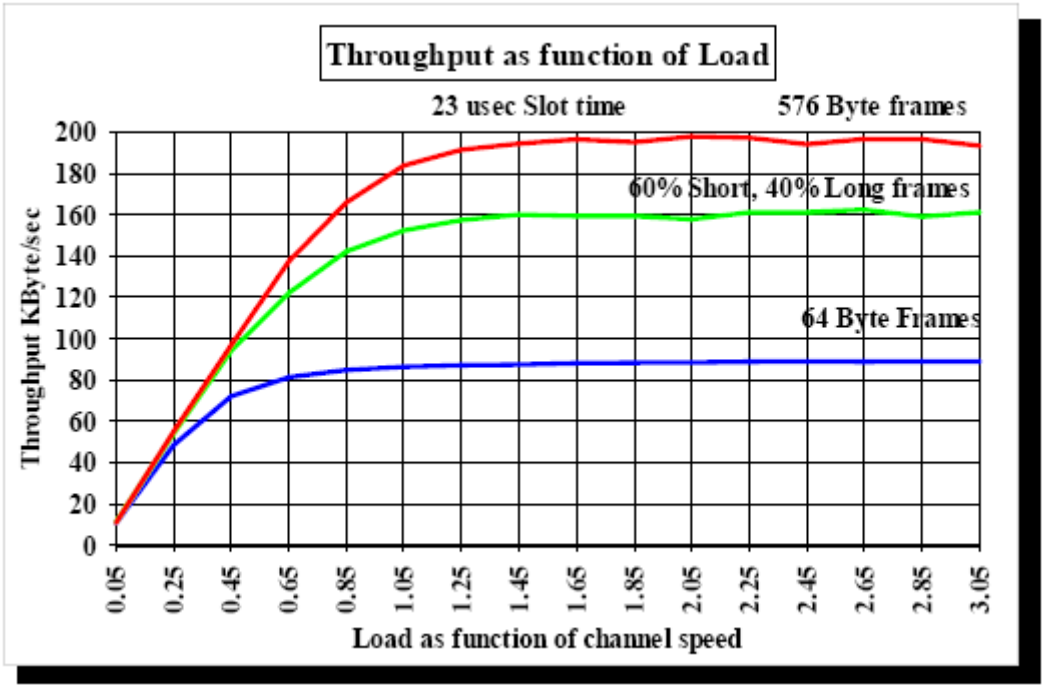
3. ACK-t vesz adott fragmentre, vagy

4. Úgy dönt, hogy a fragmentet túl sokszor adta újra és eldobja az egész keretet.

Meg kell jegyezni, hogy a szabvány lehetővé teszi, hogy egyazon fragment újraadásai között különböző címeket használjanak. Ez különösen hasznos ha egy Apnek több különböző címre kell csomagokat küldenie és az egyik nem válaszol. A 18. Ábra egy keret (MSDU) fragmentekre (MPDU) való bontását mutatja. Mivel SIFS kisebb, mint DIFS ezért a fragmentek között más nem veheti el a csatornát. A fragmenteket külön-külön nyugtázzák. Az exponenciális visszatartás a nyugtázatlan fragmentekre is vonatkozik. A NAV paraméter beállításának folyamatosságát a fragmentek és a nyugták biztosítják.



19. ábra Keret fragmentálás



20. ábra Stabilitás túlterhelés esetén is, börsztös forgalmat is támogatja.

Tegyünk most egy apró lépést technikai irányba és nézzük meg, hogyan "beszélgetnek" egymással a WLAN képes eszközök a valóságban.

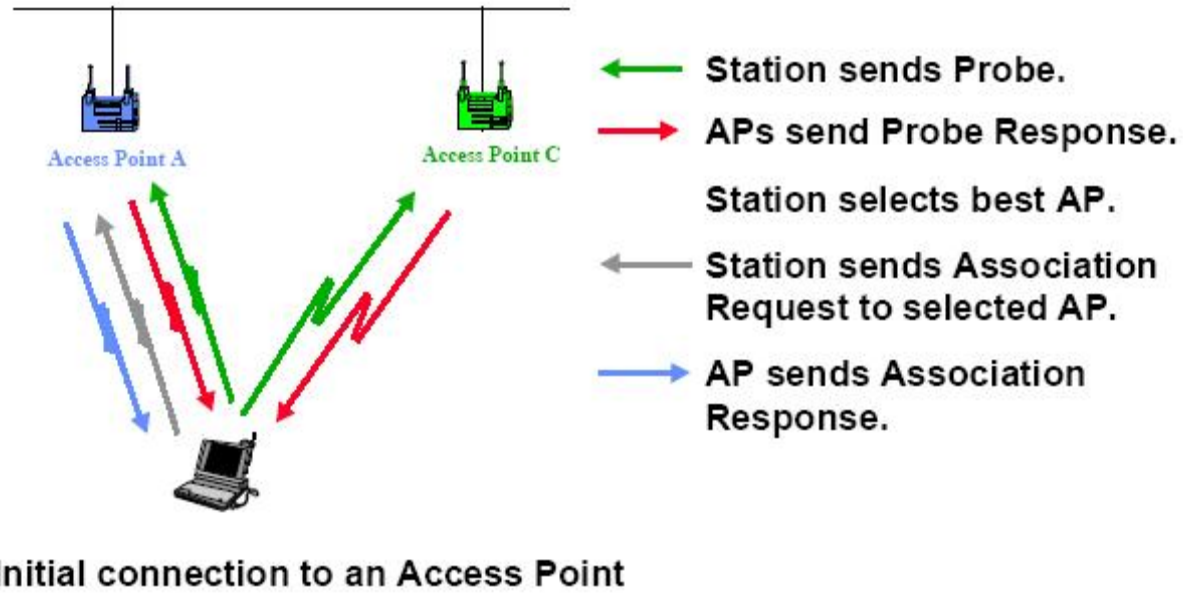
5.2.3 MAC Management Layer

Ha egy állomás egy létező BSS-hez akar kapcsolódni (bekapcsolás után vagy, alvó mód esetén vagy a BSS területre lépéskor), az állomásnak szinkronizációs információt kell kapnia az AP-től (adhoc üzemmód esetén, lásd később). Ezt az információt az állomás kétféle módon kaphatja meg:

1. Passive Scanning: ekkor az állomás egy Beacon Frame-t vár az AP-tól (a bacon keretet az AP periodikusan küldi szikronizációs információval ellátva, vagy

2. Active Scanning: ekkor az állomás megpróbál egy AP-találni Probe Request Frame-ek küldésével és ezután Probe Response-ra vár az AP-től.

Mindkét eljárás érvényes. A kiválasztás a teljesítményfelvétel/hatékonyság közötti kompromisszum alapján történik.



21. ábra Az aktív asszociáció lépései

A hitelesítési eljárás (Authentication Process)

Ha egy állomás megtalált egy AP-t és eldöntötte, hogy a BSS-éhez kapcsolódik, akkor végre kell hajtani egy hitelesítési eljárást. Ennek során mindkét fél bizonyítja, hogy ismer egy adott jelszót.

A csatlakozási eljárás (Association Process)

Ha egy állomás átesett a hitelesítésen, akkor egy csatlakozási eljárást kezd, melynek során információkat cserélnek a BSS-sel a képességeikről. Az eljárás lehetővé teszi továbbá a DSS (AP-k egy halmaza) számára az állomás aktuális helyének meghatározását. Egy állomás csak a csatlakozási eljárás után lesz képes a csomagok adására és vételére.

5.2.3.1 Roaming

A Roaming azt a folyamatot jelenti, amikor egy állomás az egyik cellából (vagy BSS-ből) egy másikba lép át a kapcsolat elvesztése nélkül. Ez a funkció hasonló a cellás telefonoknál megismert handoverhez két lényeges különbséggel:

1. Egy csomag alapú LAN rendszerben a cellaváltás megvalósítható két csomag átvitele között, szemben a cellás telefonnal, ahol ez beszélgetés közben is bekövetkezhet. Ez lényegesen egyszerűsíti a handovert, de

2. egy beszéd alapú rendszerben az időszakos megszakadás nem okoz gondot a beszédátvitelben, miközben csomag alapú rendszerben lényegesen csökkenti a hatékonyságot a felsőbb rétegbeli újraadások miatt.

A 802.11 szabvány nem definiálja, hogyan kell lebonyolítani a handovert, de alapvető eszközöket definiál. Ezek magukban foglalják az active/passive scanning-et, az újracsatlakozási folyamatot (re-association process), ahol a roamingoló állomás az új AP-hez csatlakozik.

A cellaváltás mobil oldali döntéssel történik. Az új hozzáférési pont kiválasztása történhet aktív és passzív módon is. Passzív mód esetén az állomás a beacon jeleket figyeli, míg aktív esetben minden lehetséges csatornán küld egy Próba jelet és figyeli az erre kapott válaszokat és kiválasztja a legjobb csatornát. Ezután állomás jelzi a közeghez való kapcsolódási szándékát a hozzáférési pontnak. A hozzáférési pont ennek elfogadása esetén egy azonosítót rendel az állomáshoz (ID), amit a kérésre adott válaszában elküld és értesíti a fölötte elhelyezkedő elosztó hálózatot a terminál cellaváltásáról, az elhagyott cella hozzáférési pontját az elosztó hálózat értesíti.

5.2.3.2 A szinkronizáció megtartása

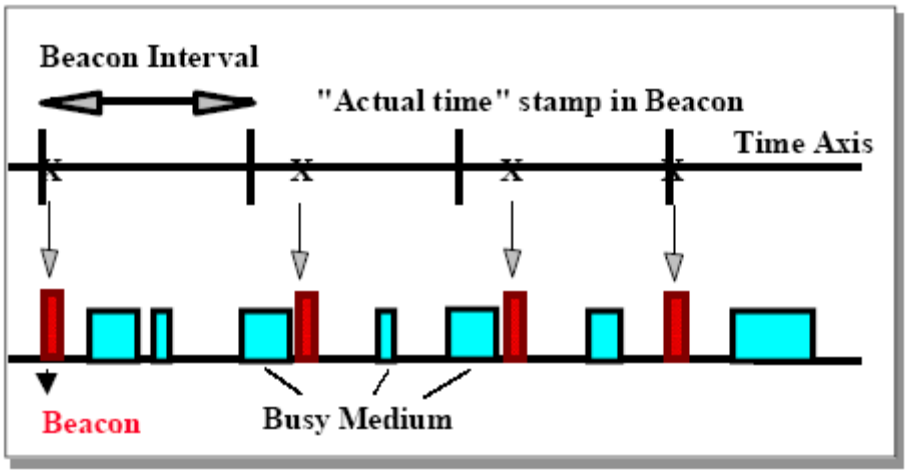
A szinkronizáció biztosítására a szabvány egy időszinkronizáló eljárást definiál (Timing Sychronization Function, TSF), amely minden egyes állomásban működik, ennek a feladata a teljesítmény menedzsment támogatása, a versenymentes eljárás során ez jelöli ki a versenymentes időintervallum kezdetét, frekvencia ugratásos fizikai réteg esetén pedig az új ugrási frekvencia alkalmazásának kezdetét és az ugrás hosszát.

Egy infrastruktúra BSS esetén ez úgy valósítható meg, hogy minden állomás az AP órájához szinkronizálja a sajátját az alábbi eljárással:

Az AP periodikusan ún. Beacon Frame-ket ad. Ezek a keretek tartalmazzák az AP órájának értékét az adás pillanatában (figyelem, ez az adás tényleges időpontja és nem amikor a sorba beállt a keret. Mivel a Beacon Frame-t a CSMA szabályok szerint küldik, ezért az átvitel lényeges késleltetést szenvedhet). A vevőállomás a vétel pillanatában ellenőrzi az óráját és kijavítja, ha szükséges az AP órájához való szinkronitás megőrzéséhez. Ez megakadályozza az óra elcsúszását, ami néhány órás üzem után bekövetkezne. A szinkronizáció fenntartásához egy állomásnak nem kell minden beacon jelet vennie. A beacon jelek az időzítési információn kívül más információt is visznek (teljesítmény menedzsment, barangolás).

A beacon jelek átvitelének folyamata:

A hozzáférési pont küldi a beacon jeleket adott intervallumonként, átvitele ezeknek a jeleknek nem ütközik a csomagok átvitelével, ha a közeg foglalt a beacon jel átvitelét késleltetik. Az egymást követő beacon jelek átvitele adott időközönként következik be, amennyiben az előző beacon jel átvitele késleltetve volt, akkor a következő beacon jel még nem lesz késleltetve szükségszerűen, csak akkor ha a tervezett adásának idejében a közeg éppen foglalt. A beacon jellel átvitt időbélyeg a jel adási idejét tartalmazza.



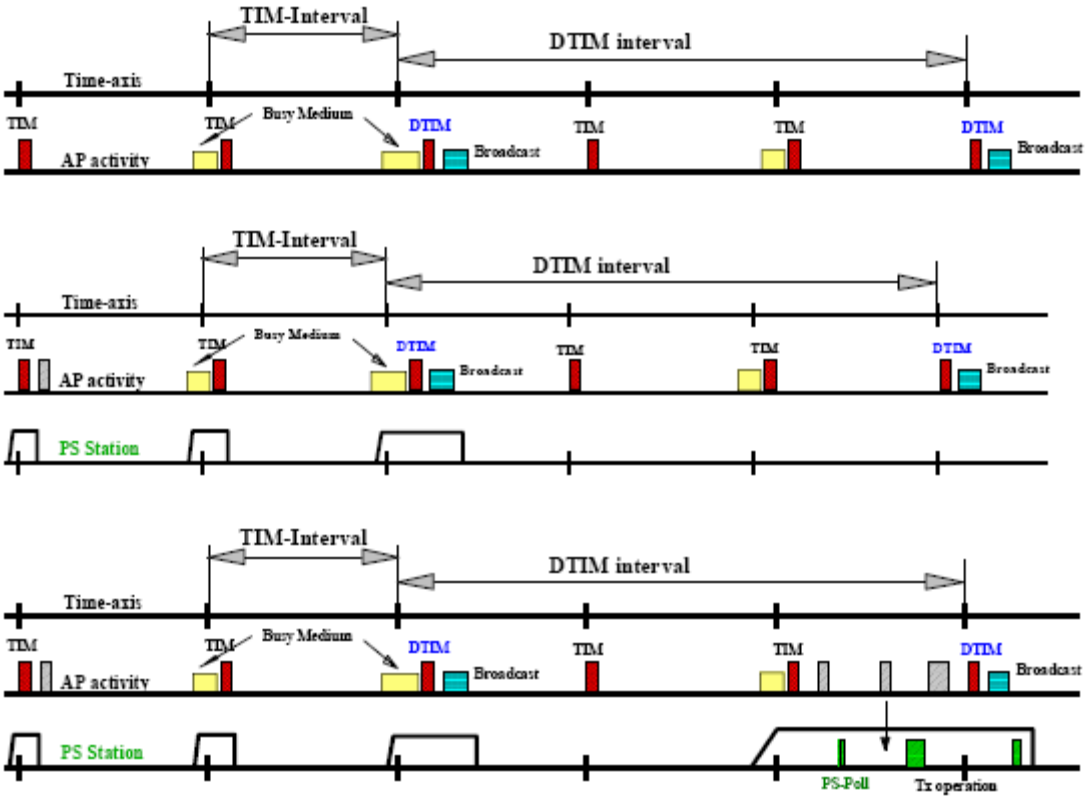
22. ábra Beacon jelek átvitelének folyamata

5.2.3.3 Teljesítménykímélő üzem (Power Saving)

A WLAN-ok tipikusan mozgó alkalmazásokhoz kapcsolódnak. Ezeknél az alkalmazásoknál a telep teljesítmény értékes erőforrás. Ezért a 802.11 szabvány speciális, ún. Power Saving üzemmódot definiál, ami lehetővé teszi az állomások számára, hogy alvó állapotba kerülhessenek hosszú időre információvesztés nélkül.

Az alapelv a következő: az AP folyamatosan frissíti az alvó módban levő állomás számára fenntartott bejegyzését és tárolja a neki küldött csomagokat amíg vagy az adott állomás ezeket külön nem kéri egy polling kéréssel vagy üzemmódot nem vált.

Az AP a Beacon Frame-k részeként periodikusan szétküldi, hogy mely Power Saving állomások számára tárol csomagokat és az állomások felébrednek, hogy vegyék a Beacon Frame-t. Ha jelzés van arra, hogy az AP-nál továbbításra váró keretek vannak, akkor az állomás ébren marad és egy Polling üzenetet küld az APnek. Multicast és Broadcast üzeneteket az AP tárolja és egy előre ismert időpontban (minden DTIM, ami a TIM (Traffic Indication Map) többszöröse) szétküldi őket. Azok az állomások, melyek ilyen típusú üzenetekre kíváncsiak, felébrednek erre az időpontra.



23. ábra Teljesítménykímélő üzemmód

5.2.4 Keret (csomag) típusok (Frame Types)

Három fő keret (csomag) típus létezik:

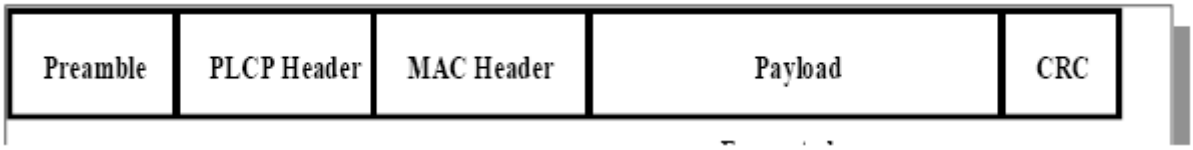
• Data Frame-k: adatátvitel céljaira

• Control Frame-k: a közeghozzáférés vezérlés céljaira (pl. RTS, CTS, és ACK),

• Management Frame-k: az adat keretekkel megegyező módon küldik őket a menedzsment információk cseréje végett, de nem továbbítják őket a felsőbb rétegekhez (pl. beacon keretek).

A keret típusokat altípusokra osztották a megfelelő funkciók szerint.

5.2.4.1 Keret formátumok



24. A fizikai réteg keretformátuma a M**E**AC P**t**D**d**U-val

Valamennyi 802.11 keret az alábbi összetevőkből áll:

Preamble

A PHY-től függ és tartalmazza:

• **Synch**: egy 80-bites sorozat, melyben 0-k és 1-ek váltakoznak, a PHY az antenna kiválasztására használja (ha van diverziti) és a frekvencia offszet korrekció alapállapotba hozására és a vett csomaggal való szinkronizálásra.

• **SFD**: egy Start Frame határoló, ami 16-bites bináris minta: 0000 1100 1011 1101, amit a keretidőzítéshez használnak.

PLCP Header

A PLCP Header-t mindig 1 Mbps-mal adják és logikai információkat tartalmaz, melyet a PHY réteg használ a keret dekódolásához. Felépítése a következő:

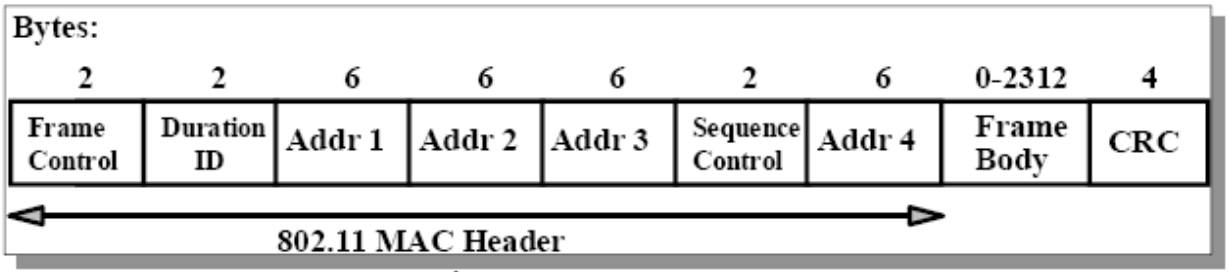
• **PLCP_PDU Length Word**: a csomag bájtjainak számát adja meg. Erre a PHYnek van szüksége a helyes detektáláshoz.

• **PLCP Signaling Field**: jelenleg csak a sebesség információt tartalmazza, 0.5 Mbps-enként kódolva 1 Mbps-tól 4.5 Mbps-ig.

• **Header Error Check Field:** egy 16 Bites CRC hibajavító mező.

MAC Data

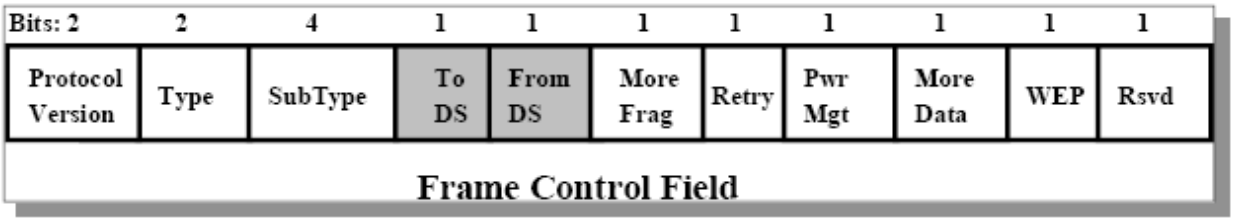
A 23. ábra az általános MAC keretformátumot mutatja. A mezők egy részét később ismertetjük. A Frame Control mező függ a keret típusától (vezérlő, menedzsment vagy adat)



25. ábra Általános MAC keretformátum

Frame Control Field

A Frame Control mező az alábbi információkat tartalmazza:



26. ábra Frame Control mező

Protocol Version

Ez a mező 2 bitből áll, a802.11 verziók azonosítására szolgál.

Type and Subtype

Ez a 6 bit definiálja a keret típusokat és altípusokat az alábbi táblázatnak megfelelően.

Type Value	Type Description	Subtype Value	Subtype Description
b3 b2		b7 b6 b5 b4	
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Association Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-0001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-ACK + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
10	Data	0000-1111	Reserved

27. Type és Subtype mező

ToDS

Ezt a bitet 1-be kell állítani ha a csomagot az AP-nek küldték az elosztó rendszer felé való továbbításra címezték (beleértve azt az esetet amikor a célállomás ugyanabban a BSS-ben van és az AP relay-ezi a keretet. 0-ba kell állítani minden más keretre pl. CTS,RTS, ACK.

FromDS

Ez a bit 1 ha a keret a Distribution System-ből érkezett.

More Fragments

Ez a bit 1 ha a jelenlegi fragment keretéhez még tovább fragmentek tartoznak.

Retry

Ez a bit jelzi, hogy ez a fragment egy korábbi fragment újraadása. Ennek segítségével a vevőállomás felismerheti egy keret duplikált adásait ha az ACK csomag elveszett.

Power Management

Ez a bit jelzi, hogy ezen keret átvitele után az állomása Power Management üzemmódba megy át. Ezt azok az állomások használják, melyek Power Save állapotból Active állapotba lépnek vagy fordítva.

More Data

Ez a bit jelzi, a Power Management-nek az AP révén, hogy további tárolt keretek vannak az állomás részére Ennek segítségével az állomás eldöntheti, hogy lekérdez vagy éppen Active mode-ba megy át.

WEP

Ez a bit jelzi, hogy a keret törzsét a WEP-nek megfelelően titkosították

Duration/ID

A keret típustól függően ezen mezőnek két jelentése van:

• Power-Save Poll üzenetekben az Station ID.

• Minden más keretben ez az időtartam érték, melyet a NAV számításhoz használnak.

Address Fields

Egy keret max. 4 címet tartalmazhat a ToDS-től és a FromDS bitektől (Control Field-ben adják meg őket) függően az alábbiak szerint:

• **Address-1** mindig a Recipient Address (azaz az a BSS állomás, ami a csomag közvetlen vevője). Ha a ToDS 1-be van állítva, ez az AP Address, ha ToDS=0 akkor ez a végállomás címe.

• **Address-2** mindig a Transmitter Address (azaz azé az állomási, amelyik fizikailag elkülde a csomagot). Ha FromDS=1, akkor az AP címe, ha FromDS=0, akkor az állomás címe.

• **Address-3** a legtöbb esetben a maradék hiányzó cím. Egy keretben ahol FromDS=1, Address-3 az eredeti Source Address,ha a keretben ToDS=1, akkor Address 3 a célcím.

• **Address-4** speciális esetekben használják, amikor Wireless Distribution System-t alkalmaznak és az éppen adás alatt levő keretet egyik Ap-től a másiknak küldik. Ilyen esetben mind ToDS=1 és FromDS=1, így az eredeti cél és forrás cím is hiányzik. A következő táblázat összefoglalja a különböző címeket.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

28. ábra A különböző címek összefoglalása

DA: Destination Address, RA: Receiver Address

TA: Transmitter Address, SA: Source Address

Sequence Control

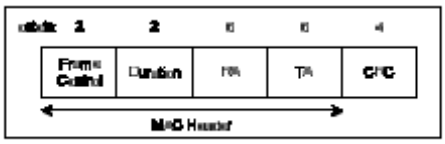
A Sequence Control Field mutatja az egyazon kerethez tartozó különböző fragmentek sorrendjét és segít a csomagduplikációk felismerésében. Két almezőt tartalmaz, Fragment Number és Sequence Number, melyek megadják a keret és a fragment sorszámát a keretben.

CRC

A CRC 32 bites mező 32-bites Cyclic Redundancy Check-t (CRC) tartalmaz.

5.2.4.2 A legáltalánosabb keret formátumok

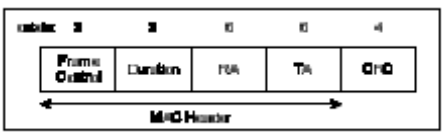
RTS keretformátum



29. ábra RTS keretformátum

Az RA (Receiver Address) a vezeték nélküli közegben azon állomás címe, amelyik a közvetlen vevője a következő Adat vagy Menedzsment keretnek. A TA (Transmitter Address) az RTS-t küldő állomás címe. A Duration érték az az idő mikroszekundumban, ami a következő Adat vagy Menedzsment keret küldéséhez szüksége plusz egy CTS keret, plusz egy ACK, plusz egy SIFS.

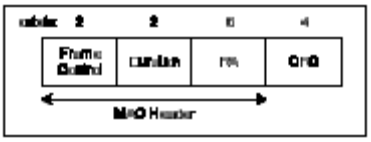
CTS keretformátum



30. ábra CTS keretformátum

A Receiver Address-t (RA) a közvetlenül megelőző RTS keret Transmitter Address (TA) mezőjéből másolják át, amire a CTS vonatkozik. A Duration értéket a közvetlenül megelőző RTS keret Duration értékéből számítják, mínusz a CTS küldéséhez szükséges idő mikroszekundumban és a SIFS.

ACK keretformátum



31. ábra ACK keretformátum

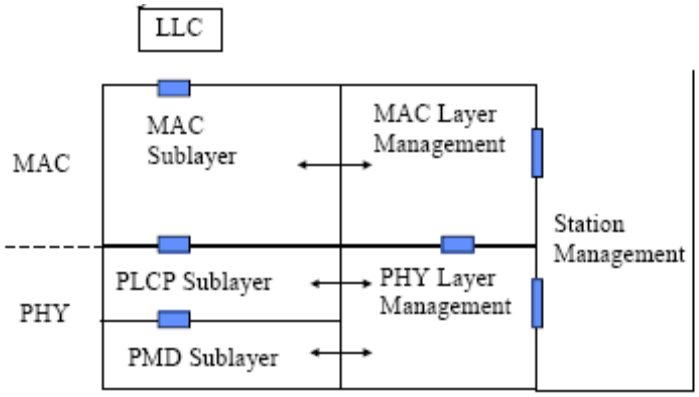
Az ACK Receiver Address mezőjét a közvetlen megelőző keret Address 2 mezőjéből másolják át. Ha a More Fragment bit 0 az előző keret Frame Control mezőjében, akkor a Duration értéke 0, egyébként a Duration az előző keret Duration mezője mínusz az ACK küldéséhez szükséges idő mikroszekundumban és a SIFS.

5.2.5 Fizikai réteg

A fizikai réteg az átviteli közegtől független rétegek adategységeit az átviteli közeg számára megfelelőre alakítja. A fizikai réteg konvergencia eljárás (PLCP) támogatja a közeg-hozzáférési réteg csomagjainak átalakítását olyan formára, amely alkalmas a fizikai közegen történő megbízható átvitelre.

Az átviteli közeg függő része a fizikai réteg jellegzetességeit definiálja két terminál között. A fizikai réteg a közeg hozzáférést szabályzó entitás számára a fizikai réteg szolgálat elérési pontján érhető el (PHY_SAP). A szabvány definiálja a szolgálati primitíveket a két réteg között.

A fizikai réteg menedzsment entitás a közeg-hozzáférési réteg menedzsment entitással együttműködve a menedzsment információs bázisra támaszkodva végzi a fizikai réteg menedzsmentjét.



32. ábra 802.11 protokoll entitások

5.2.5.1 FHSS fizikai réteg

A 802.11 PHY 79 egymást nem átfedő csatornát használ 1MHz osztással.

Ezáltal 26 átfedő hálózat üzemelhet egyidejűleg. Főbb paraméterek:

• 1 MHz sávszélesség

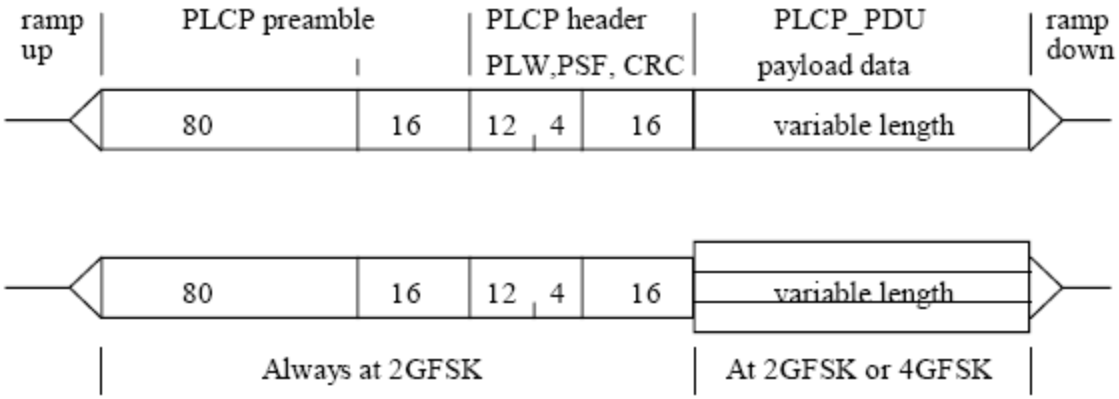
• 79 csatorna Euróbában és Észak –Amerikában, álvéletlen ugratási sorozatok

• 23 csatorna Japánban

• Max. 1W adóteljesítmény, de a 100mW-nál többre képes eszközöknek legalább egy 100mW-nál kisebb lépcsővel kell rendelkezniük.

Konvergencia alréteg (PLCP)

A konvergencia alréteg keretformátuma lehetővé teszi a MAC alréteg szolgálati adategységeinek átvitelét a WLAN hálózaton belül.



33. ábra FHSS PLCP keretformátum

A Preamble-t és a Header-t mindig 1 Mbps-mal adják, az adat lehet 1Mbps vagy 2 Mbps.

A PLCP adategység bevezető (Preamble) szakasza a szinkronizációs és keretet bevezető mezőket tartalmazza, ez teszi lehetővé a fizikai réteg modulációs áramkörének az egyensúlyi állapot elérését, a jel jelenlétének detektálását, az antennadiverzitit, a bit szinkronizációt és a keretkezdet felismerését. A 80 bites szinkronizációs mező 0, 1 váltakozó bitsorozatot tartalmaz, amely nullával kezdődik és eggyel végződik. A jel detektálása ezzel a sorozattal kezdődik, ennek ideje alatt történik az antenna kiválasztása (antenna diverziti alkalmazása esetén), a frekvencia offszet korrekció és a szinkronizácó a vett adat időzítésével. Ezt követi a Start Frame Delimiter (SDF) a 0000 1100 1011 1101 16 bites bitsorozattal, mely szimbólum szintű keretszinkront biztosít, valamint az autokorreláció tulajdonságot javítja az őt megelőző 0101 mintával. A PLCP fejrészében lévő PLW (PLCP_PDU Length Word) mező tartalmazza a közeg hozzáférési réteg protokoll adategységeinek hosszát byte-ban beleértve a CRC-t is, a 0-4095 tartományban.

A PSF (PLCP Signaling Field) mező négy bitje közül az utolsó jelzi a “PLCP_PDU, azaz a hasznos teher” átviteli sebességét, amely 1, vagy 2 Mbps lehet. Az első 3 bit foglalt.
A HEC mező a fejrész hibaellenőrző mezője, a CCITT CRC-16-os eljárással generált biteket viszi. A generátor polinom: G(x) = x16+x12+x5+1

A PLCP_PDU formázása

Scrambling

A PLCP_PDU a közeg hozzáférési réteg protokoll scramblerezett adategységeit szállítja. A PLCP fejlécet nem scramblerezik. A scramblerezés az adatbiteket „fehéríti”. A szinkron scrambler generátor polinomja: S(x) = x7+x4+1. 127-es periódussal működik, bináris összeadással (XOR) adják az adatfolyamhoz. A scramblerezés és a de-scramblerezés ugyanazt az eljárást használja.

Az adási teljesítmény szabályozása:

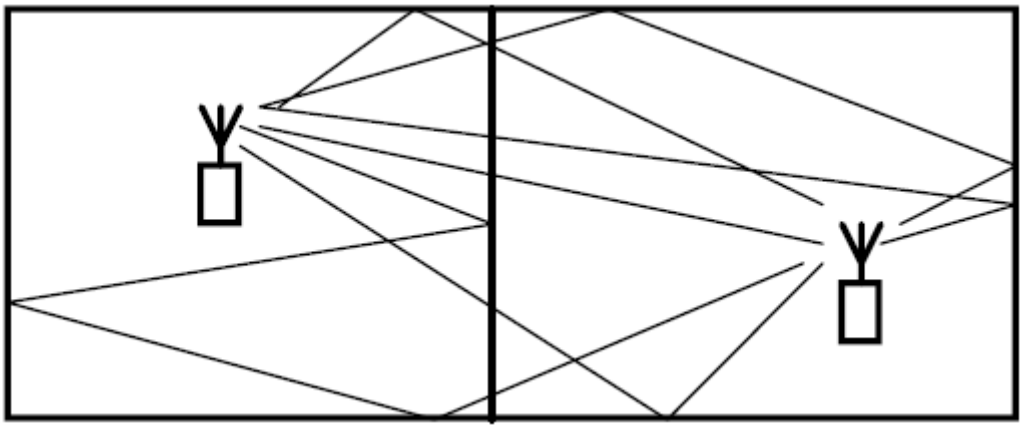
A fokozatos teljesítmény felszabályozás és leszabályozás megkívánt, a szomszédos csatornák közötti teljesítmény csúcsok csökkentése céljából a csomag kezdeténél és végénél 8 μs-ig a PLCP bevezető szakasza kezdetén és 8 μs-ig a PLCP_PDU utolsó szimbólumát követően fokozatosan növelik és csökkentik az adási teljesítményt.
A minimális fel- leszabályozási időt a szomszédos csatorna interferncia specifikációja határozza meg, nincsen közvetlenül szabályozva a szabványban.

FHSS átviteli közegfüggő fizikai alréteg:

Ez az alréteg a PLCP alréteg szolgálati primitívjeit fogadja és átalakítja a rádió csatornán átvihető alakra. A vevőben az eljárás fordított. A csatornák által elfoglalt sávszélesség 1 MHz (ilyen távol vannak a vivők). A csatornák váltási idejét a közeghozzáférési réteg szabályozza. A frekvencia váltások gyakoriságának szabályozása a nemzeti hatóságok jogkörébe tartozik.

Ugratási sorozatok megválasztása

Egymással interferáló többutas terjedés esetén frekvenciaszelektív fading alakul ki, melyek a szomszéd csatornákban erősen korreláltak és ez néhány MHz után szűnik meg beltéri környezetben



34. ábra Beltéri környezet szemléltetése

Tervezési kritériumok

• Megfelelő ugratási távolságokat kell biztosítani a többutas diverzitihez.

• Minimalizálni kell az egyes sorozatok közötti ütközések számát, valamint a szomszéd csatornás ütközéseket.

• Az egymás utáni ütközések számát minimalizálni kell a különböző sorozatok között.

Alsó határ [GHz]	Alsó határ	Kijelölt frekvencia tartomány	Ugrási frekvenciák száma (minimum)*	Földrajzi terület
2,402	2,480	2,400 - 2,4835	79 (75)	Észak-Am.
2,402	2,480	2,400 - 2,4835	79 (20)	Európa
2,473	2,495	2,471 - 2,497	23 (10)	Japán

35. ábra Működési frekvencia tartomány és a frekvencia csatornák száma

*A nemzeti hatóságok által szabályozott

5.2.5.2 DSSS fizikai réteg

Főbb jellemzők:

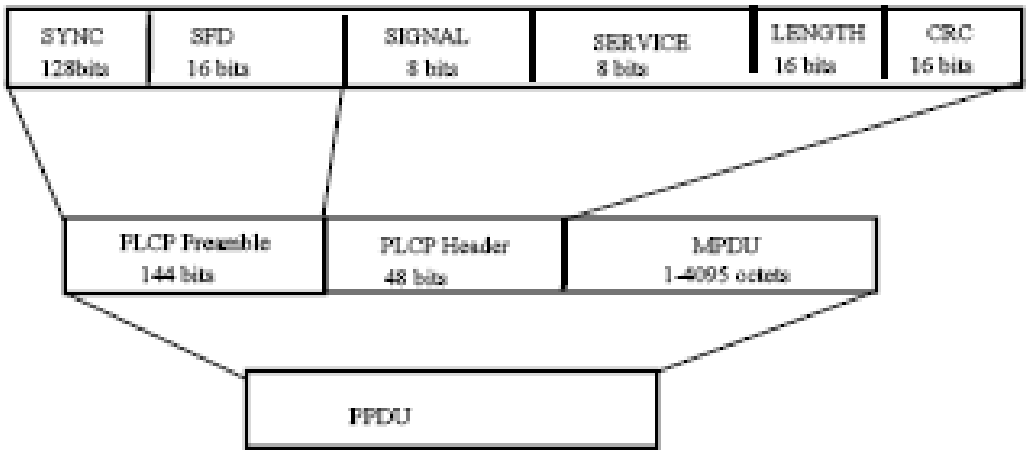
• 2,4 GHz ISM sáv

• 1 és 2 Mbps adatsebesség (DBPSK és DQPSK moduláció)

• Szimbólumsebesség 1Mbps

• Chipsebesség 11 MHz 11 chipes álvéletlen Barker sorozattal (feldolgozási nyereség 10.4 dB->11MHz), jó autokorrelációs tulajdonságok. A DSSS fizikai réteg az FHSS fizikai réteghez hasonlóan két részre bontható. Az egyes részek szabvány által definiált funkciói megegyeznek az FHSS fizikai rétegnél ismertetettekkel.

DSSS konvergencia alréteg

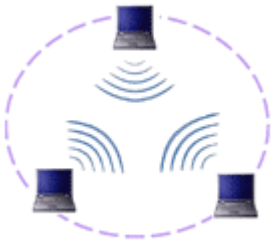


36. ábra DSSS PLCP réteg keretformátum

6. ÜZEMMÓDOK

6.1 Ad-Hoc kapcsolat

A WiFi világában alapvetően két módon létesíthetünk kapcsolatot. Az egyik, egyszerűbb eset az ún. *Ad-Hoc* vagy *pont-pont topológia*, amikor néhány WiFi képes eszköz közvetlenül egymással kommunikál. Ez a módszer - nevéből adódóan - alkalomszerű, azaz olyan esetben érdemes használni, amikor gyorsan, rövid időre kell összekapcsolnunk két eszközt, vagy ez a legolcsóbb módja a kommunikációnak (vezetékes kapcsolattól eltekintve), például át szeretnénk másolni néhány fájlt, vagy kedvenc játékunk többjátékos üzemmódjában szeretnénk játszani ismerősünkkel.



Az elnevezés onnan származik, hogy ez a típusú vezeték nélküli LAN leggyakrabban minden megelőző tervezés nélkül létrehozható és annyi ideig működik, ameddig szükséges. A lefedettségi területet az állomások adási teljesítménye korlátozza. A BSS-en belüli mozgás lehetséges csak a terminál számára. Hozzáférési pont alkalmazása ezekben a hálózatokban ritka, ha mégis sor kerül erre annak az oka a lefedettségi terület kiterjesztése (ismétlőként működik).
Az AP-k ebben az esetben nincsenek és feladataik egy részét a célállomások veszik át (Beacon Generation, szinkronizálás, stb.). Számos AP funkció pedig nincs támogatva (frame-relaying két hatótávolságon kívüli állomás között, vagy a Power Saving).

6.2 Infrastructure mód

A másik - komolyabb - lehetőség az *Infrastructure* (infrastrukturális) *mód*. Az elnevezésből azonnal kiderül, itt már egy bonyolultabb összeállításról van szó.

Egy vagy több központi egység (access point, AP) segítségével összeálló hálózat. A csillag topológia, ami ma a világon a legelterjedtebb, olyan hálózatot jelent, ami egy központi bázisállomás vagy más néven hozzáférési pont köré épül. A kiinduló csomópont elküldi az információcsomagot a központi állomásnak, amit az a célcsomópontra irányít. Ez a központ
W LAN-ok biztonsági kérdései
jelentheti a hidat egy vezetékes hálózat számára, amin keresztül elérhet további vezetékes klienseket, az Internetet, más hálózati eszközöket, vagy bármi egyebet. A "szoftveres hidat" egy megfelelő vezeték nélküli hálózati eszköz ilyen célra kitalált programja jelentheti azok között a vezetékes hálózatok és szolgáltatások között, melyek nem rendelkeznek speciális hardverrel vagy AP-vel. E szoftver segítségével minden olyan számítógép lehet híd, amelyik vezetékes hálózathoz kapcsolódik és rendelkezik vezeték nélküli hálózati-csatolókártyával.
A WLAN hálózatokat az esetek többségében a vezetékes hálózat kiterjesztéseként alkalmazzák, így szükség van az access pointra (AP), azaz hozzáférési pontra és általában ennek az átbocsátóképessége jelenti a szűk keresztmetszetet. Ekkor több AP-t is üzembe állítva osztható el a terhelés. Egy állomás a bekapcsolása után ahhoz az AP-hez csatlakozik, amelyiknek a jelét legerősebbnek érzi. Amennyiben az állomás a mozgása miatt távolodik az AP-tól, ezt a jelek gyengülésével érzékeli, megvizsgálja, hogy nincs-e hozzá közelebb egy másik, erősebb jelet adó AP. Ha talál ilyet, akkor átjelentkezik, ez a roaming.
Az infrastruktúra módra jó példa a napjainkban már egyre elterjedtebb úgynevezett hotspotok, olyan nagy látogatottságú, forgalmas közterületek, ahol a helyi wireless hálózatelérési szolgáltatás biztosított. (hotelekben, konferencia központokban, reptereken, kávézókban).

Az egyes AP-ok elérhetőségi körzetét (cellát) Basic Service Setnek (BSS) nevezik. A jól felépített WLAN – beleértve több BSS-t, az access pointokat, és az elosztórendszert – a felsőbb rétegek számára egy egyszerű Ethernet hálózatnak látszik. Az így megvalósított összetett rendszert Extended Service Set-nek (ESS) nevezik. Egy komplett, vezetékmentesen kialakított hálózatot pedig WDS-nek, azaz Wireless Distribution System-nek neveznek.

Access Point

Az *Infrasctructure mód* esetében vezeték nélküli eszközeink nem közvetlen egymással kapcsolódnak, hanem egy ún. *Access Point* (hozzáférési pont) segítségével. Ez az eszköz rendszerint vezetékes és vezeték nélküli hálózatunk között teremt kapcsolatot, mintegy hídként (Bridge) funkcionálva. Egy Access Point több eszközzel is képes egyidejűleg kommunikálni, hogy pontosan mennyivel, azt megtudhatjuk a készülék felhasználói kézikönyvéből, de általában mindegyik bőven elegendő számú kliens (kapcsolódó) eszközt tud kiszolgálni. Egy fontos szempontot azonban figyelembe kell vennünk: minél több eszköz kapcsolódik és kommunikál egyszerre egy Access Point -tal, annál keskenyebb sávszélesség jut egy-egy eszközre, azaz annál lassabbnak érzékeljük hálózatunk sebességét az egyes eszközökön. Ez természetesen elmondható minden hálózatról, vezetékesről és vezeték nélküliről egyaránt, azonban míg egy vezetékes hálózaton elegendő a sávszélesség mondjuk 100 felhasználó számára, hogy egyidejűleg digitális filmet nézzen, addig egy átlag vezeték nélküli hálózat egyetlen Access Point -jához kapcsolódó 5 felhasználó képes ugyanerre.

7. BIZTONSÁGI PROBLÉMÁK

A vezeték nélküli helyi hálózatok a médium alapvető tulajdonságaiból adódóan más biztonsági jellemzőkkel bírnak, mint vezetékes társaik. A legfontosabb különbségek e tekintetben abból adódnak, hogy a jel térben hová jut el vezetékes és vezeték nélküli hálózatokban. Mind réz, mind optikai vezetékekben a jelterjedés gyakorlatilag a kábelben – vagy legalábbis a kábel vonalán – történik.

Ezzel szemben a vezeték nélküli helyi hálózatokban a rádiófrekvenciás jel minden irányban terjedhet, amerre azt a tereptárgyak lehetővé teszik, illetve a visszaverődések, elhajlások által elősegítik. Természetesen az alkalmazott antennák karakterisztikája is nagymértékben befolyásolja a jelek terjedését.

A hálózati forgalom – pontosabban az átvitt jelek – lehallgatásának lehetőségét tekintve ez azt jelenti, hogy vezetékes hálózatok esetén mindenképen a kábel közelébe kell jutni ahhoz, hogy lehallgathassuk a hálózatot. Réz kábelek esetén a lehallgatás gyakorlatilag triviális a vezetékekhez történő galvanikus csatlakozással, de rendszerint lehetséges a vezetékekhez való közvetlen hozzáférés nélkül is, az azok körüli elektromágneses tér analizálása alapján.

Optikai hálózatok lehallgatásához pedig feltétlenül szükséges a közvetlen hozzáférés az optikai szálakhoz. Szemben ezekkel a vezeték nélküli hálózatok lehallgatásához elegendő, ha a támadó a kommunikáló lokális hálózati eszközöktől távolabb – az adott szituációtól függően akár 50-100 méterre – helyezi el a lehallgatáshoz használt eszközt. Szintén lényeges különbség a lehallgatás bonyolultságát illetően, hogy míg a vezetékeken átvitt jelek lehallgatásához valamilyen többé-kevésbé speciális eszközre van szükség, addig a vezeték nélküli közegen átvitt jelek egy egyszerű hálózati kártyával vehetők sok esetben.

A pusztán passzív lehallgatás mellett a hálózatra aktív állomásként való csatlakozásról hasonlók mondhatók el. Vezetékes hálózatok esetén a csatlakozáshoz szükséges a hálózati vezetékhez való hozzáférés, legyen az akár optikai, akár réz vezeték. Pl. egy csavart érpáros Ethernet LAN esetén praktikusan egy működő fali csatlakozó aljzatot vagy switch portot kell találnia annak, aki csatlakoztatni akarja a gépét a hálózathoz. Vezeték nélküli hálózat esetén egyéb intézkedés hiányában egyszerűen elég annyi, hogy az állomás a hálózat hatósugarába kerüljön. Ez – a

médium korábban említett tulajdonságai miatt – rendszerint nehezen ellenőrizhető, és még nehezebben akadályozható meg.
A (passzív) lehallgatás és a hálózathoz való illetéktelen (aktív) hozzáférés problémája tehát egyaránt létezik vezetékes és vezeték nélküli helyi hálózatoknál is, de a vezeték nélküli hálózatok esetén ezek a problémák rendszerint sokkal gyakoribbak. Természetesen mindkét médiumfajta esetén lehetőség van ezen problémák kiküszöbölésére vagy a kockázatoknak megfelelő mértékű enyhítésére, adminisztratív és műszaki eljárásokkal, intézkedésekkel.

A következőkben öt pontban összefoglaljuk a WLAN hálózatok biztonságos kialakításához és üzemeltetéséhez szükséges védelmi intézkedések körét.

1. Fel kell fedni, és ki kell zárni a WLAN hálózatokat illegálisan használó személyeket

A WLAN hálózatok esetében az illetéktelen rendszerhozzáférések jelentik az egyik legkomolyabb problémát. A vezetéknélküli hálózatok és eszközök (beleértve a hozzáférési pontokat (Access Point, AP), a WLAN kompatibilis notebookokat, a vezetéknélküli vonalkódolvasókat, és nyomtatókat) komoly fenyegetettséget jelenthetnek a vállalati hálózatok számára, ugyanis szabad belépési pontokat adhatnak a támadók és a rosszindulatú felhasználók kezébe. Sok esetben elég lehet egy hozzáférési pont, valamint egy WLAN kártya egy notebookba, és a jogosulatlan hálózati hozzáférés máris megvalósítható.
További problémát jelent, hogy általában a vezetéknélküli hálózatokhoz kapcsolódó eszközök alapértelmezésként olyan beállításokkal működnek, amelyek csekély biztonságot nyújtanak, és ezért könnyen felhasználhatók különböző támadásokhoz. Ugyancsak veszélyesek lehetnek az egymáshoz közel lévő vezetéknélküli hálózatok, ugyanis megvan annak a kockázata, hogy nem megfelelő konfigurációk esetén a két hálózat "összeakad".
Több olyan megoldás is létezik, amelyek segítenek kiszűrni a jogosulatlan hozzáférési pontokat, és a hálózati sérülékenységeket. A sebezhetőségek felderítésére léteznek kereskedelmi alkalmazások is, de az ingyenes szoftverek is hatékonyak lehetnek. Ezek közé tartozik például a

NetStumbler és a Kismet is. John Girard, a Gartner egyik biztonsági szakértője szerint jó megoldás a sebezhetőségek kiszűrésére, hogy egy kézi "sniffer" eszközzel végig kell járni a hálózat határait, és felderíteni az illetéktelen hálózati hozzáféréseket.
Sok biztonsági szakértő szerint a legjobb megoldást a folyamatos hálózatfigyelés jelenti. Ebből azonnal kiderül, hogy a felhasználók az adott hozzáférési ponton keresztül mikor csatlakoztak a hálózathoz, és mennyi adatot forgalmaztak. Ezek mellett az adatforgalom is valós időben monitorozható. John Girard a vezetéknélküli IDS (Intrusion Detection Sensors) érzékelők bevezetését is javasolja.

2. Hozzáférési pontok felügyelete

A vezetéknélküli hálózatok esetében is figyelmet kell fordítani a határvédelem megfelelő kivitelezésére. A hordozható számítógépeket olyan szoftverekkel kell ellátni, amelyek az esetleges sérülékenységeket felismerik, és értesítést küldenek ezekről a notebook felhasználójának valamint a vállalat IT szakembereinek. Az ilyen szoftvereknek a vállalati biztonsági szabályok betartatását is elő kell segíteniük. A könnyebb kezelhetőség, és a nagyobb biztonság érdekében érdemes vállalati szintű hozzáférési pontokat telepíteni.
A hozzáférési pontok SSID (Service Set Identifiers) azonosítóját lehetőleg meg kell változtatni, ugyanis minden gyártó cég saját azonosítót használ, amelyek felhívhatják a támadók figyelmét a vezetéknélküli hálózat gyenge biztonsági szintjére. Néhány SSID:
Cisco - "tsunami"
Linksys - "linksys"
Intel és Symbol - "101".
Fontos, hogy az új SSID-t úgy válasszuk meg, hogy az ne közöljön információkat a hálózat helyéről és egyéb paramétereiről, mert ebből a támadók értékes adatokhoz juthatnak.
A vállalati szintű elérési pontok többsége lehetővé teszi a MAC címek alapján történő hozzáférés szabályozást. Ezt érdemes használni, hiszen egy olyan alap segédeszközt nyújt, amellyel jól behatárolható a WLAN-hoz kapcsolódó számítógépek köre. A módszer egyik hátránya, hogy nagyobb hálózatok esetében ennek kezelése nem egyszerű feladat, és sokkal komplexebb szűrési

módszereket kell bevezetni.
Egyes hozzáférési pontok olyan funkcióval is rendelkeznek, amely csak akkor engedélyezi a hálózathoz való kapcsolódást, ha az adatátviteli sebesség elér egy meghatározott értéket. Ezt felhasználhatjuk arra, hogy a távolabbról (pl. parkoló autóból vagy egy másik emeletről) hálózatunkhoz kapcsolódni próbáló (a távolság miatt alacsonyabb sávszélességgel rendelkező) támadót kizárjuk.

3. Titkosítás és autentikáció

A titkosítás és az autentikáció a vezetéknélküli hálózatok biztonságának alapkövei. Több módszer is elterjedt ezek megvalósítására, de az alkalmazásukkor nagyon körültekintőnek kell lenni. 2001-ben a kutatók és a hackerek is bemutattak olyan módszereket, amelyek a 802.11-es előírásoknak megfelelő WLAN hálózatokhoz tartozó WEP (Wired Equivalency Policy) titkosítást hatástalanították. A hackerek az Interneten olyan szoftvereket is közzétettek, amelyekkel szintén a WEP titkosítást lehet feltörni. A WEP könnyű feltörhetőségének bebizonyítása után sok fejlesztő cégnél megrendült a bizalom a WEP iránt, így a vezetéknélküli megoldások még védtelenebbé váltak. Mindezek ellenére a WLAN hálózatok esetében is lehet alkalmazni hatásos biztonsági megoldásokat. Ezek közé tartozik a RADIUS szerverek használata, és a VPN (Virtual Private Network) alkalmazása is. A VPN segítségével biztonságos kapcsolat építhető fel a végponti eszköz és a szerver vagy a tűzfal között. A RADIUS szerverek pedig az autentikációt támogatják annak érdekében, hogy a hálózati erőforrások elérése minél biztonságosabb legyen.

4. A vezetéknélküli hálózatok használatának szabályozása

Napjainkban a cégeknél már szükség van megfelelően összeállított biztonsági szabályzatokra. Ezeknek természetesen a vezetéknélküli hálózatok használati módjára is ki kell terjedniük. A szabályzatoknak tartalmaznia kell a WLAN eszközök biztonságára vonatkozó utasításokat, és a kezelésükkel valamint a karbantartásukkal kapcsolatos követelményeket. Az összeállításuknál azonban arra is ügyelni kell, hogy ne hozzunk olyan szükségtelen intézkedéseket, amelyek a

hálózat hatékonyságát feleslegesen csökkentik.

A WLAN-hoz kapcsolódó szabályok közül a legfontosabbaknak a hozzáférési pontok használatával kell foglalkozniuk. Ezekben a szabályokban meg kell határozni, hogy ki veheti igénybe a hozzáférési pontokat, és ki, milyen beállításokat végezhet el azokon. Gondoskodni kell arról, hogy csak az arra kijelölt személyek módosíthassák a konfigurációkban szereplő WEP, SSID, VPN, stb. beállításokat. Szabályozni kell, hogy ki, milyen sebességű WLAN csatornához férhet hozzá, és milyen időpontokban használhatja azt. Természetesen ebben az esetben is igaz, hogy a leírt szabályok nem érnek semmit, ha azok betartatásával senki sem foglalkozik.

5. Behatolás érzékelés és behatolás megelőzés

A behatolás érzékelés és megelőzés nemcsak a vezetékes hálózatok esetében nagyon fontos. A WLAN hálózatokhoz is hatékonyan használhatók, és a segítségükkel a támadások még azelőtt kiszűrhetők még mielőtt azok elérnék a vezetékes helyi hálózatokat.
Az IDS megoldások a WLAN hálózatok esetében is 24 órás monitorozó funkciót látnak el, és használhatók a 802.11a/b/g protokollok esetében is. A folyamatos hálózatfigyelés révén nemcsak megakadályozhatók a támadások, hanem ki is elemezhetők. Protokoll analízisek, statisztikák és szabálymegsértési jelentések is készíthetők a segítségükkel.
Összefoglalva elmondható, hogy a vezetéknélküli hálózatok bevezetése és üzemeltetése kellő odafigyelés hiányában meglehetősen nagy kockázatot jelenthet a vállalatok informatikai infrastruktúrájára. Azonban megfelelő, többszintű biztonsági intézkedésekkel hatékony és kockázatarányos védelem valósítható meg.

7.1 Támadási módszerek

WLAN hackereszközök

1. Ingyenes (freeware) szoftverek

Ezek beszerzése manapság már sajnos nem ütközik különösebb nehézségbe, mindössze Internet-kapcsolat szükségeltetik

2. Antennák

A csatlakozási távolság akár több száz méterrel is megnövelhető, ha a hacker nagy hatótávolságú antennát használ. Ezeket a kereskedelmi forgalomban is meg lehet találni, de némi szakértelemmel akár otthon is elkészíthetőek, így nagy hatótávolság-növekedést elérve. A betolakodóknak így nem is szükséges hálózatunk közelében tartózkodniuk.

1. Kódtörés

Kódfejtéshez szükséges programok (pl. WEPCrack, Aircrack) hatékony működésének alapja a WEP-kódolás gyengeségeiből származik.

2. War Driving

Ez az egyik legelterjedtebb „kalózkodási” forma, ami egyszerűségének köszönhető. Tulajdonképpen a nyitott WLAN-ok fizikai jelenlétét lokalizálja, s nem kell hozzá egyéb, mint a hackerek által fejlesztett scanner eszköz, valamint egy gépkocsi, amellyel körbejárva a várost számos védtelen vezeték nélküli hálózatot lehet felderíteni. A passzív vezeték nélküli adatforgalom monitorozására használható windowsos platformon a Netstumbler, linux alatt pedig a Kismet elnevezésű program. Ezek párban működnek a globális helyzetmeghatározó

rendszerekkel (GPS=Global Positioning System), hogy pontosan feltérképezzék a védtelen WLAN-okat. Majd ezek elérhetőségét a hackerek előszeretettel teszik fel az internetre is (www.wigle.net, www.wifinder.com).

7.2 Támadási formák

1. Rosszindulatú támadások általános formája

Széles körben alkalmazott eszközök segítségével a hackerek gyanútlan állomásokat tudnak kényszeríteni. Egy hacker első lépésként AP-ként funkcionál. Az „áldozat" gép requestet küld közvetve az access pointnak, majd az válaszüzenetet küld vissza, sőt ha szükséges, IP-címet is kap a rosszindulatú AP-tól. Innentől fogva pedig „szabad a vásár". Az ilyen támadások ellen a virtuális hálózatok (VPN) alkalmazása az egyedüli jó megoldás. A nagyvállalatok pedig monitorozzák az étert, s csak a hitelesített elérési pontokat engedik hálózatukba kapcsolódni.

2. Visszaélés a MAC-címmel

Sok vállalat a hitelesített MAC-címek listájával (ACL) teszi biztonságossá saját vezeték nélküli hálózatát. Azonban a felhasználók könnyedén képesek MAC-címük megváltoztatására!
A különböző szoftvereszközök, mint például a Kismet vagy az Ethereal lehetővé teszik a hackerek számára, hogy megszerezzék egy hitelesített felhasználó MAC-címét, s ennek segítségével hitelesített felhasználóként tudnak csatlakozni a WLAN-hoz. A nagyvállalatok ezt a problémát is monitorozással küszöbölik ki, ugyanis kiszűrik a szimultán használt MACcímeket.
A WLAN betörő-detektáló rendszerek MAC-cím azonosításra is képesek a hálózati kártya gyártójának „ujjlenyomatát" analizálva, mivel a MAC-címek gyártónként előre kiosztottak.

3. Közbeékelt támadás (Man-in-the-Middle Attack)

Ennek során a kalózok meg tudják törni a VPN-kapcsolat biztonságát a hitelesített állomás és az AP közé férkőzve. A rosszindulatú támadó az hozzáférési pont és az áldozat állomás közé állva képes magáról elhitetni a klienssel, hogy ő egy AP, az hozzáférési ponttal pedig, hogy ő egy hitelesített kliens. Kezdetben a hacker passzív, figyeli amint a kliens csatlakozik a hozzáférési ponthoz, s eközben a hitelesítéssel kapcsolatos információkat gyűjti csupán. Ezek felettébb fontos információk: felhasználónév, szervernév, kliens és szerver IPcím, a kliens által használt azonosító, valamint az AP által küldött hívó (challenge) és összerendelési üzenet (associate).
Mikor a hacker megpróbál az access pointhoz csatlakozni a megszerzett információk birtokában, az AP számára úgy tűnik, hogy egy hitelesített állomás kérése érkezik be hozzá. Az access point egy hívó üzenetet (challenge) küld az általa hitelesítettnek vélt állomásnak, amely miután kiszámította a visszaküldendő választ, ezt válaszként vissza is küldi az access pointnak.
A hackerállomás ezután szerzi meg az access point által kiküldött hitelesítési üzenetet, melynek segítségével már a kliens és az elérési pont közé állhat anélkül, hogy bármelyik is tudna erről, hiszen mindkét irányba tartó üzeneteket elkapja s továbbítja. A nagyvállalatok csak a 24x7 típusú monitorozásban látják ennek a támadási fajtának az egyetlen ellenszerét.

Lehallgatás

A lehallgatás problémájára a következőket mondhatjuk el:
A vezeték nélküli hálózat felhasználóinak saját érdeke, hogy a hálózaton átvitt érzékeny információikat megfelelő módon védjék lehallgatás ellen. Az esetek döntő többségében a felhasználók kezében vannak az ehhez szükséges eszközök. A megoldást rendszerint kriptográfiai eljárások használata jelenti.
A hálózat üzemeltetőjének nem feladata a felhasználók hálózati forgalmának lehallgatás elleni védelme. Természetesen amennyiben lehetősége van rá, akkor jó, ha az üzemeltető megszűnteti vagy enyhíti a lehallgatás veszélyét.

A hálózat üzemeltetőjének feladata a felhasználók tájékoztatása a lehallgatás veszélyéről a lehetőségeknek megfelelően, hiszen ebben az esetben a felhasználók nagy része nem rendelkezik a szükséges ismeretekkel.
Ezen túl elmondható az is, hogy a hálózat üzemeltetőjének több okból érdeke is a felhasználók tájékoztatása a lehallgatás veszélyéről csak úgy, mint a védelem a lehallgatás ellen. Egyrészt ugyanis az érzékeny információk lehallgatásából később adódhatnak más biztonsági incidensek a hálózaton, amivel az üzemeltetőnek is foglalkoznia kell. Másrészt a lehallgatás számtalan olyan esemény forrása lehet, amely a felhasználó megelégedettségét csökkenti, többek közt az üzemeltetővel is.

Védelem a lehallgatás ellen

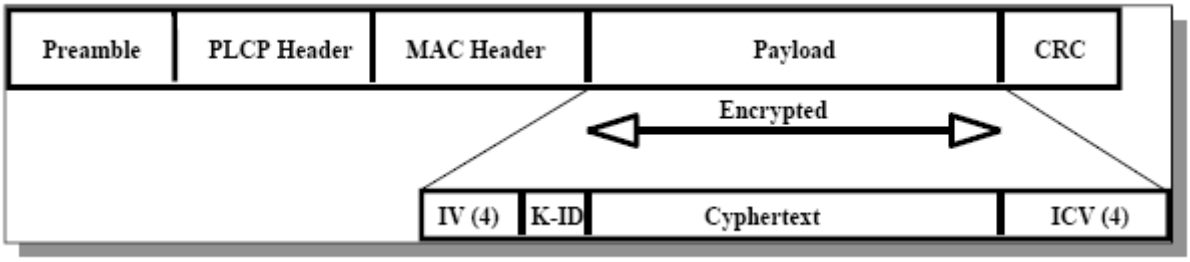
Sajnos a jelen műszaki lehetőségek mellett a lehallgatás ellen leginkább a felhasználók tudnak csak védekezni, a hálózat üzemeltetői keveset tudnak ehhez hozzátenni. A felhasználóknak lehetősége van biztonságos, a hálózati forgalmat titkosító protokollokat használniuk (pl. ssh, scp, SFTP, HTTPS, IPSec ESP), amelyek gyakorlatilag minimálisra csökkentik az érzékeny információk lehallgatásának veszélyét. Ezzel szemben az üzemeltetőnek nincs igazán jó lehetősége a lehallgatás elleni védelemre.

7.3 Védelem az adatkapcsolati rétegben

A vezeték nélküli szakaszon, az adatkapcsolati rétegben az alábbi lehetőségek vannak a lehallgatás elleni védekezésre:

7.3.1 WEP (Wired Equivalent Privacy)

A biztonság az egyik legelső szempont a WLAN-ok fejlesztésekor. A 802.11 esetében a WEP (Wired Equivalent Privacy) megoldást választották.
A felhasználók szemszögéből a behatoló nem lehet képes:
• hozzáférni a hálózati erőforrásokhoz hasonló WLAN eszközöket használva,
• WLAN forgalom elfogására (lehallgatás).
802.11-es szabvány szerint a rendszerek nyitottak, vagy osztott kulcsúak, vagy egyedi hitelesítési mechanizmusok is csatolhatók lehetnek a hitelesítési eljárás szempontjából. A nyitott rendszerek esetén bárki, aki hitelesítést kér az meg is kapja.
Osztott kulcsú hitelesítés megkívánja a WEP titkosítási algoritmus használatát, a titkos kulcs átvitelére nem kerül sor az átviteli közegben, ezt a menedzsment információs bázisban tárolják.
A WEP algoritmus alkalmazásával a vezetékes hálózatok titkosságával megegyező védelem érhető el a lehallgatással szemben.



37. ábra WEP és a keretformátum kapcsolata
WEP jellemzők:

• Széleskörű elterjedtség

• Csak állomások között és nem vég-vég között (a MAC entitásba ágyazva)

• RC4 PRNG (véletlen szám generáló) algoritmus:

o 40 bites titkos kulcs (kulcsszétosztás nincs szabványosítva)

o 24 bites IV (időfüggő titkosítási paraméter, Initialiation Vector, hasonló mint a GSM-ben vagy a TETRA-ban), melyet az adattal küldenek

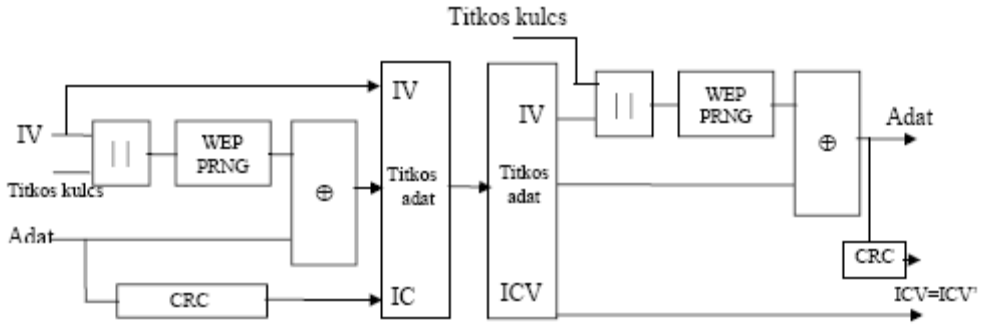
o ICV használata az integritás ellenőrzéshez

• Csak a payload-ot titkosítják a keretben (titkosítás MPDU alapon)

• Csak a Confidentiality funkciót valósítja meg (az információ csak a tulajdonos beleegyezésével szerezhető meg.) WEP bit jelzi a Frame Control mezőben a WEP használatát

• Minden keret új IV-t kaphat vagy korlátozott számúszor újrahasználható az IV.

• Ha az integritás ellenőrzés hibázik, a keretet nyugtázzák, de eldobják.



38. ábra A kódoló és dekódoló felépítése

A hálózati erőforrásokhoz való hozzáférés megakadályozása

Ezt a hitelesítés biztosítja, ahol a felhasználónak ismernie kell az aktuális kulcsot. Ez nagyon hasonló a vezetékes LAN-okhoz abban az értelemben, hogy a behatolónak be kell jutnia az épületbe (fizikai kulcsot használva) azért, hogy a gépét a vezetékes LAN-hoz csatlakoztathassa.

Lehallgatás

A lehallgatás ellen a WEP véd, mely egy álvéletlen szám generátor (PRNG), amit egy titkos szétosztott kulccsal inicializálnak. Ez a PRNG egy álvéletlen bitsorozat formájában egy kulcssorozatot ad ki, melynek hossza megegyezik a lehető leghosszabb csomag hosszával. Ezt a sorozatot kombinálják a hasznos információval. A WEP az RSA-n alapuló egyszerű algoritmus az alábbi jellemzőkkel:

• Meglehetősen erős: a nyers erő (Brute-force) támadások bonyolultak, mivel minden egyes elküldött kerethez egy Initialization Vector tartozik, ami újrainicializálja a PRNG-t minden egyes keretre.
• Önszinkronizáló: az algoritmus minden egyes üzenetnél újraszinkronizál. Erre szükség van a kapcsolat-mentes (connection-less) környezetben való működéshez, ahol csomagok veszhetnek el (mint minden LAN-nál).

A WEP régebbi titkosítási módszer, amelyről bebizonyosodott, hogy az általános WLAN biztonság garantálására is alkalmatlan, az üzleti WLAN-ok biztosítására pedig teljesen.

A WEP legnagyobb hibája, hogy gyenge kódolást használ: rövid kulcsokat, viszonylag sokáig. A kulcs az a kódsorozat, amelynek alapján egy matematikai függvény az érthető szöveget érthetetlenné teszi, illetve visszaalakítja érthető szöveggé. A kulcsok hossza 40 és 2048 bit között változhat, de lehet ennél hosszabb is. Általában igaz, hogy minél hosszabb a kulcs, annál nehezebben fejti meg egy számítógép a kódolt üzenetet azzal, hogy kipróbálja a számok és betűk összes lehetséges variációját. A hosszabb kulcsok titkosító és visszafejtő függvényeinek futtatása nagyobb processzorteljesítményt igényel, így a rövidebb kulcsok használata a működési sebességet növelő kompromisszum. Néhány rövid kulcsot használó program nagy gyakorisággal változtat a kódon (mondjuk percenként), így ha a támadó fel is törne egy kulcsot, mindent elölről kellene kezdenie, amikor az új kulcs működésbe lép.

Mivelhogy a WEP rövid kulcsokat, viszont hosszú időszakokat használ, és a kulcsok is nagyon gyengék, a kutatók hamar felfedezték, hogy rövid idő alatt meg lehet fejteni a WEP-kódolású üzeneteket. Hamar megjelentek az Interneten a WLAN-támadásra alkalmas programok. A legaljasabb az AirSnort nevű, amely percek alatt képes feltörni a WEP-kódolással védett üzeneteket.

7.3.2 WPA (Wireless Protected Access)

Mivel a 802.11i-re még várni kell, a Wi-Fi Alliance 2002-ben kidolgozta a WPA ajánlást, amely a WEP hibáinak kiküszöbölésére szolgál, és a 802.11i draft bizonyos elemeiből áll. A WPA lényege, hogy egyrészt kvázi szabvány lévén lehetővé teszi a biztonságos vezeték nélküli

hálózatok interoperábilis implementálását, másrészt a szabványos 802.11 eszközökön általában hardware módosítás nélkül, csupán software-ben is megvalósítható.

A WPA (Wireless Protected Access, Vezeték nélküli Védett Hozzáférés) a 802.11i biztonsági szabvány része, amely 802.11x hitelesítést és TKIP (Temporal Key Integrity Protocol, Ideiglenes Kulcs Integritás Protokol) kulcskiosztást használ. A WEP leváltása céljából fejlesztették ki, tanulva annak hiányosságaiból.

Az IEEE 802.11i a WLAN hálózatok biztonsági szabványa, amelynek fő komponensei a 802.11x hitelesítés, a TKIP protokoll és az AES (Advanced Encryption Standard, Továbbfejlesztett Titkosítási Szabvány) titkosító algoritmus. A legújabb készülékek illetve több korábbi termék új firmware frissítése is támogatja már ezt a fontos szabványt, vásárláskor érdemes erre is figyelni!

A TKIP a kulcs disztribúcióért (elosztásért) felelős protokoll, amely ellenőrzi az üzenetek integritását is. A már 802.11x módszerrel hitelesített eszközök esetében, a forgalmazott adatcsomagokban dinamikusan képes váltogatni a titkosítást szolgáló kulcsokat, azaz hiába szerzi meg a támadó az éppen használt kulcsot a forgalom lehallgatásával összegyűjtött adatokból, a TKIP-nek elég 5 percenként változtatni a kulcson, a kalóz már kezdheti is elölről munkáját, sőt a TKIP adatcsomagonként is képes új kulcsot generálni.

A WPA két működési módban alkalmazható. Az egyik a Pre-Shared Key mode (Megosztott kulcs mód), amely otthonra és kisvállalkozások számára ideális megoldás. A titkos kulcsot az Access Point adminisztrációs felületén kell megadnunk, ahogy az egyes klienseknél is. Ez első pillantásra megegyezik a WEP módszerével, a WPA azonban a kapcsolódást követően folyamatosan változtatja a titkos kulcsot, így szinte lehetetlen az éppen érvényben lévőt megfejteni. Újabb kapcsolódás esetén ismét az eredeti kulcsot kell megadni, tehát csak arra kell figyelnünk, hogy titkos kulcsunkat senki ne ismerje meg rajtunk kívül.

Aki korábban már ismerkedett a WLAN hálózatokkal és azok biztonsági kérdéseivel, bizonyára ismerősen cseng neki a RADIUS szerver, pontosabban RADIUS alapú hitelesítő szerver megnevezés. Ez a WPA másik működési módja (Enterprise mode) nagyvállalatok számára nyújt biztonságos megoldást, otthoni implementálása meglehetősen körülményes. EAP protokolt (Extensible Authentication Protokol, Kiterjeszthető Hitelesítési Protokol) használ a kliensek azonosítására és 802.11x biztonsági szabványt a kliens eszközökön. Az Enterprise mode továbbá alkalmas többszintű felhasználói jogosultság kezelésére is, azaz (leegyszerűsítve)

meghatározható, hogy a hálózaton ki milyen erőforrásokhoz fér hozzá, például ki éri el csak az internetet és ki érhet el egyéb információkat is.
Otthon tehát, saját kis WLAN hálózatunk esetében válasszuk a WPA Pre-Shared Key módot az Access Pointunk adminisztrációs felületén, ekkor nincs szükségünk külön RADIUS szerver konfigurálására a hitelesítéshez. Ezután válasszuk a TKIP vagy AES algoritmust a titkosításhoz, de előtte győződjünk meg arról, hogy eszközeink melyik algoritmust támogatják! Majd adjunk meg egy hosszú, kis/nagybetűkből és számokból álló kulcsot, amit majd a kliens gépek konfigurálásakor is meg kell adnunk. Utolsó beállításként pedig határozzuk meg, milyen időközönként cserélje le az érvényben lévő kulcsot az Access Point.
A kliens kofigurálás esetén a lényeg, hogy azonos beállításokat válasszunk, mint az Access Point-on. Meg kell adnunk az SSID-t, a WPA-PSK (WPA Pre-Shared Key) biztonsági módszert és a választott (TKIP vagy AES) titkosítást, végül a titkos kulcsot (Network Key). Ezek után már biztonságosan kapcsolódhatunk vezeték nélküli hálózatunkhoz.

7.3.3 WPA2

WiFi Alliance a végleges 802.11i-t alapul véve megalkotott egy továbbfejlesztett WPA verziót, melyet WPA2-nek nevezett el. Továbblépés a WPA-hoz képest a komplexebb, robosztusabb AES-CCMP (AES in Counter Mode with CBC-MAC Protocol) titkosító mechanizmus támogatása, mely egy speciális változata a standard AES-128 protokollnak
A WPA tulajdonképpen még a 802.11i biztonsági szabvány végelegesítése előtt jött létre, utódja WPA2 néven már a ratifikált 802.11i szabvány szerves részeként vált ismerté, amely kötelezően tartalmazza az erősebb AES (másnéven CCMP) titkosítási módszert is, lecserélve a WPA első verziója által alkalmazott (gyengébb) RC4 titkosítási algoritmust (amit a WEP is használ).

7.3.4 TKIP

A TKIP protokollt a 802.11i szabvány definiálja. Tervezőinek köztes megoldást kellett találniuk a megfelelő szintű adatbiztonságot és a meglévő vezeték nélküli eszközökkel való

együttműködést együttesen figyelembe véve. Ebből adódóan a protokoll ugyanazt az RC4 kódolási algoritmust használja, melyet a WEP-hez is meghatároztak, bár a TKIP által alkalmazott RC4 kódolás már 128 bites kulcsokkal dolgozik. Legfontosabb változás a WEP-hez képest, hogy minden egyes adatcsomaghoz saját kulcs generálódik (per-packet kulcs). A kulcsot különböző adatok keverésével hozzák létre: a küldő csomópont fizikai címétből és a csomag azonosítójából. Minden egyes csomag melyre alkalmazzuk a TKIP-t, rendelkezik egy 48 bites széria számmal, mely eggyel növekszik, amint egy újabb csomag kerül átvitelre. Az algoritmus ezt az értéket használja Inicializációs Vektorként (IV) és a kulcs részeként is. Ez a szekvencia szám biztosítja, hogy minden egyes csomaghoz külön kulcs tartozzon. Emellett, nem kevésbé jelentős továbblépés, hogy az alap kulcsot (base key) belekeveri a TKIP kulcsba.

A TKIP minden egyes kliens-bázisállomás unicast kommunikációhoz négy kulcsból álló kulcshalmazt rendel, valamint további két kulcsot a multicast, illetve broadcast forgalom számára.

Az eljárás a következő ideiglenes kulcsokat (PTK - Pairwise Transient Key) használja az unicast adatok titkosítására:

1. Data encryption kulcs: 128 bites kulcs az unicast keretek titkosítására.
2. Data integrity kulcs: 128 bites kulcs, mellyel kiszámolható a MIC az unicast keretekhez.
3. EAPOL-Key encryption kulcs: 128 bites kulcs az EAPOL-Key üzenetek titkosítására.
4. EAPOL-Key integrity kulcs: 128 bites kulcs, mellyel kiszámolható a MIC EAPOL-Key üzenetekhez.

A pairwise ideiglenes kulcsok (PTK) meghatározásához az alábbi értékeket használja a WPA:

1. Pairwise Master Key (PMK): 256 bites kulcs, melyet az EAP-TLS vagy PEAP hitelesítési eljárásból származtat.
2. Nonce 1: A bázisállomás által meghatározott véletlenszerű érték.
3. MAC 1: A bázisállomás MAC címe.
4. Nonce 2: A kliens által meghatározott véletlenszerű érték.
5. MAC 2: A vezetéknélküli kliens MAC címe.

A PMK-t az EAP hitelesítés során a hitelesítő (RADIUS) szerver és a vezeték nélküli kliens együttesen határozzák meg, majd a szerver eljuttatja a bázisállomáshoz egy Access-Accept üzenetben. Ezután az AP kezdeményezi a négylépéses Key Handshake algoritmust:

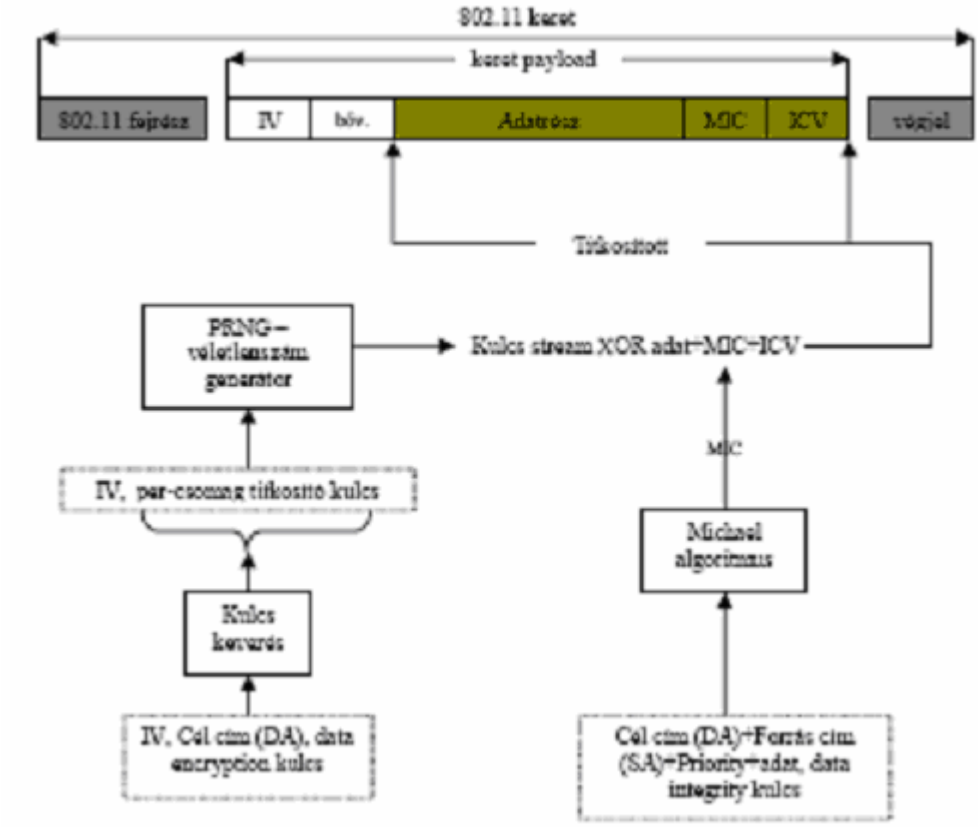
1. A bázisállomás küld egy Nonce1-et és a MAC1-et tartalmazó EAPOL-Key üzenetet. Mivel az ideiglenes unicast kulcsokat még nem határozták meg, ez az üzenet kódolatlan szöveges formában, integritási védelem nélkül jut el a klienshez. Ezáltal a kliens rendelkezni fog minden információval a pairwise ideiglenes kulcsok kiszámításához.
2. A mobil kliens visszaküld egy EAPOL-Key üzenetet, mely tartalmazza az Nonce2-t és a MAC2-t, továbbá a MIC értéket. A kliens kiszámította az ideiglenes kulcsokat, emellett meghatározza a MIC értéket is, felhasználva EAPOL-Key integrity kulcsot. A bázisállomás Nonce 2 és MAC 2 értékek alapján határozza meg az ideiglenes kulcsokat, és érvényesíti a MIC értékét.
3. Az AP ismételten küld egy EAPOL-Key üzenetet egy MIC értékkel és egy kezdeti szekvencia számmal. Ezzel jelzi, hogy készen áll titkosított unicast és EAPOL-Key üzenetek küldésére.
4. A mobil kliens visszaküld egy EAPOL-Key üzenetet egy MIC értékkel és egy kezdeti szekvencia számmal. Ezzel jelzi, hogy ő is felkészült titkosított unicast és EAPOL-Key üzenetek küldésére.
A fenti lépések kettős célt szolgálnak: 1. az ideiglenes kulcsok (PTK) meghatározása. 2. a kapott MIC értékkel ellenőrizhető, hogy mind a kliens, mind a bázisállomás ténylegesen rendelkezik-e a PMK-val.
Az adatkeretek tikosításához az alábbi adatokra van szüksége a protokollnak:
Inicializációs Vektor (IV).
A PTK kulcsok közül a data encryption kulcs, vagy a group encryption kulcs.
A keret cél- és forráscíme (DA, SA).
A priority mezőértéke, ami alapesetben “0”.
A PTK kulcsok közül a data integrity kulcs, vagy a group integrity kulcs.
A TKIP titkosítási algoritmusa:
1. A WPA keverési funkciójának – amely kiszámítja a per-csomag kulcsot – bemenetei az IV, a DA, és a data encryption kulcsok lesznek.
2. A Michael adatintegritási algoritmus a MIC előállításához bemenetként a célcímet, a forráscímet, a priority értéket, az adatrészt (a titkosítás nélküli 802.11 payload), és a data integrity kulcsot alkalmazza.

3. Az ICV-t a CRC-32 checksum-ból határozza meg.

4. Az RC4 programozott véletlenszám generátorának (PRNG) bemenete az IV és a perpacket kulcs lesz. Ezekből állítja elő a generátor a kulcs stream-et, melyek mérete megegyezik az adatrész, a MIC és az ICV értékek együttes méretével.

5. A kulcs stream és az adatrész, MIC és ICV kombinációval elvégez egy logikai XOR műveletet, így hozza létre a titkosított 802.11 adatrészt.

6. Végül hozzáadja az IV-t az így kapott titkosított adatrészhez, majd az eredményt becsomagolja egy 802.11 fejrésszel és végjellel.



39. ábra A TKIP titkosítás blokksémája

7.3.5 AES-CCMP

A CCMP hasonlóan a TKIP-hez ideiglenes kulcsokat (PTK) alkalmaz az adatok titkosítására. A PTK meghatározásához a TKIP-nél már ismertetett 4 lépéses Key Handshake eljárást használja. Mivel tartalmaz adatintegritási védelmet, ezért egyszerre válthatja ki a TKIP-t és a Michael algoritmust. Az AES-CCMP a 802.11 payload és MIC titkosításához counter módú AES-t alkamaz, és a MIC meghatározását CBC-MAC algoritmussal végzi, az alábbiak szerint:
1. AES-sel titkosít egy 128bites kezdő blokkot és a data integrity kulcsot. Ez 128 bit hosszúságú kódot eredményez (X1).
2. Végrehajt egy XOR műveletet az előbbi 128 bites kódón és a következő 128 bites adatblokkon, miközben a MIC értéket is meghatározza. Az éredmény szintén egy 128 bites kód (X2).
3. Az X2 kódot titkosítja AES-sel a data integrity kulcsot felhasználva. Így létrejön X3.
4. Ismét XOR műveletet hajt végre X3-n és a következő 128 bites adatblokkon.
Az eljárás a 3. és 4. lépést ismétli minden újabb 128 bites adatblokkra. A 128 bites kód felső 64 bitje lesz a MIC érték.

7.4 Védelem a hálózati rétegben

Lehetőség van arra is, hogy a lehallgatás elleni védelmet remote access IPSec VPN kialakításával valósítsuk meg. Ez lehet szintén központilag kötelezővé tett védelem, amikor a felhasználónak mindenképp IPSec titkosítást kell használnia a teljes hálózati forgalmához. Itt a titkosítás nem az adatkapcsolati, hanem a hálózati rétegben történik. A „távoli” VPN felhasználók tehát a wireless LAN felhasználói, a „védett” hálózat pedig – ami a VPN gateway mögött található – az Internet. A vezeték nélküli hálózatról csak IPSec forgalmat engedünk a vezetékes hálózatba, és azon belül is csak a VPN gatewayhez, így a felhasználók az Internetet csak úgy tudják elérni, ha a forgalmukat a saját gépüktől először IPSec titkosítással a VPN átjáróhoz küldik, ami majd visszafejti a titkosított csomagokat, és továbbítja azokat a tényleges cél cím felé.

Illetéktelen hozzáférés

A hálózathoz történő illetéktelen csatlakozásokat meg kell akadályoznunk.
Egyrészt azért, mert az érvényes felhasználási szabályzatok ezt megkövetelik.
Másrészt pedig azért, mert a hálózat üzemeltetője bizonyos felelősséggel tartozik azért, ami a hálózatán történik, és ezek az események igen könnyen kézben tarthatatlanná válnak, ha a hálózatot bárki idegen is használhatja. A hálózathoz való csatlakozást tehát autentikációnak kell megelőznie, és az azonosításnak lehetőleg személy szerintinek kell lennie.

MAC address

A WLAN access pointok többsége, így az általunk használt típusok is lehetőséget nyújtanak arra, hogy ha egy állomás csatlakozni akar hozzájuk, akkor először egy RADIUS servernek küldjék el az állomás MAC címét, és a RADIUS server válasza alapján engedjék vagy ne engedjék az állomást csatlakozni a hálózathoz. Ehhez természetesen szükség van arra, hogy nyilvántartsuk a vezeték nélküli hálózat használatára jogosultak WLAN interface kártyáinak MAC címét.
A módszer nagy előnye, hogy bármilyen operációs rendszerrel és WLAN interface kártyával működik, hiszen az autentikációban a felhasználó gépe csak teljesen passzívan vesz részt. Azaz a felhasználó gépének semmit sem kell az autentikáció érdekében tennie, mivel az access point a RADIUS server segítségével dönti el annak adatbázisa alapján, hogy beengedi-e a hálózatba az adott gépet. Hátránya a MAC address alapú autentikációnak viszont, hogy nem annyira biztonságos, hiszen az interface kártyák MAC címe rendszerint software-es úton módosítható. Ha tehát egy amúgy jogosulatlan felhasználó tudomására jut egy regisztrált MAC cím, akkor a saját WLAN interface kártyájába azt a címet programozva megszemélyesítheti a jogosult felhasználót, és így hozzáférést kaphat a vezeték nélküli hálózathoz. Regisztrált MAC címet pedig könnyen megtudhat a támadó, pl. úgy, hogy lehallgatja a vezeték nélküli hálózatot. (Az így lehallgatott címet persze csak akkor használhatja sikeresen, ha az adott helyen a cím jogos tulajdonosa éppen nem használja a hálózatot, hiszen különben a MAC címek ütközése hibát eredményezne.)

802.1x

Az IEEE 802.1x szabványban leírt EAPoL (Extensible Authentication Protocol over LAN) lehetővé teszi, hogy a (mind vezetékes, mind vezeték nélküli) lokális hálózathoz csatlakozni kívánó végberendezések azonosságát ellenőrizzük, mielőtt a hálózathoz való hozzáférésüket engedélyezzük. Az alkalmazott EAP típus többféle lehet, mint ahogy azt a neve is mutatja. Az EAP-TLS, az EAP-TTLS, a LEAP és a PEAP azok az EAP típusok, amelyek lehetővé teszik, hogy a felhasználókat azonosítjuk.

7.4.1 EAP

A 802.1X az EAP protokollt üzenetek cseréjére használja a hitelesítési folyamat közben. Az EAP protokollal tetszőleges hitelesítési módszer használható, mint például tanúsítványok, intelligens kártyák vagy hitelesítő adatok. Az EAP nyitott végű párbeszédet tesz lehetővé az EAP-ügyfél (például egy vezeték nélküli számítógép) és az EAP-kiszolgáló (például egy IAS-kiszolgáló) között. A párbeszéd a kiszolgáló hitelesítési adatok iránti kérelmeiből és az ügyfél válaszaiból áll. A sikeres hitelesítés érdekében az ügyfélnek és a kiszolgálónak ugyanazt a hitelesítési módszert kell használnia.

7.4.2 Az EAP-infrastruktúra

Az EAP olyan belső komponensekből áll, amelyek felépítésbeni támogatást biztosítanak minden beépülő modul formátumú EAP-típusnak. A sikeres hitelesítéshez a távelérésű ügyfélre és a hitelesítőre ugyanazt az EAP hitelesítő modult kell telepíteni. A Windows Server 2003 család az EAP két típusát tartalmazza: MD5-Challenge és EAP-TLS. Az EAP-TLS csak tartományi tagok esetében használható. Ha azonban szükséges, további EAP-típusokat is telepíthet. Az egyes EAP-típusok komponenseit minden távelérésű ügyfélre és minden hitelesítőre telepíteni kell.

7.4.3 MD5-Challenge

A Message Digest 5 Challenge (MD5-Challenge) olyan nélkülözhetetlen EAP-típus, amely ugyanazt a kihívás-kézfogás (challenge handshake) típusú protokollt használja, mint a PPP alapú CHAP, de a kihívások és a válaszok EAP-üzenet formátumúak.

Az MD5-Challenge jellemző használati módja a távelérésű ügyfelek hitelesítő adatainak hitelesítése felhasználónévre és jelszóra épülő biztonsági rendszerekkel. Az MD5-Challenge az EAP-együttműködés ellenőrzésére is használható.

7.4.4 EAP-TLS

Az EAP-Transport Layer Security (TLS) a tanúsítvány alapú biztonsági környezetekben használt EAP protokolltípus, amely a legerősebb hitelesítési és kulcsmeghatározási módszert biztosítja. Az EAP-TLS kölcsönös hitelesítést, a titkosítási módszer egyeztetését és a titkosított kulcs meghatározását teszi lehetővé az ügyfél és a hitelesítő kiszolgáló között. Amennyiben a felhasználók és az ügyfélszámítógépek hitelesítéséhez tanúsítványokat vagy intelligens kártyákat kíván alkalmazni, akkor az EAP-TLS protokollt vagy azzal együtt a Protected EAP (PEAP) protokollt kell használnia.

7.4.5 EAP-MS-CHAP v2

Az EAP-Microsoft Challenge Handshake Authentication protokoll 2-es verziója (MS-CHAP v2) a jelszó alapú felhasználó- vagy számítógép-hitelesítést támogató, kölcsönös hitelesítési módszer. Az EAP-MS-CHAP v2 hitelesítési folyamat közben annak eredményessége érdekében mind a kiszolgálónak, mind pedig az ügyfélnek igazolnia kell, hogy ismeri a felhasználó jelszavát. Az EAP-MS-CHAP v2 segítségével a sikeres hitelesítést követően a felhasználók megváltoztathatják jelszavukat, illetve értesítést kapnak annak lejártáról is.

7.4.6 PEAP

A PEAP egy olyan hitelesítési módszer, amely TLS-t használ az EAP hitelesítési protokollok biztonságának növeléséhez. A PEAP előnyei a következők: a PEAP protokollon belül futó, az EAP módszereket védő titkosítási csatorna, a TLS-ből dinamikusan létrehozott kulcsalapok, gyors újracsatlakozás (újracsatlakozási lehetőség vezeték nélküli hozzáférési pontokhoz gyorsítótárazott munkamenetkulcsokkal, amelyek a pontok közti gyors vándorlást teszik lehetővé) és a nem hitelesített, vezeték nélküli hozzáférési pontok telepítésétől védő kiszolgáló-hitelesítés.

A PEAP hitelesítési folyamat

A PEAP hitelesítési folyamat két fő fázisból áll:

- A kiszolgáló hitelesítése és a TLS titkosítási csatorna létrehozása. A kiszolgáló a tanúsítványadatokkal azonosítja magát az ügyfél előtt. Miután az ügyfél ellenőrizte a kiszolgáló azonosságát, egy fő titok jön létre. Az ebből származtatott munkamenetkulcsok segítségével hozható létre a TLS titkosítási csatorna, amely ezután a kiszolgáló és a vezeték nélküli ügyfél közti teljes kommunikációt titkosítja.
- EAP párbeszéd és a felhasználó, illetve az ügyfélszámítógép hitelesítése. A TLS titkosítási csatornába ágyazva a teljes, ügyfél és kiszolgáló közti EAP párbeszéd megtalálható. A PEAP protokoll segítségével az EAP hitelesítési módszerek (például jelszavak, intelligens kártyák és tanúsítványok) közül bármelyik használható a felhasználó és az ügyfélszámítógép hitelesítéséhez.

A PEAP hitelesítési folyamat közben létrejött munkamenetkulcsok biztosítják a kulcsalapot a WEP (Wired Equivalent Privacy) titkosítási kulcsokhoz, amelyek a vezeték nélküli ügyfelek és hozzáférési pontok között küldött adatokat titkosítják.
A PEAP az alábbi hitelesítési módszerek bármelyikével használható vezeték nélküli hitelesítéshez:

- EAP-TLS, amely tanúsítványok segítségével hitelesíti a kiszolgálókat, és tanúsítványok vagy intelligens kártyák segítségével a felhasználókat és az ügyfélszámítógépeket.
- EAP-MS-CHAP v2, amely tanúsítványokat használ a kiszolgáló, és hitelesítő adatokat a felhasználó hitelesítéséhez.

Megjegyzés :

- A PEAP és az EAP-MD5 közös használata nem támogatott.
- A PEAP a 802.11 vezeték nélküli ügyfelek hitelesítési módszereként használható, de nem támogatott virtuális magánhálózati (VPN) vagy más távelérésű ügyfelek esetében. Ezért a PEAP csak az Internetes hitelesítési szolgáltatással (IAS) együtt állítható be egy távelérést szabályzó házirend hitelesítési módszereként.

7.4.7 IPSec

Az IPSec protokoll alkalmazása hosszú távú megoldást jelent a biztonságos hálózati kommunikációban. A magánhálózat valamint a külső hálózat felől érkező támadások ellen kulcsfontosságú védelmi eszközt biztosít.
Az IPSec protokoll két legfontosabb célja, hogy

- megvédje az IP-csomagok tartalmát, és hogy
- védelmet nyújtson hálózati támadásokkal szemben a csomagszűréssel és a megbízható kommunikáció kikényszerítésével.

Az IPSec a titkosításon alapuló védelmi szolgáltatások, a biztonsági protokollok és a dinamikus kulcskezelés alkalmazásával mindkét célnak megfelel. E biztos háttér szolgáltatja azt a hatékonyságot és rugalmasságot, amely a magánhálózatok számítógépei, a tartományok, webhelyek, távoli webhelyek, extranetek és a telefonos kapcsolattal rendelkező ügyfélszámítógépek közötti biztonságos kommunikációt lehetővé teszi. Sőt, az IPSec a megadott forgalomtípusok fogadásának vagy továbbításának blokkolására is használható.

Az IPSec végponttól végpontig alkalmazható biztonsági modell, amely a forrás IP-címtől a cél IP-címig megbízható és biztonságos adatátvitelt tesz lehetővé. Magát az IP-címet nem kell szükségszerűen azonosító elemnek tekinteni, inkább az IP-cím mögötti rendszernek van (hitelesítési eljárással ellenőrizhető) identitása. Az adatforgalom titkosított voltáról csak két számítógépnek kell tudnia: a küldő és a fogadó számítógépnek. Biztonsági szempontból mindkét számítógép a saját biztonságát tartja szem előtt, mivel eleve feltételezi, hogy a kommunikációt lebonyolító közvetítő közeg nem biztonságos. Azoknak a számítógépeknek, amelyek csupán irányítják az adatokat a forrás és a cél között, nem szükséges támogatniuk az IPSec protokollt, hacsak nem tűzfalra alapuló csomagszűrést vagy hálózati címfordítást kell végrehajtania a két számítógépnek.

A remote access IPSec VPN megoldást – ami már a lehallgatás elleni védekezési lehetőségként is felmerült – természetesen a felhasználók autentikálására is lehetne használni. A problémák az IPSec VPN ilyen célú alkalmazásakor is azonosak a lehallgatás elleni védelemről szóló fejezetben leírtakkal.

8. ÖSSZEFOGLALÁS

A jövőben a WIFI eszközök árának csökkenése, valamint a teljesítményének a növekedése miatt illetve könnyű telepíthetőségük miatt valószínű, hogy ezek az eszközök szélesebb körben is el fognak terjedni. Az viszont hogy az új szabványok közül melyik fog elterjedni, már nehezebb megmondani, hiszen láthattuk, néhányat ezek közül, amelyek nem jutottak el a végső piacra. Ezért a szakdolgozatom nem is kíván ebben állástfoglalni. Viszont az előre látható, hogy mivel a mobil internet kiépítése nagyon komoly beruházást igényel, így ha a különböző cégek ilyen szolgáltatást terveznek indítani, akkor az biztosan drágább lesz, mint a jelenlegi vezetékes internet.

Ennek ellenére a mobil internet számos helyen kifejezetten előnyös és célravezető megoldást jelent. Gondoljunk csak az otthoni internet megosztásra, amellyel akár a kertből is használhatjuk az internetet a laptopunk segítségével, vagy a munkahelyeken, ahol a már meglévő hálózatot terjeszthetjük ki anélkül, hogy kábeleket fektetnénk le, illetve a nyilvános helyeken, mint például vasútállomás, kávézók.

Nemszabad azonban elfelejtkeznünk a biztonság kérdéséről sem. A jövőben várhatóan új szabványok jelennek meg, amelyek várhatóan betömik a mostani biztonsági réseket.

A szakdolgozatom célja a vezeték nélküli számítógép-hálózatok bemutatása volt középpontban az IEEE által deklarált 802.11 szabvánnyal.

Szakdolgozatom bevezetésében felvázoltam a vezeték nélküli hálózatok előnyeit és hátrányait, általánosan felvázoltam a működését, illetve összehasonlítottam a vezetékes hálózattal.

A továbbiakban felvázoltam a vezeték nélküli szabványokat, ezen belül a ma legelterjetebb 802.11a,b és g illetve a közeljövőben bevezetésre kerülő újabb lehetséges szabványokat.

Ezenkívül röviden bemutattam az egyéb egyéb vezeték nélküli megoldásokat is, mint az

infravörös és lézeres optikai adatátvitel, a Bluetooth (és az utódául szánt NFC), a HomeRF, valamint a lassan már elhaló, HiperLAN/2. Az optikai megoldások egyértelmű hátránya a közvetlen rálátás problémája, míg a Bluetooth és a HomeRF kis hatótávolsága miatt szorul a háttérbe.

Ezután kitérek magára a 802.11 felépítésére, ezen belül pár OSI-réteg leírására, a hálózatok működésének megértése céljából.

Bemutatom az ad-hoc és infrastructure mode, valamint a kliensek mozgását, illetve elérési pontok közötti barangolása során történő váltását megvalósító roaming funkciót.
A biztonsági problémák elemzése alkotta a hetedik fejezetet. A rendszer biztonsági szempontból gyenge pontja, a WEP-titkosítás hibáival s az ezek elleni védekezéssel szintén foglalkoztam, ám igazi megoldásként a WPA-t és a WPA2-t tekinthetjük.

Köszönetnyilvánítás

Szeretnék köszönetet mondani Dr. Krausz Tamásnak, hogy tanácsaival, javaslataival segítette a szakdolgozatom elkészítését.

IRODALOMJEGYZÉK

Wenig, Raymond P. (1996). *Wireless LANs.* Academic Press Inc.

CISCO Systems Inc. (2001).*CISCO wireless LAN course*. www.cisco.org

Wi-Fi Alliance (2003). *Securing Wi-Fi Wireless Networks with Today's Technologies.* www.Wi-Fi.org

Marshall, Trevor (2001). *Antennas Enhance WLAN Security.* www.trevormarshall.com/byte_articles/byte1.htm

Bates, Regis J. (1994). Wireless Networked Communications. Concepts. Technology and Implementation. McGraw-Hill Inc.

Merritt, Maxim (2002). *Wireless Security.* McGraw-Hill

Tanzella, Fred. (2003). *Wireless LAN intrusion detection and protection.* www.airdefense.net

Wi-Fi Alliance: Wi-Fi Protected Access. www.Wi-Fi.org/OpenSection/protected_access.asp

Wireless LAN Association: High-Speed Wireless LAN Options. www.wlana.org

Geier, Jim. *Minimizing 802.11 Interference Issues.* www.Wi-Fiplanet.com/columns/article.php/947661

AirDefense White Paper (2003).*Wireless LAN Security. What Hackers Know That You Don't.* www.airdefense.net

www.computerworld.hu

www.tomshardware.hu

www.mobilvilag.hu

technet2.microsoft.com

www.biztonsagportal.hu

www.bluetooth.com

www.hyperlan2.com

www.irda.org

www.pdamania.hu

www.nokia.com