Széchenyi István Egyetem

Távközlési Tanszék

Kommunikációs Rendszerek Programozása

(Wireless modul)

Szerzők ABC sorrendben:

Drotár István

Kovács Ákos

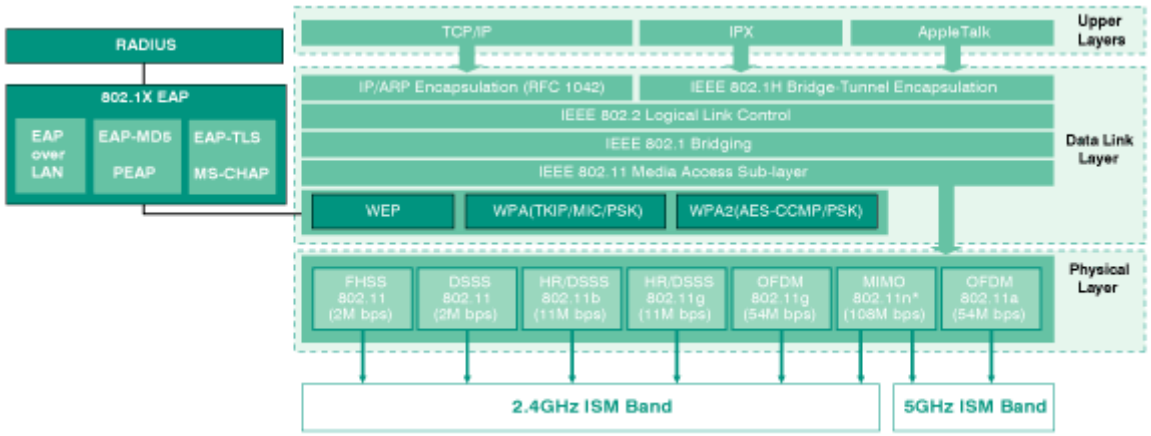
2013. 11. 14.

1.1.Bevezetés az IEEE 802.11 szabványcsaládba

Az Ethernet hálózatokhoz hasonlóan, a vezeték nélküli helyi hálózatok (WLAN – Wireless Local Area Network) kapcsolatai is előre meghatározott módon üzemelnek, amelyet az IEEE (Institute of Electrical and Electronics Engineers) 1997-ben kibocsátott, majd 1999-ben normaként elfogadott IEE802.11 szabvány definiál. Ez nem más, mint egy egyezmény, hogy a hálózat résztvevői, hogyan képesek az egymás közötti kommunikációt megvalósítani. Alapjaként, a több gyártó együttműködésével létrejött, ma már Wi-Fi Alliance-ként ismert szervezet több alapvetése szolgált. A WLAN-ok elterjedése ezután vette kezdetét, és a technológia is virágzásnak indult.
Az irányelv egy általános MAC réteget, több vezeték nélküli fizikai hordozóréteget (WM – Wireless Medium), és az általuk használt frekvenciákat, modulációs eljárásokat és sávszélességeket adja meg. WM-ként infravörös- és lézer fény, valamint rádiófrekvenciás hullám (tipikusan mikrohullám) alkalmazható, melyek közös alapja az elektromágneses terjedés. A legelterjedtebb médium a rádiófrekvenciás hullám, mivel technológiája biztosítja a nagyobb lefedettséget (akkor is, ha nincs közvetlen rálátás) és adatátviteli sebességet. Dolgozatom ezért a továbbiakban a rádiófrekvenciás technológiájú WLAN-on alapul.
A WLAN szabványt az IEEE-n belül létrejött 802.11 TaskGroup (munkacsoport) gondozza, fejleszti, és újabb technológiákat dolgoznak ki a felmerülő igények kielégítésére. Az eredeti szabvány rengeteg fejlődésen ment keresztül, közülük kiemelkednek az adatátviteli sebesség (változó modulációs eljárás), a szolgáltatás-minőség, valamint a biztonság terén véghezvitt fejlesztések.

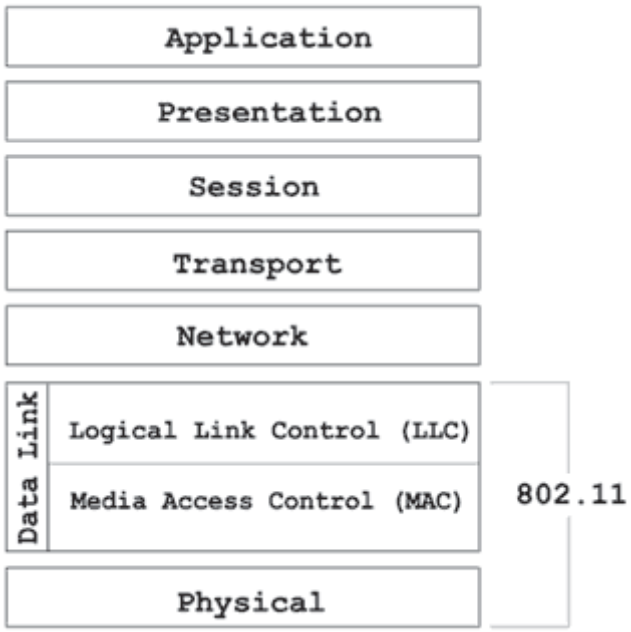
A Wi-Fi Alliance közösség által kiadott Wi-Fi (Wireless Fidelity) minősítés garantálja a berendezések gyártó független együttműködését, mivel követelményeinek alapját az IEEE802.11 szabvány képzi. A gyakorlatban sokszor tekintik a Wi-Fi és IEEE802.11 neveket rokon értelmű szavakként, azonban ez az elnevezés a hétköznapokban inkább magát a vezeték nélküli hálózati technikát takarja.

2. IEEE802.11



1. ábra IEEE802.11 Protokoll Stack

Az IEEE802.11 irányelv a WLAN-ra vonatkozó szabványok gyűjteménye, mely a referencia OSI (Open Systems Interconnection) modell fizikai- és adatkapcsolati réteg funkcióit látja el.



2. ábra OSI referencia modell

A WLAN hálózatok funkcionalitás szempontjából megegyezhetnek az Ethernet hálózat által nyújtott funkciókkal, azaz a felsőbb protokoll rétegek, lehetnek azonosak. Ezzel ellentétben a fizikai- és az adatkapcsolati réteg teljesen eltérő, hiszen míg Ethernet hálózat esetén szükséges a fizikai (kábeles) kapcsolat, úgy WLAN esetében ezt a szerepkört, a már említett elektromágneses hullámok veszik át. A fizikai réteg a használt modulációs eljárást, működési frekvenciát és adatátviteli sebességet irányozza elő, az adatkapcsolati réteg pedig a benne helyet

foglaló közeghozzáférés-vezérlési alrétreget (MAC – Media Access Control) és az adatkeretek típusát definiálja.

Fontos megjegyezni, hogy a vezetékes és vezeték nélküli hálózatok között az átjárhatóság biztosított, mivel az adatkapcsolati rétegen belül elhelyezkedő logikai kapcsolatvezérlő alréteget (LLC - Logical Link Control), ugyanaz az IEEE802.2 szabvány definiálja, mint LAN-ok esetén, így a teljes 48 bites fizikai címkiosztás megegyezik.

Az OSI modellt alapul véve láthatjuk, hogy a 802.11 szabványok funkciója az adott vezeték nélküli összeköttetésen keresztüli kapcsolat és kommunikáció létrehozása a társ LLC alrétegek között. [2]

2.1. WLAN hálózati architektúra

2.1.1. Építőelemek

„Az IEEE802.11-es hálózat építőelemi biztosítják a mobil állomások átlátszóságát a felsőbb rétegek számára.”[2]

Minden egyes WLAN hálózat cellás elvre épül, ahol a lefedni kívánt területet cellákra osztják, és az alábbi alkotórészekből áll össze:[2]

- DS

„Rendszer, mely a hozzá kapcsolódó, majd összekapcsolt alap szolgáltatáskészletek és LAN integrációkon keresztül kiterjesztett hálózati szolgáltatást (ESS) hoz létre.”

Tipikusan rajtuk keresztül kapcsolódnak egymáshoz a hozzáférési pont-ok, gerinchálózatnak tekintő az AP-k számára (DS – elosztó hálózat= Distributed System).

Átviteli közege mind logikailag, mind fizikailag is elkülönül a BSS-en belül használt WM-től, ezáltal biztosítva az architektúra flexibilitását.

- STA

„valamennyi eszköz, amely illeszkedik az IEEE802.11 MAC és PHY réteg interfészére a WM-en keresztül.”

Adott hálózati eszközre kapcsolódó állomás. Lehet helyhez kötött illetve mobilis. WLAN esetén alapvetően mobil állomásokról (STA – Station) beszélünk gyakoriságuk miatt.

- AP

„Entitás, mely egyaránt rendelkezik STA funkcionalitással, valamint biztosítja a DS-hez való hozzáférést a hozzá WM-en csatlakozó STA számára. Interfészein keresztül a BSS-t az elosztási rendszerhez kapcsolja.” Hozzáférési pont, amely a WLAN hálózat alapjául szolgáló aktív eszköz.

A definíció rámutat, hogy a hozzáférési pont (AP - Access Point) Bridge-ként működik, azaz összeköti, áthidalja a vezetékes- és vezeték nélküli hálózatot, így teremtve közöttük kapcsolatot. Az előző állításokból következik, hogy pont-multipont kapcsolattal dolgozik, ezáltal minél több STA csatlakozik rá egy időben, annál keskenyebb sávszélesség jut egy STA-re és úgy csökken az átviteli sebessége is. Ez előremutat a gondos PHY réteg megválasztására, valamint az AP-k számának megválasztására.

Fontos megjegyezni, hogy a DS felé kapcsolódó felület lehet, mind vezetékes, mind vezeték nélküli interfész.

- BSS

Az alap szolgáltatáskészlet (BSS - Basic Service Set) tehát egy AP-ból és a hozzá csatlakozó STA-k csoportjából áll. Egybefüggő rádiófrekvenciás terület (cella), amely a hozzáférési pont elérhetőségi területét jelenti.

- IBSS

A legegyszerűbb WLAN hálózat. A független alap szolgáltatáskészlet (IBSS - Independent Basic Service Set) az egymással direkt kommunikáló STA-k csoportja. Független, mivel a hálózat mentes a dedikált eszközöktől, azaz nem tartalmaz AP-t. A kommunikációban résztvevő felek számát a szabvány nem maximalizálja.

- ESS

„Egy vagy több BSS összekapcsolásából álló csoport, mely az LLC alréteg és bármely benne álló BSS-hez kapcsolódó STA számára egyetlen független BSS-ként látszik.”

A kiterjesztett szolgáltatáskészlet (ESS - Extended Service Set), a definícióból következően DS-en keresztül összekapcsolt BSS rendszerek, melyek felsőbb rétegek számára transzparensek. Ez azt jelenti, hogy az STA-k az ESS-en belül mozoghatnak és kommunikálhatnak a BSS-ek között. A BSS-ek között lehet overlap (átlapolódás), valamint határaiknak nem szükséges összeérniük.

- SSID

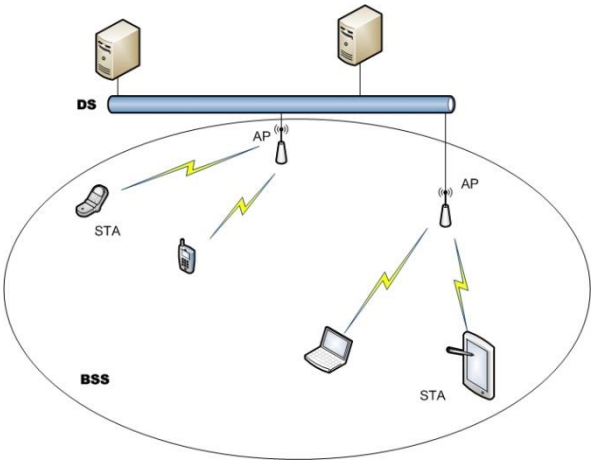
A vezeték nélküli technológiában a jelek szórással terjednek, ezért szükséges az egyes hálózatokat megkülönböztetni egymástól, hiszen egy fogadó állomás több különböző adó körzetében is helyet foglalhat. Ezt a megkülönböztetést szolgáltatáskészlet azonosítónak (SSID – Service Set Identifier) nevezzük, és az adatcsomaghoz kapcsolódnak. Minden egyes WLAN hálózati eszköz (adó- és vevőállomás) az SSID-vel határozza meg, hogy mely node-nak sugározzon.

Amennyiben BSS, valamint ESS hálózatról van szó, úgy BSSID ill. ESSID-nak hívjuk a hálózati azonosítót, IBSS esetén IBSSID-nak.

2.1.2. Topológia

A WLAN hálózatokat kétféleképpen szervezhetjük [2]:

2.1.2.1. Csillag



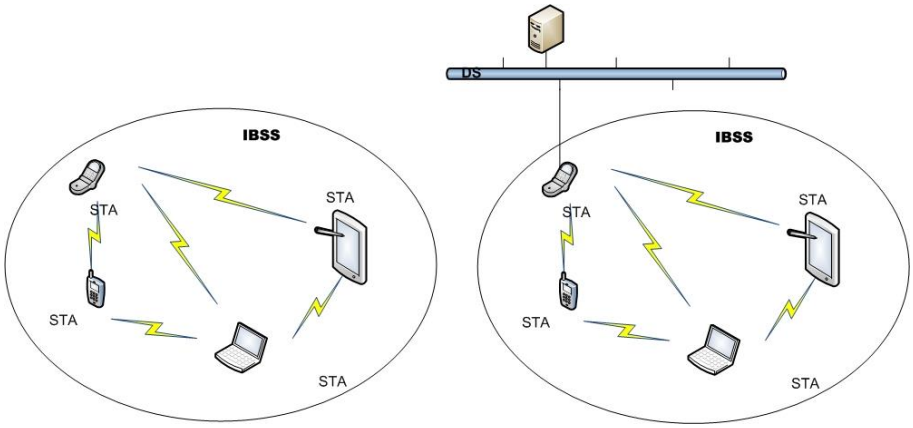
3. ábra Infrastrukturális mód (BSS)

Fókuszpontjában egy mester hálózati eszköz, az AP foglal helyet. Ezen kihelyezett állomáshoz csatlakoznak az STA-k, azaz közvetlenül nem kommunikálnak egymással, csak az AP-n keresztül. A hozzáférési pont vezérli az információ cserét. A kiinduló node elküldi a megcímzett információ csomagot ezen master node számára, majd az, a csomagot a cél STA-re irányítja. Minden egyes slave node csak a master node-nak küldhet, illetve tőle fogadhat megcímzett adatokat.

Mivel a teljes kommunikáció egyetlen dedikált állomáson keresztül zajlik, így a hálózat nem hibatűrő. Amennyiben a master node meghibásodik, kiesik a hálózatból, úgy minden kommunikáció megszakad, hiszen az rajta keresztül üzemelt. További hátránya a szerveződésnek a hatótávolság viszonylag kis mérete (üzemi frekvencia és az adóteljesítmény korlátozottsága miatt). Javulás elérhető irányított antennák használatával, ez azonban a lefedett terület nagyságát csökkenti, így a megoldás a terület növelésére a további AP-k letelepítése és összeköttetése Ethernet alapú DS-n keresztül. Ilyen esetben érdemes site survey-t (előzetes felmérés) alkalmazni a kiépítés előtt.

Az esetek nagy részében az Ethernet hálózat vezetékes kiterjesztéseként alkalmazzák ezt a módszert. Jó példa erre, az egyre elterjedtebb hot spotok alkalmazásával létesített WLAN (például konferencia központban, hogy biztosítsák a látogatók számára az Internet elérést).

2.1.2.2. Ad- hoc



4. ábra Ad-hoc topológia lahetőségei

Más néven egyenrangú mód, mely teljes egészében az IBSS-n alapul és azonos azzal.

Pont-pont alapú kapcsolódási forma, amely a legegyszerűbb WLAN megoldás.

Wi-Fi képes eszközök közötti direkt kommunikáció megvalósítását teszi lehetővé, kihelyezett hozzáférési pont nélkül, azaz nincs szükségünk hálózati erőforrásra, kiépített fix infrastruktúrára. Bizonyos esetekben alkalmaznak AP-kat, ilyenkor azok Repeater-ként funkcionálnak, azaz közbenső node -ként a lefedett terület kibővítése céljából, hiszen az egyes node-ok hatósugara korlátozott.

Mivel nincsenek kijelölt bázisállomások, forgalomirányító eszközök a kommunikáció önszerveződő módon, az ugyanazon IBSS-hez tartozó node-ok között zajlik közvetlenül. Minden eszköz azonos szerepet tölt be.

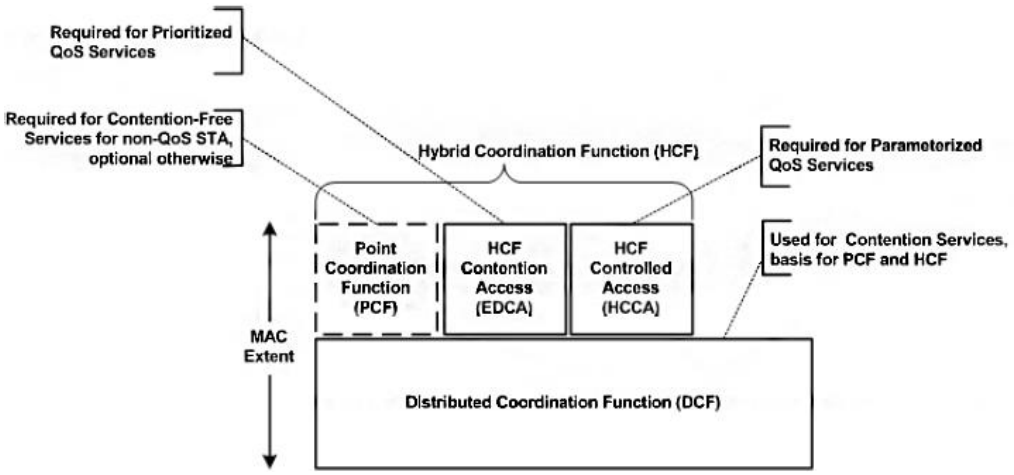
Minden egyes node-ban működik az útvonalkereső protokoll, ezáltal topológia változás esetén újraszerveződnek, hiszen tetszőlegesen csatlakozhat a hálózathoz, vagy léphet ki abból bármilyen node. Az újraszerveződésből következik egyik előnyös tulajdonsága, név szerint a redundancia, mivel egy csomópont meghibásodása esetén, azt kikerülve, új útvonalat keres, ha az a hatókörön belül helyezkedik el. Ez biztosítja a működőképesség további fennállását (azonban számolnunk kell valamekkora csomagkésleltetéssel is).

Fontos megemlíteni további két tulajdonságát, melyek hátrányként jelentkeznek. Egyrészt, hogy csak ad- hoc módban üzemelő kliensek csatlakozhatnak hozzá, másrészt, hogy minden állomás manuális konfigurálást igényel, azaz minden egyes node-ot ugyanarra az SSID-ra és csatornára kell hangolni (ez keskeny sávszélességet tesz lehetővé, így a hálózat áteresztőképessége csökken).

Ez a módszer nem igényel site survey-t, alkalomszerű, minden Wi-Fi képes kártyán elérhető, könnyű segítségével WLAN-t létrehozni és annyi ideig működőképes, ameddig szükséges.
Amennyiben Ethernet hálózathoz akarjuk kapcsolni, úgy ki kell jelölni egy node-ot az IBSS-ből, amely ettől kezdve átjáróként (gateway) üzemel.
Ezen kívül általában rövid idejű, kis hatótávolságú hálózatokat hoznak létre egymás közötti fájlcserére.

2.2.MAC réteg

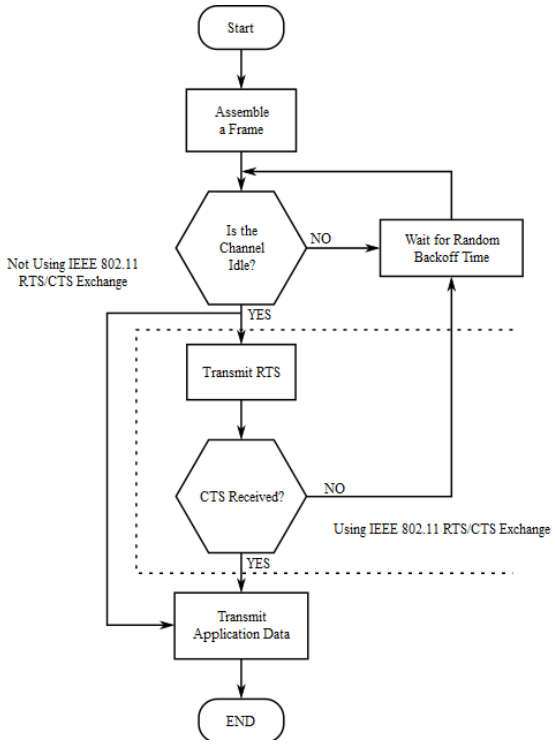
A MAC alréteg, a WM-hez való hozzáférés irányításával tartja fent, vezérli az állomások közötti kommunikációt, koordinálja a PHY réteg működését. Ahhoz hogy az állomások kommunikáljanak egymással, kereteket küldjenek, először meg kell szerezniük a WM használati jogát. Több protokollt is kidolgozásra került (DCF,PCF,HCF).



5. ábra MAC Layer rétegződése

2.2.1.1. CSMA/CA

Mivel a WLAN hálózatokban a kommunikálni óhajtó felek között fél-duplex összeköttetés épül ki, így nem képesek párhuzamosan sem ütközésvizsgálatra, sem annak eldöntésére, hogy sikeres volt-e az adattovábbítás, valamint nem tételezhetjük fel, hogy minden állomás hallja a többit. Ezen oknál fogva WLAN-oknál a CSMA/CD (Collision Detection) megvalósítása nem célszerű, így mielőtt egy állomás kereteket továbbíthatna, hozzáférést kell kapnia a közeghez, ezt az ún. CSMA/CA ütközést elkerülő közeghozzáférés szabályozásával éri el.
Fontos, hogy az ütközési helyzeteket fel lehessen ismerni, mivel így nem a felsőbb rétegeknek kell ezzel foglakozni, ami jelentős késleltetést okozna.
Működés:

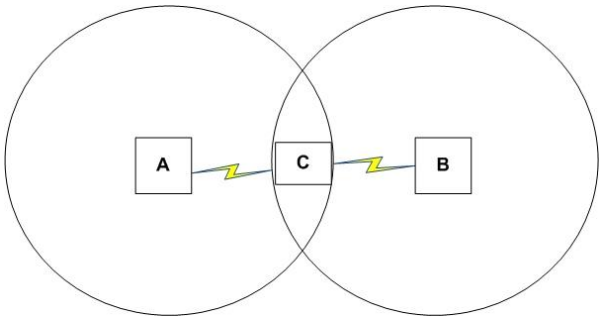


6. ábra CSMA/CA működési algoritmusa

Az adni kívánó állomás figyeli a közeget, ha az foglalt, akkor vár egy álvéletlen generátorral sorsolt ideig (elhalasztja az adást egy későbbi időpontra), majd megvizsgálja ismét a csatornát. Ha azt szabadnak érzékelte egy bizonyos ideig, akkor elkezdi a késleltetési idejét csökkenteni. Ha eltelik egy Slot Time és egyetlen terminál sem kezdte meg adását, akkor csökkenthető a késleltetési idő értéke tovább még eggyel, ezután ismét a közeg figyelése következik. Ez a folyamat addig tart, míg a közegen átvitelt nem érzékel, valamint ha értéke 0-ra nem csökkent. Amint a késleltetési idő 0-ra csökkent, a terminál elkezdhet adni. Amennyiben a szabad közegen egyszerre több állomás kezd adni egy időben, úgy ütközés lép fel, elmarad a sikeres

adást jelző nyugta ACK, az adatot újra kell küldeni, azaz újra kezdetét veszi a versengés időszaka.

2.2.1.2. Rejtett terminál probléma

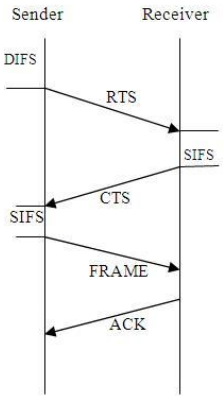


7. ábra Rejtett terminál probléma szemléltetése

Vegyük azt az esetet, amikor két állomás (A és B) egyszerre kíván adni egy harmadik terminál (C) számára. Tegyük fel, hogy A és B állomás egymás jeleit nem képesek venni a köztük lévő távolság miatt, azaz szabadnak érzékelik a közeget. Ilyenkor mindkét (A, B) állomás adni kezd, ezáltal C oldalán csomagütközés lép fel. Ez lehetetlenné teszi a kommunikációt és rejtett terminál problémának nevezzük.

2.2.1.3. Virtual Carrier Sense

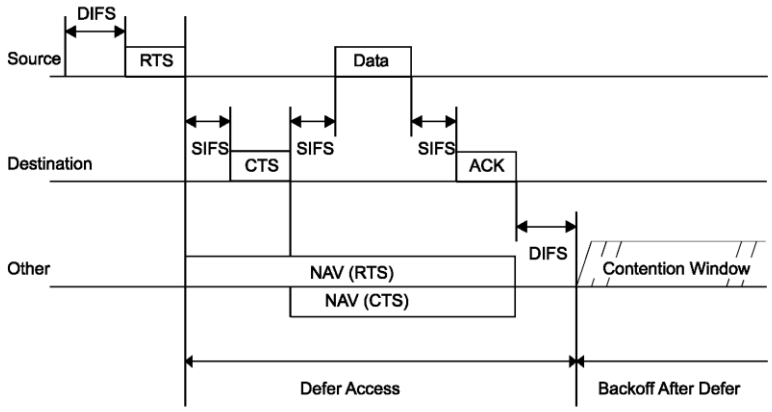
Nem más, mint az IEEE 802.11 szabvány által, a rejtett terminál probléma feloldására definiált virtuális vivőérzékeléses technika, amely egyben a fizikai réteg-béli CCA (Clear Channel Assessment) vivő érzékeléses hozzáférés tiltás kiegészítése. Négy utas kézfogásnak is nevezik (Four Way Handshaking).



8. ábra Négyutas kézfogás és a közöttük eltelt idő

Az adást kezdeményező állomás először egy RTS keretet küld, jelezve adási szándékát. A cél válaszol (ha szabad a közeg) egy CTS kerettel (az RTS-sel azonos időtartam információkat tartalmaz), jelezve, hogy készen áll az adat vételére. Minden állomás, amelyik vette az RTS

és/vagy CTS keretet, beállítja a VCS indikátorát (NAV - Network Allocation Vector), amely azt tartalmazza, hogy hány időrésnyi ideig nem próbálkozhat az adással (a csatornát sem kell hallgatnia) és a fizikai CCA-val kombinálva visszatartja az adást. Így a küldő-, és a célállomás hatósugarán belüli állomások is tudni fognak az adatküldésről, és nem fogják azt megzavarni. A CTS válasz az RTS vétele után SIFS idő múlva kerül elküldésre. A CTS vétele után újabb SIFS idő múlva küldheti az adó az adatkeretet.



9. ábra Rejtett terminál probléma megoldása V-CS-NAV-val

A szabvány definiál egy RTS Threshold változót, ezáltal RTS lényegesen rövidebb a csomagnál. Mivel RTS és CTS rövid csomagok, ezért ütközés esetén az újraindítás hamar elkezdődhet, valamint az ütközési overhead is csökken.
Kizárólag az RTS Threshold-nál nagyobb csomagokra alkalmazható ez a módszer.
A sikeres adatküldést a vevő egy nyugtázó ACK (Acknowledgement) üzenettel jelzi.

2.2.2. Legfontosabb MAC szolgáltatások

2.2.2.1. Reassembly (Fragmentáció és visszaállítás)

A LAN protokollhoz képest, mely maximálisan 1518 bájtos Ethernet keretet használ, vezetéknélküli hálózatok esetén célszerűbb a rövidebb csomagok használata. Ez szükséges, mert:

- rádiós kapcsolat mellett minnnél nagyobb a csomag mérete, annál nagyobb valószínűséggel hibásodik meg a csomag a magas BER miatt.
- FHSS rendszer esetén a közeg sokszori megszakítása miatt érdemesebb kisebb csomagot használni, mert azt kisebb eséllyel kell elhalasztani.
- Kerethiba esetén rövidebb keret mellett kisebb az újraküldési overhead.

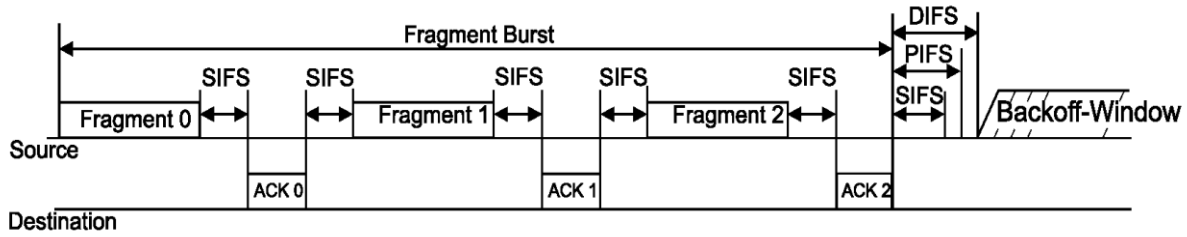
Ezen igényeket a fragmentáció/visszaállítás módszerével oldották meg a MAC alrétegben.

- Töredékek között más nem vehet a csatornán.

- Minden egyes töredék nyugtázva van.
- Töredék újraadások között biztosított a különböző címek használata.

Az eljárás a Send-and-Wait algoritmus, melynél addíg nem lehetséges új töredék küldése, míg:

- az adó állomás ACK-t kap adott töredékre, vagy
- ,ha eldobja az egész keretet a sokszori újraadás miatt.



10. ábra Reassembly folyamata

2.2.2.2. Cellaváltás/Roaming

Egy 802.11 eszköz, mozgás közben, új kapcsolatot kezd keresni, ha elhagyta a lefedett területet. Ez egy szükséges „védelmi” mechanizmus, mivel kapcsolatszakadás esetén a felsőbb rétegbeli protokollok hiba miatti újraadás-kérése lecsökkenti az adatátviteli teljesítményt.

A 802.11 szabvány nem határozza meg, a cellaváltási folyamatot (handover), de definiálja az aktív- és passzív handovert, illetve a roaming-ot.

- *Handover*

Teljesítménycsökkenés szempontjából:

soft-handover – csomagvesztés és észrevehető teljesítménycsökkenés nélküli cellaváltás,

hard-handover – soft-handover ellentettje.

A szinkronizáció megtartását infrasrtukturális hálózatokban a Beacon keret időinformációja alapján érik el. Az állomások periodikusan az AP órájához állítják sajátjukat az említett Beacon csomagok segítségével. A Beacon-keret egy speciális keret, amelyet az Access Point sugároz periodikusan és szinkronizációs információt illetve rendszer specifikációt tartalmaz.

A szabvány a cellaváltásra két módszert definiál:

Passzív - a kliens vár, hogy kapjon egy Beacon-keretet az AP-tól, és ez után történik a handover.

Aktív - a kliens megpróbál egy AP-t találni Probe Request keret küldésével, amelyre válaszként egy Probe Response-ot vár egy közeli AP-tól.

Mindkét módszer egyaránt használható.

- *Roaming*

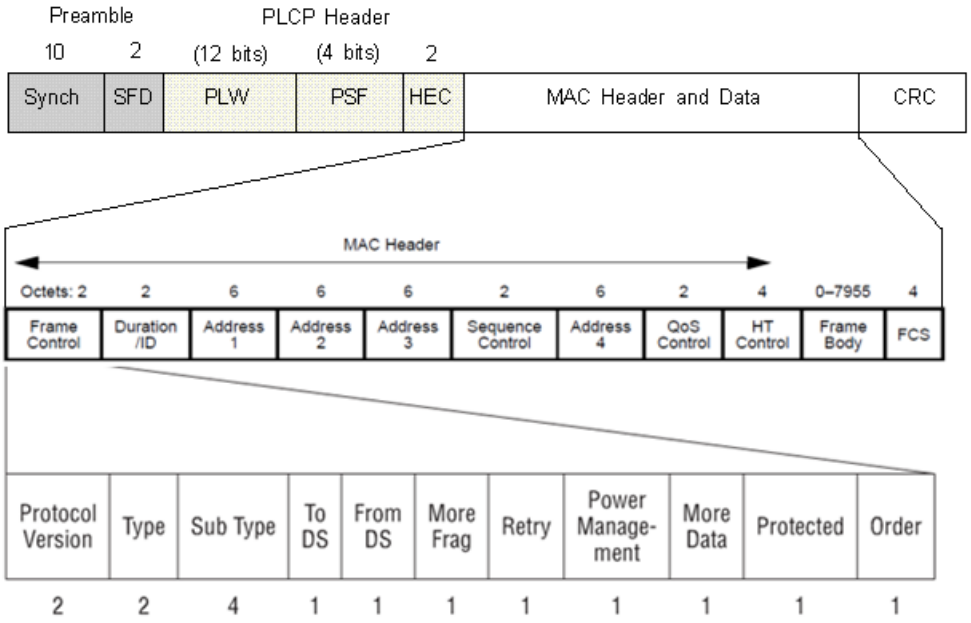
Nem más, mint egy kapcsolatvesztés nélküli BSS váltás.

Amennyiben a mobil STA a helyzetváltoztatás következtében adott AP jelerősségének csökkenését érzékeli, úgy újra megvizsgálja a közeg, hogy van-e a hatókörében erősebb jelet sugárzó Access Point és ha lát ilyet átjelentkezik, újraasszociál. Ez a folyamat a roaming.

Adott STA, mielőtt csatlakozna egy hozzáférési ponthoz, megvizsgálja az átviteli közeget, majd ahhoz a bázisállomáshoz kapcsolódik, amelynek az STA helyén mért jelerősség értéke a legnagyobb.

2.2.3. Keret formátum

Mivel a 802.11e (QoS) 2005-ben került elfogadásra, a 802.11n (HT támogatás) 2009-ben, ezért a korai szabványok nem definiálták a QoS- és HT Control Filed mezőket, azok csak a szabványok megjelenése után lettek támogatottak az újabb eszközökben, így csak megemlítem jelenlétüket a MAC keretben, mint köztes mezők. [1][6]



11. ábra 802.11 frame

Valamennyi 802.11 keret az alábbi összetevőkből áll:

PLPC Preamble

A PHY-től függ és további két almezőre bomlik:

• Synch - egy 80-bites mező, mely váltakozó 0 és 1 mintájú sorozatot alkot (0-val kezdődik, 1-el végződik. A PHY haszálja a vett jel detektálására, az antenna kiválasztására (ha van diverziti), hogy alapállapotba rakja a frekvencia korrekciót (offset), valamint a fogadott csomag szinkronizálására.

• SFD - egy 16-bites bináris minta: 0000 1100 1011 1101, melynek első bitje követi a Sync mező utolsó bitjét. Megadja a keret időzítését.

PLCP Header

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

• PSDU Length Word (PLW) – 12 bit-es almező, megadja a csomag bájtjainak számát, valamint a fogadó STA meghatározza a PLW-vel és egy kódoló algoritmussal a csomag utolsó bitjét.

• PLCP Signaling Field (PSF) – a 4 bit-es almező sebesség információt tartalmaz kódolva, 0,5 Mbps-onként 4,5 Mbps-ig.

Bit	Parameter name	Parameter values
0	Reserved	Default = 0
1:3	PLCP_BITRATE	b1 b2 b3 = Data Rate 0 0 0 = 1.0 Mb/s, 0 0 1 = 1.5 Mb/s, 0 1 0 = 2.0 Mb/s, 0 1 1 = 2.5 Mb/s, 1 0 0 = 3.0 Mb/s, 1 0 1 = 3.5 Mb/s, 1 1 0 = 4.0 Mb/s, 1 1 1 = 4.5 Mb/s

12. ábra PSF mező lehetséges állapotai

• PLPC Header Error Check Field (PLPC HEC) - 16 bites CRC hibadetektáló/hibajavító mező.

2.2.3.1. MAC Header és Data

A MAC alréteg három alapvető kerettípust használ:

- *adatkeret* - adatok továbbításakor alkalmazzuk
- *vezérlő keret* – médiumhoz való hozzáférést szabályozza, további három keretformátumot definiál (adatküldés kérelem (RTS - Request To Send), adatküldésre felkészülve (CTS - Clear to Send), megerősítés (ACK – Acknowledgment))
- *menedzsment keret* – kezelési információkat tartalmaz (ilyen például a Beacon keret, mely az AP-ról tartalmaz információkat, és azt az AP periodikusan sugározza)

A MAC keretek felépítése

Frame Control

2 oktet hosszú, keretvezérlő információkkal. További almezőkre bomlik:

- Protocol Version - 2 bitből áll és azonosítja az IEEE 802.11 –es szabványt.
- Type – típus almező,2 bit hosszú és a MAC alréteg kerettípusát adja meg (adat, vezérlő vagy menedzsment keret).

- Subtype: altípus almező, 4 bit hosszú, melynek értéke az előbbi mező értékétől függ.

A Type és Subtype mező közös 6 bit-je definiálja a keret típusát, altípusát és annak funkcióját.

- More Fragments – 1 bit hosszú, és 1 az értéke az összes adat- és menedzsment típusú keretre, ha az aktuális keretet további tördelt keret követi. Minden más keret esetén 0 az értéke.
- Retry - 1 bit hosszú, és ha be van állítva, akkor megadja minden adat- és menedzsment keret esetén, hogy ez egy korábbi keret vagy töredék újraadása. Minden más keret esetén 0 értékű. Segítségével a vevőállomás felismeri egy keret duplikált adásait.
- Power Management - 1 bit hosszú, jelzi, ha egy STA energiagazdálkodási módban üzemel. 1 értékű, ha az állomás az említett módban üzemel (Power Safe Mode) és addig nem fogad keretet, míg nem kéri, vagy állapota meg nem változik CAM módura. 0 értékű, ha az STA folytonos ébrenléti módban (CAM - Constant Awake Mode) üzemel és fogadja a kereteket.
- More Data - 1 bit hosszú és jelzi az STA számára, hogy további tárolt keretek vannak fenntartva részére és azok az aktuális után érkeznek az AP-tól.
- Protected – 1 bit hosszú, 1 értékű, ha a Frame Body mező olyan információt tartalmaz, melyet egy kriptográfiai algoritmus feldolgozott. Kizárólag az Authentication altípusú adat- és menedzsment keret számára érhető el. Minden más keretre 0 értéket ad.
- Order – 1 bit hosszú, 1 értékű minden nem QoS adatkeret vagy töredék számára, amely StrictlyOrdered szolgáltatás osztályon keresztül került átadásra, azaz minden megérkezett adatkeretet sorrendben kell feldolgoznia. 0 értéket ad minden más keret illetve QoS STA esetén.

Duration/ID

16 bit hosszú, időtartam / azonosító mező. A táblázatban feltüntetett eseteket kivéve minden más esetben a keret fogadásához szükséges hátralévő időtartamot jelöli.

Address1, Address2, Address3, Address4

Egyenként 48 bit hosszú mező, mely a To DS és From DS értékeitől függően lehet BSS azonosító (BSSID), forrás címe, cél címe, adóállomás címe, és a fogadó állomás címe.

Nem minden keret tartalmazza az összes mezőt.

- Address-1 - mindig azon célállomás címe, ami a csomag közvetlen vevője.

Ha ToDS=1, akkor az AP címe, ha 0, akkor a végállomás címe.

- Address-2 - mindig azon forrásállomás címe, amelyik fizikailag elkülde a csomagot.

Ha FromDS=1, akkor az AP címe, ha FromDS=0, akkor a forrásállomás címe.

- Address-3 - a legtöbb esetben a maradék, hiányzó cím. FromDS=1 az eredeti Source

Address, ha ToDS=1, akkor a célcím.

- Address-4 - Wireless Distribution System (WDS) hálózatok esetén alkalmazzuk és két AP közötti keretküldésre vonatkozik. Ilyen esetben ToDS és FromDS is azonosan 1 értékű.

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

13. ábra To- és From DS alapján az Address mezők típusai

DA: Destination Address, RA: Receiver Address,

TA: Transmitter Address, SA: Source Address.

Sequence Control

16 bit hosszú mező, amely 2 almezőt tartalmaz, amelyek megadják a keret és a fragment sorszámát a keretben:

Qos Control

l6 bit hosszú mező, azonosítja a különböző QoS-sel kapcsolatos információkat, melyek a típus és altípus mező által generáltak, valamint azonosítja a keret forgalmi kategóriáját és folyamát.

HT Control

24 bit hosszú mező, mely menedzsment és QoS adatkeret esetén mindig jelen van, és az Order mező értékétől függ. Ha az említett két kerettípus esetén az Order értéke 1, akkor jelzi, hogy a keret HT vezérlési mezőt tartalmaz. Ez a 802.11n PHY esetén a csatornahasználat módját adja meg.

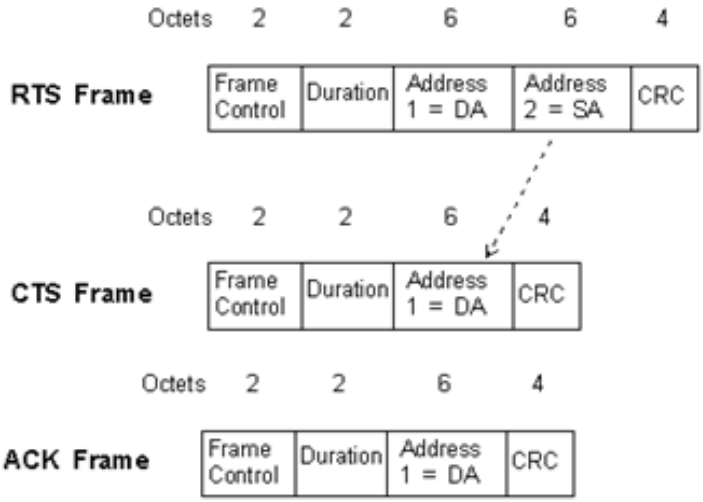
Frame Body

Változó hosszúságú adatmező (keret törzs). A keret típusától függően különböző információkat tartalmaz.

Frame Check Sequence

32 bit hosszú mező, mely 32 bites CRC ellenörző összeget tartalmaz (az összes mezőt felhasználva számolja ki).

2.2.3.2. A legáltalánosabb keret formátumok



14. ábra Általános 802.11 MAC keretek

RTS (Request To Send)

- Destination Address (DA) - a következő keretet (Adat- vagy Menedzsment keret) fogadó állomás címe,
- Source Address (SA) - az RTS keretet adó állomás címe,
- Duration - a következő keret (Adat- vagy Menedzsment keret) küldéséhez szükséges idő, hozzáadva egy CTS, egy ACK keretidő valamint egy SIFS idő értéke µs-ban mérve.

CTS (Clear To Send)

- Destination Address (DA) - az aktuális keretet közvetlenül megelőző RTS keret SA mezőjéből átvett cím
- Duration - egy CTS keretidővel és egy SIFS intervallum idővel csökkentett, az aktuális keretet közvetlenül megelőző RTS keret Duration idő értéke µs-ban mérve.

ACK (Acknowledgement)

- Destination Address (DA) - az aktuális keretet közvetlenül megelőző keret (RTS vagy más egyéb keret) SA mezőjéből átvett cím,
- Duration

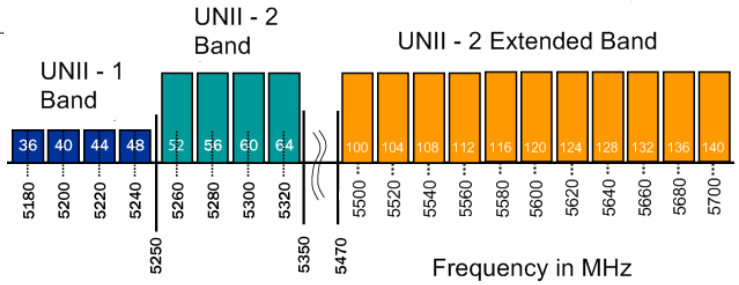
2.3. Fizikai réteg (PHY)

Az előző alfejezetben tárgyalt közeghozzáférés-vezérlő alréteg előírásai, csak az IEEE802.11 szabvány egyik részét alkotják. Az irányelv másik részét a fizikai rétegre (PHY) vonatkozó specifikációk definiálják. A PHY réteg előírásokat fogalmaz meg a működési frekvenciát, a WM-hez való hozzáférést, a spektrumhasználatot és átviteli sebességeket illetően.
(Mint azt korábban írtam, a WM a szabvány alapján többféle lehet, azonban a dolgozat a rádiófrekvencián alapuló megoldásokkal foglalkozik.)

2.3.1. ISM

[7]
Az IEEE802.11 szabvány, következésképpenen a WLAN rádiófrekvenciás eszközök számára a Federal Communications Commission (FCC) a korábban kialakított ISM (Industrial, Scientific, and Medicine) sávot illetve az U-NII (Unlicensed National Information Infrastructure) sávot engedélyezte. Az ISM és U-NII sávok több frekvenciatartományra bonthatók fel:

ISM frequency	Tolerance
6.78 MHz	±15.0 kHz
13.56 MHz	±7.0 kHz
27.12 MHz	±163.0 kHz
40.68 MHz	±20.0 kHz
915 MHz	±13.0 MHz
2,450 MHz	±50.0 MHz
5,800 MHz	±75.0 MHz
24,125 MHz	±125.0 MHz
61.25 GHz	±250.0 MHz
122.50 GHz	±500.0 MHz
245.00 GHz	±1.0 GHz



15. ábra ISM és U-NII sávok Európában

A Wi-Fi képes eszközök számára 3 frekvencitartományt definiál a szabvány:

- 2,4Ghz (2400MHz-2483,5MHz)
- 5,2GHz (5150MHz-5250MHz-5350MHz)
- 5,8GHz (5725MHz-5825MHz)

Az imént felsorolt frekvenciasávokat a világ legtöbb országának hatóságai szabadon tarthatják és nem szükséges engedély a kommunikációs eszközök üzemeltetéséhez a meghatározott adóteljesítmény-korlátok betartása mellett. Hátránya ezért szabad felhasználásában rejlik, mivel rengeteg eszköz működik ezekben a sávokban (például Bluetooth, mikrohullámú sütő időjárás megfigyelő rendszerek, stb.).

Előnye a nagyobb frekvenciatartomány használatában lakozik, amire a nagyobb átviteli sebesség igény miatt van szükség. Továbbá fizikai tulajdonságainak köszönhetően (kisebb hullámhossz), kisebb antennákkal és jelfeldolgozó eszközökkel lehet kivitelezni a Wi-Fi képes eszközöket (olcsóbbak), valamint a frekvencia újrafelhasználása is megvalósulhat ugyanazon tereületen.

Magyarországon a hatályban lévő üzemeltetési feltételek a rádióállomások (jelen esetben WLAN eszközök) számára a következők:

Sáv megnevezés	Frekvenciatartomány	Egyedi engedélyezés
2,4 GHz	2400 – 2483,5 MHz	mentes
3,5 GHz	3410 – 3494 / 3510 – 3594 MHz	köteles
5,2 GHz	5150 – 5350 MHz	mentes
5,6 GHz	5470 – 5725 MHz	mentes

16. ábra NMHH által engedélyezett szabad sávok és engedélykötelességük

„2400 – 2483,5 MHz es sávban

- EIRP maximum 100 mW
- Spektrális teljesítmény sűrűség
  - FHSS (hoping) esetén: max. -10 dBW/100 kHz,
  - FHSS-től eltérő rendszer esetén: max. -20 dBW/1 MHz,
- Berendezésre meghatározott adatsebesség: min. 250 kbps,
- Antenna:
  - integrált (nincs antenna-csatlakozó), vagy
  - dedikált (a berendezés tartozékát képező külső antenna)

Az üzemeltetési feltételek között nincs előírás a csatornaosztásra és a kitöltési tényezőre, minthogy ezekre a mennyiségekre a magyar és európai szabályozás nem ír elő korlátozást”

„5150 – 5350 MHz es sávban

Az 5,2 GHz-es sáv a szélessávú adatátviteli hozzáférési rendszerek körében csakis épületen belüli (beltéri) használatra megengedett. Épületen kívüli (kültéri) használat tilos!

Az alapvető követelmények szempontjából a 200 MHz széles sávot két 100 MHz-es alsávra kell bontani, a két alsáv szabályozása különbözik:

	5150 – 5250 MHz	5250 – 5350 MHz
Max. EIRP	200 mW	200 mW (működő TPC-vel) 100 mW (nem működő TPC esetén)
Max. EIRP sűrűség	0,25 mW/25 kHz	10 mW/1 MHz (működő TPC-vel) 5 mW/1 MHz (nem működő TPC esetén)
DFS	nem szükséges	kötelező
TPC	nem szükséges	kötelező

17. ábra NMHH 5GHz-es tartomány béli üzemeltetési feltételei

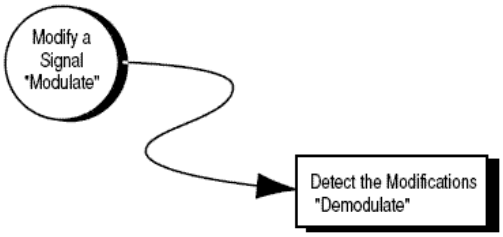
TPC - Adóteljesítmény szabályozás”

(A fent említett ekvivalens izotrop kisugárzott teljesítmény (EIRP - Equivalent Izotropic Radiated Power), közvetlenül nem mérhető számítási mennyiség. Értéke egyenlő az antenna által lesugárzott összteljesítmény és az antennanyereség szorzatával.)

2.3.2. Modulációs technikák

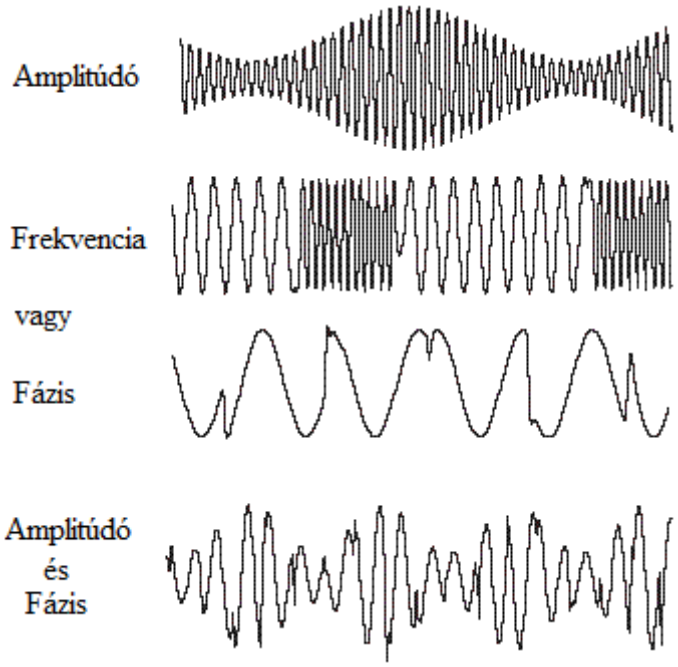
A felhasználók számának és igények növekedésével a rendelkezésre álló RF spektrumot (melyet igénybe vesznek) meg kell osztani. Ehhez nyújt segítséget a különböző digitális modulációs módszerek alkalmazása (nagy kapacitást biztosít a nagy adatmennyiségek számára) valamint a szórt spektrumú modulációs eljrás.

RF csatornában az adatátvitel három lépésben történik: Az adó generál egy vivőt (tipikus szinuszos jel), melyre a modulátor (modulációs technikát alkalmaz) ráülteti a továbbítandó adatot. Ez az adat továbbításra kerül a médiumon keresztül, majd a vevő oldalra érve a demodulátorra kerül a jel, amely felismeri a jelben érzékelt változásokat és demodulálja azt. A moduláció tehát nem más, mint a továbbítandó adat vivőfrekvenciára ültetése.



18. ábra Leegyszerüsített adattovábbítás RF csatornán

A modulációs eljárás során a szinuszos vivő három jellemzőjét változtathatjuk meg, képessé téve így, az információhordozásra. Ez a három paraméter az amplitúdó, a frekvencia és a fázis. Az utóbbi kettő ugyanazon jelbeli változás kétféleképp való megközelítése.



19. ábra Alapvető modulációs sémák

Az amplitúdómoduláció (AM) csak a jel amplitúdóját, a fázis moduláció (PM) csak a jel fázisát (ezt a kettőt egyszerre is alkalmazhatjuk), a frekvenciamoduláció (FM) csak a jel frekvenciáját változtatja meg.

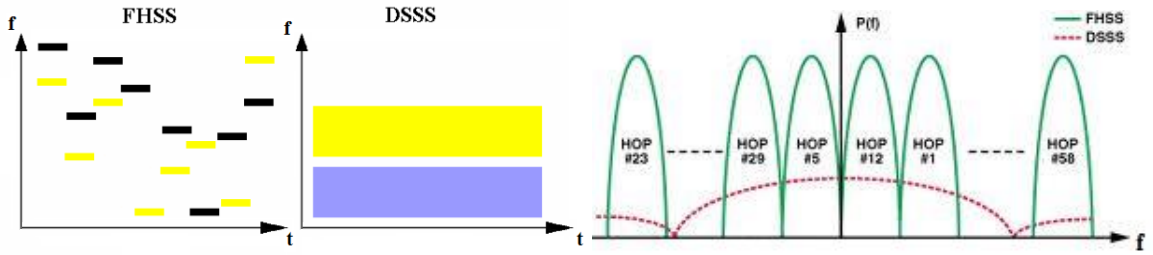
A digitális modulációt rendszerint I/Q modulátorokkal végezzük el, ezáltal biztosított, hogy egyszerre változtathassuk a jel amplitúdó- és fázisállapotát. Ahogyan a jel az egyik állapotból a másik állapotba halad, egyidejű amplitúdó- és fázisváltozás következik be. A modulációt tehát általában azonos fázisú (I) illetve kvadratúra (Q) kifejezésekkel adjuk meg.

2.3.2.1. Spreed Spectrum

A szórt spektrumkiterjesztés egy szélessávú RF átviteli eljárás, amelyben speciális kódolás segítségével szélesebb frekvenciasávban terítik szét az átviendő jelet, a szokásos átviteli eljárásokhoz képest.

Az átvitel fő célja a zajvédelem és az interferencia csökkentése redundanciával, mivel ezen rendszerek többsége az ISM sávokban üzemelnek, melyben nagyszámú zavarforrás található a Wi-Fi képes eszközök számára.

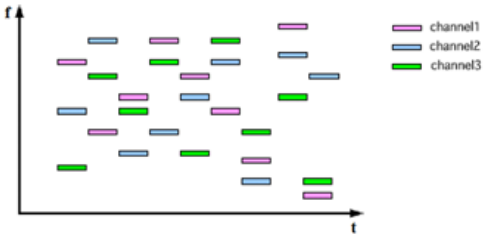
Az IEEE802.11 szabvány két szórt spektrumú technikát dolgozott ki, az egyik a közvetlen sorrendű (DS – Direct Sequence), a másik a frekvenciaugratásos (FH – Frequency Hopping) eljárás.



20. ábra Szórt spektrumú modulációs eljárások különbsége

- **Frequency-Hopping Spread Spectrum**

Az FHSS eljárás lényege, hogy a kommunikációban résztvevő felek nem az egész spektrumot, hanem annak csak egy keskenysávú részét használják oly módon, hogy a használt frekvenciasáv folyamatosan változik. A rendelkezésre álló frekvenciatartomány így több csatornára van felbontva. A kommunikáló felek az ugrási sorozatot pszeudo-véletlen módon határozzák meg 2-4 szintes Gauss-féle frekvenciaváltó kódsorozat (GFSK) alapján. Ezt a frekvenciaugratási sablont felhasználva meghatározzák a működési frekvenciát, majd megadott ideig használják (mivel a szekvenciát mindkét fél ismeri, így szinkronban maradnak). A használati idő eltelte után csatornaváltás következik. A folyamatosan végbemenő változást ugrásnak (hop), a két frekvencia közötti kapcsolási időt ugrási időnek (hop time) nevezzük.



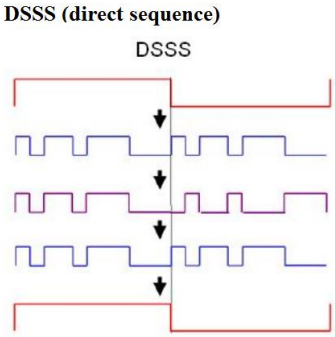
21. ábra Frekvencia ugratás

Összességében a kisugárzott jel szélessávú zajként jelenik meg, azonban a szinkron miatt a vevő követni tudja a hoppokat. Ez az eljárás ezért biztonságos (az illetéktelenek nem tudják, hogy az aktuális frekvencia után melyik következik) és interferenciatűrő is egyben.
Szükséges megemlíteni azt a tényt, miszerint az FHSS nem működik együtt semmilyen más 802.11 fizikai réteggel!

- **Direct Sequence Spread Spectrum**

A DSSS eljárás lényege, hogy a rendelkezésre álló frekvenciatartományt több részre osztja fel, melyben az RF vivőt egy nagy sebességű digitális kóddal (chip code) modulálja, és a felhasznált csatornán szétterítve továbbítja.

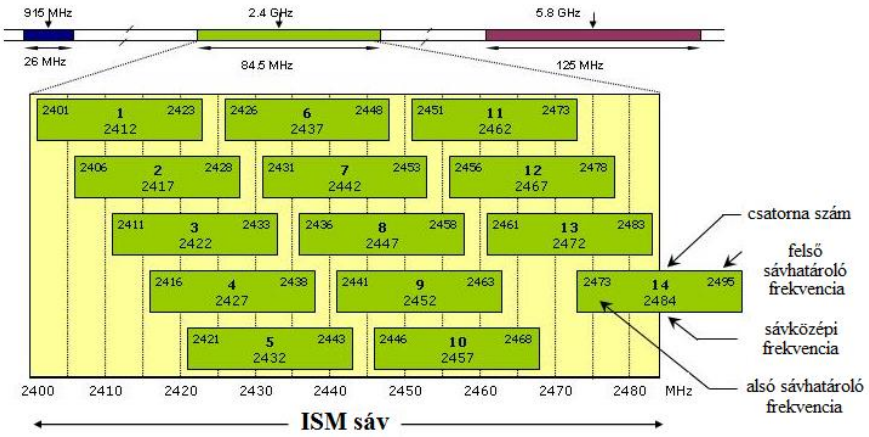
A kódolás során kialakult adatbiteket csak kommunikációban résztvevő felek által ismert mintába ágyazza.



22. ábra DSSS kódolás / dekódolás

A frekvenciatartományt 14 darab 22MHz széles csatornára bontja fel, melyet egybefüggő frekvenciasávnak tekint. A kapcsolat a használt csatorna teljes szélességében épül fel.

A csatornák között jelentős átlapolódások (overlap) vannak, köszönhetően a 22MHz széles sávoknak és az egymástól 5MHz-re elhelyezkedő sávközépi frekvenciáknak. Az átlapolódás a helyes csatornaválasztással elkerülhető. Mivel a teljes csatorna szélesség 22MHz és minden csatorna sávközépi frekvenciája 5MHz-re helyezkedik el egymástól, ezért a nem átlapolódó (non-overlap) csatornák sávközépi frekvenciáját megkapjuk, ha a 22MHz-et követő olyan frekvenciát keresünk, ami 5-tel osztható, azaz egymástól 25MHz-re lévő csatornák nem fedik át egymást. Ezek a csatornák a rendelkezésre álló frekvenciasávban hármasával helyezkednek el. (A korábban említett országonkénti csatornahasználat továbbra is érvényes!)



23. ábra 2,4GHz-en rendelkezésre álló csatornák

Fontos megjegyezni, hogy az egy ugyanazon csatornát használó állomások között a sávszélesség megoszlik. Minden állomás „hallja” egymást, azonban csak azokat az információkat fogadják, amelyek nekik szólnak, a többit eldobják.

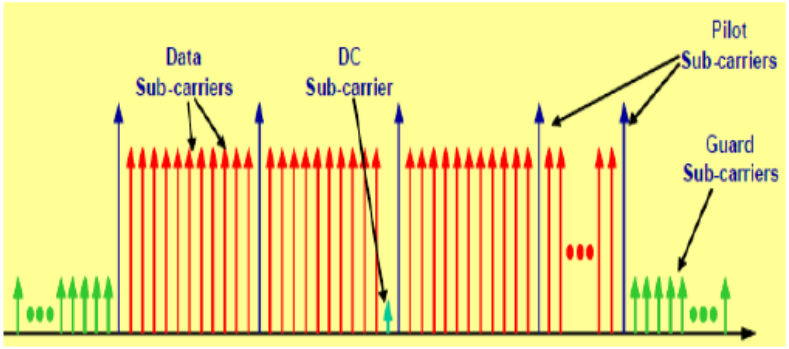
2.3.2.2. Orthogonal Frequency Division Multiplexing

Jellegéből adódóan nem egyszerű eldönteni, hogy modulációs vagy multiplexelési technika, azonban a szabványcsaládok a korábbi modulációs megoldásokhoz képest egy fejlettebb modulációs technológiaként kezelik.

Az OFDM egy speciális modulációs technika, melynél az adatfolyamot több párhuzamos adatfolyamra osztják fel, majd több vivőfrekvenciára felkeverve sugározzák ki. Ezáltal a csatorna több, egymástól független, nem szelektív fadinges alcsatornára van felosztva. Az erőforrásokat időrések és csatornasávok jelentik, így egy felhasználó több időrést és/vagy több csatornasávot használhat egyszerre, az egyes vivőkön akár dinamikusan osztozhatnak a kommunikáló felek.

Az eljárás egy nagysebességű hordozót további kisebb sebességű alcsatornára oszt szét, és ezeket összefogva egyidejűleg használja információ továbbítására. Minden nagysebességű vivő 52 alcsatornára van felosztva.

Az OFDM Nem mindegyik alvivőt használja adatátvitelre, arra csak 48 alcsatornát használ, a fennmaradó 4 alcsatorna pedig hibajavítási célokat szolgál.



24. ábra OFDM - vivők alvivőkre bontása

Az aktív alvivők részhalmazokra, más néven részcsatornákra bonthatók. Ezek hatására, így több adó tud működni egyidejűleg. Ezek úgy vannak kialakítva, hogy a sugárzott jelek egymással ortogonálisak legyenek.

Mivel a csatornák szűkösen vannak elhelyezve egymás mellett, ez az eljárás jobban kihasználja a rendelkezésre álló spektrumot.

Megjegyzés: Mivel egy alcsatornát alkotó alvivők nem feltétlenül szomszédosak, így a szimbólumokat is felosztják alcsatornákra, amelyeket logikai alcsatornáknak nevezünk. Általuk a rendszer biztosítani tudja a skálázhatóság, a többszörös hozzáférés és az összetett antennák kezelésének képességét.

Az ezzel a modulációval kialakított rendszer biztosítja az interferenciamentes átvitelt, akár NLOS (Non-Line-Of-Sight – nincs közvetlen rálátás két kommunikáló fél között) környezetben is. Az elemi vivők sok esetben megoldják a reflexió, több utas terjedés okozta problémákat is. Ha néhány vivő esetén interferencia tapasztalható, akkor is a többi rendelkezésre áll, ennél fogva ezen eltérő frekvenciákon a kellemetlen hatások nem tapasztalhatók.

Segítségével az adatsebesség nagymértékben növelhető az információ párhuzamos csatornákon történő átvitelével, ezen kívül robusztus megoldást jelent a szimbólumközi áthallás, valamint a frekvencia szelektív fading csökkentésére. Az OFDM továbbá még megbízhatóbbá teszi az átvitelt, hiszen a csatornaként felhasznált frekvenciasávot több elemi vivőre osztja.

A rendszer skálázhatóságának megvalósítását két dolog szolgálja: az FFT (Fast Fourier Transformation) méretének változtatása, miközben az alvivő frekvenciája állandó értéken marad.

2.3.3. IEEE802.11 szabványcsalád

Az IEEE802.11 szabványcsalád az 1997-es megjelenése óta rengeteg fejlődésen ment keresztül, és sorra jelentek meg az új szabványok.
Jelen fejezet szabványai a PHY réteg számára definiáltak, így azok az adatátviteli technológia alapjaival foglalkoznak (frekvenciatartomány, moduláció, kapacitás, hatótávolság).
Szükséges megemlíteni az irányelvek interferencia kezelésének hatását (visszaverődések, más culprittól származó jelekkel való ütközés), ugyanis jelenléte rontja az átvitelt, ami az adatátviteli sebesség csökkenéséhez vezet. Szintén az átviteli sebesség kárára válik az overhead, ami az egységnyi idő alatt továbbított protokoll fejrész nagysága (minél nagyobb a protokoll header, annál inkább csökken a valós adatátviteli sebesség), az overlap, ami csatorna átlapolódást jelent, azaz szintén interferenciához vezet. A kódolás során létrejött kompakt és spektrálisan hatékony jelet a modulációs technika megválasztásával ültetjük a vivőre. A fejlődő modulációs technológia jobb jelminőséget, jobb minőségű csatornát, gyorsabb adatátviteli sebességet eredményez, azonban minél nagyobb az állapotszám annál inkább érzékenyebb a hibaarányra.
A következőben bemutatott négy hivatalos IEEE802.11 szabvány: IEEE802.11b,a,g,n.

2.3.3.1. IEEE 802.11b

A 802.11b szabványt 1999-ben publikáltak és az eredeti 802.11 szabvány első revíziója.
PHY rétegében a DSSS moduláció nagysebességű átvitelre képes kiterjesztett változatát használja. Ebből rögtön adódik előnye a korábbi szabványhoz képest, azaz jeleinek szétterítésére a 2,4 GHz-es ISM sávban képes megnövelt (5,5 illetve 11 Mbps) átviteli sebességet biztosítani.
Elvi maximális adatátviteli sebessége 11Mbps, azonban többféle átviteli sebességet is támogat, melyet az eltérő modulációs technológiák segítségével ér el:

- 1 Mbps – legalacsonyabb sebessége, melyet különbségi bináris fázisbillentyűzés (DBPSK) modulációs technikával ér el. Ez egy kétállapotú fázis moduláció, tehát a vivő két állapota a továbbítandó információ függvényében 180°-kal tér el egymástól. Kódoló mechanizmusa Barker kódot használ, mely egy N hosszú sorozat szintén két állapottal (+1, -1).
- 2 Mbps – Kódolási algoritmusa megmaradt a Barker kódnál, azonban a modulációs technológia változott. Kétállapotú DBPSK helyett nagyobb állapotszámú modulációt alkalmaz, mely esetén a csatorna minősége és áteresztőképessége javul. Az eljárás neve DQPSK (Differential Quadrature Phase Shift Keying), mely már négyállapotú fázis modulációt alkalmaz, ezáltal duplázódik adatátviteli sebessége.

- 5,5 Mbps és 11 Mbps – Mindkét esetben marad a DQPSK moduláció, viszont a Barker kód helyett CCK (Complementary Code Keying) kódolási sémát használ. Ez 64 darab 8 bites kódszó sorozatából áll.

A nagyobb állapotszámú modulációs technika és kódolási mechanizmus segítségével az eredeti IEEE802.11 szabványhoz képest lényegesen gyorsabb adatátviteli sebességet ér el, viszont zavarérzékenysége is nagyobb lett a rendszernek. Minél több a zavar, illetve annak mértéke erősebb, annál inkább csökken az átviteli kapacitás. Az elméleti 11Mbps-os sebességről először 5,5, majd 2 és végül 1 Mbps-ra esik az átvitel. Ez a folyamatosan csökkenő technika az ARS (Adaptive Rate Selection).

A szabvány egyik nagy előnye, hogy nagy hatótávolsággal rendelkezik, ami épületen belüli alkalmazásnál akár 90 méter távolságot is áthidalhat, viszont csak a közepes teljesítményű alkalmazások kiszolgálására alkalmas.

2.3.3.2. IEEE 802.11a

Az IEEE802.11a alszabvány az IEEE 802.11b szabvánnyal együtt jelent meg, azonban attól több aspektusban is eltér. A legszembetűnőbb változás, hogy elérhetővé tette az 5GHz-es frekvenciatartományt az U-NII sávban, ezáltal nagyobb sávszélesség áll rendelkezésre. A felhasznált 5GHz-es sáv több szempontból is előnyösnek bizonyult: még nem telített, nagyobb átviteli sebességek érhetők el, nagyobb teljesítményszint elérése válik lehetővé illetve az interferencia lehetősége is kisebb. Amennyiben több, egymást nem átfedő csatornát veszünk egyszerre igénybe, növelhetjük konkrét sávszélességünket.

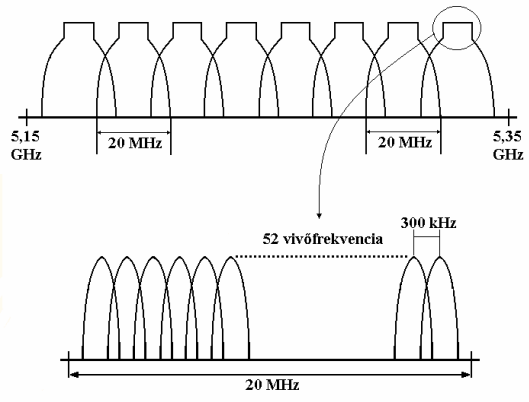
A legnagyobb hátrányt az okozza, hogy mivel más frekvenciatartományt használ, ezért kompatibilitási problémákat okoz a 802.11b eszközökkel. Az ilyen eszközök nem, vagy csak bővítő modulok behelyezésével képesek kommunikálni egymással. További hátránya az 5GHz-es sávnak, hogy hullámhossza kisebb, ezáltal hatótávolsága is kisebb (mindössze 10-25 méter épületen belül).

A 802.11a modulátora különböző modulációs mechanizmust és kódarányt használ a nagyobb adatátviteli sebesség eléréséhez. A modulációs sémákat, kódarányokat és a velük elért adatátviteli sebesség elméleti határértékét a következő táblázat reprezentálja:

DATA RATE (MBPS)	MODULATION	CODING RATE
6	BPSK	1/2
9	BPSK	3/4
12	QPSK	1/2
18	QPSK	3/4
24	16-QAM	1/2
36	16-QAM	3/4
48	64-QAM	1/2
54	64-QAM	3/4

25. ábra IEEE802.11a modulációs eljárásai a sebesség függvényében

Az elméleti maximális átviteli sebességhez OFDM modulációs eljárást alkalmaz, melyben az 5,15GHz- 5,35 GHz közötti frekvenciatartományt 8, egyenként 20 MHz-es csatornákra bontja fel. Egy 20 MHz-es csatornában 48 darab adat vivőt és 4 szinkronizációs vivőt alkalmaz, egymástól 300kHz-es távolságokra. Amennyiben egyetlen 802.11a képes Wi-Fi eszköznek osztjuk ki a csatornát, akkor az elérhető max. elvi átviteli sebességként megkapjuk az 54Mbps-ot.



26. ábra IEEE802.11a OFDM moduláció

Az IEEE 802.11a szabvány egyik nagy előnye, hogy 12 nem átlapolódó csatornát (8 épületen belüli és 4 pont-pont átvitelnek) alkalmaz, emiatt a lehető legnagyobb csatornakapacitást biztosítja. Ebből adódóan nagy sűrűségű felhasználói területeken és nagyobb teljesítményű alkalmazásoknál előnyösen használható.

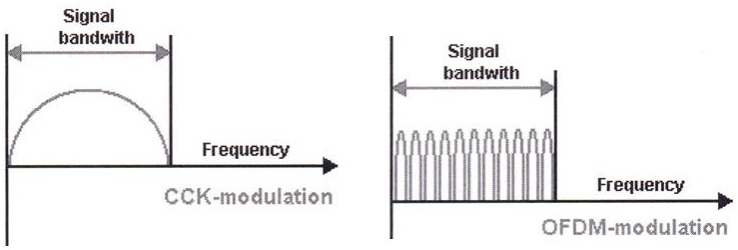
Frequency Band	Channel ID	FCC (GHz)	ETSI (GHz)	MKK (GHz)	SG (GHz)	ASIA (GHz)	TW (GHz)
Lower Band (36 = default)	34	—	—	5.170 [1]	—	—	—
	36	5.180	5.180	—	5.180	—	—
	38	—	—	5.190	—	—	—
	40	5.200	5.200	—	5.200	—	—
	42	—	—	5.210	—	—	—
	44	5.220	5.220	—	5.220	—	—
	46	—	—	5.230	—	—	—
	48	5.240	5.240	—	5.240	—	—
Middle Band (52 = default)	52	5.260	5.260	—	—	—	5.260
	56	5.280	5.280	—	—	—	5.280
	58	5.300	5.300	—	—	—	5.300
	60	5.320	5.320	—	—	—	5.320
H Band	100	—	5.500	—	—	—	—
	104	—	5.520	—	—	—	—
	108	—	5.540	—	—	—	—
	112	—	5.560	—	—	—	—
	116	—	5.580	—	—	—	—
	120	—	5.600	—	—	—	—
	124	—	5.620	—	—	—	—
	128	—	5.640	—	—	—	—
	132	—	5.660	—	—	—	—
	136	—	5.680	—	—	—	—
	140	—	5.700	—	—	—	—
Upper Band (149 = default)	149	5.745	—	—	5.745	5.745	5.745
	153	5.765	—	—	5.675	5.675	5.675
	157	5.785	—	—	5.785	5.785	5.785
	161	5.805	—	—	5.805	5.805	5.805
ISM Band	165	5.825	—	—	5.825	—	5.825

27. ábra 5GHz-es sáv csatorna kiosztása

Az ilyen hálózatok tipikus hatótávolsága 54 Mbps sebesség mellett 12 méter, 6Mbps sebesség mellett 90 méter.

2.3.3.3. IEEE 802.11g

A 802.11g szabványt 2003 júliusában publikálták. Az elméleti maximális adatátviteli sebesség ezen szabvány által is 54 Mbps, azonban a 2,4GHz-es ISM sávra.
Legnagyobb előnye, hogy lefelé kompatibilis. A használt frekvenciatartomány miatt a 802.11g képes Wi-Fi eszközök a korábbi 802.11 és 802.11b hálózatokkal kompatibilisek. Azonban a 802.11b és 802.11g szabványok együttes használata során probléma merül fel, mely probléma forrása az eltérő modulációs eljárás alkalmazása.



28. ábra IEEE802.11g által használt modulációk különsége

A kompatibilitási probléma kiküszöbölésére azonos modulációt alkalmaznak a megkívánt sebesség eléréséhez, és így már jelezhetik egymás felé az átviteli közeg használatának szándékát.

Összességében a használt modulációs eljárások így két részre bonthatók. Mivel ugyanazokra a sebességekre képes, mint a 802.11a ezért, ezen sebességekhez, ugyanazon modulációs sémákat alkalmazza, mint a 802.11a. Ahhoz, hogy megmaradjon kompatibilitása lefelé, ugyanazon eljárásokat alkalmazza, mint a 802.11b.

Rate, Mbps	Carrier Single/Multi	802.11b @2.4GHz		802.11g @2.4GHz	
		Mandatory	Optional	Mandatory	Optional
1	Single	Barker		Barker	
2	Single	Barker		Barker	
5.5	Single	CCK	PBCC	CCK	PBCC
11	Single	CCK	PBCC	CCK	PBCC

29. ábra IEEE802.11 b és g kompatibilitás

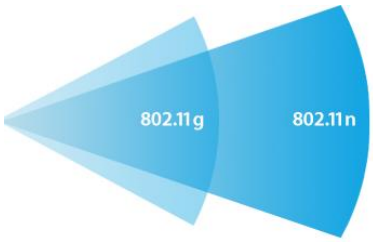
Csatornahasználata megegyezik az 802.11b által használt frekvenciatartományokkal, ezért ugyanolyan interferencia érzékeny is maradt.

Lefelé kompatibilis vegyes üzemmódú (Mixed mode) esetén a „g" eszközök sebességét jelentősen befolyásolja a használt védelmi mechanizmus *(RTS/CTS vagy CTS-to-self)*. „Ez a beállítás az adatütközések elkerülésére szolgál vegyes 802.11b/11g/11a/11n környezetekben. Célszerű használni az RTS/CTS jelpárt, ha az ügyfélgépek esetleg nem hallják egymást. A CTS mindenkinek (CTS-to-self) engedélyezésével javítani lehet az átbocsátást az olyan környezetekben, ahol az ügyfelek közel vannak egymáshoz és hallják egymást (802.11n esetén a CTS-to-self nem támogatott.)"

A 802.11g hálózatok tipikus hatótávolsága 54 Mbps sebesség mellett 15 méter, 11 Mbps sebesség esetén pedig 45 méter.

2.3.3.4. IEEE 802.11n

A Wi-Fi Alliance 2009–ben véglegesítette a 802.11n szabványt. Az addigra már elavultnak számító 802.11b/g szabványt hivatott leváltani. A kor megnövekedett sebességigényének és állományméretének e korábbi szabványok már nem tettek eleget. Ezt a két igényt az IEEE802.11n szabván teljes mértékben kielégíti, hiszen a szabvány célja az átviteli sebesség jelentős növelése és a lefedettség kiterjesztése volt.



30. ábra Megnövekedett hatótávolság IEEE802.11n esetén

A fent említett előnyöket több új technológia bevezetésével érték el:

- Redued Inter-Frame Spacing (RIFS) - Keretek közötti várakozási időt a felére csökkentette (400ns-ra).
- 40MHz-es csatornák implementálása– Az új szabvány megengedi a szomszédos csatornák összevonását, ezáltal 40MHz-es sávra növekedett, mivel az eddigi szabványok 20MHz-es csatornával operáltak. A 40 MHz-es csatornahasználat kétszer annyi segédvivőt jelent, ezáltal sebessége megduplázódik. Az új szabvány definiálja, hogy a rendszernek folyamatosan figyelnie kell, vannak-e a környezetében olyan régebbi eszközök, melyek nem képesek kezelni a szélesebb frekvenciatartomány. Ha talál ilyet, leszabályozza önmagát, és csak az egyik 20 MHz-es sávon küldi az adatokat. (HT20 ill. HT40 mód). Adatküldés előtt ellenőrzi mindkét csatorna foglaltságát.
- Multiple Input Multiple Output - Képes összeilleszteni a jeltöredékeket a MIMO segítségével. Ez egy többantennás rendszer, amely a reflektált RF jeleket, a több utas interferenciát használja a jel teljesítményszintjének növelésére és a hatósugár kiterjesztésére. Az utóbbi állítás nem más, mint az adatátviteli csatornák párhuzamos használata. A MIMO lényegében megegyezik a térbeli multiplexeléssel (SDM - *S*pace Division Multiplexing). A több antenna révén egy időben megy végbe a vétel és adás egyaránt, lehetővé téve az elmélet maximális átviteli sebesség elérését.
  paraméterezése: adók száma x vevők száma: adatfolyam

- Modulációs technika – A korábbi szabványokhoz képest csak a használt kódarányban tér el, ahogyan azt a következő táblázat is mutatja:

MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbit/s)			
				20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00
16	3	BPSK	1/2	19.50	21.70	40.50	45.00
17	3	QPSK	1/2	39.00	43.30	81.00	90.00
18	3	QPSK	3/4	58.50	65.00	121.50	135.00
19	3	16-QAM	1/2	78.00	86.70	162.00	180.00
20	3	16-QAM	3/4	117.00	130.70	243.00	270.00
21	3	64-QAM	2/3	156.00	173.30	324.00	360.00
22	3	64-QAM	3/4	175.50	195.00	364.50	405.00
23	3	64-QAM	5/6	195.00	216.70	405.00	450.00
24	4	BPSK	1/2	26.00	28.80	54.00	60.00
25	4	QPSK	1/2	52.00	57.60	108.00	120.00
26	4	QPSK	3/4	78.00	86.80	162.00	180.00
27	4	16-QAM	1/2	104.00	115.60	216.00	240.00
28	4	16-QAM	3/4	156.00	173.20	324.00	360.00
29	4	64-QAM	2/3	208.00	231.20	432.00	480.00
30	4	64-QAM	3/4	234.00	260.00	486.00	540.00

31. ábra IEEE802.11n adatátvitelis sebesség és az alkalmazott modulációs eljárás

Mivel modulációs eljárása nem változott és a csatornahasználata továbbra is kezeli a 20MHz-es csatornákat, ezért az összes eddig ismertetett szabvánnyal (, azaz lefelé) kompatibilis.

OFDM rendszere szintén a már ismertetett módon üzemel, azaz 52 alvivőből 48 szolgál adatok szállítására, a fennmaradó négyet pedig a vevők fázis szinkronizációjára használja, 300KHz-es távolságokban elhelyezve ezeket és egymással parallel módon, tehát egy időben kerülnek átvitelre. A különbség a nagysebességű vivőben rejlik, mely 10, 20, vagy 40MHz-es lehet.

- A WEP már nem szerepel a szabvány leírásában (pozitív lépés a biztonságosabb hálózatok felé), ezáltal WEP-titkosítást használva eszközünk 802.11b/g módban fog működni.
- Dual Band (hibrid) -, azaz kétsávos típusok, képesek a 2,4GHz-es ISM és 5GHz-es U_NII sávban is sugározni. Abban az esetben hasznos ezen tulajdonsága, ha túl sok 2,4 gigahertzes sávot használó eszköz van környezetünkben.
- Quad Band – szimultán képesek mindkét frekvenciasávban sugározni. Ezeket külön SSID SSID azonosítja, így a STA egyszerre csak az egyik frekvencián sugárzott hálózatra csatlakozhat.

	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Szabvány elfogadásának éve	1999	1999	2003	2009
Adatátviteli sebesség (elméleti)	54 Mbps (30m)	11Mbps (100m)	54 Mpbs (30-37m)	300 Mpbs (50m)
Effektív átviteli sebesség	20-23	4 Mbps	20 Mbps	90-100 Mbps
Működési frekvenciatartomány	5 GHz	2,4 GHz	2,4 GHz	2,4/5 GHz
Csatornák száma	12	14	14	14/12
Modulációs technika	OFDM	DSSS	OFDM, DSSS	MIMO-OFDM
Sávszélesség	20 MHz	20 MHz	20 MHz	20/40 MHz

32. ábra IEEE802.11 alszabványok összehasonlítása

3. IEEE 802.11s (WMN's)

Az IEEE802.11s szabványtervezet rengeteg fejlődésen ment keresztül. 2003-ban indult útnak tanulmányként, majd 2004-ben létrejött számára a szabványok kidolgozására és fejlesztésére szakosodott TaskGroup, majd hivatalos szabványként 2006-ban fogadták el IEEE802.11s Draft1.01 „Wi-Mesh" néven. Innen két lépcsőn keresztül (2008 szeptemberében Draft 2.00, majd 2009 márciusán kiadott Draft 2.07) jutott el, a mai legfrissebb P802.11s D3.0 verziószámú szabványhoz.

3.1. WMN hálózati architektúra

Jelenleg a legtöbb 802.11 WLAN infrastruktúra-BSS módban funkcionál, amelyben minden STA egyetlen vezeték nélküli ugráson keresztül kommunikál a központban elhelyezett entitással, az AP-val. Ez az eszköz a korábban bemutatott módon hidat képez a 802.11 és nem 802.11 hálózatok között.

Amennyiben több BSS kapcsolódik egymáshoz DS-en keresztül, úgy ESS-ről beszélünk. Ezen módban az állomások vándorolhatnak a BSS-ek között anélkül, hogy megszakadna a szolgáltatás, viszont mindig egy központi AP-hoz csatlakoznak. Ezt hívtuk roamingnak.

A 802.11 technológia elérhetővé teszi szolgáltatások elérését ott, ahol a vezetékes infrastruktúra nem kívánatos.

A Wireless Mesh Network gerinchálózattól független, olcsó telepítésű eszközökkel teszi elérhetővé a szolgáltatásokat a kliensek számára. Ehhez szakított a single-hop üzemmóddal, helyette multi-hop technológiát és adatkapcsolati réteg béli, útvonal-választási és csomagtovábbítási metódust alkalmaz, mely továbbra is transzparens a felsőbb rétegek számára.

A továbbiakban bemutatom logikai és hálózati architektúráját.

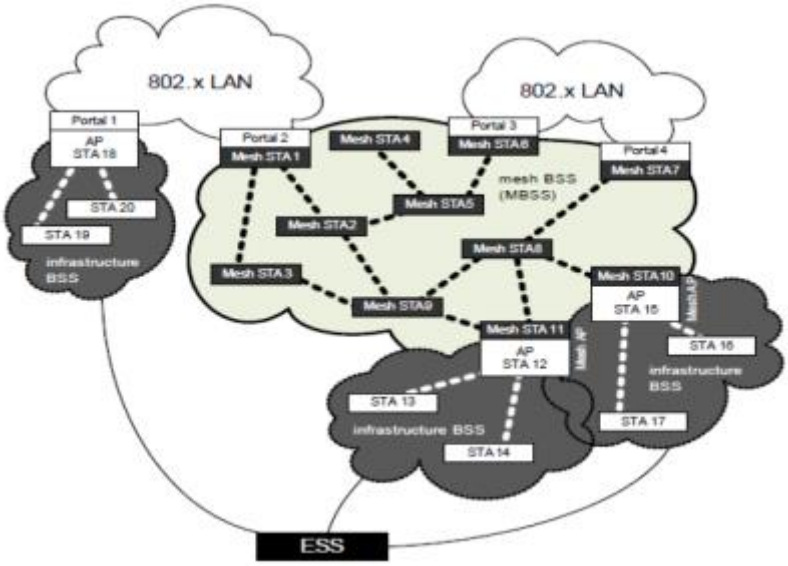
3.1.1. Topológia

Mesh

Szövevényes topológia, mely az ad- hoc hálózati architektúrához hasonló. Pókhálószerű csomópontokból épülnek fel, és ezekből automatikusan, önszerveződés révén jönnek létre. A hálózat jellemzője, hogy node-jai között kölcsönös kapcsolat van, és jellemzően nincs központi entitás.

A 802.11s egy sor összehangolt mesh állomás összekapcsolódásából áll, melyek között minden lehetséges útvonal kiépül. Ezt Mesh-BSS-nek nevezzük, és eszközei a MAC adatkeret által biztosítják a multi-hop technológiát. Mint azt már említettem, az átlátszóság továbbra is biztosított a felsőbb rétegbeli protokollok számára.

„IBSS-en belül, egy keret terjedése egyik ugrástól (forrás–AP) másik ugrásig tart (AP-cél), így az egyszerre nem tud kommunikálni a Service Set többi tagjával (single-hop). Az MBSS-ben ezzel szemben a keret multi-hop-okon keresztül terjed ez biztosítja, hogy a kapcsolat minden állomással kialakul. Továbbá az IBSS egy önálló csoportot alkot (standalone), amelyhez semmilyen más külső hálózat vagy átjáró nem csatlakozik, míg MBSS-en belül több gateway is előfordulhat.”



33. ábra IEEE802.11 hálózati architektúrák MBSS-sel

Az architektúra egy sor rövidebb ugrással tartja fenn a jelerősséget, azaz elég sűrűn telepítettek az eszközök. A közbenső node-ok nemcsak a jelerősség szempontjából fontosak, de együttműködnek, így adattovábbítási döntéseket is hoznak a feltérképezett hálózati útvonalak alapján. Egy ilyen architektúra gondos megtervezése magas rendelkezésre állást, magas adatátviteli sebességet, spektrális hatékonyságot és gazdasági előnyt jelent a lefedett területen. A topológia redundanciát is biztosít, így stabilnak tekinthető, több node kiesése esetén is.

4. Tervezés

Az ISM és U-NII sávok közkedvelt használata, az egyre dizájnosabb és olcsóbb Wi-Wi képes eszközök megjelenése, dinamikus elterjedésnek indította a vezeték nélküli hálózatokat. Ez sűrű telepítésű, egymástól független WLAN hálózatok megjelenéséhez vezetett, mely így rengeteg hibaforrás kiinduló pontját jelenti. A legfontosabb közülük az eszközök interferenciás zavartatása, mivel túl sok AP illetve antenna esetén az egymáshoz közel elhelyezkedő elérési pontok jelei interferálhatnak (káros interferencia esetén csökken a hálózat hatásfoka, legrosszabb esetben az összeköttetés megszakad).
Az előbbiek miatt, a legfontosabb feladat, hogy a lehető legnagyobb hatékonyság elérésével, még a kiépítés előtt tervezzük meg a hálózatot, az üzemeltetési és környezeti szempontok figyelembe vételével, ezáltal megfelelő rádiófrekvenciás lefedettséget biztosítva a felhasználók számára. Leegyszerűsítve, meghatározzuk az AP-k elegendő számát és azok megfelelő helyét, így a tervezési fázis lehet a legfontosabb lépés egy sikeres WLAN létrehozásakor.

A vezeték nélküli hálózattervezés több részfolyamatból áll, azonban a fejezet csak a hálózat megtervezése, a tervezés elengedhetetlen részét képező rádiós mérés, és az általuk közösen alkotott eredmények kiértékelésével foglalkozik, mivel a további fejezetek tartalmazzák a biztonság és kivitelezés kérdéskörét.
(Megjegyzés: A jelterjedést befolyásoló tényezők, hatások, melyekkel tervezés során számolni kell:

- a bizonytalanul lefedett területek,
- a rossz minőségű átvitel,
- különböző csillapító (például válaszfalak, burkolók) anyagok,
- interferenciát okozó további eszközök,
- a pontszerű sugárzó jele fokozatosan gyengül az adótól távolodva (négyzetes arány),
- a rádiófrekvenciás jel irányváltoztatást szenved a különböző tereptárgyakon bekövetkező visszaverődés (reflexió), elhajlás (diffrakció), törés (refrakció), elnyelődés (abszorpció) miatt,
- többutas jelterjedés (reflexió, diffrakció, refrakció következtében).)

4.1. Vezeték nélküli hálózat megtervezése

4.1.1. Követelményelemzés

A hálózattervezési folyamatot egy előzetes igényfelmérés, úgynevezett követelményelemzés előzi meg. Ilyenkor a leendő hálózat legalapvetőbb tulajdonságai kerülnek meghatározásra (elvárt minimálás átviteli sebesség, lefedendő terület nagysága, titkosítás, adatbiztonság, várható adatforgalom, valós-idejű átvitelt biztosító hálózatra van-e szükség).
Amennyiben ezeket a kérdésköröket rosszul mérjük fel, úgy rossz tervet, illetve nem megfelelő hálózatot fogunk készíteni.
A dolgozatban megtervezett hálózat a laborépület teljes lefedésére vonatkozik, ezért a követelményeket a következők alapján határoztam meg:

- A laborépületben kiépített vezetékes hálózat áll rendelkezésre. A laborok munkaállomásai erre a hálózatra csatlakoznak, ezáltal nem szükséges a lefedettség biztosítása. A fókuszpont a folyosókra helyeződik át.
- A kapcsolódni kívánt állomás kompatibilitása miatt, a rendelkezésre álló ISM sáv 2,4GHz-es frekvencia tartományára építve tervezünk (a dolgozat által megvalósított mesh hálózat Single Channel módban üzemel, ezáltal egy frekvenciasáv kijleölésére van lehetőség).
- A vezeték nélküli hálózat célja a közepes energiaigényű internetes alkalmazások kiszolgálása (levelezés, böngészés).

(*Megjegyzés:* Minden hálózatot úgy kell megtervezni, hogy az később könnyen módosítható, továbbfejleszthető, bővíthető legyen.)

4.1.2. Lefedettségi terv elkészítse

Lefedettség tervezésekor a legalapvetőbb követelmények:

- Magas rendelkezésre állás
- Skálázhatóság

Az utóbbi esetet a lefedett területen elhelyezkedő AP-k számának növelésével érhetjük el, melyek feladata, kifejezetten a terhelésmegosztás. Magas rendelkezésre állás esetén redundáns berendezéseket iktatunk a hálózatba és igyekszünk a lefedni kívánt terület lehető legpontosabb megtervezésére.
A lefedendő terület tervezésekor többféle módszer áll rendelkezésünkre:

- prediktív,
- túlméretezéses,
- aktív, környezeti méréssel történő feltérképezés.

Túlméretezés – A leginkább használatban lévő eljárás. A lefedni kívánt területre többleteszközök kerülnek, így biztosítva a kommunikáció fennmaradását. Nem követ semmiféle stratégiát, ezáltal az eszközök sem feltétlenül a szükséges helyekre kerülnek. Mivel

nem szisztematikus az eljárás, ezért optimalizálatlan, nem megbízható, terhelt hálózati tervet ad eredményül.

Aktív, méréses hálózattervezés – Hagyományos eljárás, mely során teszt hozzáférési pontokat telepítünk a hálózat kiépítése előtt, és feltérképezzük, a fix ponton elhelyezkedő AP esetén a jelszint- és interferencia-méréseket, a lefedni kívánt terület, különböző pontjain. Interpolálva a mérési eredményeket, megkapjuk a lefedni kívánt terület térerősség-eloszlását. Az eljárás kevés erőforrás segítségével megvalósítható, kézzelfogható és egyszerű, azonban rendkívül időigényes. Viszonylag elavult technika, mivel nem veszi igénybe a letelepíteni kívánt elérési pontok közötti kommunikációs igényeket, illetve a sávszélességgel kapcsolatos feltételeket.

Prediktív – Modellezésen, szimuláción alapuló hálózat tervezési metódus. Dolgozatom témáját adó mesh hálózatot ezen eljárás segítségével terveztem meg és építettem ki, így következőkben erre fokuszálok.

4.1.2.1. Prediktív tervezés

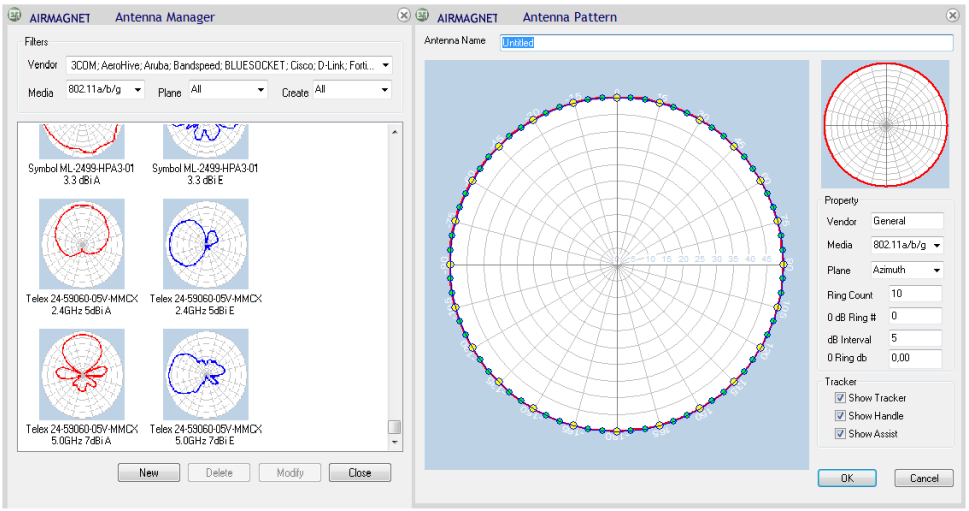
Egy passzív hálózattervezési eljárás a prediktív hálózatoptimalizálás, mely előzetes tervet készít a kiépítendő rádiós hálózatokról, és meghatározza a hozzáférési pontok közelítő számát és helyét.

Ennek során a lefedni kívánt terület alaprajzát valamint a környezeti tényezőket is beleértve létrehozható az épület RF-térkép modellje. A modell számítógépes szimuláció segítségével meghatározza a lefedendő terület pontjaiban mérhető térerősség értékeket. Az elektromágneses térszámítás, ezáltal alkalmas az EM hullámok viselkedésének, csillapodásának illetve kölcsönhatásának más hullámokkal illetve a közeggel történő szimulációjára. Az eljárás a hálózati teljesítménnyel kapcsolatban, a környezeti elemek (fal, nyílászáró, stb.) csillapító és szóródó hatását, az AP konfigurációkat és az antenna jellemzőket figyelembe véve, szimulációt végez, majd ennek megfelelően hőtérképen jeleníti meg a WLAN AP-k rádiófrekvenciás besugárzási jelszintjeit. Ezáltal eredményt kapunk a területi lefedettség várható mértékét illetően (automatizálható az AP elhelyezés), előre tervezhetjük a kiépítendő vezetéknélküli hálózat node-jai közötti kapacitást.

- ***Kezdeti lépések***

Mielőtt hozzákezdenénk a szimulációhoz, előkészületeket kell tennünk, hogy a tervezés folyamat végeredménye ne okozzon később meglepetéseket, a nem definiált jelterjedést befolyásoló tényezők miatt.

Antenna Manager – Amennyiben szeretnénk a végleges hálózatban használt rádióantennát megadni a szimulátornak, hogy annak paramétereivel számoljon, úgy erre lehetőség van az Antenna Manager beépített funkcióval. Itt a tervezés kezdete előtt, definiálhatjuk antennánk különböző paramétereit. Ezt a következő ábra szemlélteti.



Ezen felül lehetőség van több gyártó anennájának kiválasztására is beépített adatbázisából.

(Megjegyzés:

A WLAN által használt antennák egyik, általános csoportosítási módja a következő:

- Körsugárzók (omnidirectional): 360 fokos sugárzási minta jellemzi

- Irányított (directional) antennák: energiájukat egy kitüntetett irányba fókuszálják. Minél nagyobb a nyeresége, annál kisebb a sugárzási szög (kisebb lefedettség), viszont annál nagyobb a hatótávolsága.

Antenna paraméterek:

- iránykarakterisztika - megadja az antenna körüli térben, az antenna által létrehozott azonos teljesítménysűrűségű pontokat. izotróp antennára vonatkoztatva.

- sugárzási karakterisztika - az antenna milyen irányban mekkora intenzitással sugároz

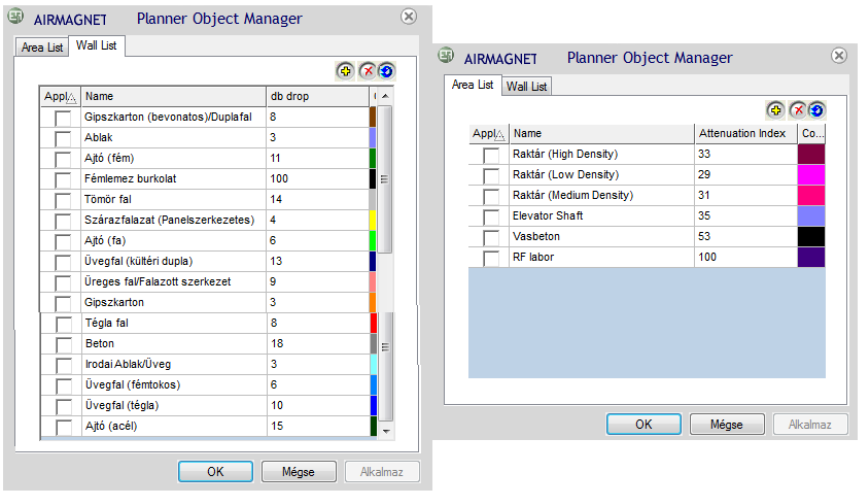
- sugárzási minta – radiation pattern, az antenna által kibocsátott elektromágneses hullámtér relatív térerősségének geometriai mintázata

- nyereség (gain) - ami a főirányban kisugárzott teljesítménysűrűség,

- nyílásszög (beamwidth) - az iránysugárzó antennák irányhatásának mérőszáma, hogy mennyire képesek a beléjük táplált teljesítményt egy nyalábba gyűjteni és egy konkrét irányba kisugározni.)

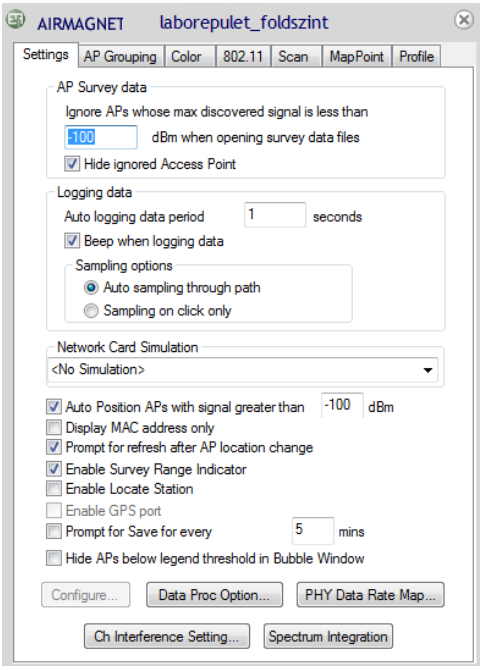
Planner Object Manager – Előre definiálhatjuk a lefedni kívánt intézmény karakterisztikáját (környezeti tényező, építészeti anyagok), mely fontos szerepet tölt be a jel terjedésének meghatározásában. Itt csillapításértékeket adunk meg.

Az általam definiált és a laborépületben fellelhető építészeti anyagokat az alábbi ábra szemlélteti.



Ezen felül szintén lehetőség van a beépített adatbázisából kiválasztani a környezeti tényezőket.

Configure – Specifikáljuk a minimális lefedettségi mutatókat (threshold), illetve a csatorna használatot.

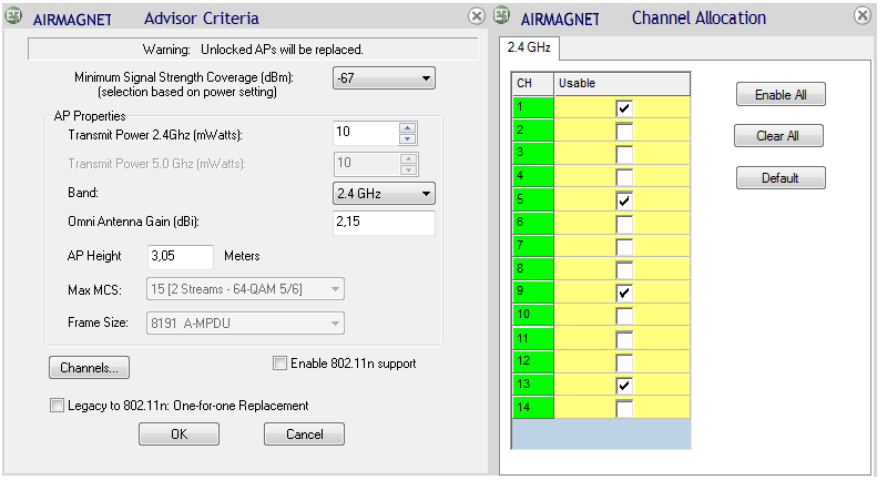


Miután végeztünk az előkészületekkel, nekiállhatunk projektünknek.

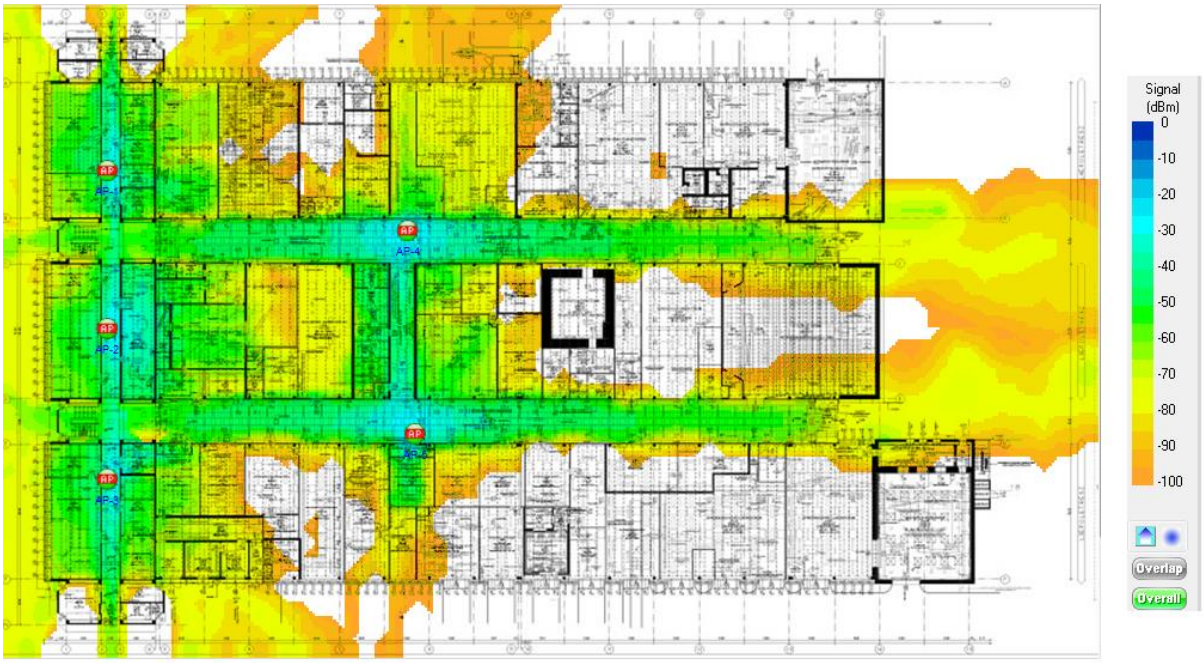
- A lefedettség igényét méretezett, méretarányos alaprajzon definiáljuk első lépésként. Ehhez betöltjük a lefedni kívánt intézmény alaprajzát, így egyszerűen és gyorsan, méretarányos tervrajzot kapunk. Ehhez a beépített kalibráló funkciót használjuk, mely pixel/méter aránypárral kalibrálja az alaprajzot.

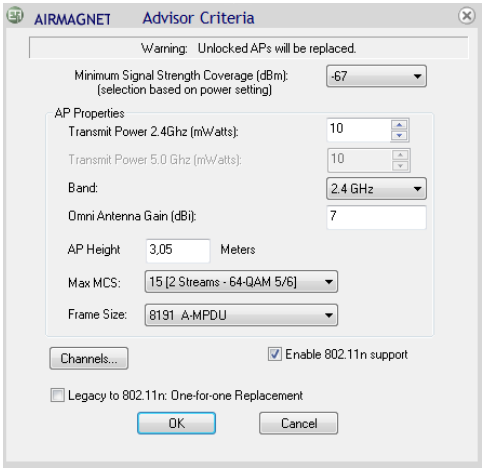
- Átvitelt befolyásoló tényezők tervre illesztése – a folyamat során kijelöljük a lefedendő terület által használt építészeti jellemzőket (válaszfalak, nyílászárók, reflektáló, abszorbciós területek, stb.) tipikusan a csillapító közegeket, melyeket korábban definiáltunk az object managerben. Miután ezzel végeztünk, kijelöljük a lefedni kívánt területeket, és azokat ahova nem tervezünk vezeték nélküli hálózatot. Mindezt a pontosabb becslés érdekében tesszük, hiszen ezek a tényezők hatással lehetnek az RF hullám terjedésére, ezáltal a vezeték nélküli hálózat teljesítményére.

- hozzáférési pontok jellemzői – a szimuláció indítása előtt beállítjuk a kivitel során használt AP-ok jellemző értékeit (magasság, antennanyereség, médium 2,4GHz/5GHz – 802.11a/b/g/n, használni kívánt csatornák, és minimálisan engedhető térerősség értéket)



Miután definiáltuk és beállítottuk az összes paramétert, elkezdhetjük a szimulációs folyamatot. Az alábbi alaprajzon az általam kivitelezésre szánt vezeték nélküli mesh hálózati terv szimulációs eredményét, illetve beállításait láthatjuk:



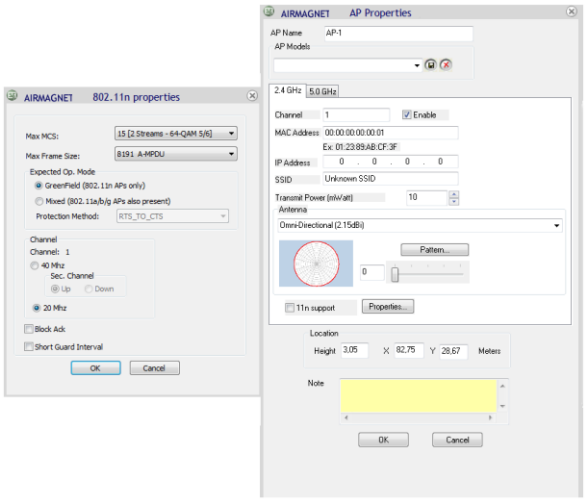


(A végleges terv meghatározásához több szimulációt futtattam, mind a program által ajánlott, mind az általam próbált elhelyezések alapján. Ezen paraméterek és a generált tervrajzok a mellékelt CD-n megtalálhatóak. Továbbá dolgozatom részét képezte a laborépület első emeleti lefedettsége is, melynek csak végleges eredményét tüntetem fel dolgozatomban, hiszen az eljárás teljes egészében megegyezik a földszinti trervezés során bemutatottakkal. A további adatok a mellékletben találhatóak.[CD]).

A tervezés során a rádió antennák nyereségét 7dBi szintűre állítottam, mivel a kivitelezés során ugyanilyen paraméterű körsugárzó antennákat használok közel 3 méter magasságban. További tervezési szempontokat a kompatibilitás és gyorsabb adatátviteli sebesség összefonódásával

vettem figyelembe, azaz a tipikus 2,4GHz-es ISM sávra terveztem IEE802.11b/g/n típusú hozzáférési pontokkal. A minimális jelszint értékét a magas csillapítási tényezővel rendelkező környezeti elemek sokasága miatt -67dBm szintre választottam, ezáltal biztosítva a megfelelő lefedettség és térerősség elérését.

Egy másik lehetőség, vagy a szimulált terv kiegészítésének céljára is szolgálhat, ha magunk helyezzük el az előkészített tervrajzon az AP-kat (rendszerint szubjektív módon, azaz tapasztalati eredmények alapján). Ezen módszer során az AP-t bármely területre elhelyezhetjük, megadhatjuk a csatorna kiosztását, 2,4GHz vagy 5GHz-es médiumot, IP címeket, adási teljesítményt, antenna típust, irányát, magasságát és a 802.11n specifikációkat is paraméterezhetjük.



A telepítendő mesh hálózat szubjektív szimulációs tervezése során a paramétereket az előzőekben ismertetett értékeken hagytam. A fenti telepítési pontokba helyezve az AP-kat, a rádióhullámok a területet teljes egészében lefedik. A szubjektív eljárás a korábban szerzett tapasztalatainkra alapozott becslést jelenti.

Mindkét esetben, ha végzett a szimuláció lehetőség nyílik a további módosításokra (AP paraméterek változtatása, környezeti tényezők, tervrajz módosítása) ezáltal optimálisabb tervrajz elkészítésére.

- A szoftveres hálózattervezés előnyei:

gyors, csökkent a tervezésre fordított idő, hatékony, legkülönfélébb méretű és környezeti adottságú helyszínek lefedése, precíz prediktív RF tervező képesség.

A tervrajz által megvalósított hőtérkép elsődleges célja a lefedettség demonstrálása. Az általam szimulált tervrajzon a két szint lefedettségi térképe látható. Megfigyelhető, hogy a hosszanti folyosók gipszkarton borítású, beton falszerkezete, milyen nagymértékben befolyásolja a jel terjedését.

Az ilyen és hasonló jelenségek miatt feltétlenül fontos, hogy a kivitelezést megelőzően mérésekkel meghatározzuk a zavaró tényezőket. Erre egy folyamatosan mozgó adóvevő használatával van lehetőség, melyet egy laptophoz csatlakoztatva, mint szenzorral feltérképezhető a térerősség értéke, az épület különböző pontjain. Leegyszerűsítve, a szimulációs tervezés mellett is szükséges, hogy a rendszer telepítésére szánt környezetet feltérképezzük, mivel a szoftver által szimulált „jóslás" nem azonos a vezeték nélküli hálózat telepítésekor végzett felméréssel (Site Survey).

4.1.3. Site Survey

A kialakítandó rendszer optimális kihasználhatósága érdekében szükséges a környezet előzetes rádiófrekvenciás vizsgálata is.
Mivel az RF hullámokat nem érzékeljük, ezért ahhoz, hogy egy adott terület lefedéséhez szükséges AP-k optimális számát meg tudjuk határozni, mérni kell:
– az adott helyszín és környezetének rádiófrekvenciás telítettségét,
– a lefedendő terület rádiófrekvenciás interferencia zavartatást kiváltó tulajdonságait,
– Meglevő vezeték nélküli infrastruktúrát.
Az RF mérés valós idejű RF paramétereket (csatorna forgalom, jel-zaj viszony, térerősség) és detektált eszközöket (üzemelő AP-k) gyűjt össze, melyek jellemzőit is megtekinthetjük, vizuálisan, a méretarányos alaprajzon hő térkép formájában. Segítségével leegyszerűsíthető a WLAN környezet teljesítmény analízise, feltérképezhető, hogy hol és miért romlik a WLAN hálózat minősége.

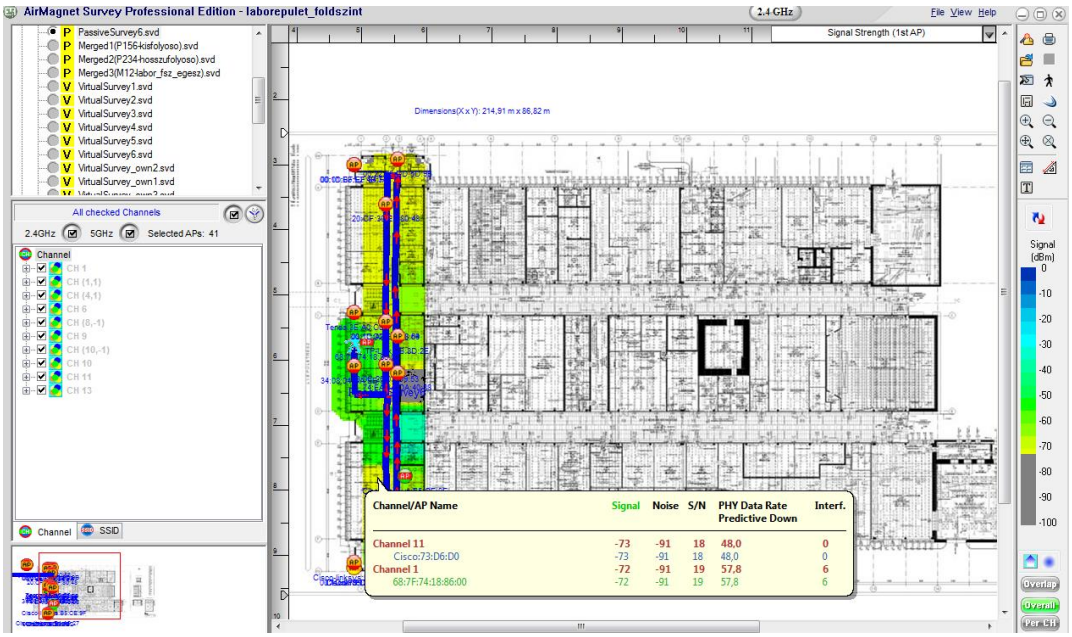
- A hőtérkép részletes teljesítmény adatokat tartalmaz, amely így megkönnyíti a kapacitástervezést és a hálózat optimalizálást. Pontosan azonosíthatják, dokumentálhatják a WLAN-al lefedett területet és a holttereket.
- A mérési pontok számát a vizsgálandó helyszín mikrohullámú telítettsége határozza meg. Teljesen más mennyiségű mérési pont szükséges nyílt, vagy zárt helyiségek esetében. Nyílt tér esetében nagy valószínűséggel biztosítható a sugárzó elemek optikai láthatósága, ezért kevesebb mérőpont is elégséges. Zárt, zsúfolt tér esetében minél részletesebb mérés készítése a cél. A mérési pontokat az általunk definiált útvonal mentén vesszük fel. Ezért az alaprajznak a mérést megelőzően, hosszúságra kalibráltnak kell lennie. (Ezt a lefedettségi résznél ismertetett módon itt is megtehetjük.)
- A mérés során a két fontos jellemzőt kell vizsgálni:

- A vevő által mért rádiófrekvenciás jelteljesítmény nagyságát a vizsgált frekvenciasávban.

A vevőben indukált hasznos bejövő jelszint nagyságát mérjük, mely a hely függvényében jellemzi az adott térrész rádiófrekvenciás lefedettségének jellemzőjét és a vevő vételi képességét.

- A vevő által érzékelt RF jel-zaj viszony értékét, Signal to Noise Ratio (SNR).

Ezt a két paramétert a vizsgált helyszín térrészére húzott egér kurzor segítségével tehetjük meg, amikor is a program megmutatja a detektált jelszint nagyságát és SNR-t.



- Site Survey alatt többféle módban vizsgálódhattunk:

Aktív vizsgálat - Egy AP-hez (vagy SSID-hez) asszociál a mérőeszköz, ezáltal részletes adatokat rögzíthetünk az eszközről. A kapcsolat fennállása során valós idejű csomag adatokat gyűjt (kapcsolat sebessége, csomag újraküldés, csomagvesztés).

Aktív Iperf vizsgálat – Aktív vizsgálat Iperf szolgáltatás kiegészítéssel. Ez a felépített kapcsolat tényleges minőségi paramétereit méri illetve lehetővé teszi a kliens emulálást.

Passzív vizsgálat – Az eddig tárgyalt RF adatokat rögzíti a terület mikrohullámú telítettségéről (minden eszközről, minden csatornán). Dolozatom erre a módszere épül.

- A mérőrendszer

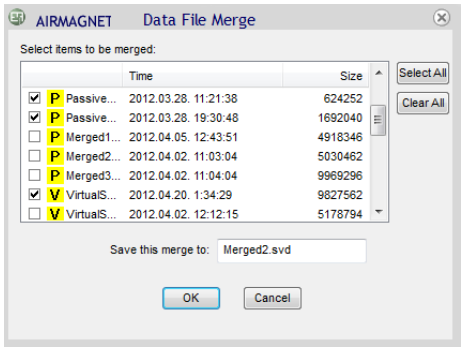
A mérések elvégzéséhez Proxim 8494-wd wireless 802.11a/b/g/n adaptert használtam. A modul alkalmazásához a feltérképező szoftver (AirMagnet Survey PRO) és egy laptop szükséges, amely biztosítja a tápfeszültséget, a kommunikációt, valamint a működés ellenőrzésére szolgáló visszajelző LED-et.

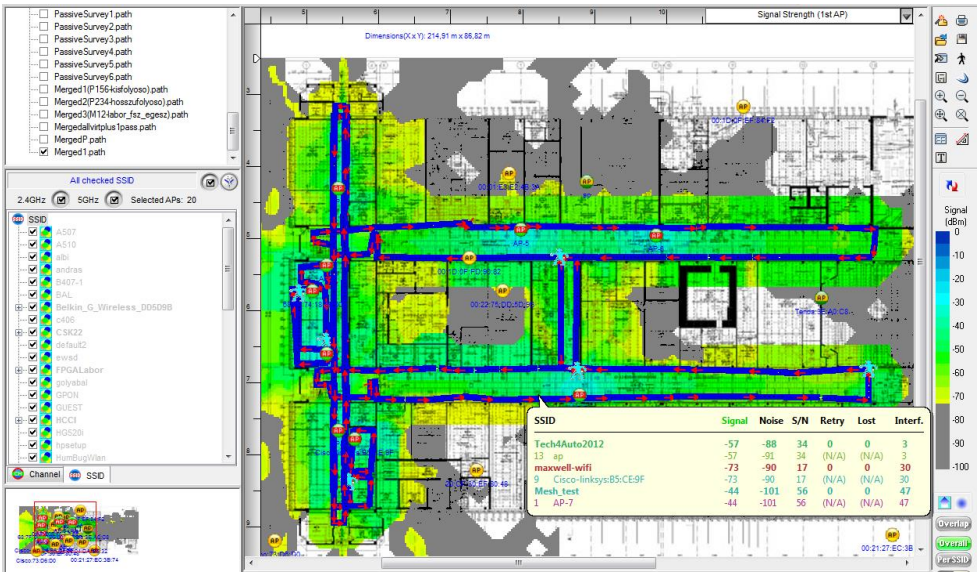
(specifikációja a mellékelt CD-n megtalálható [])

A mobil adapter folyamatosan méri a térerősséget, amely a mérni kívánt helyen leolvasható vagy folyamatosan naplózható. A mérés során a feltérképezendő területet körbejártam, folyamatosan bejegyeztem az útvonalat (szaggatott vonal) és feltérképeztem a környezetben

fellelhető mikrohullámú eszközök által indukált rádiófrekvenciás jelszint nagyságát. Ehhez ki kell választani annak módját, a feltérképezni kívánt médiumot, csatornát, mintavételi időközöket, jelszint mértékét valamint, hogy mutassa az AP-kat, illetve az asszociált STA-kat (ezeket a beállításokat a már ismertetett Configuration menüpont alatt érhetjük el).

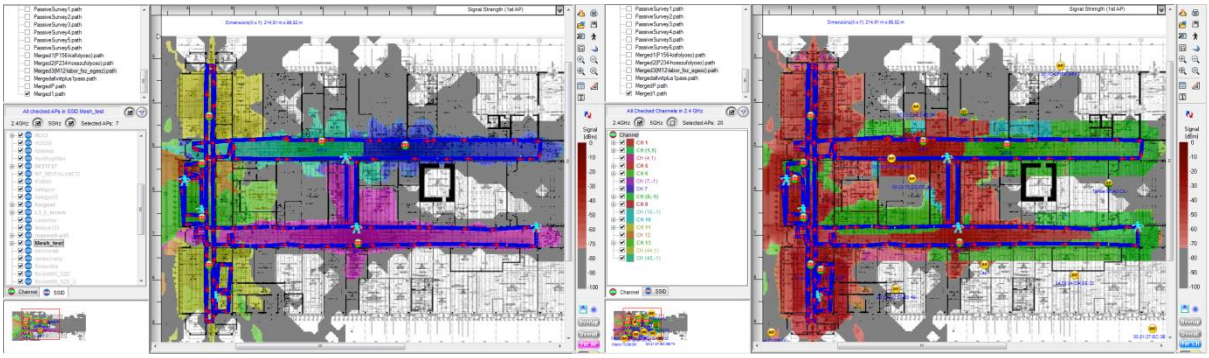
A későbbi hitelesebb eredmény miatt, a mérést a lefedettségben magadott magasságban végeztem. Lehetőség nyílik egyesített eredmények ábrázolására is a beépített Data Merge funkció segítségével. Ez a mód összerendel több feltérképezés által tárolt adatot és útvonalat, ezáltal alkotva egy átfogó összetett képet, információ halmazt a lefedni kívánt területről. (Továbbiakban az általam szimulált terv és a mért értékek merge-elt változatát mutatom be).





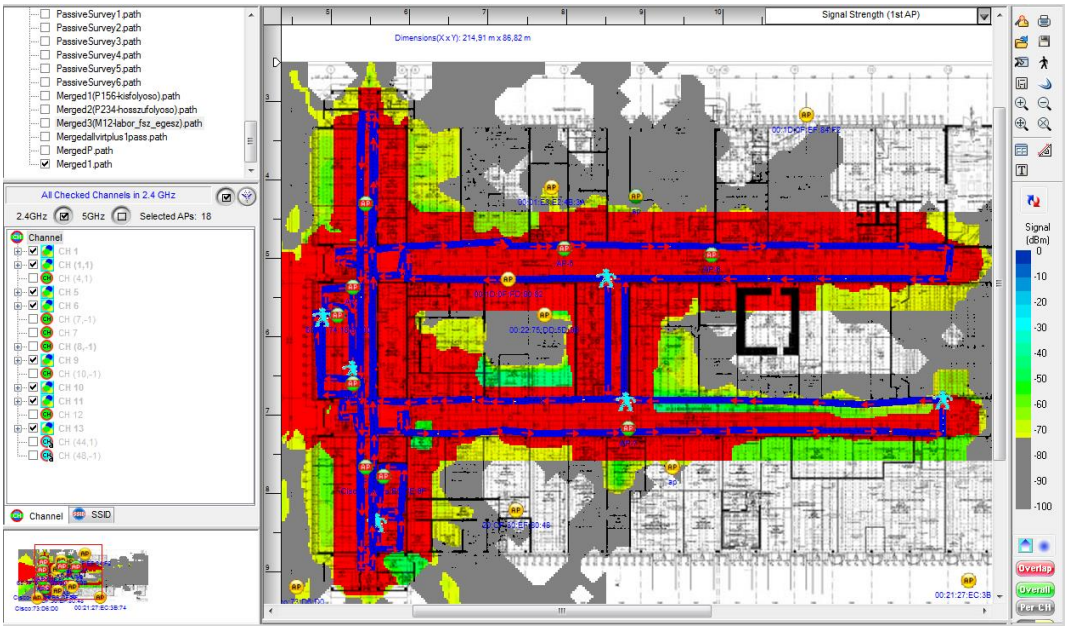
A -90 dB –es érték azt jelöli, hogy ha 1 mW a kibocsátott teljesítmény, akkor ennek csak a 10^9 –ed része ér el a mérés helyére. Gyakorlati tapasztalatok alpján elmondható, hogy a -70 dB –es érték még elfogadható térerősséget jelent. Ugyanis a jel minőségét nemcsak erőssége, hanem a környezetben fellelhető interferencia mértéke is befolyásolja. Előfordulhat, hogy a jel erős azonban minősége mégis gyenge. Ilyen esetekben nagy az interferencia, azaz kicsi az SNR.

További egyszerű analizálási módszert segíti az SSID illetve csatorna alpú megjelenítés.

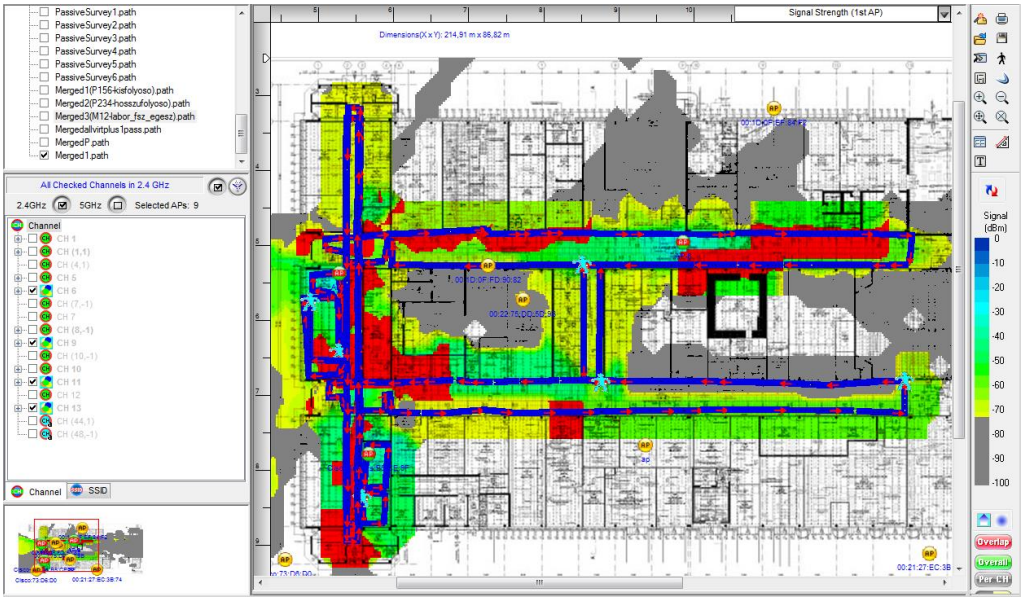


(A Per CH módon látszik, hogy problémák fognak jelentkezni, mivel a folyosók nagy részén több 1-es csatorna is elérhető.)

Overlap megjelenítés módja az átfedés és interferencia analízist segíti AP-k között. Segítségével láthatóvá válik az RF interferencia terület, illetve roaming területek.



Látható, hogy az eszközök nagy része az 1-es csatornán kommunikál ezért az átlapolódás rendkívül magas, ez a hálózat nem megfelelő, alternatív csatornákat érdemes választani (6,11,13). Ezt a következő ábra remekül szemlélteti:



- Használatának előnyei:

- Ideális AP elhelyezés és konfiguráció,
- RF interferencia- és zajterület azonosítás,
- SNR vizsgálat,
- Roaming területazonosítás,
- Kliens emuláció valós kapcsolatminőség információ gyűjtés céljából,
- Network hop optimalizáció.

A fentiekben megvalósított mérőrendszer, tervező- és mérőszoftver teljes mértékben alkalmas tetszőleges épületgeometria feltérképezésére, tervezésére, lefedésére. A generált eredmények jól alkalmazhatók a rendszer topológiájának kialakítása során. Mivel a vezeték nélküli hálózatok egyre dinamikusabban terjednek, a nagy elemszámú hálózatoknál a hálózattervezés létjogosultsága is megnő. A szimulációs tervezés, méréssel támogatott metódusa a gyakorlatban is hasznosítható.

Azonban a helyesen elkészített és mérésekkel alátámasztott hálózatterv sem garancia a WLAN megfelelő működésére. Például egy már meglévő jól működő hálózat mellé egy újat telepítenek, és ez okoz problémát. DE nagyban elősegíti annak kivitelezését és megközelítését.

A mérés során kiderült, hogy az üzemeltetés alatt használt paraméterek figyelembevételével, 5 db AP-val biztonságosan lefedhető a földszint, és további 3 segítségével az emelet is, az egyes AP-k által lefedett területek között megfelelő átfedéseket biztosítva.

A hálózat megvalósítása során már csak ellenőrző mérésekre lesz szükségünk, ami jelentős időmegtakarítás a teljes és részletes előzetes méréshez képest.

5. Vezeték nélküli hálózatok biztonsága

Az IEEE802.11 szabvány, létrejötte óta szemelőtt tartja a biztonságot. Vezeték nélküli hálózatok esetén, alap követelmény, hogy a node-ok csak a nekik szánt csomagokat dolgozzák fel, ezáltal olyan környezetet létrehozva, ahol az erőforrásokhoz csak a megfelelő jogosultság megléte mellett lehetséges hozzáférni.

Vezeték nélküli hálózatok legfőbb problémája, hogy a hálózathoz való kapcsolódáshoz nem igényeltetik fizikai hozzáférés az AP-hoz, az RF csatorna könnyen lehallgatható, mindenki számára elérhető. Az ily módon keletkező problémák elkerülése érdekében authentikáció és adattitkosítási eljárásokat definiálnak, melyeket a gyártók eszközeikbe hardvware-esen vagy szoftveresen implementálnak, elérhetővé téve a felhasználók számára. Ezek a védelmi mechanizmusokat folyamatosan biztosítani kell és teljes körű zárt rendszert kell képezniük.

Dolgozatom terjedelmi korlátok miatt, nem térek ki a biztonságtechnikai alapfogalmak, valamint azok működési elvének ismertetésére. Ezen fejezet az adatkapcsolati rétegben használt WLAN biztonságtechnikai eljárásokat ismerteti.

5.1. Alapvető WLAN biztonsági fogalmak

- *Nyílt és titkosított hálózatok*

Két csoportra oszthatók a vezeték nélküli hálózatok: nyílt vagy titkosított hálózatokra. A csoportosítás a hálózaton terjedő csomagok közvetítési módjára utal.

A korábban ismertetett WLAN szabványok mindegyike támogatja mindkét lehetőséget, viszont az alkalmazott titkosítást már nem feltétlenül.

Nyílt hálózatok alkalmazása, nevéből adódóan veszélyes, mert arra azonosítás nélkül bárki rácsatlakozhat. A biztonsági kockázatot tovább fokozza, hogy az adatok szöveges (plain text) formában továbbítódnak, ezáltal könnyen sniffelhető a hálózati forgalom.

A titkosított hálózat adott eszköz által támogatott, biztonsági szabvánnyal védett hálózat. A berendezések által használt biztonsági szabványok, erősségi sorrendben a következők: WEP, WPA, WPA2.

- *Hitelesítés*

Ellenőrzött körülmények melletti azonosítást tesz lehetővé. Biztosítja a vezeték nélküli hálózat erőforrásaihoz csatlakozó erőforrások, folyamatok megkülönböztetését.

Emellett integritásvédelmet is biztosít üzenethitelesítéssel.

Kétféle hitelesítési metódust használhatunk WLAN esetében (eltekintve a 802.1x-től):

Open System Authentication – Nyílt vezeték nélküli hálózatok nem követelnek hitelesítést, illetve nyílt rendszerű hitelesítést alkalmaznak. Első esetben, az AP minden csatlakozási kérést elfogad, így a hálózathoz bárki kapcsolódhat, elérhetővé válik számára, ha annak hatótávolságon belül tartózkodik. Utóbbi esetben, MAC cím alapján történik az azonosítás, az AP ellenőrzi, hogy a mobil állomás MAC címe szerepel-e listájában. Ezért MAC cím alapján történő hitelesítésnek is nevezik, azonban a címlisták karbantartási nehézsége miatt nem közkedvelt.

Mindkét esetben a forgalom titkosítatlan módon terjed.

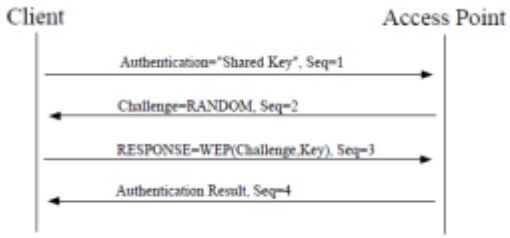
Shared Key Authentication – Titkos kulcs (jelszó) alapú hitelesítés, azonban a kulcsmenedzsment nem definiált, ezért közös kulcsot használ, melyet az elnevezés is szemléltet. Osztott kulcsú hitelesítés alatt az AP ellenőrzi, hogy a csatlakozni szándékozó állomás, rendelkezik-e a megfelelő titkos kulccsal és az alapján azonosít. A titkosított hálózat mindig autentikál, mely után a csomagok különböző kriptográfiai algoritmust használva, titkosítva terjednek tovább. Ez eredményezi a hitelesítés és a titkosítási protokollok szoros együttműködését.

5.2. Védelem az adatkapcsolati rétegben

5.2.1. Wired Equivalent Privacy

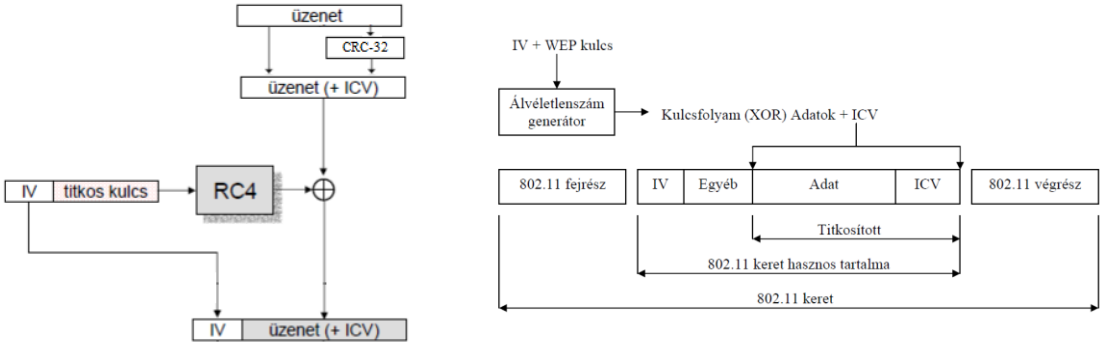
Korai IEEE802.11 biztonsági protokoll. A legegyszerűbb védelmi mechanizmus, melyet szemléltet, hogy megjelenését követően pár éven belül feltörték. Ennek oka a hibás protokolltervezés volt. A régi eszközök kompatibilitásának biztosítása végett a mai napig érvényben van.

A WEP ismeri mindkét alaphitelesítési eljárást, és amennyiben PSK hitelesítést alkalmaz, úgy a közös kulcs a WEP kulcs. Az eljárás során 4 lépéses üzenetváltással hitelesíti magát. Első lépésben a STA authenticate request üzenettel jelzi hitelesítési szándékát AP felé, ami egy generált véletlen számot küld válaszként (authenticate challenge). STA kódolja azt az üzenetet a WEP kulcsával és azt authenticate respond üzenetben visszaküldi az AP-nak. Az AP a WEP kulcs alapján dekódol, és ha az így kapott üzenet megegyezik az eredetivel, authenticate success, hiba esetén authenticate failure formában válaszol.



Sikeres hitelesítés után az adatforgalom titkosított, melynek kulcsa, a hitelesítés által használt kulcs és kriptográfiai algoritmusa az RC4 stream kódoló.

Az RC4 alapú titkosítás működése a következő:



A nyílt szöveghez egy 32 bites ellenőrző részt (ICV- Integrity Check Value) kalkulál, a csomagintegritás ellenőrizhetősége végett. Ezt az ICV rész hozzáfűzi a szövegrészhez (adat+ICV). Az RC4 kódoló inicializálásához egy 24 bites eseti kulcsot (IV - Initialization Vector) társít a titkos kulcshoz (40 vagy 104 bites WEP kulcs), majd ebből egy álvéletlen-számgenerátor létrehoz egy

Adat+ICV méretével egyező kulcsfolyamot. Ezt bitenkénti kizáró vagy (XOR) művelettel hozzákeveri az adat +ICV bitsorozathoz, így áll elő a titkosított folyam.

A titkosított bitsorozatot átvitelekor a MAC keret Protection tartalmazza az IV-t is.

Dekódolás végén Az ellenőrző összeg újraszámolódik, majd összehasonlításra kerül a fogadott, előzőleg dekódolt ellenőrző összeggel. Ha egyeznek, akkor a csomag módosítás nélkül, sértetlenül megérkezett. Amennyiben nem minősíthető érvényesnek a csomag, eldobja a rendszer.

A kódolási és hitelesítési mechanizmusból látszik, hogy több hibával is rendelkezik.

Az egyik alapvető hiba a gyenge hitelesítése, mivel az csak egyszer történik meg a hálózathoz való csatlakozáskor és csak az AP hitelesít. További gondot jelent az üzenet integritási probléma, mely a CRC lineáris voltából adódik.

Legnagyobb hibája maga a titkosítás, mivel a titkosítatlan IV kezdővektor az adatfolyamhoz hozzárendelve átkerül a vevő oldalra, ezáltal az adatforgalmat monitorozva visszafejthetővé válik a WEP kulcs (titkos kulcs). A dolgot tovább tetézi, hogy a hitelesítési kulcs, és a titkosítási

kulcs egy és ugyanaz, valamint az átlagos méretű (24bit) IV véges számú és ismétlődik (minél nagyobb az adatátviteli sebesség, annál hamarabb ismétlődik, annál gyorsabb a kódfejtés).
(További fejlesztéseket kíséreltek meg WEP esetén, azonban ezeket a vezeték nélküli eszközöknek csak egy része támogatja, és az IV alapvető problémáit nem sikerült kiküszöbölni, hiába növelték méretét (128bit) – WEP+, WEP2).)

5.2.2. IEEE802.11i

Az IEEE által jóváhagyott, jelenleg hatályban lévő biztonsági előírások szabványa. Az új koncepció neve Robust Security Network (RSN).
A WEP protokollhoz képest új kriptográfiai algoritmusokat és egy további protokollt definiál az azonosítás és hitelesítés folyamatára (korábbi vezetékes környezetben alkalmazott eljárás implementálása vezeték nélküli rendszerekhez). A következő felsorolás az újításokat tartalmazza:

- Dinamikus kulcs csere és menedzsment:

IEEE 802.1x, EAP, RADIUS

- Új titkosítási algoritmusok és erre épülő protokollok:

CCMP (AES - Counter CBC-MAC Protocol), TKIP (Temporal Key Integrity Protocol),
WRAP (AES - Wireless Robust Authenticated Protocol).

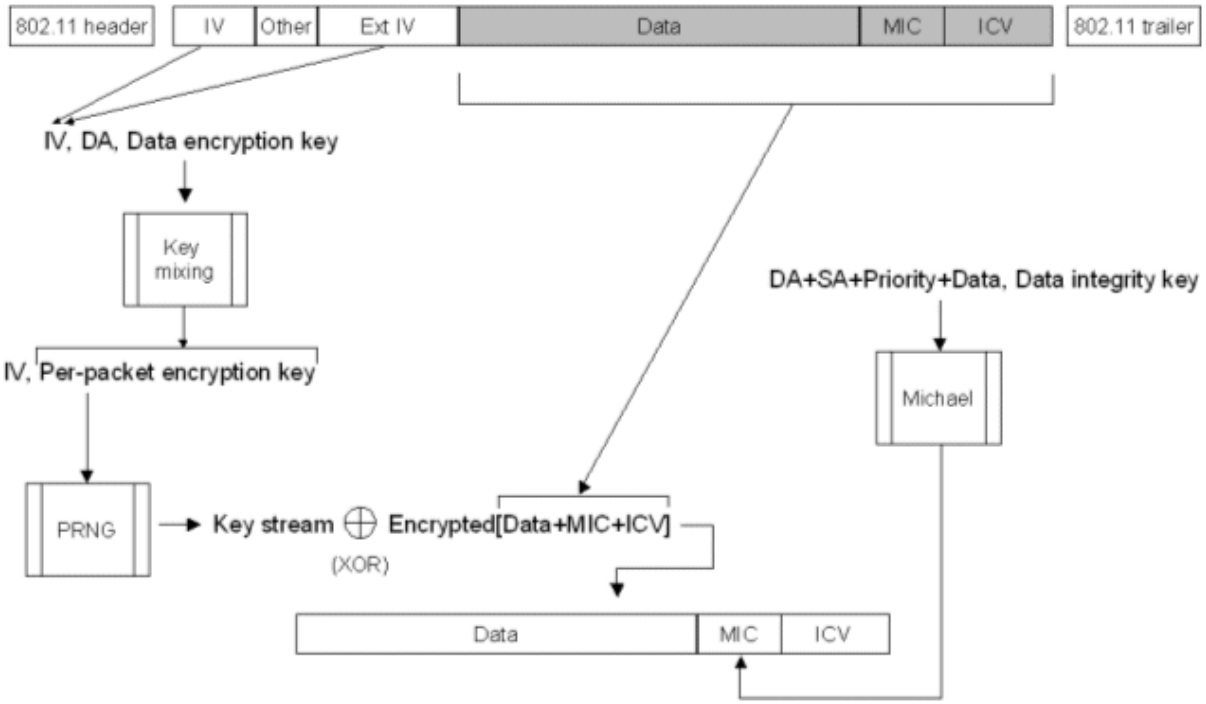
WPA,

RSN (Robust Security Network).

- Temporal Key Integrity Protocol

A 802.11i egyik alappillére, mely opcionális titkosítási lehetőséget nyújt.
Használata nem igényel új hardware-t, egy driverfrissítéssel integrálható bármely régebbi eszközbe, mely csak a WEP-et támogatja.
Sok esetben kiküszöböli a korábbi WEP protokoll hiányosságait, ilyen például, hogy szétválasztja a titkosító kulcsot a hitelesítésnél használttól, az alapkulcsot belekeveri a TKIP kulcsba, minden egyes adatcsomaghoz külön új kulcsot generál (minden TKIP csomag egy 48bit-es sorozat számot tartalmaz, mely új csomag esetén eggyel növekszik), 128bit-es RC4 kódolást használ. Az említett sorozatszám, mint az IV. Integritás-védelme is megváltozott, mely a MAC alrétegbe érkező adatokon tördelés előtt számol integritás-védő ellenőrző összeget. Az új eljárás neve Michael. ez teszi lehetővé a régi hardware-ekbe való implementálást.

Ami a WEP protokollból megmaradt, az a hitelesítési eljárás, mely továbbra is a 4-utas kézfogást használja azonosításra.



A TKIP titkosítási algoritmusa:

Első lépésként egy per-csomag kerül kiszámításra, melynek bemenetei az IV, a cél cím (DA) és az adat-rejtjelező kulcs. A Michael adatintegritási algoritmus előállítja az üzenet integritás-ellenőrző (MIC - Message Integrity Check) értéket a bemenetére érkező célcím, forráscím, adatrész (a titkosítás nélküli 802.11 payload), prioritási érték és adat-integritási kulcs alapján. Az ICV-t pedig a CRC-32 checksum-ból határozza meg. Az RC4 programozott véletlenszám generátorának (PRNG) bemenete az IV és a perpacket kulcs lesz. Ezekből előállítja a kulcsfolyamot. Ennek mérete megegyezik az adatrész+MIC+ICV összegével. A kulcsfolyam és az előbbi kombináció között logikai XOR műveletet hajt végre és létrejön a titkosított adatrész. Utolsó lépésként integrálja az IV-vel együtt a 802.11 keretbe.

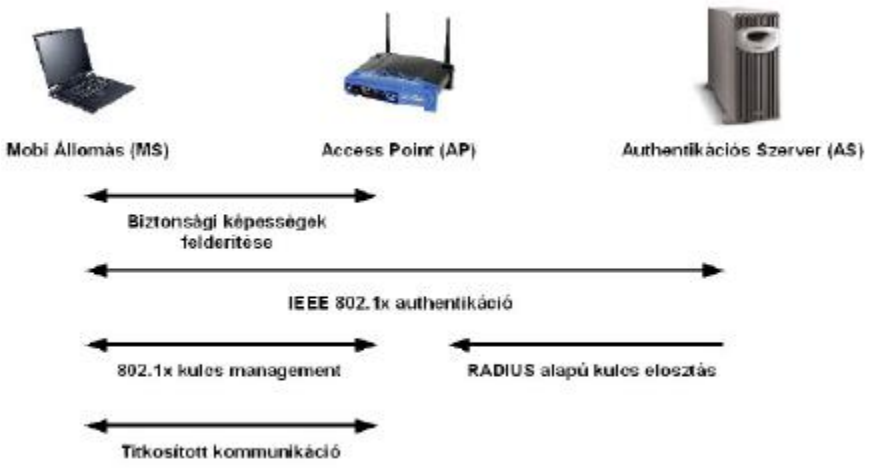
- Advanced Encryption Standard

Rijndael algoritmus alapú szimmetrikus titkosító szabvány. 128 bites blokkokat használ, 128, 192 vagy 256 bites kulcsokkal titkosítva. A blokkokat 10, 12, vagy 14 lépcsőben újrakódolja, attól függően, hogy mekkora volt a kulcs mérete.

A 802.11i szabványban az AES blokkrejtjelezőre építve, teljesen új használati módot definiáltak. Ez a mód egy kombinációs mód lett, az addig használt Counter (CTR)- és Cipher Block Chaining–Message Authentication Code (CBC-MAC) mód felhasználásával. Ezt nevezzük CCMP-nek a két mód rövidítése alapján. Az üzenetet adni kívánó fél először kiszámolja annak CBC-MAC értékét (az üzenet fejlécére is), majd az üzenethez csatolva CTR

módban kódolja (hasznos tartalom + CBC-MAC), ezáltal egy időben biztosítja az integritás-védelmet és a titkosságot. Minden egyes üzenetet sorszámmal lát el, így visszajátszástól védett. A titkosítás során a TKIP-hez hasonlóan ideiglenes kulcsokat használ (PTK), melyek meghatározására a TKIP által használt „4utas kézfogás" hitelesítési eljárást alkalmazza.
Hátránya, hogy hardveres támogatást igényel.
(A WRAP algoritmus nem kerül bemutatásra, mivel az a CCMP-hez hasonló mechanizmust használ, illetve nem elterjedt titkosítási mód a vezeték nélküli hálózatok számára.)

A szabvány az IEEE802.11 szabvány által definiált biztonságos kapcsolat felépítési procedúrát alkalmazza, mely a biztonságos csatornán való adatküldést megelőző három lépésből áll:
Képesség-felderítés, hitelesítés és kulcslétesítés.



3. ábra Az IEEE 802.11i biztonsági kommunikációs folyamatai

1.1.1.1. Képesség-felderítés (Probing)

Probing során, a STA és AP meghatározza egymás biztonsági beállításait. Ha a STA talál egy WLAN-t (SSID broadcast, vagy manuális beállítás alapján), Probe Request üzenetet küld az AP felé, amely egy Probe Response üzenettel válaszol. Az üzenet RSN-IE (Robust Security Network - Information Element) csomagot tartalmaz, amely a következőket specifikálja:
AP hitelesítő képességei, Unicast titkosítási módok, Multicast titkosítási módok.
A STA és AP között lejátszódik a már említett nyílt rendszerű hitelesítés, mely végén az AP Success üzenettel válaszol, ha nincs beállítva ez a funkció az AP-n illetve, ha szerepel a STA MAC- címe a listáján. A STA Association Request + RSN-IE csomaggal válaszol, mely saját képességeit és a hálózathoz való hozzáférés kérését tartalmazza. Amennyiben a kérés sikeres, úgy az AP Association Response - Success üzenettel nyugtáz.

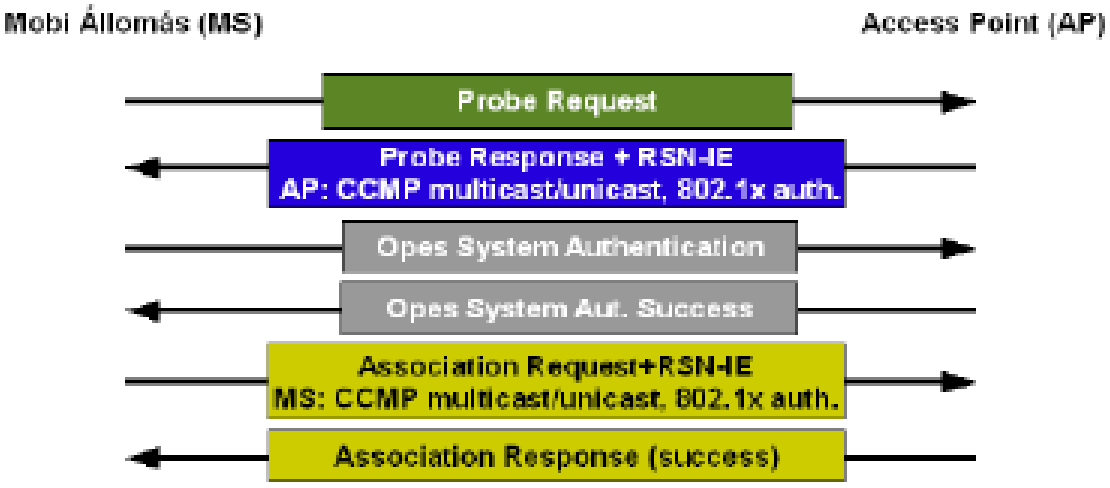
A speciális RSN-IW csomag legfontosabb mezője a képességválasztó almező (Suite Selector):

Hitelesítési és kulcs menedzsment funkciók

• 00:00:00:1 – 802.1X authentication and key management
• 00:00:00:2 – no authentication, 802.1X key management

Kulcspár és titkosító funkciók

• 00:00:00:1 – WEP
• 00:00:00:2 – TKIP
• 00:00:00:3 – WRAP
• 00:00:00:4 – CCMP
• 00:00:00:5 – WEP-104



4. ábra Az IEEE 802.11i - Discovery folyamat

1.1.1.2. Hitelesítés (IEEE802.1x)

Az IEEE802.11i szabvány a hitelesítés és hozzáférés-védelem modelljét az eredetileg LAN számára tervezett IEEE802.1X szabványból vette át. A WLAN hálózatok számára is ugyanolyan alkalmas 802.1X rendszerekben, a kliensnek és a hálózatnak is igazolnia kell önmagát, ezáltal kölcsönös hitelesítést biztosít, emellett többféle hitelesítési eljárás közül is választhatunk.

- *Hitelesítés és hozzáférés-védelem*

A hitelesítés folyamatában 3 fél vesz részt: a hitelesítendő fél (supplicant – a hálózat erőforrásaihoz szeretne hozzáférni), a hitelesítő (authenticator – a hálózathoz történő hozzáférést irányítja), és a hitelesítő szerver (Authentication server – engedélyező szerepet tölt be). WLAN esetén a supplicant egy mobil állomás, az authenticator pedig az AP. A hitelesítő szerver szerepet egy szoftver végzi el, mely akár az AP- ben, akár egy erre a célra kitüntetett hoszton futó szerveralkalmazás.

Az eredeti 802.1x szabvány port-alapú eljárást használ, azonban a WLAN eszközei, RF jelekkel kommunikálnak, ezért fizikai port helyett, a szoftver által megvalósított logikai csatlakozási

pontot használják. Ennek állapotát vezérli a hitelesítő. A logikai „porton” hitelesítés előtt csak az AS-sel kommunikálhatunk. Amennyiben a hitelesítés sikeresen lezajlott, úgy az adatforgalom engedélyezett a logikai csatlakozási ponton.

LAN esetén a hitelesítendő fél csak fizikai csatlakozáskor autentikál, egyszer. További védelemre nincs szükség. WLAN esetén fizikai kontaktus híján további kiegészítésre van szükség. Ez definiálja, hogy a hitelesítés során létre kell hozni egy titkos kulcsot a kommunikáció kriptográfiai védelmére STA és AP között, biztosítva a logikai kapcsolat védelmét.

A hitelesítés EAP (Extensible Authentication Protocol) illesztő-protokoll használatával történik, ami egy tetszőleges hitelesítő protokoll üzeneteit szállítja. Ebből következik, hogy nem az EAP végzi a hitelesítést.

Több elterjedt hitelesítő protokoll közül választhatunk (PEAP, LEAP, EAP-TLS…), azonban az illesztő-protokollba történő beágyazást külön kell specifikálni.

EAP üzentből négy van: request, response, failure és success. A beágyazott hitelesítő protokoll üzeneteit az EAP- request és EAP- response továbbítja. A fennmaradó két üzenet a hitelesítés eredményét jelzi a supplicant felé. Mivel a hitelesítést valójában az AS végzi, ezért az EAP- és a beágyazott hitelesítő protokollt az MS és AS futtatják. Az AP csak EAP üzenetek továbbítására szolgál az előbbi két fél között. Az EAP üzenetek közül csak a failure és success üzeneteket érti, így ha kap egy success üzenetet, engedélyezi MS csatlakozását a hálózathoz. MS és AP között az EAP üzenetek továbbítása EAPoL (EAP over LAN) protokoll segítségével történik. AS és AP között több megoldás is alkalmazható. Az IEEE802.11i WPA esetén RADIUS (Remote Access Dial-In User Service) protokoll, WPA2 esetén tetszőleges (EAP üzenet szállítására alkalmas) protokoll használatát írja elő. Népszerűsége miatt, azonban mindkét esetben a hálózat RADIUS-t használ. Amennyiben az AP, RADIUS képes, úgy annak segítségével egyszerű, beágyazott EAP üzeneteket továbbít és fogad az AS-től. RADIUS üzenetek esetén, egymás között statikus kulcs alapján, MD5 hash-ek alkalmazásával kommunikálnak. A négy RADIUS üzenet:

Access- Request: AP - AS irányba, lekéredzés küldése,

Access- Challenge: AS – AP, válaszüzenet, Request elfogadása után,

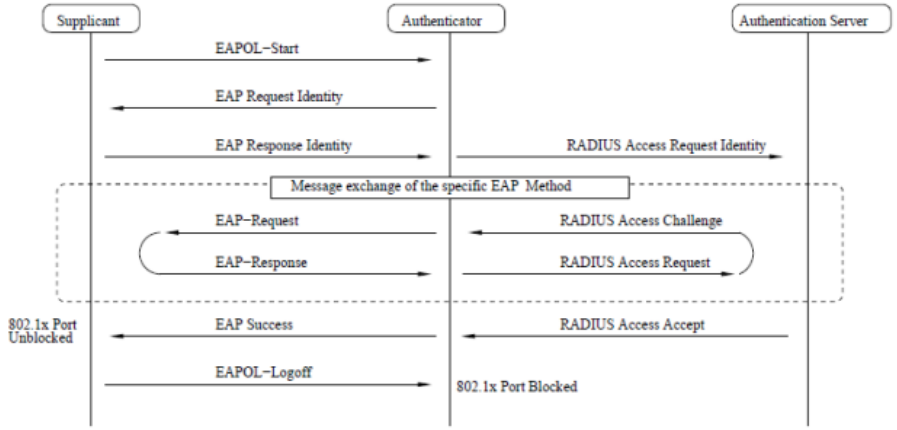
Access- Accept: AS – AP, sikeres hitelesítés esetén,

Access- Reject: AS – AP, sikertelen hitelesítés esetén.

A korábban említett kiegészítés alapján, hitelesítés eredményeként létrejön egy titkos kulcs az MS és AP közötti további kommunikáció védelmére. A hitelesítő protokoll lefutása az MS és AS között zajlik, így ezt a kulcsot csak ez a két fél birtokolja, így ezt az AP-nak is továbbítani

kell. Erre ad megoldást a RADIUS a kulcs-szállításra specifikált MS-MPPE-Recv-Key RADIUS üzenet-attribútum formájában. A kulcs az AP és AS között korábban létrehozott kulcs segítségével, kódoltan továbbítódik.

A RADIUS szerver többféle adatbázist támogat, a felhasználói információk tárolására.



- *Hitelesítő protokollok:*

EAP-MD5 - A RADIUS szerver a klienseket a felhasználó jelszavának MD5 ujjlenyomata alapján azonosítja, ezért WLAN esetében nem ajánlott a használata, mert sniffelhető az MD5 hash.

LEAP (Lightweight EAP) - Cisco által kidolgozott és használt eljárás (kompatibilitási problémákat okozhat). Kétirányú azonosítást használ, MD5 lenyomatok mellett.

EAP-TLS (Transport Layer Security) - RFC 2716 szabvány definiálja. Kétirányú azonosítást használ, PKI kulcsinfrastruktúrán alapul, X.509v3 tanúsítványokat használ MS és AS publikus kulcsának hitelesítésére. SSL-en (Secure Socket Layer) alapul. A legtöbb platformon (Linux, Windows, MacOS X) telepíthető kliens szoftver vagy modul.

Hátránya, a PKI kulcsinfrastruktúra okozta költségek.

A legbiztonságosabb hitelesítési eljárás.

EAP-TTLS (Tunneled Transport Layer Security) - EAP- TLS- PKI infrastruktúra nélküli verziója, ahol a kliens jelszóval azonosítja magát. AS számára tanúsítvány szükséges.

PEAP (Protected EAP) - Működés tekintetében egyezik a PEAP hitelesítő protokollal, viszont az eljárás mögött a Microsoft és a Cisco áll.

1.1.1.3. 2.1. Kulcs hierarchia/létesítés

Az IEEE802.11i szabvány, változást hozott a korábban használt kulcskezelésre. A korábbi rendszerek mindössze egyetlen titkos kulccsal oldották meg a hitelesítést és adattitkosítást. Az

új eljárásban dinamikus kulcskezelési – generálási hierarchiát vezettek be a kulcsok rendszeres időközönkénti cseréjére, így ez a hierarchia képezi a biztonsági magot.

- *Kulcshierarchia*

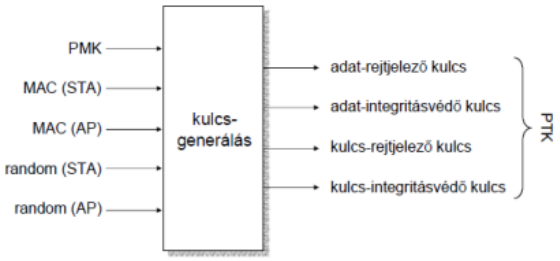
A legfelső titok a mester kulcs (MK - Master Key). Ezt a kliensnek és a hitelesítést végző eszköznek is ismernie kell, azonban nem használják közvetlenül kódolásra, hanem ebből további kulcsokat generálnak.

A következő szintet a PMK - Pairwise Master Key jelenti, melyet a hitelesítő szerver (AS – Authentication Server) és a mobil állomás (MS – Mobile Station), minden egyes bejelentkezésnél az MK-ból generál.

PMK-ból MS és AP is 4 további kulcsot generál:

Egy adatrejtjelező kulcsot, Egy kulcsrejtjelező kulcsot,

Egy adatintegritás-védő kulcsot, Egy kulcsintegritás-védő kulcsot



Ezeket együttesen páronkénti ideiglenes kulcsnak (PTK - Pairwise Transient Key) nevezik.

A PTK minden bejelentkezéskor, illetve frissítési kérelemnél újra generálódik.

A kulcsrejtjelező kulcs célja csoportos átmeneti kulcs (GTK – Group Transienk Key) titkosított kiosztása. A GTK-t multicast és broadcast üzenetek titkosítására használhatják az egy csoportban lévő MS-ek és az AP, így ezt a kulcsot az összes MS és az AP is ismeri. AP generálja és a következő részben ismertetett folyamat során létrehozott kulcsrejtjelező kulcsokkal titkosítva juttatja el az összes MS számára egyenként. A GTK tartalma egy rejtjelező- és egy integritás-védő kulcs. AES-CCMP esetén ez a kettő egy és ugyanaz.

- *Kulcslétesítés*

Célja PMK-ból PTK kulcs generálása, beállítása és verifikálása, mely „4 utas kézfogás” segítségével történik. További feladat, hogy a felek meggyőződjenek róla, hogy mindketten ismerik a PMK-t:

Először az AP elküldi az általa generált „AP-nonce”-t a MS számára, mely miután megkapta az üzenetet (RSN-IE tartalommal), ismeri a PTK előállításához szükséges összes információt (PMK, AP-nonce, MS-nonce, AP MAC címe, saját MAC címe), majd legenerálja az ideiglenes kulcsokat az EAPOL-PRF (pseudo random function) függvénnyel.

Második lépésként a MS is elküldi a maga által generált „MS-nonce”-t az AP-nek, méghozzá úgy, hogy azt ellátja kriptográfiai integritás-ellenőrző összeggel (MIC), amit a frissen kiszámolt kulcsintegritás-védő kulcs segítségével állít elő. Miután az AP veszi az üzenetet, számára is ismert a PTK számításához szükséges összes információ, majd szintén kiszámolja a PTK-t. A kulcsintegritás-védő kulcs segítségével ellenőrzi a MIC-et. Ha ez a folyamat sikeres, elhiszi, hogy MS ismeri a PMK-t.

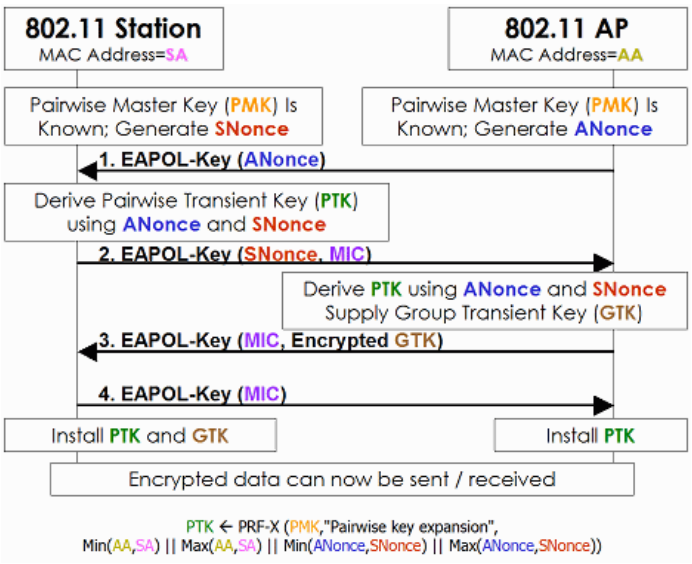
Következő lépésben az AP küld egy MIC, RSN-IE, AP-nonce-t tartalmazó üzenetet MS számára. Ebben tájékoztatja, hogy a kulcsokat sikeresen telepítette, és készen áll a további adatforgalom rejtjelezésre. Leegyszerűsítve, az AP felszólítja a klienst a PTK használatára.

Az üzenetben megtalálható egy kezdeti sorszám is, melyet arra használnak, hogy a felek által egymásnak küldött csomagokat sorszámozzák ettől az értéktől, így detektálva a visszajátszásos támadásokat.

Az üzenet vétele után MS ellenőrzi a MIC-et a kulcsintegritás-védő kulccsal, és ha az sikeres, ő is elhiszi, hogy az AP is ismeri a PMK-t.

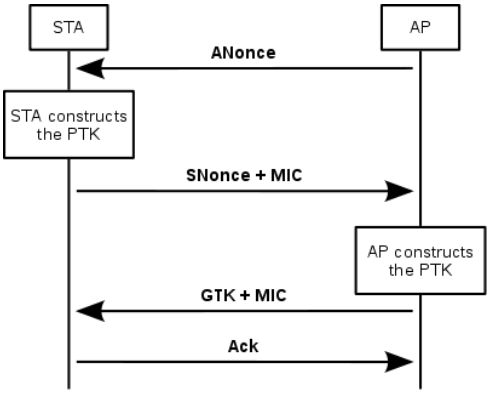
Utolsó lépésként MS nyugtázza (csak egy MIC-et tartalmazó EAPOL üzenet) az AP előző üzenetét, azaz jelzi, hogy készen áll az adatforgalom rejtjelezésére. Ezután mindkét fél beállítja a PTK kulcs TK részét adattitkosítás céljára.

Az egymásnak küldött üzeneteket a továbbiakban adatintegritás-védő és adatrejtjelező kulccsal védik.



1.1.1.4. Wi-Fi Protected Access

A WPA az IEEE802.11i szabvány részét képzi, azonban mégis elődjeként tekintendő, mivel egy ipari csoport, a szabvány elfogadása előtt definiálta és javasolta használatát.
Tervezésekor elsődleges szempont a teljes kompatibilitás megvalósítása volt, azaz mind a korábbi WEP, mind a későbbi WPA2 szabvánnyal együtt kellett, hogy működjön. Másképp fogalmazva a régi hardware-ek számára készül, mely egyben teljesíti az IEEE802.11i szabványban foglaltak egy részét.
Ahhoz, hogy a protokoll működjön, a TKIP titkosításra adaptálására van szükség, ezt a vezeték nélküli mobil állomások és AP-k egy driver frissítés révén érhetik el, amennyiben régi eszközről van szó.
A protokoll egy speciális módja, hogy vegyes módban is képes üzemelni, tehát az Access Point egyidejűleg képes kiszolgálni a WEP és WPA klienseket egyaránt. Az alkalmazott mód hátránya, hogy a fejlettebb titkosítást alkalmazó állomásoknak le kell mondaniuk a dinamikus kulcskezelésről.
Hitelesítése osztott kulcs (PSK), illetve dinamikus kulcs (802.1x – „Enterprise") alapú eljárás alapján történik.
Pre-Shared Key – WPA-PSK módban jelszó vagy hexadecimális karaktersorozat segítségével történik a hitelesítés. Ezt a PSK-t a hozzáférési ponton és a hozzá összes csatlakozni kívánó eszközön be kell állítani.
Az adatok titkosításához használt ideiglenes kódoló kulcs (TK) meghatározása 4-utas kézfogás és „nonce" (véletlenszám generátor által létrehozott szám) számok segítségével történik, azonban a kommunikáció továbbra is normál üzenetcsomagokkal történik. A PSK és az ebből generált további kulcsok (például TK) nem kerülnek átvitelre.



TK meghatározása, azaz hitelesítés után AES-CCMP vagy TKIP titkosító algoritmust használhatunk. A módszer alkalmas Ad- hoc hálózatok hitelesítési és adattitkosítási funkciójának megvalósítására, mivel az architektúrában nincs kitüntetett vezérlő állomás.

„Enterprise” – a RADIUS (központosított hitelesítő kiszolgáló rendszer) és EAP hitelesítéseket egyaránt alkalmazandó eljárás.

A kapcsolat felépítésekor, megállapodnak a felek, hogy melyik EAP változatot használják:

- EAP TLS
- EAP TTLS / MSCHAPv2
- PEAPv0 / EAP – MSCHAPv2
- PEAPv1 / EAP – GTC
- PEAP-TLS
- LEAP
- EAP-AKA
- EAP-FAST
- EAP SIM

A rendszer *több szintű felhasználói jogosultságokat is* kezel, segítségével ellenőrzés alatt tartható az erőforrásokhoz való hozzáférés.

1.1.1.5. Wi-Fi Protected Access2

A végleges IEEE802.11i szabványt alapul véve a Wi-Fi Alliance alkotta meg a WPA-hoz képest robosztusabb, komplexebb, új kriptográfiai algoritmusokat alkalmazó WPA2-t, vagy más néven RSN-t. 2006 óta, az összes Wi-Fi képes hardware számára kötelező támogatása.

A jelenleg legerősebb titkosítást (AES-CCMP) alkalmazó protokoll lefelé (WPA) kompatibilis (TKIP). Hátrány a már említett hardware függőség.

Hitelesítési eljárásai megegyeznek a WPA-nál használttal, viszont elérhető a TKIP helyett az AES-CCMP adatfolyam titkosítás.

	WEP	WPA	WPA 2 (802.11i)
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Packet Size	Concatenated	Mixed Function	Not Needed
Data Integrity	CRC-32 IV	Michael	CCMP
Header Integrity	None	Michael	CCMP
Replay Attack	None	IV Sequence	IV Sequence
Authentication	Shared Key	802.1x	802.1x
Key Management	None	EAP-based	EAP-based

5.3. Védelem felsőbb rétegekben

- *VPN (Virtual Private Network)*

A kommunikáció a hálózati rétegben, titkosított csatornán (tunnel) keresztül, végponttól-végpontig folyik. A kommunikációban résztvevő felek egy biztonságos átjárón (VPN gateway) keresztül forgalmaznak. Ezek az átjárók titkosítják a beérkező forgalmat, illetve kilépéskor dekódolják azt. A vezeték nélküli hálózatról csak IPSec forgalmat enged a vezetékes hálózatba a már említett VPN gateway-hez, VPN gateway-en keresztül, így a kliensek forgalma IPSec titkosítással védett.
Lassabb kommunikációt jelent, mint a közvetlen TCP/IP kapcsolat által biztosított.
Az IPSec protokoll alkalmazása hosszú távú megoldást jelent a biztonságos hálózati kommunikációban, hiszen célja az IP csomag védelme csomagszűréssel és a megbízható kommunikáció kikényszerítésével.
A protokoll a titkosítási szolgáltatások, biztonsági protokollok és a dinamikus kulcskezelés alkalmazásának is eleget tesz.

- *Captive portal*

Magyarul begyűjtő portálok. Fő célja a hálózati hozzáférés szabályozása, ez azonban nem nyújt védelmet a csatlakozott állomás számára.
A csatlakozni kívánó állomás, először ehhez a nyílt SSID-re csatlakozik, majd egy azonosító felület jelenik meg számára. Amíg a kliens nem végzi el a szükséges feltételeket, addig minden HTTP és HTTPS kérése átirányításra kerül az authentikációs szerverre, minden más forgalom pedig szűrve van (kivéve, amelyek a whitelist-ben szerepelnek).
Miután a kliens azonosította magát, vagy elfogadta a feltételeket (AUP - Acceptable Use Policy), létrejön a valós kapcsolat.
A kliens felőli DNS lekérés sikeresen lezajlik, majd egy HTTP kérést küld az lekérdezett címre.
A Captive portal-t üzemeltető állomás tűzfala ezt a kérést átirányítja a Redirect Servernek, amely 302-es Status Code-ú üzenetet küld válaszként és a csatlakozást kezdeményező állomást átirányítja a Captive Portal-ra.
Minden egyes átirányítást a hálózati réteg valósít meg, ezáltal a felhasználók számára teljesen transzparens a működése, valamint a Layer 3 miatt előfordulhat IP-cím probléma.
DNS lekérdezés során a CP-t üzemeltető szerver a kliens állomást egy fix DNS szerverhez csatlakoztatja (ezáltal egy DNS poisoning támadás esetén konfrontálódhat a forgalom)

5.4. Biztonsági technológiák értékelése

Összegezve az ismertetett hitelesítő és titkosítási eljárásokat, több szempontot is figyelembe kell vennünk a megfelelő védelmi mechanizmus kiválasztásához. Ilyen a biztonság szintje és

megbízhatósága, felhasználók változatossága, a hálózat kiterjedése, felhasználók igényei, és még sorolhatnánk. Sok esetben az alkalmazott robosztus védelmi megoldás a teljesítmény, kezelhetőség vagy használhatóság rovására megy. Ezért egyensúlyt kell teremteni az ellenőrzés és a használhatóság között, mivel a rendszer védelme a leggyengébb láncszem biztonságától függ. Ezen alfejezetben javaslatot teszek a megfelelő védvonal kiválasztására különböző környezetekben.

Amennyiben a legerősebb megoldást szeretnénk választani, arra az WPA2-Enterprise (AES-CCMP+ IEEE 802.1x- EAP-TLS (vagy PEAP with EAP-TLS)) titkosítási és hitelesítési eljárást alkalmazunk, mivel minden tekintetben a legerősebb védelmet nyújtja. Az ilyen rendszerbe a behatolás gyakorlatilag lehetetlen. A megoldást nagy kiterjedésű nagyvállalati, közigazgatási környezetben célszerű megvalósítani, ahol az erőforrás (anyagi és fizikai) és fenntartás nem okoz problémát.
Ha nem akarunk lemondani a titkosított hitelesítési eljárásról, úgy az IEEE802.1x PEAP-MS-CHAP-v2 vagy TTLS lehet a megoldás, mivel ez „csak” jelszó alapú titkosított hitelesítési eljárást takar. Rendszerint kis- és középvállalatok, valamint oktatási intézmények számára megfelelő.
Azokban az esetekben, mikor nem engedhető meg, vagy nem valósítható meg a hitelesítő szerver alkalmazása, használjuk az így elérhető legbiztonságosabb RSN (WPA2-PSK - AES-CCMA) megoldást. Ha régebbi eszköz áll csak rendelkezésünkre, akkor a kompatibilis WPA-PSK TKIP titkosító eljárást alkalmazzuk. Tipikusan SOHO környezetben alkalmazott védelmi technológia.
További megoldás lehet a felsőbb rétegbeli biztonsági megoldás az IPSec VPN alkalmazása.

5.5.Néhány támadási forma ismertetése

- Mérgezett hot spot

Ezek nyílt hálózatnak tűnő, védelem nélküli Wi-Fi hozzáférési pontok. Tipikusan adatszerzés céljából üzemeltetett ál hot spotok.

- Plain Text

Alapja, hogy a vezeték nélküli médiumban közlekedő csomagok mindegyike hordoz egy kis részletet a kulcsból. Amennyiben elegendő ilyen mozaikdarabbal rendelkezik a támadó, képes azt teljes egészében rekonstruálni, egy összehasonlító mechanizmust használva (egy kiválasztott szövegrészt, a titkosított szöveghez hasonlítva próbálja kitalálni a kulcsot). Ez csak

olyan esetben lehetséges, ha előzetesen, már ismert a titkosításhoz használt algoritmus, valamint egy titkosított adatrész.

- Rogue Access Point

Úgynevezett „kópé AP”. Tipikusan egy meglévő infrastrukturális hálózatban felállított, engedély- és védelem nélküli Access Point-ok, melyekhez bárki szabadon hozzáférhet, így a hálózat forgalmához is.

- Közbeékelt támadás (Man-in-the-Middle)

A hozzáférési pont és a kliens állomás közé ékelődött AP, amely elhiteti a klienssel, hogy hozzá kívánt csatlakozni, valamint elhiteti az AP-vel, hogy ő a hitelesített kliens állomás.
A támadó először passzívan figyel, begyűjti a hitelesítési információkat (AP által küldött hívó (challenge) és összerendelési üzeneteket (associate), kliens azonosítóját, IP-címeket), majd ezek birtokában kész megszemélyesíteni mind a klienst, mind az AP-t.

- Rejtett eszközök felderítése

A rejtett kapcsolódások megkerülésére szolgál. Ezáltal felfedhetővé válik az eszköz gyártója és típusa.

- War Driving

A nyílt, gyengén védett vezeték nélküli hálózatokat lokalizálja, mely során a hálózatokról begyűjtött információkat az Interneten mindenki számára elérhetővé teszik. Ehhez egy vezeték nélküli adapterrel szerelt mobil állomás, egy nagy nyereségű antenna és egy monitorozó szoftver szükséges. Gyakran GPS koordináták segítségével határozzák meg a sebezhető hálózatok pontos helyét.

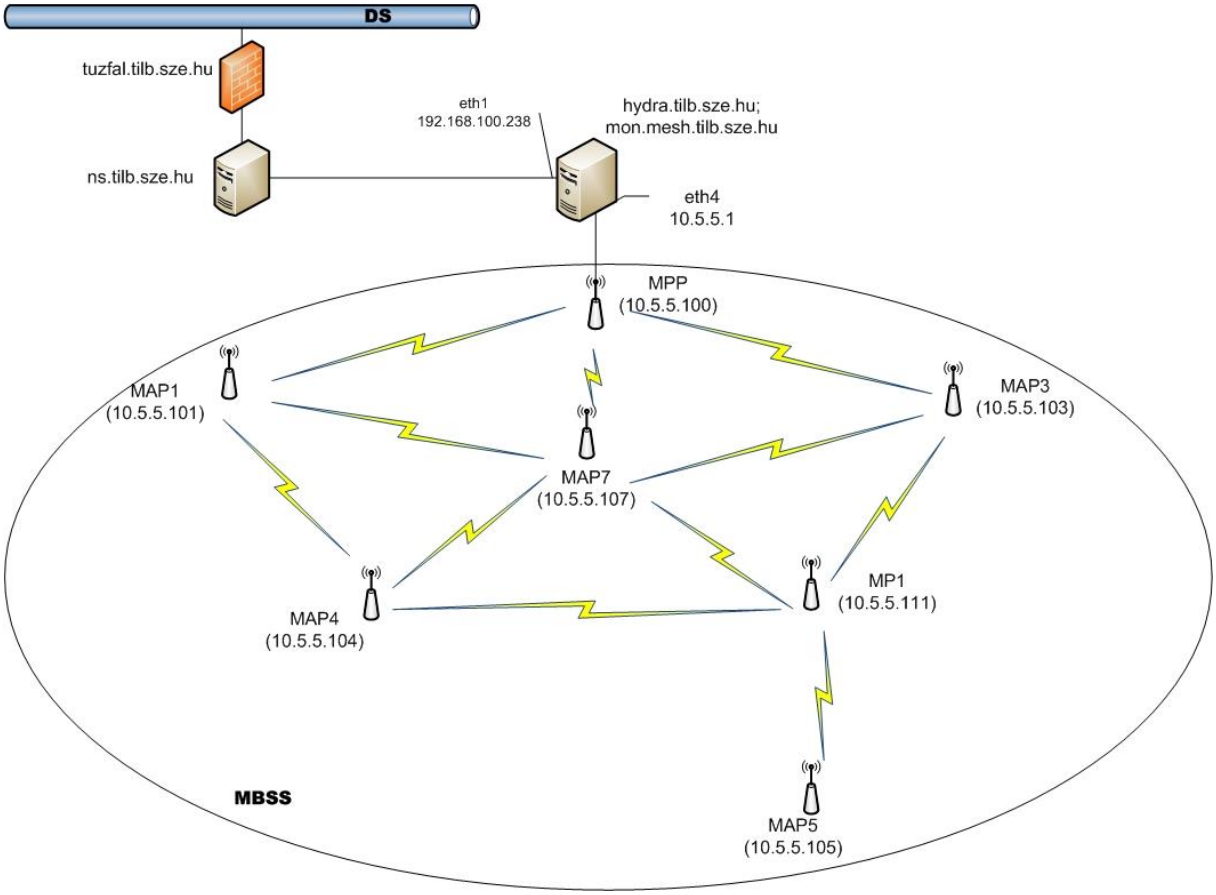
- DoS (Denial of Service)

A széles körben elterjedt szolgáltatás megtagadás támadási technika.

- Nyerserő támadás (Brute Force)
- Átirányítás rosszindulatú web helyekre

6. Kiépített hálózat vizsgálata

Miután kiépítettem a vezeték nélküli mesh hálózatot a tervezési fázis eredményei alapján, további 2 csomópontot telepítettem a laborépület földszinti folyosóira. Az egyik node a mesh portal, a másik mesh point funkciót tölt be. A módosított és a véglegesen kiépített topológiát a következő ábra mutatja.



A rádiófrekvenciás mérés során három vizsgálatot végeztem. Mértem a jel teljesítményét, az interferencia mértékét és a csatorna paramétereket.

Jel teljesítmény mérés során a vivő teljesítményét vizsgáltam és a csillapító építészeti anyagok okozta veszteséget.

Interferencia mérés során igyekeztem meghatározni a kritikus pontokat, ahol nagy a jelek közötti interferáló hatás.

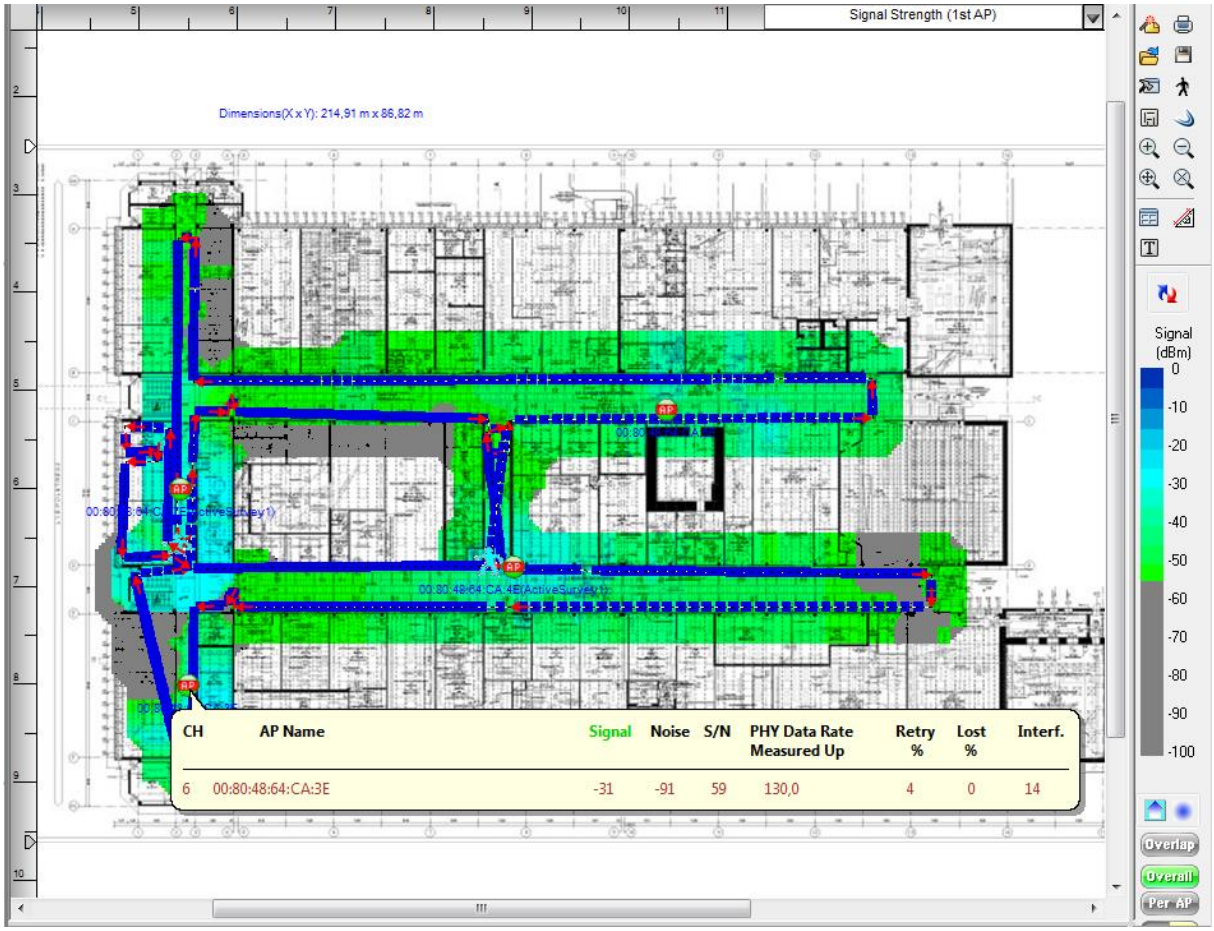
Csatorna paraméterek mérése során a roaming és átlapolódás mérése volt a célom.

6.1. Lefedettség

A hálózat lefedő képességét a már ismertetett AirMagnet SurveyPRO program segítségével végeztem. A mérés során aktív tesztet végeztem, azaz kapcsolódtam a hozzáférési pontokhoz

és bejártam a laborépületet. A folyamat során beállítottam a romaing opciót és egy threshold értéket. Amennyiben a jelszint -60dBm szint alá csökken, új átvált egy másik MAP-ra.

A mért eredményt a következő ábra szemlélteti:



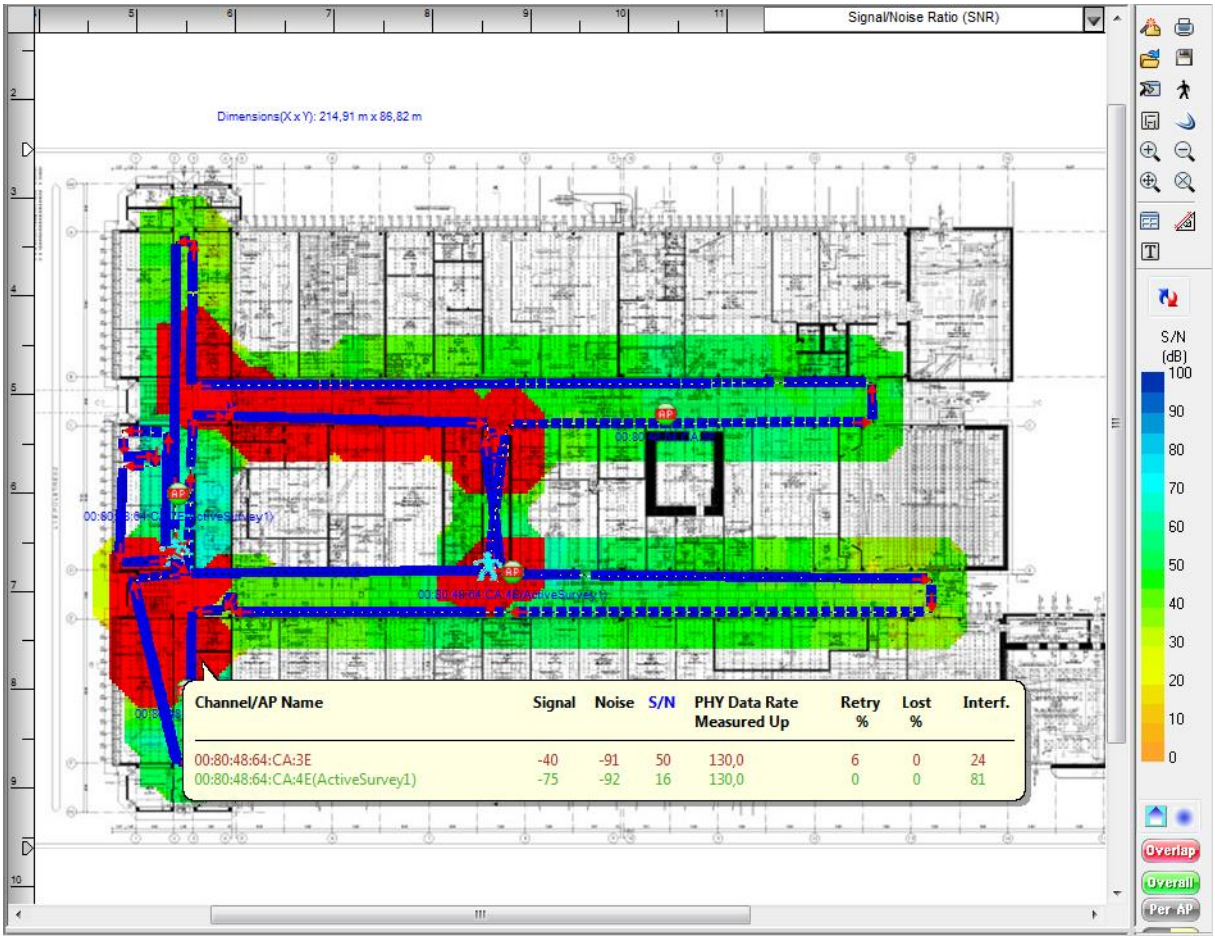
Az ábrán látható jobb oldali csúszkát addig toltam el, míg valamelyik folyosón már nem biztosított az a jelszint, ahol a görgő épp tartott. Ez alapján kijelenthető, hogy a topológia alapján a folyosó lefedettsége megfelelő, hiszen a görgő -55dBm jelszint értéke mellett a folyosók teljes mértékben lefedettek.

Interferencia tekintetében már nem ennyire jó a helyzet, mivel több olyan pont van, ahol viszonylag magas értéket képvisel ez a káros hatás:

A legsötétebb kék foltok helyén az interferáló hatás egészen nagy. Ezeken a helyeken előfordult, hogy újracsatlakozott a hozzáférési ponthoz, viszont azt a lehető leggyorsabban tette és csomagvesztés nélkül. Ezt szemlélteti a következő pár adat:

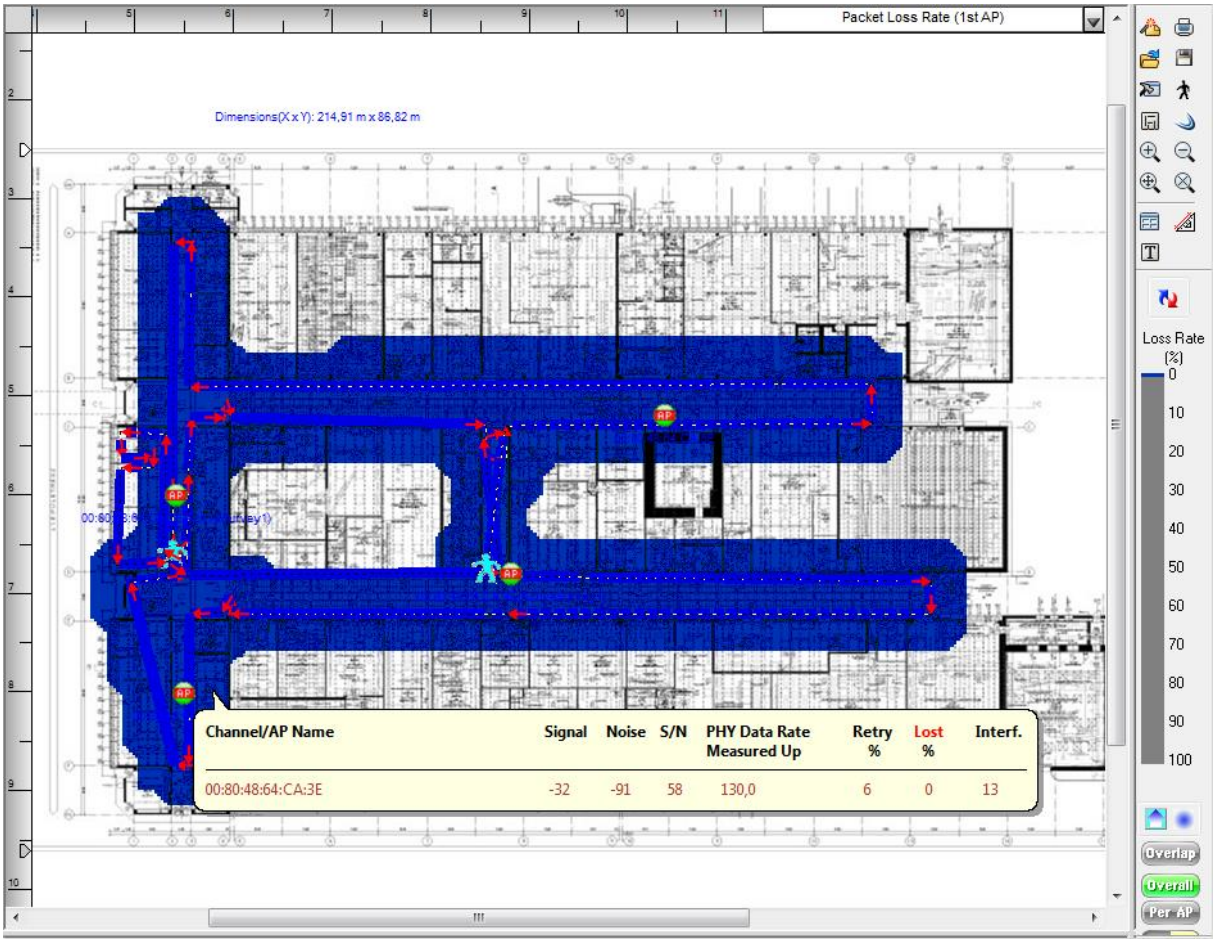
CH	AP Name	Signal	Noise	S/N	PHY Data Rate Measured Up	Retry %	Lost %	Interf.
6	00:80:48:64:CA:3E	-74	-92	18	0,0	0	0	96
6	00:80:48:64:CA:7E(ActiveSurvey1)	-75	-90	14	86,7	8	0	93
6	00:80:48:64:CA:5E	-52	-91	38	130,0	4	0	60

Mivel Single-channel rendszert alkalmaztam ezért ez a hatás elkerülhetetlen volt, annak ellenére is, hogy a laborépületben ez a csatorna a legtisztább, azaz kevés eszköz használja (a korábbi tervezési fázisban ez ismertetésre került). A csatornainterferencia helyzetét a lefedettség mellett a következő ábra szemlélteti:



A piros területek mutatják, hol van olyan átlapolódás a csatornák között, melynek hatásai károsak a jel teljesítményére nézve. Ezt az „Interf.” oszlop értekei is mutatják.

6.2.Roaming

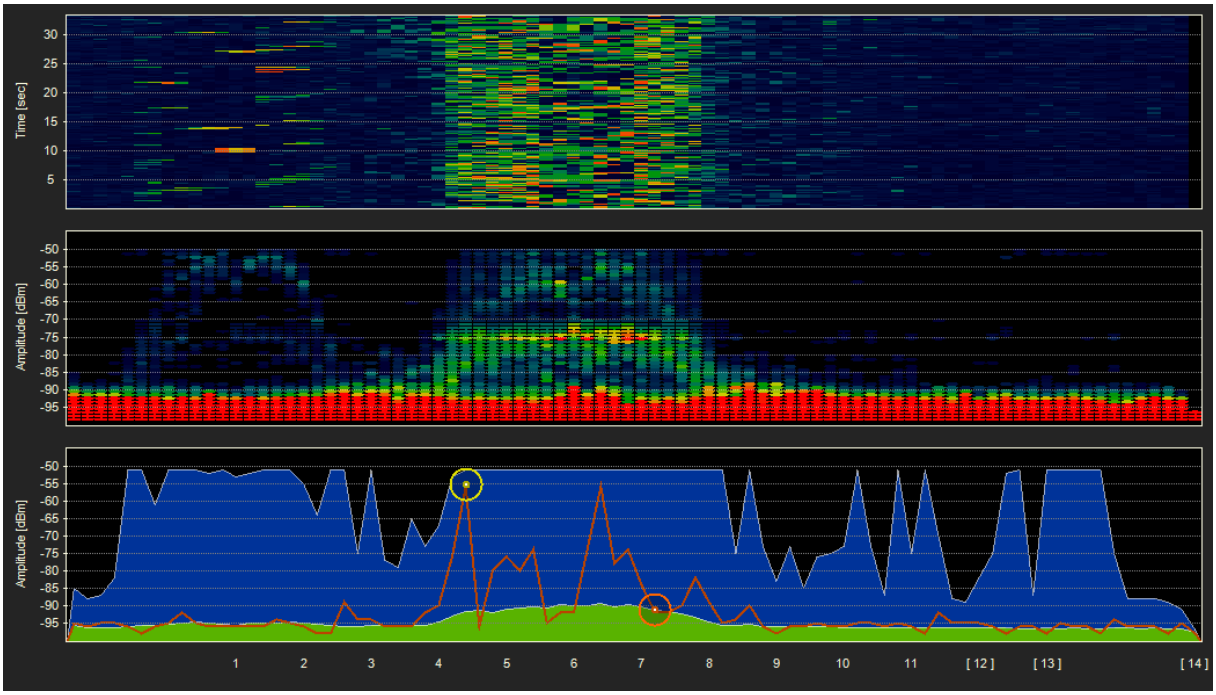


Az ábrán a csomagvesztés mértéke (packet loss rate) látható, mely alapján meghatározásra került a roaming képesség mértéke. A mérőeszköz 1 másodpercenként vizsgálta a hálózatot. A jobb oldali görgőt 0 értékre választottam, hogy felderítsem azokat a helyeket, ahol csomag kiesés volt, ezáltal nehezen váltott át egy másik MAP-ra. A mért eredmény szerint ilyen hely nem volt, azaz tökéletese újraasszociált az eszköz az egész laborépületben.

6.3.Spektrum analizátor

Wi-Spy mobil „spektrum”analizátor segítségével megvizsgáltam a használt csatorna telítettségét, valamint a közeli frekvenciákat a különböző folyosók egy-egy centralizált helyén 10 percen keresztül.

A következő ábra a távközlés-informatika laboratórium előtti RF spektrumot tükrözi, miközben folyamatos ICMP echo keretet küldtem egy külső hálózat egy hostjára.



A legalsó ábra zöld sávjában a terheltség mértéke, a kék sávban adott frekvenciákon használt maximális teljesítmény szintje látható 10 perc alatt. A felette lévő középső ábra az interferenciát mutatja, míg a legfelső gráf a használtságot mutatja időben.

Látható, hogy a mérés ideje alatt végig használatban volt a csatornánk valamint a nem átfedő 1-es csatornán is előfordult néha valamilyen kommunikáció. A középső ábra szerint interferencia nem tapasztalható és a más eszközök által használt csatornák sem zavarnak minket. Az alsó ábra eredménye alapján elmondható kevésbé terhelt a csatorna abban az esetben, ha ICMP üzenetet szórunk és emellett folyamatos a node-ok közötti kommunikáció az útvonal-választási algoritmusnak köszönhetően.

A mérés végeredményeként elmondható, hogy a tervezett hálózat, tökéletesen kielégíti a vele szemben fenntartott követelményeket. A felhasználók Internet elérését biztosítja, azonban a kritikus helyeken előfordulhatnak újrapróbálkozások, amely lassuláshoz vezethet.

A mérési eredmények és a tervezés, mérés során a SurveyPRO által készített jegyzőkönyv a mellékletben megtalálhatók. []

Összefoglalás

Irodalomjegyzék

[1] IEEE Std.802.11TM-2007, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, IEEE Computer Society, Jun.2007

[2] IEEE Wireless LAN Edition, A compilation based on IEEE Std 802.11™-1999 (R2003) and its amendments. *IEEE*, 2003

[3] http://technet.microsoft.com

[4] Official IEEE802.11 Timeline (http://www.ieee802.org/11/Reports/802.11_Timelines.htm

[5] IEEE STANDARD 802.11e-2005 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment: Medium Access Method (MAC) Quality of Service Enhancements

[6] IEEE Std 802.11n™-2009 — Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 5: Enhancements for Higher Throughput

[7] NMHH - Tájékoztató: Szélessávú adatátvitel rádiós hozzáférési eszközökkel (RLAN, WiFi, WMAN, WiMAX ...) http://www.nhh.hu/dokumentum.php?cid=9034

[8] Wikipedia - http://en.wikipedia.org/wiki/IEEE_802.11

[9] Impact of Legacy Devices on 802.11n Networks, Airmagnet (http://www.nle.com/literature/Airmagnet_impact_of_legacy_devices_on_80211n.pdf)

[10] IEEE Conference Publications: IEEE 802.11s: WLAN mesh standardization and high performance extensions May-June 2008

[11] IEEE Conference Publications: Principles of IEEE 802.11s, 13-16 Aug. 2007

[12] IEEE Conference Publications: IEEE 802.11s MAC Fundamentals, 8-11 Oct. 2007

[13] IEEE Conference Publications: Performance Evaluation of a Medium Access Control Protocol for IEEE 802.11s Mesh Networks, 27-28 March 2006

[14] IEEE Conference Publications: IEEE 802.11s - Mesh Deterministic Access, 22-25 June 2008

[15] IEEE Journals & Magazines: The IEEE 802.11s Extended Service Set Mesh Networking Standard, August 2008

[16] IEEE 802 Wireless Systems Protocols, Multi-hop Mesh/Relaying, Performance and Spectrum Coexistence

[17] IEEE Journals & Magazines: IEEE 802.11s: The WLAN Mesh Standard, February 2010

[18] IEEE P802.11sTM/D1.06, draft amendment to standard IEEE 802.11TM : Mesh Networking. IEEE, July 2007.

[19] I.F. Akyildiz, X. Wang, and W. Wang,“Wireless mesh networks: a survey”

[20] Zhang, Y., J.Luo, and H.Hu, eds., Wireless Mesh Networking: Architectures, Protocols and Standards.
[21] Ghannay, S. Gammar, S.M. és Kamoun, F., Wrieless and Mobile Networking
[22] Perkins, C.E. , Belding-Royer, E. M., and Das, S. R. Ad hoc On-Demand Distance Vector (AODV) Routing. IETF Experimental RFC3561.
[23] Airmagnet Surveyor User Guide
[24] Biztonságos Wi-Fi hálózat tervezése, Réti Zoltán, Czucz Dávid
[25] Wi-Fi Alliance - The State of Wi-Fi® Security Wi-Fi CERTIFIED™ WPA2TM Delivers Advanced Security to Homes, Enterprises and Mobile Devices
[26] Alan Holt, Chi-Yu Huang – 802.11 Wireless Networks, Security Analysis
[27] WiFi biztonság – A jó, a rossz, és a csúf, Buttyán Levente és Dóra László
[28] IEEE Std 802.11i™-2004 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements