

**Vizsgatételek a „Mobil infokommunikációs hálózatok” című tárgyból
2011 ősz**

1. Mobil távközlés evolúciója, a tanult rendszerek elhelyezése a palettán (trendek, átviteli sebességek, alkalmazhatósági területek, hálózat kiterjedése, stb.)
2. Mutassa be az OFDM működését (frekvenciaosztásos multiplexálás, Fourier transzformáció, stb.) és az OFDMA hozzáférési megoldást!
3. RFID, NFC rendszerek motivációi, típusai, főbb működési elvek.
4. Bluetooth és Zigbee hálózatszervezés
5. Bluetooth protokollok struktúra elemei és fontosabb jellemzőik
6. Adhoc hálózatok és útvonalválasztás
7. Smart metering rendszerek
8. 802.11 fizikai réteg megoldások
9. 802.11 DCF MAC réteg
10. 802.11 PCF MAC réteg
11. 802.11 menedzsment funkciók
12. 802.11 verziók
13. IPv4 és IPv6 makró mobilitás
14. IPv4 és IPv6 mikró mobilitás
15. Mobilitás HIP-pel
16. Transzport protokollok mobil környezetben
17. GSM hálózat felépítése, hálózati elemek, szerepük és az interfészek.
18. GPRS hálózat felépítése, hálózati elemek, szerepük és az interfészek.
19. GSM, GPRS és EDGE rádiós interfész.
20. UMTS rádiós interfész, QoS osztályok, HSDPA, HSUPA továbbfejlesztések
21. Az LTE rádiós interfész fontosabb jellemzői, képességei
22. Cellás hálózati architektúra fejlődése (Turányi 1)
23. SAE hálózati architektúra (Turányi 2)
24. Ismertesse az IMS architektúrát, és az IMS szerepét az NGN koncepcióban.
25. Sorolja fel és elemezze, hogy általánosságban milyen problémák jellemzik a vezeték nélküli hálózatokat biztonsági szempontból + WLAN eredeti megoldásainak tanulságai!
26. Vázolja fel mobil rendszerekben alkalmazott hitelesítés és titkosítás menetét! Mi az egyes algoritmusok szerepe és hogyan jellemezné azokat?
27. Joker: az 1-25 tételekből egy tetszőleges kiválasztása!!!

1. Mobil távközlés evolúciója, a tanult rendszerek elhelyezése a palettán (trendek, átviteli sebesség, alkalmazhatósági területek, hálózat kiterjedése, stb.)

Trendek

- (1) **globalizálódás:** világméretű hálózatok és szolgáltatások alakultak ki
- (2) **digitalizálódás:** a hagyományos átviteli rendszerek felváltása digitális eszközökkel. Minden információ „adattá” válik. Megjegyzendő, hogy az első generációs, vagyis 1G rendszerek még analóg elven működtek – nem volt egységes Európában sem.
- (3) **mobilitás:** ez a vezetékek nélküli technológiák reneszánszát jelenti. A hagyományos vezetékes rendszerek az új, mozgó távközlési szolgáltatások gyors fejlődése és rohamos terjedése a jellemző.
- (4) **integrálódás:** a különböző információk (kép, valódi adat, videó, hang) átvitele egységes technológiával történik meg. A valós idejű és a késleltetésre kevésbé érzékeny információkat egységesen kezelik. A multimédiás szolgáltatások egyre elterjedtebbek.
- (5) **konvergenciák:** a távközlés, az számítástechnika valamint a média technológiai bázisának közeledését jelenti. Azonban fontos konvergencia figyelhető meg a távközlésen belül is: a vezetékes és a vezeték nélküli rendszerek is egymáshoz egyre inkább közelednek – NGN (Next Generation Network), melynek célja az egységes menedzselhetőség, szolgáltatásnyújtás, stb. IP alapú gerinchálózaton. A konvergenciánál, mint trendnél éppen az IP hálózaté a főszerep. Így a konvergencia az alábbiakkal összegezhető leginkább: (1) csomagkapcsolt IP gerinc (2) közös szolgáltatások (3) minden hozzáférési technika támogatása (4) egységes hálózati architektúra.



Vagyis az IP egységesíti a rendszereket, mint a maghálózat legfőbb része. (Átjárók segítségével lehet az egyes hálózatokba átjutni és közös menedzsment-hálózat és kontrol-hálózat is van a maghálózatban.) Természetesen az egyes mobil technológiák között is jelentős mértékű konvergencia várható (TETRA, GSM, DECT, ERMES közeledése egy UMTS jellegű rendszer felé – IMT (International Mobile Telecomm.s)).

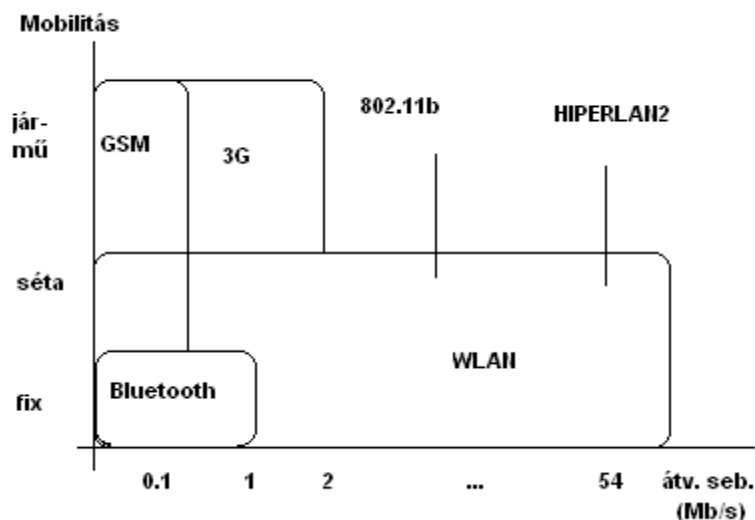
Számos új problémát kell/kellett megoldani a mobil rendszerek esetén:

- (1) mozgási sebesség ↔ átviteli sebesség (műszakilag egymással ellentmondanak)
- (2) ergonómia fontossága: kevés billentyű, kis méret, kicsi fogyasztás, stb.

Az egyes generációk rövid ismertetése – technológiák elhelyezése a palettán:

- * **1G**: analóg rendszer, beszédátvitelre, nem egységes (1980')
- * **2G**: digitális rendszer (13kbit/s), Európában egysége, beszédkodek a végberendezésben, GSM által (1990); HSCSD (High Speed Circuit Switched Data) adatsebesség növelése érdekében több csatorna kiosztása egy felhasználónak. Megjelennek új, a mobil világra jellemző szolgáltatások: SMS, MMS, WAP. Az imént említettek mind vonalkapcsolt rendszerek!!
- * **2,5G**: GPRS (General Packet Radio Service): sebesség növelésének céljából (4szerese a 2G-nek), már csomagkapcsolt!; EDGE (Enhanced Data rate for Gsm Evolution): modulációs állapotok számának növelése, kisebb hatósugárban működik, de ott gyors.
- * **3G**: UMTS (Universal Mobile Telecom. System): világméretű rendszer, mely már nagysebességű multimédiás szolgáltatásokra is alkalmas (384kb/s-2Mb/s sebességtől függően) Különböző technológiák válnak uralkodóvá az egyes 3G-s hozzáférési szintekben:
(1) **személyi hálózatok** (a személyhez kötött távk. eszköz és számítástechnikai eszközök összekapcsolása): Bluetooth vezeték nélküli helyi hálózatok (a lokális környezetben használt távk. és számítástechnikai eszközök összekapcsolása) (2) **WLAN technológia**: nagy kiterjedésű hálózatok (nagy területen mozgó távk. és számítástechnikai eszközök összekapcsolása): cellás technológiával. (3) **globális hálózatok** (földrészek összekapcsolása): műholdas technológiával
- * **4G vagy beyond 3G**: (2,5G vagy 3G) + WLAN; HIPERLAN (High Performance Radio LAN) (az egyes verzió kudarc volt, mert a 802.11a „elnyomta”), HIPERLAN2

A korszerű mobil rendszerek világa a mobilitás és az átviteli sebesség függvényében



Hálózati prognózis: A mindennapi életben a legtöbb műszaki berendezés (autó, mobil, számítógép, fűtésrendszer, stb.), mint terminál, egy közös, szélessávú, IPv6-os alapokon nyugvó (IP)hálózathoz fog kapcsolódni különböző átjárok és hozzáférési protollok segítségével.

2. Mutassa be az OFDM moduláció működését (frekvenciaosztásos multiplexálás, Fourier transzformáció, stb.) és az OFDMA hozzáférési megoldást!

OFDM alapok: ortogonális frekvenciaosztásos multiplexálás, az FDM egy speciális esete, ahol a vivőfrekvenciákat megfelelően választják meg, hogy

- (1) a vivők a lehető legsűrűbben legyenek elhelyezve
- (2) egymást minimálisan zavarják.

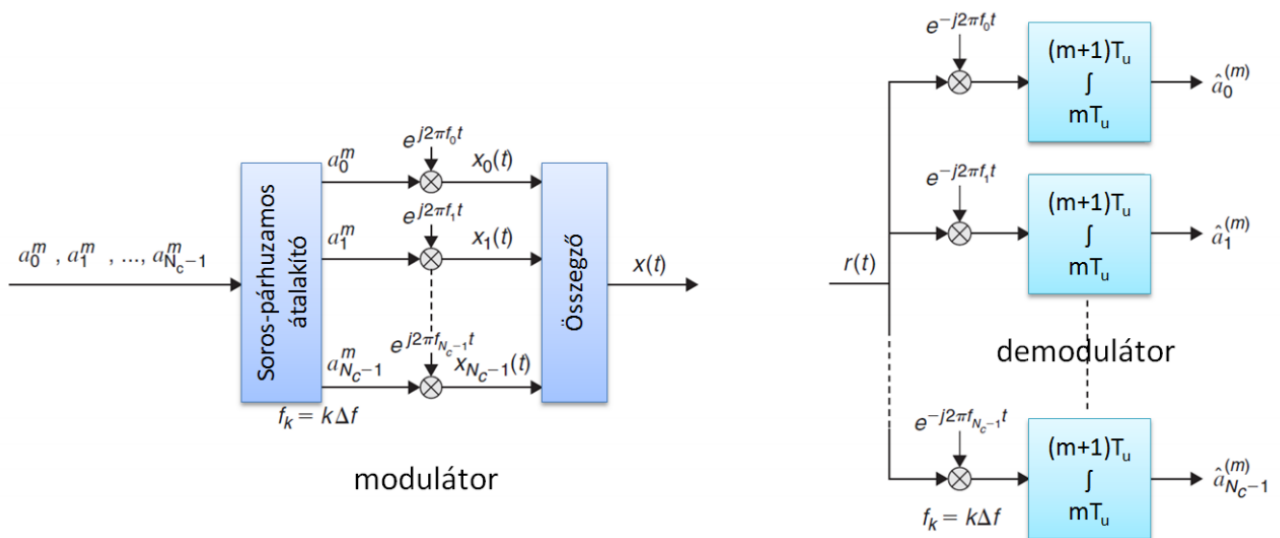
OFDM célok:

1. $t = 1/f_s$ időközönként érkező szimbólumok N darab egymástól $w_0 = 2\pi/T$ távolságra lévő vivőt modulálnak.
2. Az elemi jel: négyszögimpulzus
3. Frekvenciatartományban $\sin x/x$
4. A sávszélesség végtelen, ezért aluláteresztő szűrő szükséges

Ortogonalis alvivők: ahol egy alvivő maximuma van, más alvivő nulla. Emiatt a szomszédos alvivők zavarása minimális.

Moduláció lehetne vivőként, de ez elbonyolítaná, így azonosat alkalmaznak: digitális fázis és QAM (QPSK, 16-QAM)

Az átvitt jel időfüggvényként írható le, ezért át kell alakítani a frekvenciatartományba **Fourier-trafóval** (vissza inverz Fourier-trafóval). A digitális jelátvitel esetében diszkrét Fourier-trafó használatos (DFT), illetve ennek inverze az Inverz Diszkrét Fourier Trafó (IDFT).



3.3.ábra – OFDM modulátor (bal) és demodulátor (jobb) [2]

A diszkrét függvényértékek Fourier-transzformáltja a diszkrét Fourier-transzformációval:

$$F(n) = \sum_{k=0}^{N-1} f(k) e^{-j \frac{2\pi kn}{N}} ; \quad n = 0, 1, \dots, N-1 \quad (9)$$

ahol $F(n)$ általában szintén komplex sorokat képezhet.

Az inverz diszkrét Fourier-transzformált:

$$f(n) = \frac{1}{N} \sum_{k=0}^{N-1} F(k) e^{j \frac{2\pi kn}{N}} ; \quad n = 0, 1, \dots, N-1 \quad (10)$$

Az IDFT nagy számítási kapacitást igényel, ezért gyorsítani kell Invers Fast FT (IFFT). IFFT: különböző frekvencia komponenseknél az összegben szereplő tagok közül sok az azonos. Ezeket egyszer számolják ki, majd többször használják fel, így $\text{ordo}(n^2) \rightarrow \text{ordo}(\log n)$.

Az IFFT-hez a mintavételezések száma 2 egész számú hatványa kell legyen. A gyakorlatban a hardver gyorsítást DSP-k végzik.

ISI csökkentése

A szimbólumközi áthallás csökkentésére kitalálták, hogy a védőidőben is sugározni kell a **Ciklikus Prefixet** (CP). Ennek hossza a késleltetés szórásától függ és az adatjel hosszának tört része. Az átviteli sebesség és a bithiba növekedés között kell választani. (hosszú prefix $\leftrightarrow$ rövid prefix)

OFDMA

Ortogonalis frekvenciaosztásos többszörös hozzáférés. OFDM elv felhasználása a különböző felhasználók megkülönböztetésére. Az alvivőket külön átviteli csatornaként kezelik és tetszőlegesen hozzárendelik különböző felhasználókhoz.

Előnyei:

- a részcsatornák átvitele a szimbólumidőben gyakorlatilag fadingtől mentes
- a részcsatornák ortogonizálása és a védőidő az ISI-t jelentősen lecsökkenti
- átvitel során technikai védettséget ad
- csatornakódolással és átszövésel biztonság tovább növelhető
- FFT eljárás csökkenti a számítási műveletek számát
- időszinkronizálás és mintavételezés egyszerűbb, mint az egyvivős rendszereknél

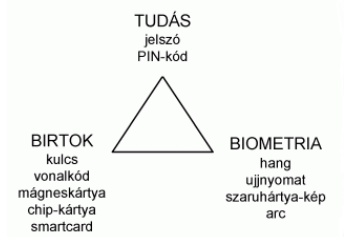
Hátrányai:

- az OFDM jel amplitúdó eloszlása
 - zajszerű
 - nagy dinamikájú
 - nagy csúcs-átlag teljesítményviszonnyal működnek, ez az erősítőkkel szemben nagy követelményeket támaszt
- az OFDM átvitel a frekvenciapontosságra és megváltozásokra sokkal érzékenyebb, mint az egyvivős rendszer a DFT sajátosságai miatt

3. RFID, NFC rendszerek motivációi, típusai, főbb működési elvek

Azonosítási rendszerek

- Felhasználó megbízható azonosítása elengedhetetlen
-> ez az informatikai rendszerek biztonságának alapja
- Ez a GYENGE PONT is egyben!
- Évtizedek alatt számos módszer született



Azonosítási rendszerek csoportosítása

Hatásfokot növeli ezen módszerek **kombinált alkalmazása!**

-> De egymástól függetlennek kell lenni a kombinációknak (Pl.:mágneskártya + PIN, de a PIN a kártyán is tárolt)

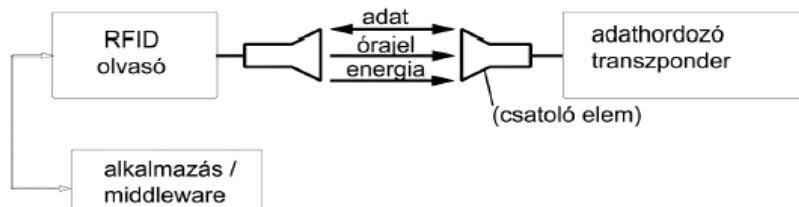
RFID – Radio Frequency IDentification

- Birtok alapú azonosítási rendszerek közé soroljuk
- Automatikus azonosítási rendszer – emberi beavatkozás nélkül olvassák ki a tag-ek adatait
- Rádiófrekvenciás működés jellemzi – különböző működési frekvenciák

RFID rendszerek felépítése

Legalább két eszközre van szükség:

- Azonosítandó
- Azonosító berendezés - adatkapcsolatot kezdeményez az azonosítandóval, mely során az egyik, vagy mindkét irányban adatátvitel történik
- **Traszponder:** azonosítani kívánt objektumon – *mikrochip + antenna*



Olvasó: olvasni és/vagy írni tudja a transzpontert

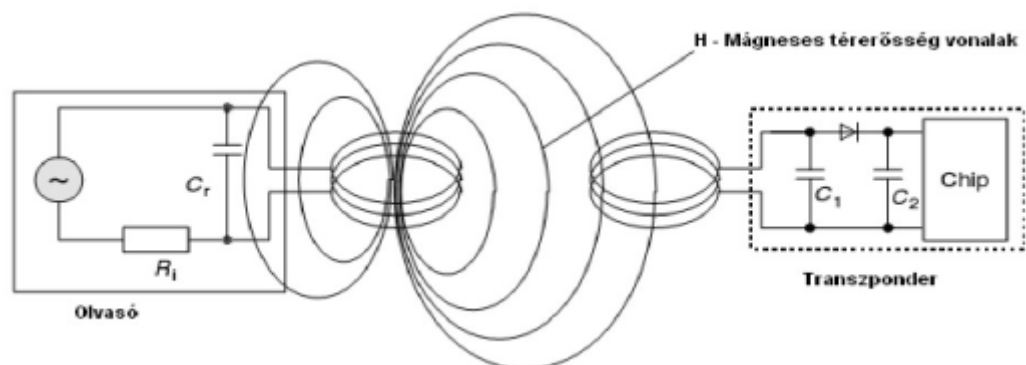
RFID rendszerek csoportosítása

- **Traszponderbe írás módja szerint**
 - Előre felprogramozott
 - Írható (EEPROM, SRAM)
- **Energiaellátás szerint**
 - Aktív – beépített tápellátás
 - Aktív – jelzésre ébred fel (díjbeszedés, ellenőrzőpont)
 - Beacon – folyamatos (nyomkövetés)
 - Passzív – energiát a mágneses/elektromos mezőből nyerik
- **Működési frekvencia szerint** (olvasó által adott jel vivőfrekvenciája)
 - LF (30..300 KHz) – low fr.
 - HF (3..30 MHz) – high fr.
 - UHF (0,3..3 GHz) – ultra-high fr.
 - Mikrohullámú (>3GHz)

Frekvencia szerinti jellemzők (táblázatosan):

Frekvencia	Előnyök	Hátrányok	Alkalmazási területek	Működés
Alacsony (9-135 kHz)	* legelterjedtebb változat * legkevésbé nyelődik folyadékokban fémekben	* 1,5 méternél kisebb olvasási távolság * nem EPC szabványos	* állatazonosítás * könyvtári nyilvántartás	* induktív csatolás
Magas (13,56 MHz)	* jelenleg is elterjedt * nedves környezetben is működik	* kicsi, közepes olvasási távolság	* raklap azonosítás * betegazonosítás * reptéri alkalmazások	* induktív/kapacitív csatolás
Ultra magas (300-1200 MHz)	* 1,5 méternél nagyobb olvasási távolság * nedves környezetben is működőképes * növekvő elterjedés * gyors adatátviteli sebesség * LF és HF tageknél olcsóbbak	* elnyelődés veszélye * Japánban nem használható	* jármű nyomon követés	* kapacitív csatolás
Mikrohullám (2,45 vagy 5,8 GHz)	* 1,5 méternél nagyobb olvasási távolság * még gyorsabb, mint az UHF	* fémek és folyadékok közelében ezek olvasási sebessége csökken leginkább	* járműbeléptetés	

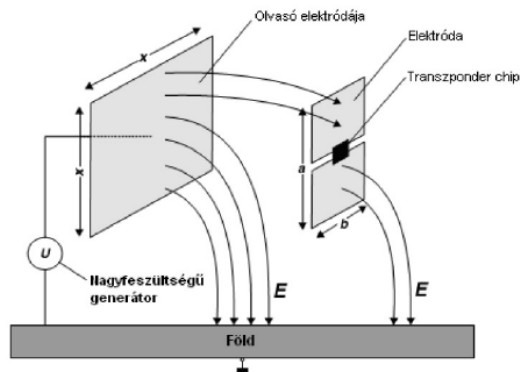
Induktív csatolás:



- olvasó antennája egy erős nagyfrekvenciás EM mező (rezgőkör) -> a transzponder tekercsében feszültség indukálódik -> chip energiaellátása. Az erős EM mező létrehozásának érdekében az olvasó antennatekercsével
- antennatekercse + C₁ hangolva: a tekercsen eső feszültség maximális (transzformátor gyenge csatolással)
- A teljesítmény-átvitel hatékonysága függ:
 - Frekvencia menetek száma a transzponder antennatekercse által körülzárt terület két tekercs egymáshoz képesti szöge

- A frekvencia növelésével a tekercs szükséges induktivitása, így annak menetszáma csökken.
 - 135 kHz-es frekvencián például 100-1000
 - 13,56 MHz-en kb. 3-10
- Legtöbbször passzív működés

Kapacitív csatolás:



- egy elektródapár vesz részt benne
- a két lemez egymással párhuzamos
- transzponder chipje a transzponder két lemeze közt helyezkedik el
- az egyik az olvasó lemezével
- a másik a Földdel képez kondenzátort
- a terhelés moduláció alkalmazható
 - ellenállás kapcsolgatásával (ohmikus)
 - egy kondenzátor kapcsolgatásával (transzponder rezonancia frekvenciáját) ezáltal az olvasó antennáján eső feszültséget amplitúdóban és fázisban egyaránt modulálja

Fő kutatási területek ma

1. Többses leolvasás
2. Helymeghatározás
3. Azonosítás, hitelesítés fejlesztése
4. Fémes környezet hatásainak kiküszöbölése
5. Újabb felhasználási területek feltérképezése

NFC olyan mint az RFID, telefonokban, aktív eszköz, pl telefonos fizetésekre használható

NFC (Near Field Communication) – A jövő

- RFID alapú 13,56MHz
- Rövid hatótávolságú rádiós rendszer
- RFID alapú 13,56 MHz
- Kb. 10 cm-ig használható
- A „kipróbált” RFID-ra épül
- Akár 424 kbps adatsebesség
- BT és WLAN kiegészítése (párosítás)

NFC előnyei

- „Piszkos” környezetben is működik
- Nem szükséges rálátás

- Egyszerű kapcsolódás
- Tápellátást is megoldja
- Szabványosított
 - Jelzések
 - Protokoll

4. Bluetooth és Zigbee hálózatszervezés

Bluetooth hálózatszervezés:

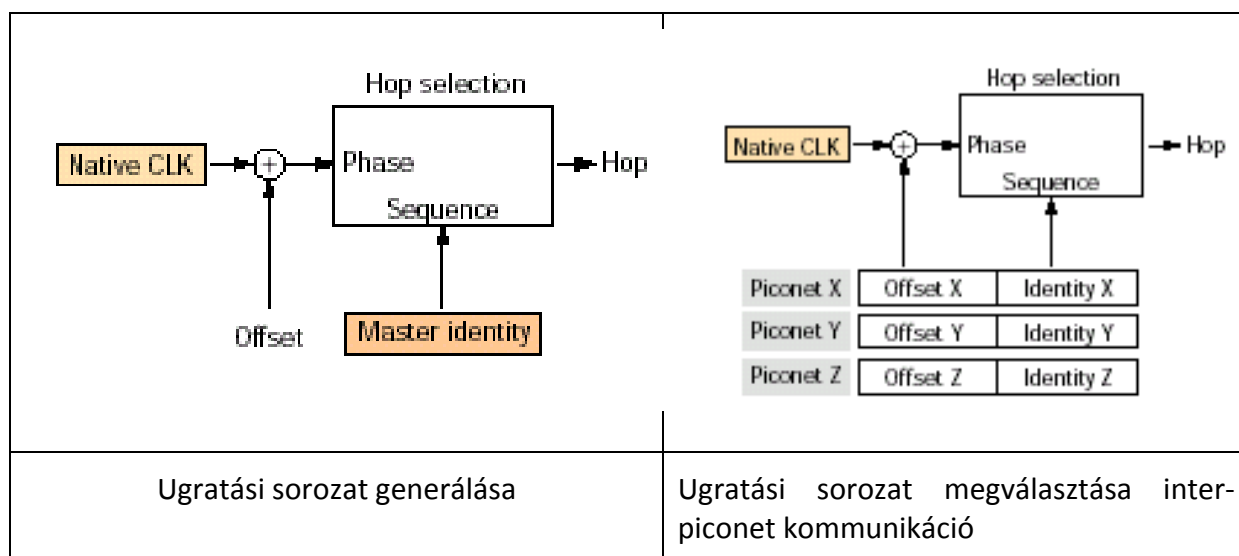
A gyakorlatban az egy alkalmazáson, Bluetooth terminológiával: piconet-en belül akár nyolc eszköz is kapcsolatban állhat egymással, akik azonos frekvenciaugratási sorozatot (kódot) használva tudtak egymással kommunikálni.

Megoldandó probléma:

- Többszörös hozzáférés az azonos kódot használók között

Piconet:

- Egy eszköz a master – forgalom irányításáért felelős
- Többi eszköz a szolga (slave)
- Működése:
 - Használt frekvencia kiválasztása a master egyedi azonosítója és belső órajele alapján történik
 - Az eszközök közötti kommunikáció alapvető információknak rendelkezésre kell állnia, így a adatcsere előtt speciális szinkronizációs eljárás szükséges
 - Slave eszközök megtudják a master egyedi azonosítóját, és mennyivel tér az az órájuk a master órájától, ezáltal képesek lesznek a közös frekvenciaugratási sorozat előállítására
 - Szükséges még a hozzáférés szabályozása a rádiócsatornához – master biztosítja időosztás segítségével – (master megmondja melyik slave melyik 625 mikrosek slotban küldheti a csomagját)



- Egy piconeten belül egyszerre egy master és legfeljebb 7 slave lehet aktív
- Problémát okozhat ha egy eszköz több piconethez is csatlakozhat, így alakulhatnak ki a scatternetbe
 - Egy piconetben csak egy master lehet, de olyan is előfordulhat, hogy egyik hálózatban az eszközünk slave a másikban pedig master

Zigbee hálózatszervezés:

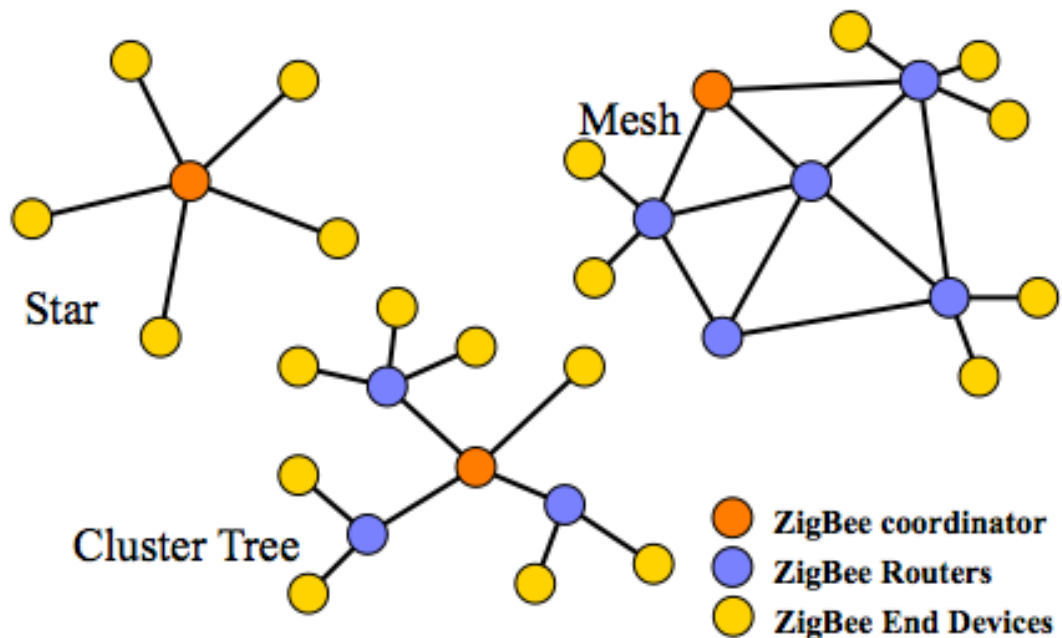
A Zigbee a IEEE 802.15.4 rádió kiegészítése alkalmazási profilokkal, amely során az alábbi célok tartották szem előtt:

- Egyszerűség
- Hosszú élettartam
- Hálózatba szervezhetőség
- Alacsony költségek (energiaellátás)
- Nagyfokú megbízhatóság

A Zigbee –t a ZigBee Alliance szervezet, amely kb.50 céget tömörít magába gondozza.

A Zigbee a hálózatszervezést a következő topológiákban valósítja meg:

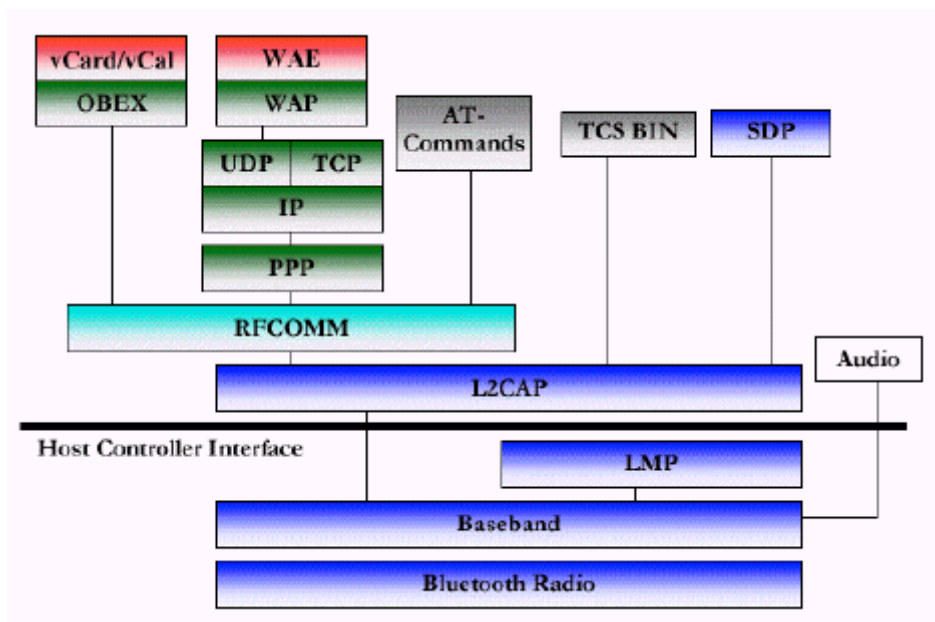
- Star
- Mesh
- Cluster Tree



	Bluetooth	Zigbee
Rádiós interfész	FHSS	DSSS
Protokollverem	250 kbyte	32 kbyte
Tápellátás	Újratöltheto	Nem újratöltheto
Eszköz/hálózat	8	255
Link/információs sebesség	1 Mbps/720 kbps	250 kbps/128 kbps
Hatótávolság	~10 m	~ 30 m

2. Táblázat: Bluetooth és Zigbee összehasonlítás

5. Bluetooth protokoll struktúra elemei és fontosabb jellemzői



Protokoll szerkezete:

- Radio
- Baseband
- Link Manager protokoll (LMP)
- Host Controller Interface
- L2CAP
- Middleware protokollok
- Applikációk

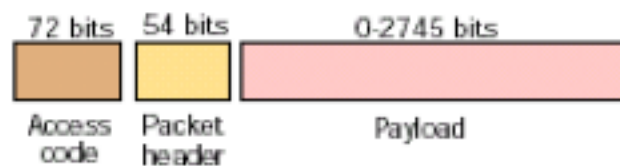
Radio:

- 2,4 GHz-es ISM sáv
- FHSS =frekvenciagratásos szórt spektrum
- 1600 hop/s, 625 mikrosek/szimbólum
- GFSK moduláció – kb. 1Mbps (bitidő 1 mikorsec, 1Mszinbólm/s)
- 79 db 1 MHz-es vivő, $f = (2402+k) \text{ MHz}$, $k=0,1, \dots, 78$
- kb 10 m-es hatósugár

- Teljesítmény osztály (3 db)
 - 20 dBm (100 mW)
 - 20 dBm (2,5 mW)
 - 0 dBm (1 mW)

Baseband:

- alapvető eljárásokat definiál a Bluetooth eszközök egymás közti kommunikációjának megvalósításához
- Definiálja a Bluetooth linket
- Definiálja a Piconet forgalmát és létrehozásának módját
- Definiálja az erőforrások megosztását piconeten belül
- Definiálja a csomagformátumot



Link Manager protokol (LMP)

- Két link menedzsment entitás között teremt kapcsolatot, segítségével állíthatóak be a Bluetooth csatonák
- Tranzakció alapú
- Feladatok:
 - Partner képességeinek kiderítése
 - Teljesítményt kímélő üzemmódok
 - Park – kommunikációnka, ha őket szólítják meg, de folyamatos szinkronizálják az órájukat, periodikusan előre definiált időtervben bekapcsolódnak
 - Hold – egy meghatározott ideig nem fogadja ACL forgalmat
 - Sniff – speciális időrésben hallgat
 - QoS
- Biztonság – végrehajtásuk ide tartozik, míg a hitelesítése és titkosítási algoritmusok a Basebandhez

Host Controller Interface:

- Inkább interfész, mint protokoll arra az esetre, ha hoszt és a Bluetooth modul külön van implementálva. Ekkor a modulon egy Host Controller-t is implementálnak
- A HCI szabványos felület a hoszt eszközök számára a szabványos Bluetooth alsóbb rétegek elérésére.
- A HCI-n keresztül utasíthatja a hoszt az alsóbb rétegeket pl. egy adott eszközhöz a kapcsolat kiépítésére, inquiry végrehajtására, hitelesítésre, teljesítmény kímélés aktiválására, stb.
- A Host Controller lefordítja a hoszt kéréseit és a modul megfelelő komponenseihez továbbítja őket. Tulajdonképpen link menedzserként működik.

Logical Link Control and Application Profile (L2CAP)

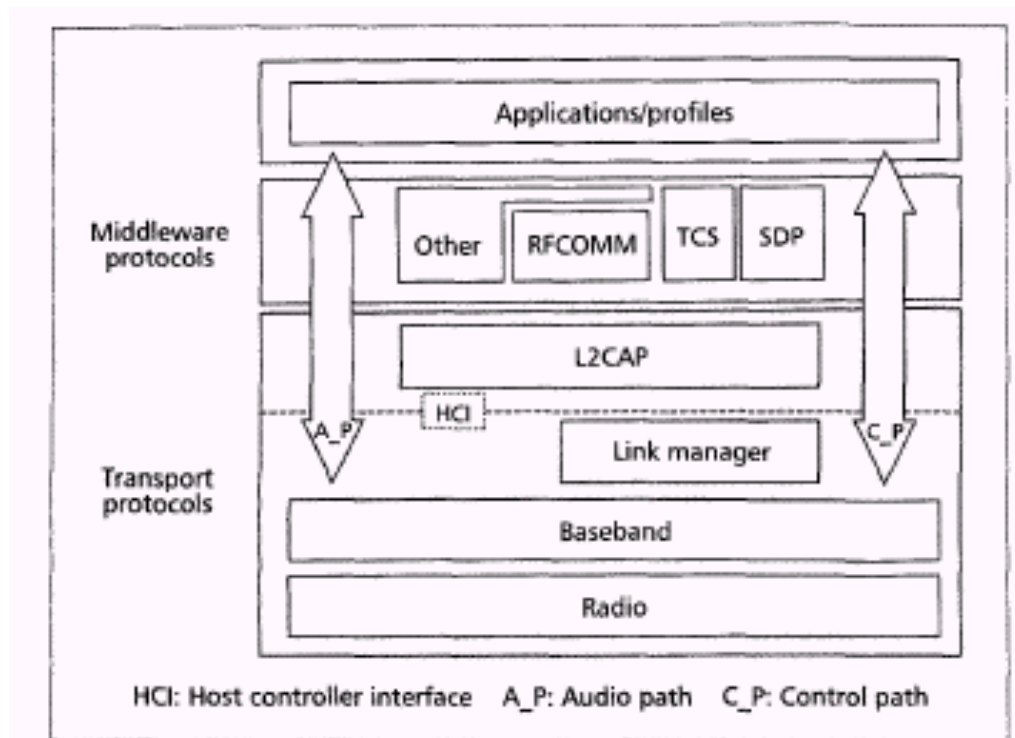
- Elrejt az alsóbb rétegek Bluetooth specifikus jellemzőit a felsőbb rétegek elől és csomag szintű illesztést biztosít a felsőbb rétegek számára.
- Itt tűnik el a mester-szolga viszony.
- Az L2CAP csomagok jóval nagyobbak lehetnek, mint a Baseband csomagok, ezért szegmentálásra lehet szükség.
 - LMP csomagok L_CH mezeje adja meg, hogy első, vagy további szegmensről van-e szó
- Az L2CAP forgalom kétféle logikai csatornán zajlik - csatorna végpontokat a Connection ID (CID) azonosítja
 - Connectionless (CL), egyirányú, nincs jelzéscsatorna, kitüntetett CID=0x'0002', de lehet más is használni
 - Connection oriented (CO), CID>0x'0002', kétirányú, kapcsolatfelépítés szükséges, jelzéscsatornát biztosítanak CID=0x'0001'-val mindkét végén. Két eszköz között csak 1 db. jelzéscsatorna lehet.
- Csomagformátum:
 - Jelzéscsatorna
 - Connectionless csatorna
 - Connection oriented csatorna

Middleware Protocol Group

- Célja a másutt szabványosított protokollok illesztése a Bluetooth-hoz.
- Csoportosítás:
 - adaptált (SDP, RFCOMM, TCS-BIN)
 - Soros port (RFCOMM)
 - Szolgáltatás felderítés (SDP)
 - IrDA alkalmazások támogatása (OBEX)
 - telefonvezérlés (TCS)
 - eredeti: IP, PPP

Application Group

- A protocol stack felett elhelyezkedő szoftverek együttese. Gyakorlatilag a Bluetooth gyártótól független alkalmazásfejlesztést tesznek lehetővé.
- Ugyanakkor néhány middleware protokollt is ide szoktak sorolni.
- Fontos elemek az ún. Bluetooth profile-ok (receptek), melyek alkalmazás elemeket definiálnak. Ezekből könnyen összeállíthatók az alkalmazások (a bevezetőben említett mintaalkalmazások is). De természetesen használatuk nem kötelező.



6. Adhoc hálózatok és útvonal választás

Kétféle típusú vezeték nélküli hálózati infrastruktúra van. Az elsőnél **infrastructured network**, fix gatewayek-kel és bázisállomással rendelkezik. A másik típus az **infrastructureless network**, másnéven Ad-hoc hálózat. A központi vezérlés nélküli, ad-hoc [Wi-Fi](#) hálózatok általában ideiglenes jelleggel jönnek létre. Ezek üzemeltetéséhez nem kell router vagy hozzáférési pont.

Ad-hoc routing protocols:

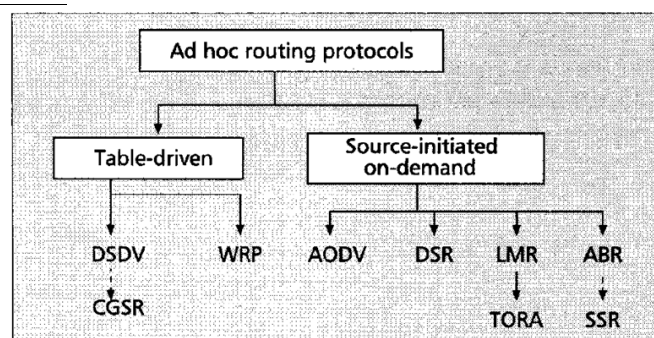
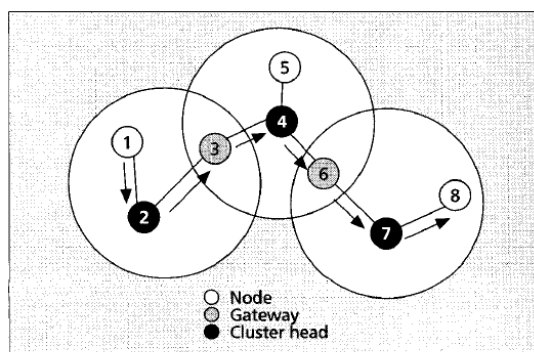


Table driven:

DSDV: Bellman-Ford routing algoritmust használ.

CGSR: Least Cluster Change algoritmust használ. Periodikus felderítés.

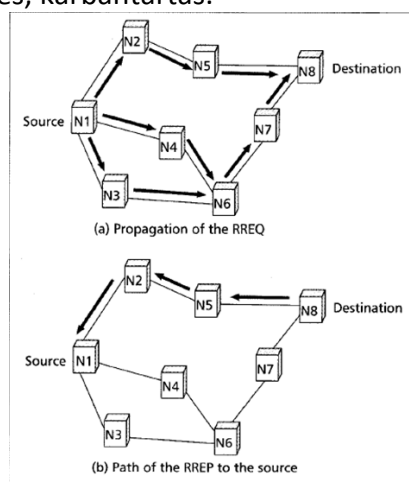


■ Figure 2. CGSR: routing from node 1 to node 8.

WRP: Minden node-nak tartalmaznia kell az alábbi táblákat: Distance table, Routnig table, Link-cost table, MRL table.

Source-initated On-Demand:

AODV: Felderítés, karbantartás.



Összehasonlítás

Paraméterek	Source-initated On-Demand	Table driven
Routing információk elérhetősége	Elérhető, amikor szükséges	Bármikor elérhető
Routing philosophy	flat	flat, kivétel CGSR
Periódikus route update	nem szükséges	szükséges
Jelzési forgalom generálása	Nő az aktív routerek számával	Nagyobb az on-demand-nál
Szolgáltatás támogatás minősége	Kis részben támogatja a Qos-t, habár a legtöbb támogatja a shortest path-t.	shortest path-t használ

7. Smart metering redzserek

Célok, lehetőségek:

- Hagyományos mérőórákat váltaná fel
- Akár az óránkénti illetve egységenként történő fogyasztás is mérhető
- Jelzési, riasztási funkciók
- Interneten keresztül továbbítja az adatokat
- Központosított
- Felhasználói szokások megfigyelése
- Új díjcsomagok
- 2015-re 130 millió háztartásban

Előnyök:

Szolgáltatói oldal:

- A mért adatok időbeli eloszlását pontosabban ismerjük
- Adminisztratív költségek csökkentése
- Veszteségek folyamatos figyelése
- Több alkalom adódik a kiskereskedelmi szolgáltatás megújítására

Fogyasztói oldal:

- Nem kell megfizetnie a mérőóra leolvasást
- Anomáliák gyors detektálása (csőtörés, gázszivárgás stb.)
- Figyelemmel kísérhető fogyasztás
- Pillanatnyi egyenleg követés

Jelenleg elérhető megoldások (szabványok):

- DASH-7
- ZigBee
- ONE-NET
- SimpliciTI
- Wavenis

Ezen technológiák legfontosabb jellemzőinek összefoglalása alább megtalálható táblázatosan. Ez alapján a DASH7 és a Wavenis emelkedik ki.

Hatékonyság vizsgálat:

A hatékonyság legfontosabb mérőszáma az egy hasznos bitre jutó energia, melyet az adott állapotokban eltöltött idő és teljesítmény adatokkal számoljuk. **[bit/Joule]**

Jele: Λ

A képletekben az eszközök következő állapotait különböztetjük meg:

- alvó mód
- felhasználói adatokat küld
- felhasználói adatokat dolgoz fel (rádiós modul kikapcsolva)

- menedzsment információt küld
- menedzsment információt dolgoz fel (rádiós modul kikapcsolva)

Az egy hasznos bitre jutó energia a táblázat legalsó sorában található:
Technológiák összehasonlítása:

Feature	DASH7	ZigBee	ONE-NET	SimpliciTI	Wavenis
International standard	ISO/IEC 18000-7	IEEE 802.15.4	-	-	-
Frequency band [MHz]	433.92	868/915 /2400 (Pro)	US: 915 EU: 866.5	480/868/ 915/955/ 2400	868 (EU) 915 (US) 433 (extension) 2400 (optional)
Indoor range [m]	20-50	10-70	60-100	10-60	200
Outdoor range [m]	1500	1500	500	1739.5 at 433 MHz 825.1 at 915 MHz 314.5 at 2.45 GHz	LOS range up to 1km 25mW; LOS range up to 4km 500mW
Transmission speed [kbps]	200	20/40/250	38.4-230.4	up to 250	4.8-100 9.6 at 433/868 MHz 19.2 at 915 MHz
Overhead bytes in PHY	20	32	15	14	7
Payload/ packet in PHY [%]	92	76	73	78	97
Latency [ms]	2500-5000 in sleep	15 in sleep	2000 in sleep typ. 50	device dependent	12.8-12800 (typ. 12800)
Scalability	15 hops	254 nodes	3 hops	2-30 nodes (4 hops)	200 nodes
Security	AES, CRC	AES, CRC	XTEA, CRC	XTEA, CRC	AES, RSA, 3DES, FEC with BCH
Technologies used in PHY/MAC	GFSK, CSMA-CA	DSSS, BPSK, CSMA-CA	2-FSK, CSMA	(G)FSK, OOK/ASK	FHSS, GFSK, SCP (Scheduled Channel Polling) similar to SMAC
Δ parameter [bit/J]	5690	2501	1003	1229	5460

Szabadtéri csillapítás számítása:

d - távolság [m]

f - frekvencia [MHz]

P_{tx} - adótéljesítmény [dBm]

G_{tx} - adó antenna nyereség [dBi]

L_{tx} - adó oldali egyéb veszteségek [dB]

L_m - terjedési veszteségek [dB]

G_{rx} - vevő antenna nyereség [dBi]

L_{rx} - vevő oldali egyéb veszteségek [dB]

L_{fs} - Line of Sight veszteség [dB]

P_{rx} - vételi teljesítmény [dB]

$$L_{fs} = 20 \cdot \log_{10} d + 20 \cdot \log_{10} f - 27,55$$

$$P_{rx} = P_{tx} + G_{tx} - L_{tx} - L_{fs} - L_m + G_{rx} - L_{rx}$$

A számítás alapján alacsonyabb frekvencián az átvitel jobb lesz. A mérések is ezt mutatják. Ezek alapján a tanszéki fejlesztésű hardver frekvenciájának 433Mhz-et választották. Beltéri jelterjedés esetén magasabb frekvencián az átvitel lényegesen rosszabb. A méréseket 433MHz-en, illetve 868Mhz-en végezték

Lehetséges hardverek összehasonlítása:

Hardver	MICA	MICAz	Telos	CC430F6137	Tanszéki
Előny	TinyOS	Gyors adattovábbítás, nagy flash	USB-n keresztül programozható	Népszerű hardver, SimliciTI	433MHz, nagy flash, nagy hatótávolság
Hátrány	Kis utasításflash, gyenge CPU	2,4GHz	2,4GHz	900MHz	Lassabb adattovábbítás

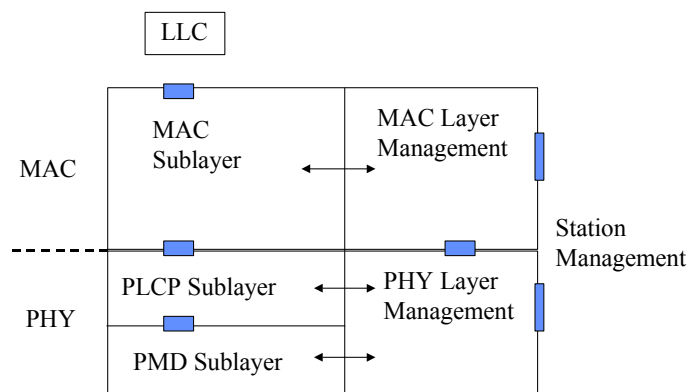
8. A 802.11 fizikai réteg megoldások

Fizikai réteg

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

4 féle megoldás létezik:

- FHSS
- DSSS
- OFDM
- Infra



2.30. ábra 802.11 protokoll entitások

Infravörös átvitel

- Hasonlóan televíziók távirányítójában levő megoldáshoz
 - Közvetlen rálátást nem igényel, hullámhossza 850-950nm
- Előnyök:
 - Egyszerű, olcsómegoldás
 - Az infravörös jelek nem hatolnak át a falakon
 - a különbözőhelységekben lévő cellák jól elkülönülnek egymástól
- Hátrányok:
 - Kis sáv szélesség
 - 1 vagy 2 Mb/s sebesség
 - Az infravörös jelek nem hatolnak át a falakon
 - Az eléréshez a hozzáférési ponttal egy helységben kell lenni
 - A napfény elnyomja az infravörös sugarakat
- Nem népszerű megoldás

FHSS

- Frequency Hopping Spread Spectrum (frekvenciaugrásos szórt spektrum)
 - 2.4 GHz-es ISM sávban
- 79 db 1 MHz-es csatorna 2.402 GHz és 2.480 GHz között (Európa, USA)
- 23 db csatorna 2.473 GHz és 2.495 GHz között (Japán)
- Álvéletlenszám generátorral előállított frekvencia ugrássorozatok
- Ha két állomás ugyanazt a kezdőértéket (seed) használja, akkor ugyanazokat a frekvenciákat fogják egyszerre végigjárni
- Időben szinkronban kell maradniuk
- 78 db ugrássorozat, mindegyik 79 csatornával (USA, Európa)
- Az 1. sorozat az USA-ban 3,26,65,11,46,19,74,50,22,64,79,32,62...
- 12 db ugrássorozat, mindegyik 23 csatornával (Japán)

Előnyök:

- Hatékony spektrumkihasználás a szabályozatlan ISM sávban
- Valamennyire biztonságos
- Aki nem ismeri az ugrássorozatot vagy a tartózkodási időket, nem tud lehallgatni
- Jó védelem a többutas csillapítás (multipath fading) ellen
- Kevésbé érzékeny a rádiós interferenciára

Hátrányok:

- Kis sáv szélesség (1 Mb/s)

DSSS

- DirectSequenceSpreadSpectrum (közvetlen sorozatú szórt spektrum)
 - Átviteli kapacitás szintén 1 vagy 2 Mb/s
 - A „hasznos” adatokat szétszórjuk a teljes frekvencia tartományban
 - XOR művelet 11 bitből álló chip-kóddal (zaj)
 - Pseudo-randomsorozat, 1-ből és 0-ból, sokkal nagyobb frekvencián mint az eredeti jel
- A zajt a fogadó ki tudja szűrni
- Vissza tudja állítani a hasznos adatokat

FHSS védettebb a keskenysávú zavarokkal szemben, mivel az egész ISM sávra kiterjed, a DSSS csak egy részére!

OFDM

- A nagyobb sáv szélesség érdekében újabb eljárásokat dolgoztak ki ('99)
- **OFDM –Orthogonal Frequency Division Multiplexing**
- 5 GHz-es ISM sávban
- Akár 54 Mb/s-os átviteli sebesség

9. 802.11 DCF MAC réteg

MAC réteg:

Ennek a rétegnek a legfontosabb feladata:

- (1) közeghozzáférés,
- (2) titkosítás,
- (3) szinkronizálás,
- (4) tördelés biztosítása.

A 802.11 MAC rétege kétféle közeghozzáférési módszert definiál:

- (1) *Elosztott*: Distributed Coordination Function (**DCF**), ahol a mobil terminálok ugyanazt az egyszerű szabályt alkalmazzák a rádiócsatorna megszerzésére, mindenféle központi „döntőbíró” nélkül, és
- (2) *Központosított*: Point Coordination Function (**PCF**), ahol a terminálok kérései alapján az **AP** (Access Point) dönt a rádiócsatorna kiosztásáról, és a döntésének megfelelően adja meg a jogot az egyes mobil állomásoknak az adásra.

Distributed Coordination Function (DCF)

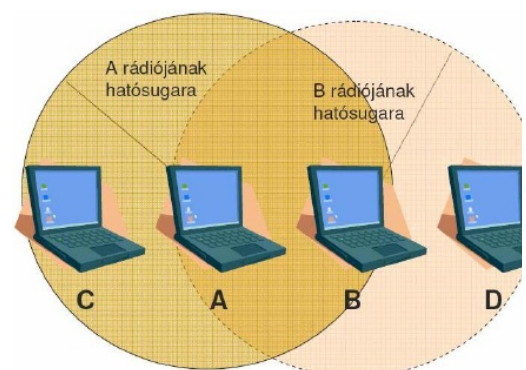
- MAC alsó alréteg funkciója
- CSMA/CA
- Nincs ütközés detektálás (Egy állomás nem tudja venni az ütközés jelet a többi állomástól)
- Különbözőkereten belüli időközök: Different Interframe Space (IFS)
 - Rövid IFS a vezérlőkeretekhez: (Short IFS = SIFS)
 - PCF IFS (PIFS)
 - Adat keretekhez: DCF IFS (DIFS)

DCF Algoritmus

- Ha a közvetítőeszköz szabad:
 - Az állomás várakozik, hogy lássa, a közvetítőeszköz IFS (InterframeSpace) ideig szabad marad-e
 - Ha az még mindig nincs elfoglalva, elkezd az adattovábbítást
- Ha a közvetítőfoglalt (vagy kezdettől fogva, vagy IFS alatt lett foglalt), az állomás folytatja a hallgatást
- Ha a közvetítőközeg szabaddá válik, az állomás vár egy IFS időnyit, majd utána választ egy véletlenszerű visszalépő ablakot (RandomBack-offWindow). Ha a visszalépő ablak eléri a nullát, elkezd adni.

RTS/CTS jelek (Handshaking)

- Olyan hálózatokban alkalmazzák, ahol nagy a versenyhelyzet az adásban.
- Jelentékeny erőforrást igényel, számottevőkésleltetést okoz
- (**M**ultiple**A**ccess with **C**ollision **A**voidance for **W**ireless)



- Virtuális csatornaérzékelés
- A szeretne küldeni B-nek
- C az A állomás vételkörzetében van
- D a B állomás vételkörzetében, de az A vételkörzetén kívül
 - A egy RTS keretet küld B-nek, és engedélyt kér egy adatkeret küldésére (**RequestToSend**)
 - Ha B megadja az engedélyt, visszaküld egy CTS keretet (**ClearToSend**)
- A elküldi a keretet és elindít egy ACK időzítőt. (Acknowledgement)
 - Ha B megkapja rendben az adatokat, válaszol egy ACK kerettel
 - Ha az A időzítője lejár mielőtt megkapná az ACK-ot, újból kezdődik az egész

10. 802.11 PCF MAC réteg

MAC réteg:

Ennek a rétegnek a legfontosabb feladata:

- (1) közeghozzáférés,
- (2) titkosítás,
- (3) szinkronizálás,
- (4) tördelés biztosítása.

A 802.11 MAC rétege kétféle közeghozzáférési módszert definiál:

- (1) *Elosztott*: Distributed Coordination Function (**DCF**), ahol a mobil terminálok ugyanazt az egyszerű szabályt alkalmazzák a rádiócsatorna megszerzésére, mindenféle központi „döntőbíró” nélkül, és
- (2) *Központosított*: Point Coordination Function (**PCF**), ahol a terminálok kérései alapján az **AP** (Access Point) dönt a rádiócsatorna kiosztásáról, és a döntésének megfelelően adja meg a jogot az egyes mobil állomásoknak az adásra.

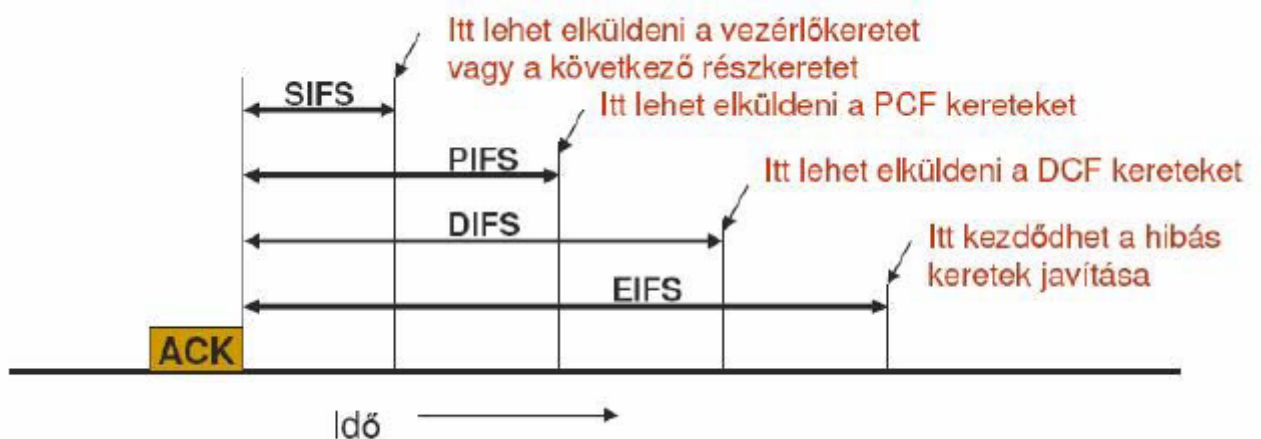
Point Coordination Function (PCF)

- A bázisállomás vezérli a kommunikációt
 - Nincsenek ütközések
- Körbekérdezi a többi állomást, hogy van-e elküldésre várókeretük
- A szabvány csak a körbekérdezés menetét szabályozza
 - Nem szabja meg annak gyakoriságát, sorrendjét
 - Nem írja elő, hogy minden állomásnak egyenlő kiszolgálásban kell részesülnie
- A bázisállomás periódikusan elküld egy beacon frame-et
 - 10-100 beacon/s
 - Rendszerparamétereket tartalmaz
 - Ugrási sorozatok és tartózkodási idő (FHSS-nél), óraszinkronizáció, stb.
 - Ezzel hívja az új állomásokat is, hogy csatlakozzanak a körbekérdezéshez
- A bázisállomás utasíthatja az állomásokat, menjenek készenléti állapotba
 - Addig, amíg a bázisállomás vagy a felhasználó fel nem ébreszti őket
 - Kíméli az állomások akkumulátorát
 - A bázisállomás pufferelem a készenléti állapotban lévőknek szánt kereteket

PCF vs. DCF

- A PCF és a DCF egy cellán belül egyszerre is működhet
 - Egyszerre elosztott és központosított vezérlés?
 - Gondosan definiálni kell a keretek közti időintervallumot
 - Egy keret elküldése után kell egy holtidő, mielőtt bárki elkezdene küldeni valamit
- Négy ilyen intervallumot rögzítettek:

- **SIFS – Short Inter-Frame Spacing**
 - A legrövidebb intervallum, a rövid párbeszédet folytatókat részesíti előnyben
 - A SIFS után a vevő küldhet egy CTS-t egy RTS-re
 - Egy vevő küldhet egy ACK-ot egy részre vagy a teljes keretre
 - A részlőket adója elküldheti az újabb részt, új RTS nélkül
- **PIFS – PCF Inter-Frame Spacing**
 - PCF keretek közti időköz
 - A SIFS után mindig egyvalaki adhat csak
 - Ha ezt nem teszi meg a PIFS végéig, a bázisállomás elküldhet egy új beacon-t vagy egy lekérdező keretet
 - Az adatkeretet vagy részlőketet küldő nyugodtan befejezheti a keretet
 - A bázisállomásnak is van alkalmá magához ragadnia a csatornát
 - Nem kell a felhasználókkal versengenie érte
- **DIFS – DCF Inter-Frame Spacing**
 - DCF keretek közti időköz
 - Ha a bázisállomásnak nincs mondanivalója, a DIFS elteltével bárki megpróbálhatja megszerezni a csatornát
 - Szokásos versengési szabályok
 - Kettes exponenciális visszalépés ütközés esetén
- **EIFS – Extended Inter-Frame Spacing**
 - Olyan állomások használják, akik egy hibás vagy ismeretlen keretet vettek, és ezt próbálják jelenteni
 - Legalacsonyabb priorítás



11. 802.11 menedzsment funkciók

Állomás csatlakozása a BSS-hez

- Egy állomás csatlakozhat egy létező BSS-hez...
 - Bekapcsolás után
 - Alvó módból való kilépéskor
 - A BSS területére lépéskor
- Passive Scanning
 - Az állomás egy BeaconFrame-et vár az AP-tól
 - Az AP periódikusan küldi azt, szinkronizációs információt hordoz
- Active Scanning
 - Az állomás megpróbál egy AP-t találni magának
 - Probe Request kereteket küld
 - Probe Response választ vár az AP-ktől
- Ha több AP válaszol, kiválasztja a „legjobbat”
 - Legjobb jel/zaj viszony

Roaming

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

1. Egy csomag alapú LAN rendszerben a cellaváltás megvalósítható két csomag átvitele között, szemben a cellás telefonnal, ahol ez beszélgetés közben is bekövetkezhet. Ez lényegesen egyszerűsíti a handovert, de
2. egy beszéd alapú rendszerben az időszakos megszakadás nem okoz gondot a beszédátvitelben, miközben csomag alapú rendszerben lényegesen csökkenti a hatékonyságot a felsőbb rétegbeli újraadások miatt.

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

A hitelesítési eljárás (Authentication Process)

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

Teljesítménykímélő üzem

- Mivel a mobil állomásoknál a telep teljesítmény fontos, a 802.11-ben definiálták a teljesítménykímélő üzemmódot.
- Az üzemmód lehetővé teszi az állomások számára, hogy alvó állapotban lehessenek hosszabb ideig is, információvesztés nélkül.
- Működés: AP tárolja az alvó állomásoknak érkező csomagokat addig, amíg polling kéréssel nem kéri azokat, vagy üzemmódot nem vált. A beacon üzenetekkel terjeszti, hogy kiknek tárol üzeneteket. Az állomások felébrednek, és ha számukra érkezett üzenet, polling üzenetet küldenek az AP-nek.

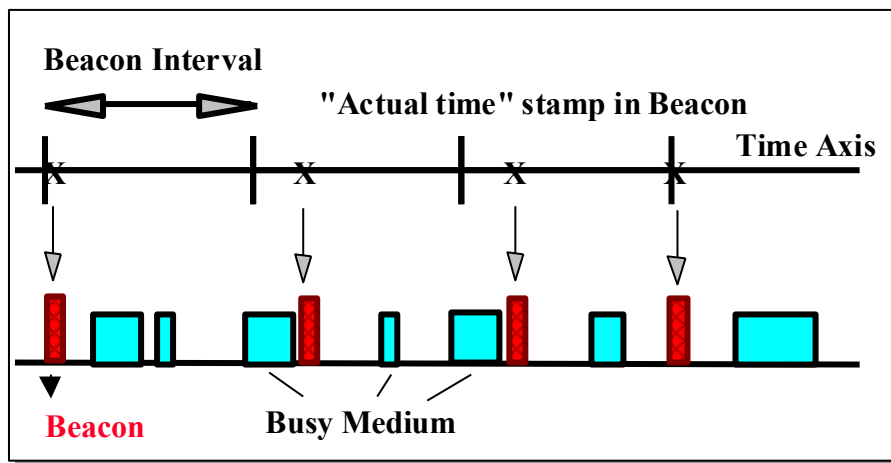
- Multicast és Broadcast üzeneteket az AP tárol, és egy előre meghatározott időpontban szétküldi ezeket (DTIM-enként, ami a TIM többszöröse). Ha valaki kíváncsi ezekre, felébred, és veszi.

Szinkronizáció

- A szinkronizáció biztosítására a szabvány egy időszinkronizáló eljárást definiál (Timing Synchronization Function, TSF), amely minden egyes állomásban működik, ennek a feladata a teljesítmény menedzsment támogatása, a versenymentes eljárás során ez jelöli ki a versenymentes időintervallum kezdetét, frekvencia ugratásos fizikai réteg esetén pedig az új ugrási frekvencia alkalmazásának kezdetét és az ugrás hosszát.
- Az AP periodikusan ún. Beacon Frame-eket ad. Ezek a keretek tartalmazzák az AP órájának értékét az adás pillanatában (figyelem, ez az adás tényleges időpontja és nem amikor a sorba beállt a keret. Mivel a Beacon Frame-t a CSMA szabályok szerint küldik, ezért az átvitel lényeges késleltetést szenvedhet).
- A vevő állomás a vétel pillanatában ellenőrzi az óráját és kijavítja, ha szükséges az AP órájához való szinkronitás megőrzéséhez. Ez megakadályozza az óra elcsúszását, ami néhány órás üzem után bekövetkezne.
- A szinkronizáció fenntartásához egy állomásnak nem kell minden beacon jelet vennie. A beacon jelek az időzítési információn kívül más információt is visznek (teljesítmény menedzsment, barangolás).

A beacon jelek átvitelének folyamata:

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



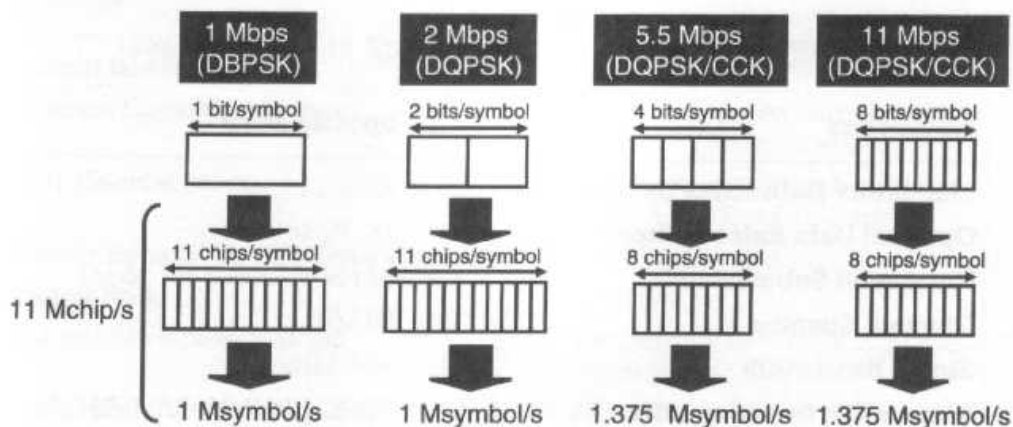
2.20. ábra Beacon jelek átvitelének folyamata

12. A 802.11 verziók (802.11 a,b,g részletesen és az új verziók).

A 2,4 GHz-es ISM sávban üzemelő eredeti 802.11 rendszert leíró szabvány 1997-ben jelent meg. Azóta pedig folyamatos fejlesztéseket végeztek rajta, ráadásul egymással párhuzamosan működő csoportok. Az új verziókat 802.11x jelöléssel látták el az ABC kisbetűit használva. Azonban a betűk sorrendje nem jelent egyértelmű időbeli sorrendet. Sokkal inkább valamilyen szempont szerinti továbblépést.

802.11b: Manapság ez a legszélesebb körben elterjedt WLAN. Előnye, hogy a szűkösebb 2,4 GHz-es ISM sávban képes megnövelt (5,5 illetve 11 Mbps a fizikai rétegben) átviteli sebességet biztosítani. A továbblépést az alap 802.11-nél is alkalmazott direkt szekvenciális CDMA kódjainak kicserélésével érték el. Ez az előrelépés a hálózati rétegben maximálisan 5,5 Mbps-os átviteli sebességet jelent.

A sebesség növekedést a DQPSK CCK-val (Complementary Code Keying) érték el (lásd ábra). Az 5,5 Mbps-os CCK használata során 4 bitet kódolnak bele 8 chipbe oly módon, hogy 2 bit kiválaszt egyet a 4 lehetséges komplex kód közül és a másik két DQPSK modulálja ezeket. 11 Mbps-os CCK-nál 6 bit alapján választanak a 64 kódból és a maradék kettővel szintén DQPSK-val modulálják a kódokat. Mindeközben nem változtatnak az alap verzió chip sebességén. Tehát nem az eredeti Barker-kódokat használják.



Sebességek összevetése

802.11a: A változtatás a fizikai réteget érintette. Megnyitotta az utat az 5GHz-es ISM sávba, ahol nagyobb sáv szélesség áll rendelkezésre. Ennek megfelelően nagyobb átviteli sebességek is elérhetők. Ez a verzió az igen korszerű ortogonális frekvenciatartománybeli multiplexálást alkalmazza (Orthogonal Frequency Division Multiplexing, OFDM), ugyanazt, amit a HiperLAN2 is.

Az elérhető maximális átviteli sebesség a fizikai rétegben 54Mbps-ra növekedett, ez a hálózati rétegben azonban csak 32Mbps, ami persze jóval több az eredeti 1,2 Mbps-nál.

802.11e: A MAC réteget érintette a változás, megjelent a szolgáltatásminőség (késleltetésre, csomagvesztésre korlát vállalása), vagyis a QoS biztosítása.

802.11i: Bővített biztonsági funkciókat tartalmaz.

802.11g: A 2,4 GHz-es sávban OFDM alkalmazásával eléri az 54 Mbps-os fizikai rétegbeli átviteli sebességet.

802.11n: nagysebességű WLAN (100 Mbps felett)

802.11r: VoIP és más valós idejű szolgáltatások WLAN felett

802.11s: szenzor hálózatok kapcsolódása WLAN AP-khez

13-14. IPv4 és IPv6 makró és mikro mobilitás

- A továbbiakban először tisztázzuk a **makro** és a **mikro** mobilitás fogalmát.
- A mikro mobilitás megoldás javaslatok csoportosításával és az egyes csoportok alapelveivel foglalkozunk.
- Két alapvető handover típust különböztetünk meg: tartományok közötti, és domain-on belüli cellaváltásokat:
- Az egyik az intra-domain handover, ami egy jól definiált területen (ún.: mikro mobilitás domain) belüli cellaváltásokra vonatkozik. Ezt kezelik a mikro mobilitás protokolljai.
- Makro mobilitásról pedig akkor beszélünk, ha két domain között mozog a mobil terminál, amit inter-domain handovernek nevezünk. Ezt már a mobil IP kezeli.
- A mikro mobilitás algoritmusainak egy fontos célja, hogy minél gyorsabban próbálják lebonyolítani az intra-domain handovereket, ezzel növelni az elérhető teljesítményt, a hálózat kihasználásának hatásfokát, és minimalizálni a felhasználó adatfolyamának megszakítását.

A mobil IP nem alkalmas a mikromobilitás kezelésére, javasolt erre a célra külön protokollt alkalmazni, ami képes együttműködni a globális mobilitást biztosító mobil IP-vel.

Makro mobilitás IPv4-el és IPv6-al:

MOBIL IPv4

Az IP protokoll 4-es verziójának (IPv4) tervezésekor egyáltalán nem gondoltak a mobilitás kezelésére. Azonban, mivel még napjainkban is az IPv4 az egyik legelterjedtebb hálózati protokoll, szükség volt úgy kiegészíteni az alap-specifikációt, hogy képes legyen az egyre szélesebb körben elterjedő mobil csomópontok (Mobile Node, MN) kezelésére. Ezért fejlesztették ki az IPv4 számára a Mobil IP-ként emlegetett kiegészítést, mely már képes a mobilitás kezelésére.

Az IPv4 alap-specifikációját több tulajdonsága is korlátozta a mobilitás kezelésében, azonban a legfontosabb ezek közül a protokollban használt hierarchikus címzési rendszer, melyben az **IP címeknek kettős szerep jutott**. Egyrészt globális azonosítóként szolgálnak a hálózathoz kapcsolódó csomópontok megkülönböztetésére, másrészt meghatározzák a hozzájuk rendelt csomópontok helyzetét a hálózatban. E két funkció egymásnak ellentmondó feltételeket támaszt, ha egyszerre akarunk egyszerű útvonalválasztást (*routing*) és mobilitáskezelést megvalósítani.

A Mobil IP ezt a problémát úgy oldja meg, hogy lehetőséget ad egy MN-nak, hogy két IP címet használjon.:

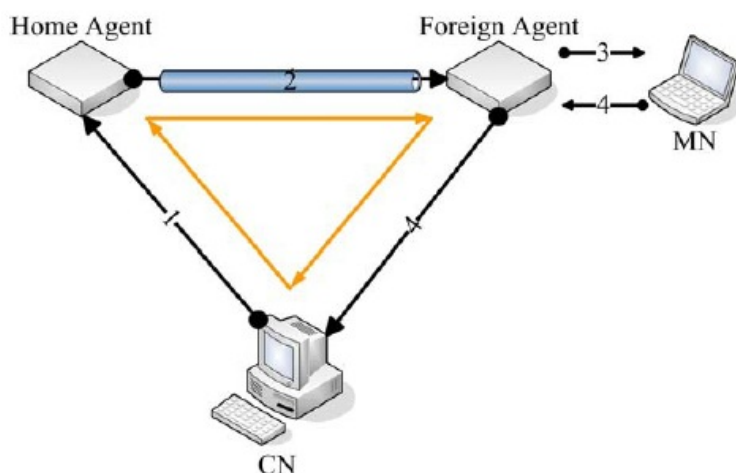
- Egyet a csomópont azonosítására (*otthoni cím, Home Address*),
- egy másikat pedig arra, hogy a mobil csomópontnak szánt csomagok eljuthassanak rendeltetési helyükre, tehát útvonalválasztásra (*közvetett cím, Care-of-Address*).

Az otthoni cím egy olyan, viszonylag hosszú életű IP cím, amely az otthoni hálózatában (*Home Network*) azonosítja a mobil csomópontot. A MN ezt a címet használja az általa

küldött IP datagrammok forrás-címeként. Ha a MN elhagyja az otthoni hálózatát, akkor kap egy közvetett IP címet, amely a MN aktuális kapcsolódási pontját adja meg. A működéshez a két IP címen kívül szükség van két speciális hálózati entitásra is:

- Az egyik az *otthoni ügynök (Home Agent, HA)*. Ez egy olyan router a MN otthoni hálózatában, amely továbbítja a MN-nak küldött csomagokat a MN aktuális kapcsolódási helyére, azaz az aktuális közvetett címre, valamint karbantartja a MN két IP címe közötti összerendelést.
- A másik szükséges hálózati entitás az ún. *idegen ügynök (Foreign Agent)*, amely egy router a MN által meglátogatott (idegen) hálózatban, és azért felelős, hogy az otthoni ügynökkel együttműködve eljuttassa a MN-nak küldött csomagokat a megfelelő helyre az idegen hálózaton belül. A protokoll működése, melynek főbb lépéseit a 4. ábra mutatja, röviden a következő.

A különböző ügynökök *ügynök-hirdetési üzenetekkel (Agent Advertisement)* ismertetik magukat a saját hálózatukban lévő többi csomóponttal. Ha egy MN kap egy ilyen üzenetet, akkor az alapján el tudja dönteni, hogy az otthoni vagy egy idegen hálózatban tartózkodik-e. Ha az otthoni hálózatban van, akkor működése nem különbözik az IP protokoll alap-specifikációjában leírtaktól. Abban az esetben, ha a MN egy idegen hálózatban van, akkor szerez egy megfelelő közvetett (ideiglenes) címet, melyet aztán jelez az otthoni ügynökének, továbbá jelez e cím minden egyes megváltozásakor. A MN-nak küldött csomagokat (1) az otthoni hálózatban az otthoni ügynök elfogja, és egy ún. IP alagút (tunnel) segítségével továbbítja a MN aktuális közvetett címére (2, 3). A MN által küldött csomagok (4, 5) rendszerint a protokoll alapspecifikációjában leírtak szerint továbbítódnak, azaz nem az otthoni ügynökön keresztül, hanem közvetlenül a *kommunikációs partnerek (Correspondent Node, CN)* felé.



4. ábra. A Mobil IP és a háromszög probléma

Bár a fent leírt mechanizmus megvalósítja a célt, azaz a mobil csomópontok kezelését, mégsem hatékony, mert az ún. *háromszög probléma* kialakulásához vezet. Az 4. ábra narancsszínű nyilai jelzik, hogy a MN és a CN között csak az egyik irányban közvetlen a kommunikáció. A CN a MN-nak címzett csomagjait először mindig az otthoni ügynöknek küldi és nem közvetlenül a MN-nak. Ez a hálózati erőforrások kedvezőtlen kihasználásához vezet. Ilyen kedvezőtlen hatások többek között, hogy nő a hálózat terhelése és a csomagok kézbesítéséhez szükséges idő, különösen akkor, ha CN közel helyezkedik el a MN-hoz. Ezen

egy újabb kiegészítéssel, az ún. *útvonal optimalizálással (route optimization)* lehetett javítani. Ennek lényege, hogy a MN kommunikációs partnerei is naprakész információval rendelkeznek a MN aktuális közvetett címéről, így a MN-nak szánt csomagok közvetlenül küldhetők, az otthoni ügynök kihagyásával. A megoldás hátránya, hogy változtatásokat kell végrehajtani az IP protokoll alap-specifikációja szerint működő, nem mobil kommunikációs partnerekben is.

Az eddigiekből látható, hogy az IPv4 és kiegészítéseként a Mobil IP protokoll képes a mobil csomópontok kezelésére, azonban a technika fejlődésével az IPv4 egyre több hiányossága került felszínre: olyan új funkciók váltak szükségessé, amelyek az IPv4 bevezetésekor még értelemszerűen fel sem merültek. A fő probléma, hogy a szabadon kiosztható IP címek előbb, vagy utóbb elfogynak, és így már nem lehet további csomópontokat az IP hálózatokhoz csatlakoztatni. Az IPv4 további hátránya, hogy címzési rendszeréből következően a routerek-nek több ezer bejegyzést tartalmazó routing táblákat kell fenntartaniuk, ezzel növelve a torlódás és csomagvesztés lehetőségét. Többek között ez vezetett egy új Internet Protokoll, az IPv6 létrejöttéhez. Az új protokoll kifejlesztésénél már a kezdetektől figyelembe vettek számos, korábban lényegtelennek tartott paramétert és szolgáltatást, amiket a protokoll integráns részévé tettek (többek között a mobilitás kezelését), és ami legalább ennyire fontos, számos szükségtelen funkciót kiiktattak. A következő alfejezet mutatja be az IPv6 legfontosabb mobilitáskezeléssel kapcsolatos tulajdonságait.

MOBIL IPv6 (MIPv6)

A Mobil IP IPv6-os és IPv4-es megvalósítása közt sok közös tulajdonság van, de nem teljesen egyeznek meg:

- Míg az IPv4 külön UDP csomagokat használ a regisztrációhoz, addig az IPv6 a jelzésrendszert az IP fejléc kiterjesztésébe integrálva tartalmazza.
- Az IPv6 esetén a mobil csomópont címe egyszerűen előállítható: elég hozzá ismerni az idegen hálózat címét és az eszközünk MAC címét.
- Ezen kívül, az IPv6-ban a címtár betelése miatt sem kell aggódni, mivel ez a protokoll 128 bites címeket használ, szemben az IPv4 32 bites címeivel.
- Az IPv6 esetén nincs szükség idegen ügynökre sem, mivel a Care-of-Address (idegen hálózatban használt ideiglenes cím) mindig a mobil csomóponthoz kapcsolódik.
- További nagyon fontos tulajdonság, hogy a MIPv6-ban nem jelenik meg a MIP-ben tapasztalható háromszög probléma, mivel a protokoll lehetőséget ad arra, hogy a mobil csomópontok ne csak az Otthoni Ügynökükkel, hanem kommunikációs partnereikkel is közölhessék aktuális kötéseiket (*binding*).

A mobilitás kezelését segíti néhány ICMPv6 (Internet Control Message Protocol az IPv6 számára) üzenet is. Ilyen a *Router Advertisement (router hirdetés)*, *Router Solicitation (router kérés)*, *Address Auto-configuration (cím automatikus konfiguráció)*, *Neighbour Discovery (szomszéd felderítés)*. Egy mobil eszköz mozgása során több különböző hálózatban megfordulhat. A hálózatot a router hirdetésekben lévő hálózati azonosító alapján azonosítja.

Ha a mobil eszköz nem akar várni a soron következő router hirdetésre, maga is kezdet router felderítő üzenetet, amiben megkéri a környező routereket, hogy kezdjenek el

hirdetni. A hálózaton lévő routerek közül a mobil csomópont kiválaszt egyet, és egészen addig őt tartja alapértelmezettnek, amíg elérhető. Az ideiglenes címet az idegen hálózatban kétféleképpen lehet kérni:

- Az egyik a **stateful** címkonfiguráció, ilyenkor a címet egy Dynamic Host Configuration Protocol (DHCP) szervertől kapjuk.
- A másik a **stateless** címkonfiguráció, ilyenkor a címet a routerektől kapott hálózat címből (*prefix*) és egy egyedi azonosítóból állítjuk elő. Ha egy idegen hálózatban tartózkodunk, a nekünk küldött üzeneteket az otthoni ügynöknek kell megkapnia. Ehhez több, a Mobile IPv6-ban megvalósított üzenetet létezik. Ilyen a *Binding Update* (*Kötési Frissítés*) üzenet, ami tartalmazza az idegen hálózatban tartózkodó mobil egységünk új ideiglenes címét. Ezt el kell juttatni az otthoni ügynöknek és az összes olyan csomópontnak, akivel épp kommunikálunk. Ha egy csomópont egy MN-tal akar kommunikálni, először az otthoni IP címünkre küld csomagot, amit az otthoni ügynökünk kap meg. Miután az otthoni ügynökünk ismeri a MN ideiglenes címét, (hisz erről folyamatosan értesíti) a MN után küldi ezt a csomagot. Miután ez a csomag tartalmazza az eredeti küldő címét, a MN-nak lehetősége van arra, hogy egy Binding Update üzenettel értesítse partnerét az új ideiglenes címről. Ezután a partner már közvetlenül tud vele kommunikálni. Ha a MN bármikor átlép a kommunikáció során egy másik idegen hálózatba, ahol azonnal új ideiglenes címet kap. Ekkor egy Binding Update üzenetben értesíti a kommunikációs partnert erről az új címről, így nem szűnik meg a kapcsolat. Amikor a MN visszatér az otthoni hálózatba, értesítenie kell az otthoni ügynököt, hogy ne kapja el ezután a neki szóló üzeneteket, hisz ilyenkor újra az eredeti IP címével kommunikál. A következő fontos üzenet a *Binding Acknowledgement*, ami a csomópontok válasza a Binding Update üzenetre. Ez lehet elfogadás, de lehet elutasítás is. Minden Binding Update üzenet tartalmaz egy időkorlátot is, ami jelzi, hogy meddig lesz még használható az ideiglenes cím. Ha ez lejár, újabb Binding Update üzenet kell, mert a velünk kommunikáló csomópontok lejárnak veszítik az ideiglenes címünket. Ha közeleg a cím lejárási ideje, egy *Binding Request* üzenettel új Binding Update üzenetet kérhetnek a velünk kommunikáló csomópontok.

Mikromobilitás

- a mikromobilitás protokollok **gyorsasága** a *cellaváltások lokális kezelésében* rejlik:
 - a felhasználó domain-en belüli mozgását "elfedi" a mobil IP elől, nincs szükség a mobil IP bevonására minden cellaváltásnál
 - a regisztrációs és a jelzés üzenetek - megvalósítástól függően - legfeljebb a tartomány gyöker routeréig kell hogy eljussanak, és a gyöker router az üzeneteket gyorsan fel tudja dolgozni.
- tehát a gyorsaság részben a *kis terület*, a *limitált számú felhasználó*, és a *mobil IP kihagyásának* következménye

Mikromobilitást támogató protokollok:

- Egyszintű hierarchikus mobil IP,
- Többosztályú hierarchikus mobil IP,
- Cellás IP (Cellular IP / CIP),
- Handoff-Aware Wireless Access Internet Infrastructure (HAWAII),

- Jelenleg egyik javaslat sem jelent tökéletes megoldást a problémára. A probléma túl komplex ahhoz, hogy bármely javaslat egymagában tökéletes megoldást adjon rá, de vannak közös vonásaik:
 - Hierarchikus mobilitás kezelés a skálázhatóság miatt.
 - Egyszerű és olcsón telepíthető hálózati eszközök a gazdaságos és könnyű telepíthetőség miatt.
 - A helyzet információkat soft-state módon kell tárolni a skálázhatóság és megbízhatóság miatt.
 - A redundáns útvonalak és a veszteségmentes handover között változtatható “trade-off” (teljesítmény kontra hatékonyság).
 - Visszamenőleges kompatibilitás a szabványos IP protokollal, és együttműködés a mobil IP-vel.
 - A mobil IP-vel azonos biztonsági megoldások használata a biztonság érdekében.
 - QoS támogatás, együttműködés QoS támogatással rendelkező protokollokkal.
- A mikromobilitási protokoll tervezeteket működésük és alap gondolatuk szerint néhány nagy csoportba lehet szervezni:
 - **Mobil IP** alapú megoldások,
 - **Proxy Agent Architectures - PAA** (hierarchikus szervezésű ágens gyorsítás),
 - **Localised Enhanced Routing Schemes - LERS** (a mikromobilitás domain-on belül módosított routing algoritmust használ), alcsoportjai:
 - Per Host Forwarding (hoszt alapú nyilvántartás és továbbítás),
 - Multikaszt alapú,
 - MANET alapú protokollok.
- A mikromobilitási domain-on belüli működés alapján:
 - **Proaktív** vagy **Reaktív**, illetve
 - **Gateway centrikus** vagy **hop-by-hop** protokollokról beszélhetünk.

Cellular IP (CIP)

A legfontosabb szempontok, amiket figyelembe vettek a CIP tervezésénél:

- olcsó passzív kapcsolat;
- rugalmas handoff támogatás;
- hatékony location management;
- a node-ok nem ismerik a hálózati topológiát;
- nincs központi adatbázis, vagy más kritikus hibaforrás;
- a hálózat elemei nem válnak bonyolultabbá, ahogy a lefedettségi terület (és így a felhasználók száma) nő.

HAWAII

- A HAWAII hierarchikusan szervezett tartományokból álló hálózat. Minden tartományhoz tartozik egy ún. *domain root router* gateway, néhány router, bázisállomás és mobil.
- Célok:
 - Minimalizálni a felhasználói forgalom megszakadásait
 - Lehetővé tenni a hálózati erőforrások hatékony kihasználását
 - Skálázhatóság
 - QoS támogatást nyújtani
 - Növelni a megbízhatóságot

CIP-HAWAII hasonlóságok:

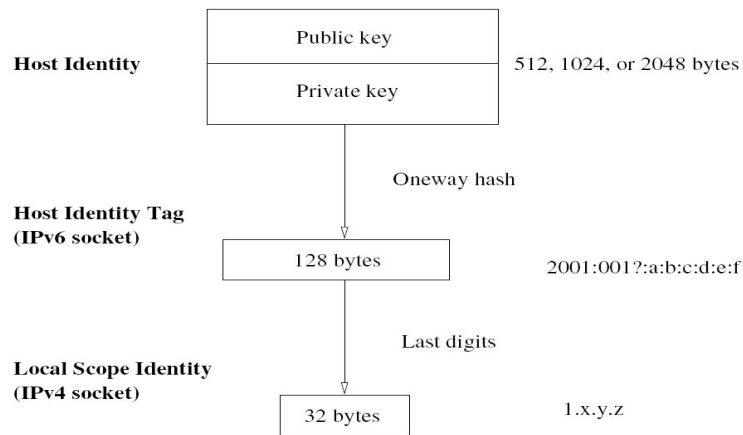
- A HAWAII a harmadik hálózati rétegben működik, és a routing algoritmuson módosít a mobilitás lokális támogatása érdekében.
- A routerekben lokálisan érvényes speciális útvonal nyilvántartást vezet, ezzel biztosítja, hogy egy földrajzilag körülhatárolt területen (domain-en) belüli cellaváltás esetén ne kelljen egészen a home agent-ig visszajelezni a handovert, illetve az új ideiglenes címet (care-of address).
- A CIP-hez hasonlóan itt is soft-state módon tárolódnak a routerben az információk, tehát ha nem frissítik őket, akkor egy bizonyos idő eltelte után törlődnek a rendszerből. Ez ugyanazokat a célokat szolgálja, mint a CIP esetében, például így nem kell a beírt adatokat törölni, ha a mobil megváltoztatja helyzetét.

CIP-HAWAII különbségek:

- Az algoritmus nem igényli, hogy megváltoztassuk a mobil terminálon használt protokollt, elég ha a mobil IP protokollt ismeri.
- Ebben az esetben nem fontos hogy a hálózat gráfja fa legyen (szemben a cellás IP-vel).

15. Mobilitás HIP-pel

A Host Identity Protocol legfontosabb tulajdonsága, hogy szétválasztja az IP címek kettős funkcióját, azonban emellett hatékonyan oldja meg a biztonságos kommunikáció és a mobilitás-kezelés feladatait is.



A HIP protokollban a csomópontok azonosítása az ún. *állomás-azonosítók* (*Host Identifier, HI*) feladata, melyek változatlanok a csomópontok mozgásától függetlenül. Tehát – habár a hálózatváltások során az IP cím megváltozik – a HI változatlan marad. Minden olyan csomópont, amely a HIP protokollt alkalmazza, rendelkezik egy *aszimmetrikus kulcs-párral*, melynek publikus része a csomóponthoz rendelt HI. A HI-k e tulajdonsága teszi lehetővé, hogy a HIP protokoll a csomópontok azonosításán túl, erős biztonsági kapcsolat létrehozására is alkalmas legyen két, egymással kommunikáló csomópont között.

A HIP, Host Identity tag előnye:

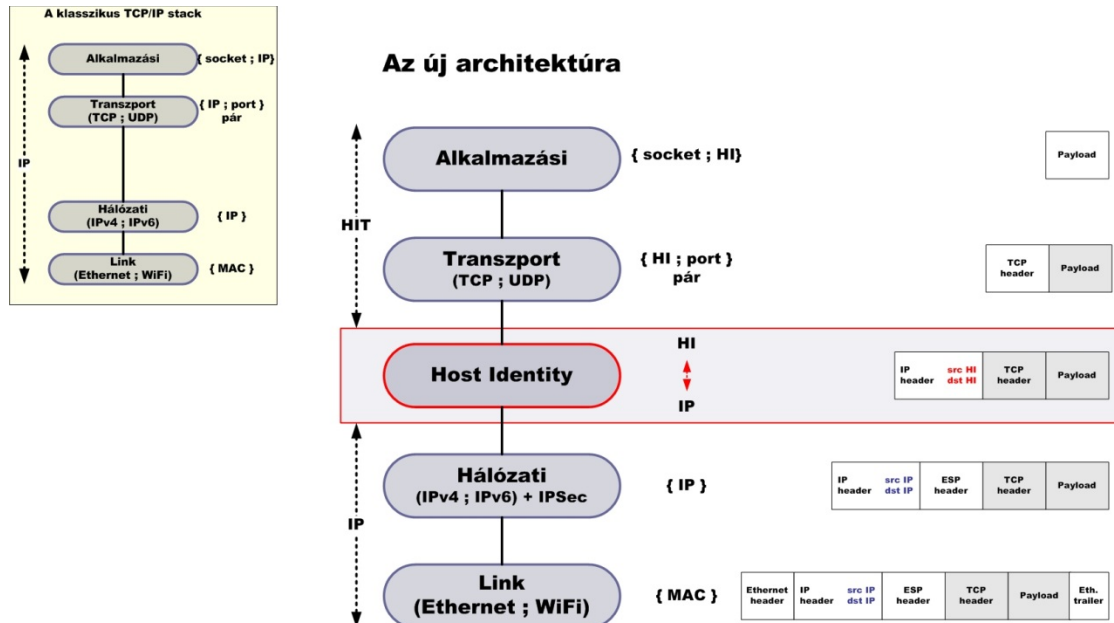
- kulcsgeneráló algoritmustól független
- fix hosszúságú
- Implementáció egyszerűbb
- 128 bit = IPv6 cím hossza
- Önmagát igazolja – ha adott egy HIT, akkor nagy számításigényű feladat annak a HI-nek a megtalálása, amiből generálták.
 - A hash függvény biztosítja (SHA-1).

A protokoll segítségével létrehozható egy IPsec alapú *biztonsági összerendelés* (*Security Association*). Ehhez azonban szükség volt egy olyan mechanizmus beépítésére, amellyel a kapcsolat felépítéséhez szükséges paramétereket a kommunikálni kívánó csomópontok megoszthatják egymással. Ez az ún. *alap-kulcscsere* (*Base Exchange, BE*) mechanizmus. Az eddigiekből viszont nem derül ki, hogy miért van szükség egy új internet architektúra bevezetésére. Ha azonban végiggondoljuk a jelenlegi rendszer működését, világossá válik a változás szükségessége.

HIP, mint új réteg:

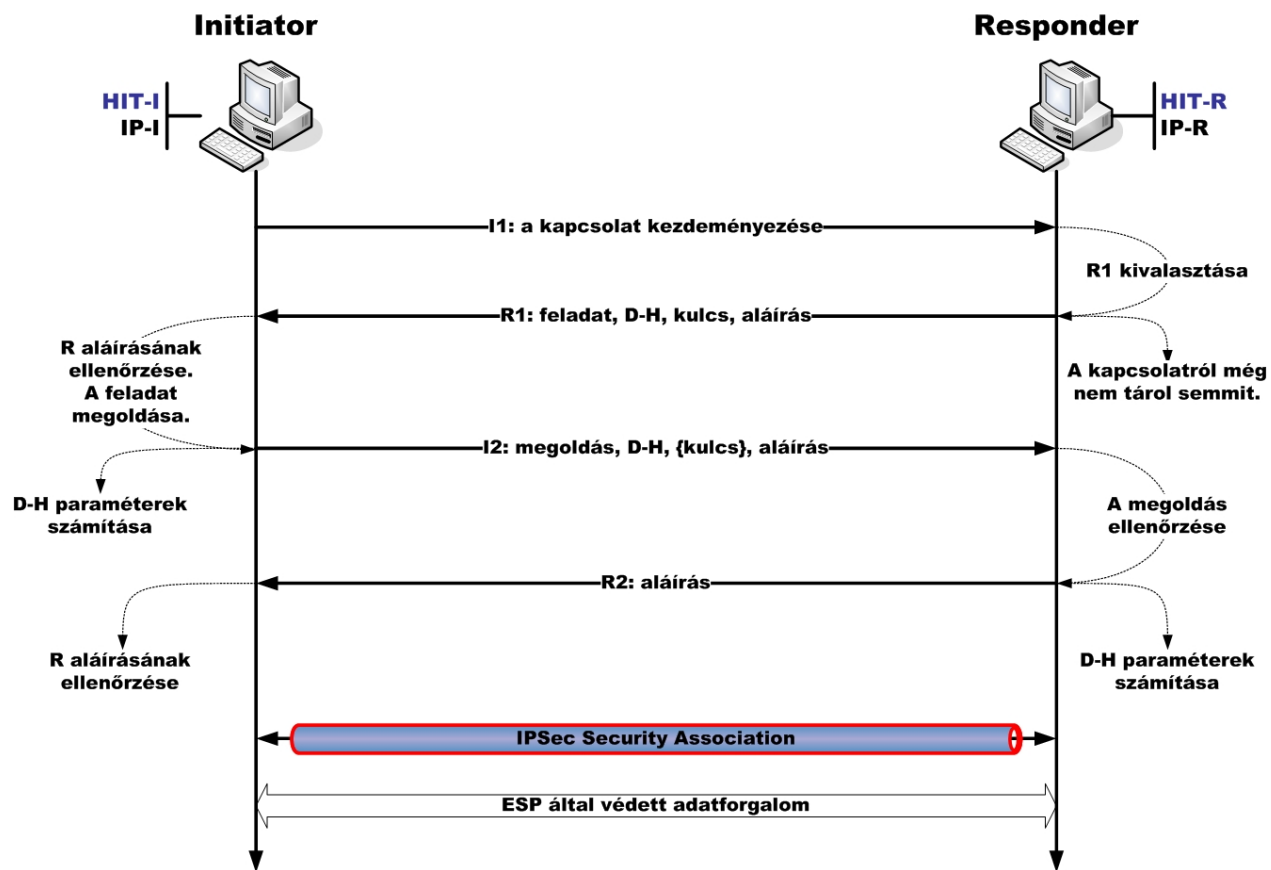
- Az hálózati (IP) és a transzport rétegek között helyezkedik el.
- A HIP réteg fölött a HIT a kapcsolatok és hosztok azonosítója.

- A HIP réteg alatt az IP cím az „azonosító”.
 - Valójában itt az IP cím már csak egyszerű helymeghatározó.
- A HIP réteg végzi többek közt a HIP-IP cím összerendelést / átalakítást.
- A HIP alkalmazásával elválasztjuk a felette lévő rétegeket az IP-től – ezek már csak a HIT-et ismerik.
- Az IP címek változása is rejtve marad.
 - Nem csak mobilitás okozhat IP cím változást.
- A felső rétegek kapcsolatai nem szakadnak meg, ha az IP címek valamilyen okból megváltoznak.



HIP kapcsolat felépítése:

- Base Exchange (BE):
 - HIP alapú kommunikációs kontextus kialakítása kriptográfiai úton két hoszt között.
 - Kezdeményező = Initiator
 - Fogadó = Responder
 - A BE után ez a megkülönböztetés értelmét veszti
 - Kulcs- létrehozó/cserélő mechanizmus (Diffie-Hellman, DH).
 - Eredménye egy IPSec biztonsági összerendelés pár (Security Association, SA), ESP transzport mód
 - Az adatsere ezen keresztül történik.
 - Authentikációs funkció



16. Transzport protokollok mobil környezetben

A vezeték nélküli közeg használata esetén számos olyan problémával kell megbirkózni, amelyek vezetékes hálózatoknál nem jelentkeznek:

- korlátozott sávszélesség
- sokkal megbízhatatlanabb átvitel, csatornahiba
- nagy zavarérzékenység
- lehallgathatóság
- dinamikus topológia
- jelentős késleltetés és késleltetés-ingadozás (jitter)
- handover – adminisztratív üzenetek - késleltetés

Mobilitás támogatás:

- Átlátszó átvitel
Hálózatok közötti váltás ne okozzon nagy adatvesztést, a váltás ne tartson sokáig és a hosszú távú kapcsolat orientált protokollokat használó programok zavartalanul futhassanak tovább
- Lokáció menedzsment
A mobil eszköznek mindvégig elérhetőnek kell lennie egy statikus azonosító segítségével függetlenül attól, hogy helyileg éppen hol van.
- Infrastruktúra mentesség
Minél jobban a hálózat szélén van a mobilitás megvalósítva, annál kevesebb változtatásra van szükség a jelenlegi hálózatokban.

Protokollok:

Megbízható:

- TCP és variánsai
- SCTP

Nem megbízható:

- UDP és UDP-Lite
- DCCP

TCP jellemzői:

- **Újraküldés**
 - a TCP feladata, hogy adott esetben (pl. egy bizonyos idő lejártával) az egyes csomagokat újra elküldje, mivel lehet, hogy az előző példány elveszett valahol
- **Sorrendhelyes átvitel**
 - A célállomáson a megérkezett csomagok sorrendje nem biztos, hogy az elküldés sorrendjével megegyezik, ezért a TCP feladata ennek a rendezése is (ha szükséges)
- **Csomagduplázódás**
 - A TCP a csomagduplázás ellen is védelmet nyújt
- **Megbízhatóság**
 - az ún. PAR (Positive Acknowledgement with Retransmission) technikával biztosítja.
- **Megbízhatóság és késleltetés**
 - A TCP esetében a megbízhatóság azt jelenti, hogy az elküldött csomagok biztosan megérkeznek, de az esetleges újraküldések miatti késleltetésre nincs garancia
 - Valós idejű szolgáltatások esetén ezért nem javasolt a TCP használata
- **Full-duplex adatfolyam**
 - A TCP-kapcsolatok full-duplexek, vagyis kétirányúak, és az elküldött adatokat a TCP strukturálatlan byte- folyamnak tekinti.

- **Forgalomszabályozás (flow control)**
 - A küldő nem terheli túl a fogadót
- **Torlódáskezelés (congestion control)**

TCP vezetékek nélküli környezetben

- A TCP nem képes különbséget tenni a csomag sérülése miatti csomagvesztés és a torlódás miatti veszteség között.
- Így minden csomagvesztés ugyanazt az adó részéről történő
 - torlódás elkerülési választ vonja maga után, ami az adó átküldési sebességének a csökkenését okozza
 - még akkor is, ha a hálózatban nincs torlódás
- A vezetékek nélküli átvitel miatt bithibák jelentkeznek, amik csomagvesztésben nyilvánulnak meg.
- A TCP vezetékes környezetre optimalizált, így a csomagvesztést torlódásként értelmezi és csökkenti az átviteli sebességet.
- A TCP zajos csatornán indokolatlanul csökkentheti az adatátviteli sebességet
- Cellaváltás (az RTT hirtelen megnő), adatforgalom leáll
- Kapcsolat megszakadásának okai:
 - Cellaváltás esetén a kapcsolat megszakad, új kapcsolat felépítésére van szükség
 - A jelerősség lecsökken (fading hatások)
- Változó sebességű csatorna
 - A felhasználók száma változik a cellán belül
- Multimédiás és késleltetésre érzékeny alkalmazások esetén a TCP nem ajánlott
- A TCP hibáinak kiküszöbölésére nehézkes, hiszen minden Internethez csatlakoztatott gépen van egy példány
 - Ezeknek együtt kell működniük
 - Lényegi változtatás így nem oldható meg
- A módosított TCP változatoknak kompatibilisnek kell maradniuk
- Megoldási javaslatok:

	Mechanizmus	Előny	Hátrány
Indirect TCP	A kapcsolat kettébontása	Egyszerű, a vezetékek nélküli szakasz elkülönítése	End-to-end koncepció elvesztése, hosszabb késleltetés handover esetén
Snoop TCP	A csomagok (adat,ACK) megfigyelése, local retransmission	Transzparens end-to-end kapcsolat	Titkosítás esetén nem működik, a vezetékek nélküli szakasz elszigetelése nem teljes
M-TCP	A kapcsolat kettébontása, a küldő visszafogása az ablakméret állításával	End-to-end kapcsolat megmarad, kezeli a gyakori és hosszabb kapcsolatszakadásokat	a vezetékek nélküli szakasz elszigetelése nem teljes, nagyobb számítási overhead a sávszélesség-menedzselés miatt
Fast retransmit/ fast recovery	Slow-start mellőzése handover esetén	Egyszerű és hatékony	Rétegek keveredése, nem transzparens
Transmission/ time-out freezing	Zárolja a TCP állapotokat kapcsolatszakadás idejére	Független a csomagtípusoktól és a titkosítási eljárásoktól, hosszabb megszakadás esetén is működik	MAC függő Jelentős változtatás a TCP-ben

UDP (User Datagram Protocol)

- Az UDP sokkal gyorsabb protokoll, mint a TCP protokoll
- Nem megbízható adatátvitel
- Multimédiás alkalmazások esetén jól alkalmazható, ahol a késleltetés a kritikus
- A TCP-vel ellentétben nem ellenőrzi az adatok sértetlen átvitelét
- Ezen kívül a fogadás sorrendjét sem garantálja a vételi oldalon.

UDP-Lite

- Az UDP módosítása
- Az UDP és az UDPLite minden jellemzője megegyezik
 - Nem kapcsolat orientált
 - Nincs hibajavítás
 - Nincs nyugtázás
- Részleges ellenőrzőösszeg alkalmazása (partial checksum)
- Ha a csomagnak abban részében keletkezik bithiba, amelyet a részleges ellenőrzőösszeg lefed, akkor a vevő érzékeli a hibát és eldobja a csomagot
- Ha a hiba olyan helyen van, amit a részleges ellenőrzőösszeg nem fed le, akkor nem dobja el
 - Ebben az esetben az alkalmazásnak kell kezelnie a hibás csomagot
 - Ha az UDP ellenőrzőösszege az egész csomagra kiterjed, az UDP Lite működése megegyezik a hagyományos UDP működésével.
- Mobil környezetben előnyös

DCCP (Datagram Congestion Control Protocol)

- Megbízhatatlan transzport protokoll
 - Nincs újraküldés
 - Van nyugtázás
- Kapcsolatorientált
 - Kapcsolatkiépítés
- Torlódásszabályozási algoritmust használ
- Sorrendhelyes csomagtovábbítás
- Cél: TCP és az UDP előnyeit egy protokollként valósítsák meg
- TCP és UDP alapján egy új protokoll
- Átvett módszerek
 - Portok használata
 - Ellenőrzőösszeg
 - Sorszámozás
 - Nyugtázási mechanizmus
 - Adatcsomaghoz csatolt nyugta
 - Háromutas kézfogás kapcsolat-felépítésnél
- Új jellemzők
 - Választható torlódásszabályozás
 - Paraméterek beállítása kapcsolat-felépítésnél
 - Két egyirányú kapcsolat ($A \rightarrow B$, $B \rightarrow A$)
- Követelmények
 - Hibadetektálási képesség
 - Csomagonként sorszám, bájtanként sorszámozás (TCP) helyett
 - A megbízhatatlan adatfolyamot feldolgozó alkalmazások számára sokkal fontosabb, hogy melyik csomag hiányzik, mint az hogy melyik adatrész
- Megoldás
 - Nyugtázási sorszám sok esetben része a csomagnak
 - Sorszám minden csomag fejlécében
 - Nincs együttes (kumulatív) nyugtázás, hiszen újraküldés nincs
 - A nyugtázási sorszám, a legutolsó megkapott csomag sorszáma, nem pedig a legelső meg nem kapott csomagé (~TCP)

Torlódásszabályozás

- Lehetőség van a választásra
 - Sőt az algoritmus kommunikáció közben is megváltoztatható
- Jelenleg elérhető torlódáskezelő algoritmusok: CCID2, CCID3

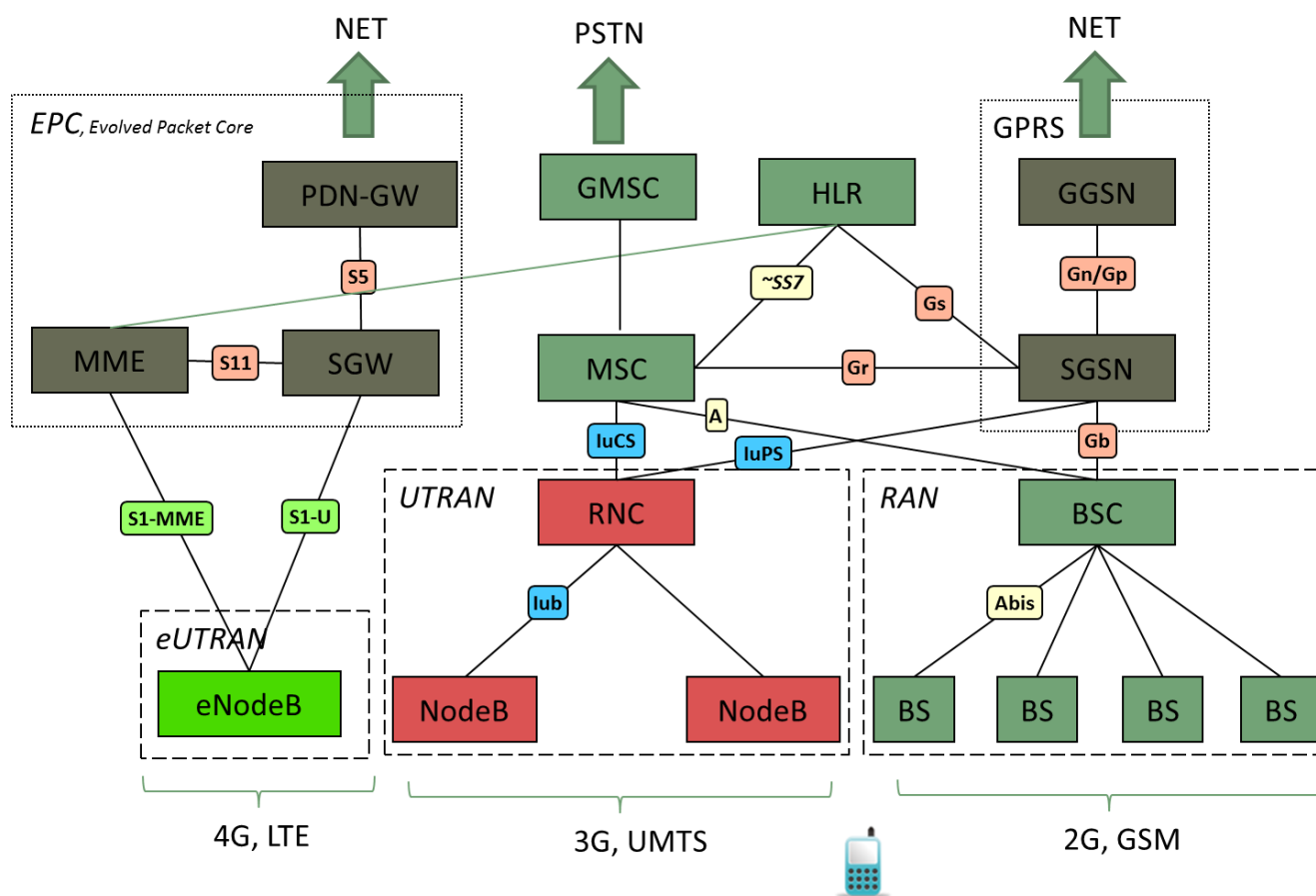
SCTP (Stream Control Transmission Protocol)

- Megbízható
 - Hibamentes
 - Duplikáció-mentes
 - Nem sorrendhelyes/vagy sorrendhelyes (beállítható)
- Több folyam kezelése egy kapcsolaton belül
- Multihoming
 - Több IP-cím
- Torlódásszabályozás
- Slow start
- MTU (Maximum Transfer Unit) felderítés
- A TCP, UDP nem elégíti ki az összes alkalmazás igényeit
- Fejlődését leginkább az IP telefónia és az ott alkalmazott jelzésrendszer indította
- A TCP-vel és UDP-vel ellentétben olyan opciókat is nyújt, amelyek a multimédiás alkalmazások esetén jelent előnyt
- TCP-hez hasonló torlódáskezelő algoritmust használ
- Rendkívül fontos tulajdonsága az SCTP-nek, hogy egy kapcsolaton belül képes több adatfolyamot továbbítani, míg a TCP-ben ehhez külön kapcsolatokra van szükség
- A független adatfolyamok külön chunk-okban kerülnek továbbításra, de egy csomagon belül
- Jó felhasználási lehetőség pl. a vezérlő és felhasználói adatok szétválasztása
 - TCP esetében meg kell várni, hogy a felhasználói adat továbbítódjon és csak utána érkezik a nagyobb prioritású vezérlő adat
- Az SCTP párhuzamossá teszi a folyamatok továbbítását, így csökkentve a késleltetést is

mSCTP

- Az SCTP protokollt arra tervezték, hogy a TCP-t és esetleg még az UDP-t is leváltsa
- Hasonlít a TCP-re, de jóval többre képes annál, például multi-streaming és multi-homing támogatása
- A multi-homing az az új tulajdonság, ami miatt az SCTP alkalmas lehet mobilitás kezelésére, méghozzá úgy, hogy nincs szükség agent-re
- A mobilitás úgy van megvalósítva, hogy a végpont úgy változtassa meg az IP címét, hogy közben a végpont-végpont kapcsolat nem szakad meg
- Egy asszociáció felépítése során a kommunikáló felek kicserélik egymással a lehetséges transzport címeiket (IP és port párosok)

17-18. GSM, GPRS hálózat felépítése, hálózati elemek, szerepük és az interfészek.



Alrendszerek

- (1) Mobil állomás (MS)
- (2) Bázisállomás Alrendszer (BSS)
- (3) Hálózati és Kapcsoló Alrendszer (NSS)
- (4) Üzemeltetési alrendszer (OSS)

Interfészek

- (1) Rádiós interfész: Um (MS-BTS)
- (2) Abis interfész (BTS-BSC)
- (3) A interfész (BSC-MSC)

(1) BSS

Tartalmazza a cellás hálózat kialakításához szükséges adó-vevő és vezérlő berendezéseket, melyek a Bázis Adóvevő állomás (BTS), Bázisállomás Vezérlő (BSC) és Transcoder (TC).

BTS

A rádió interfészen keresztül közvetlen kapcsolatban vannak a mobil állomásokkal. **Főbb feladatuk:** Csatornakódolás, dekódolás. Interleaving és de-interleaving megvalósítása. Titkosítás és visszaalakítás. Beszéd és adatsebesség adaptálás. Modulálás és teljesítményerősítés RF jelek egyesítése. Szinkronitás fenntartása a BTS és az MS között. Logikai csatornák időzítésének vezérlése. BSC felé az MS és BTS méréseinek továbbítása.

Főbb elemei: rádió adók és vevők, antennák, antenna kábel, duplexerek, esetenként splitterek.

A BSC-khez tipikusan 2 Mbps PCM vonalon kapcsolódnak, mikrohullámú vagy optikai médián keresztül.

BTS-BSC átviteli megoldások: pont-pont, többteleágazású-lánc, többteleágazású-hurok összeköttetések lehetnek.

BSC

Feladatok: Rádiós interfész konfigurálása és vezérlése. Kapcsolattartás a transcoderen keresztül a hálózat és a kapcsoló alrendszer központjaival. A hozzátartozó bázisállomások vezérlése (forgalmi jelzésátviteli csatornák lefoglalása, minőség, télerősség, BTS és MS teljesítményszintek). Előfizetők megtalálása. Frekvenciaugratás. BSC-MSC földi átviteli vonal vezérlése.

TC

A transzkóder a bázisállomás része. Lehetnek a BTS-ben, vagy a BSC-ben esetleg az MSC-ben. **Feladatok:** GSM specifikus kódolást/dekódolást végez és adatátvitel esetén sebesség adaptálást is. Downlink beszédintenzitás érzékelése.

(2) NSS

Feladata: irányítsa a GSM felhasználók és az egyéb távközlési hálózati rendszerek kommunikációját. 2 funkcionális része van: (1) Kapcsoló rendszer (2) Előfizetői és végberendezés adatbázisok.

Kapcsolórendszer: (1) Mobil szolgálati kapcsolóközpont (MSC) (2) Rövid Üzenet Szolgálati Központ (SMSC) (3) Hangposta rendszer (VMS)

Előfizetői és végberendezés adatbázisok: (1) Látogató Előfizetői helyregiszter (VLR) (2) Honos Előfizetői Helyregiszter (HLR) (3) Előfizetői Azonosító Központ (AuC) (4) Berendezés azonosító regiszter (EIR)

MSC

Alapvető kapcsolási és irányítási funkciókat lát el az NSS-en belül, a szolgáltatási területen található mobil állomások mobil kezdeményezésű és mobil végződtesű hívásainak felépülését koordinálja, követi az előfizetők mobilitását és a rádiós erőforrások foglaltságát. Együttműködési funkciók, ha más hálózatba kell átlépni (IWF): helyregisztrálás, előfizetői hívás, hívásátadás, titkosítási paraméterek átvitelét, DTMF jelzésátvitel. Általában több MSC van: ekkor az átlépő MSC lesz a Gateway MSC (GMSC), melynek feladata az előfizető helyének megállapítása és a hívás továbbítása afelé a külső hálózat vagy másik MSC felé, amely ezt az ügyfelet kiszolgálja.

HLR

Az előfizető helyére és a számára nyújtható távközlési szolgáltatásokra vonatkozó információt tárol (kiegészítő szolgáltatásokat nem feltétlenül). Két szám minden felhasználóhoz: **(1) Mobil Állomás Nemzetközi ISDN száma (MSISDN):** előfizető telefonszáma, melyet a mobil hívásakor tárcsáznak, amely az előfizető szolgáltatását definiálja, nem pedig a készüléket. **(2) Nemzetközi Mobil Állomás Azonosító (IMSI):** SIM kártya hálózaton belüli egyedi azonosító száma. Előfizető aktiválásakor rendelik az MSISDN-hez. AuC és SIM is tárolja. Lehetővé teszi a hívások átirányítását azon MSC/VLR szolgáltatási területre, amelyben a mozgó felhasználó éppen elhelyezkedik.

VLR

Egy vagy több MSC-hez kapcsolódva, több cellát vezérel. **Feladat:** az MSC-k szolgáltatási területén tartózkodó előfizetők adatainak átmeneti tárolása, előfizetők helyének a HLR-nél pontosabb ismerete. GSM cellák egy-egy csoportja forgalmi területet képez. Valahányszor egy mobil állomás átlép egy forgalmi területből a másikba vagy más helyen kapcsolják be, mint előzőleg bekapcsolva volt a VLR megkísérli a helyregisztrációs eljárást (location update).

EIR

Adatbázis, amely a készülékeket három csoportra osztva tárolja az IMEI számuk alapján (fehér, szürke, fekete lista)

AuC

Előfizetők azonosítására szolgáló biztonsági adatokat kezel. Feladata a hálózat illetéktelen használata elleni védelem és az azonosítás (min den regisztrálaskor, hívás-felépítési kísérletkor, kieg. szolg. aktiválás deaktiválás, regisztrálás vagy törlés esetén)

SMSC

Feladat: Az írott üzenetek továbbítása, mint az MSC-nek a beszéd és adathívások kezelése.

VMS

Lehetővé teszi a hangüzenetek tárolását és visszajátszását. Kiértécsítő rendszer is bennük foglaltatik.

(3) OSS

Üzemeltetési alrendszer lehetővé teszi, hogy a hálózatot fenntartó nyomonkövesse és vezérelje a GSM hálózatot. Menedzsment funkciók: hiba, konfiguráció, számlázás, teljesítőképesség, biztonság. MSC, BSC, HLR és egyéb hálózati eszközökhöz csatlakozik, ember-gép interfészt biztosít az üzemeltető személyzet számára. Szolgáltatás minőség ellenőrzése paraméterek segítségével: forgalom, torlódás, hívásátadások, eldobott hívások, interferencia, hogy fel lehessen deríteni a szűk keresztmetszeteket, vagy beavatkozhatnak egy-egy probléma megoldása során.

OMC

Üzemeltetési és karbantartó központ: hálózati adatbázisból és munkaállomásokból áll, amelyek az OMC-t menedzselik. Lehet több OMC is. Napi karbantartási feladatok ellátása. Riasztások kijelzése és összegyűjtése.

GPRS

A GSM architektúra módosításával max 115 kbps, átlagosan 40 kbps csomagkapcsolt adatátvitel érhető el. A GPRS készülékek folyamatos online üzemmódban vannak, de csak a tényleges adatátvitelért kell fizetni, de új felhasználói készülékek szükségesek, a beszéd és adat hívások külön csatornát igényelnek.

Új elem a gyökérhálózatban:

Serving GPRS Support Node (SGSN):

Csomagkapcsolt routing, link mngmt. MS attach/detach és autentikáció megvalósítása. Mobilitás menedzsment: mobilok helyzetének követése. Számlázás: rádiós interfész és hálózati erőforrások használatáért. Titkosítás, adattömörítés. Cellaváltás.

Gateway GPRS Support Node (GGSN):

Átjáró külső hálózatokhoz (IP, X.25): csomagformátum konverzió, címkonverzió.

Új elem a BSS-ben: **Packet Control Unit (PCU)**

Interfész a GPRS gyökérhálózat és a GSM BSS interfész közt. Keretekké formálja az adatot. Rádiós erőforrás menedzsment a csomagkapcsolt szolgáltatásokhoz.

19. GSM, GPRS, EDGE rádiós interfész

GSM RÁDIÓS JELLEMZŐK

- közeghozzáférés: TDMA/FDMA/FDD
- frekvenciaosztás: 200 kHz -es sávok
- időosztás: egy-egy vivőn nyolc időrés
- duplexitás: uplink és downlink kommunikációs irány frekvenciában elválasztva
- Világméreteken 7 féle GSM sáv létezik, Európában csak 4:
 - P(rietary)-GSM900 \
 - E(xtended)-GSM900 - 45 MHz duplex táv
 - R(ail)-GSM900 /
 - DCS - GSM1800 - 95 MHz duplex

Keretfelépítés

1 keret = 8 kb. 577 microsec időrés

1 multikeret TCH/F: 26 keret, BCCH: 51 keret

1 superkeret: TCH/F: 51 multikeret, BCCH: 26 keret

1 hiperkeret: 2048 superkeret: periódusidő 3.5 óra

Frame number: keretsorszám: a szinkron működéshez van rá szükség

Logikai csatornatípusok

- (1) Forgalmi csatornák: TCH: felhasználói adatátvitelre
- (2) Vezérlőcsatornák: *CCH: vezérlési és jelzésátviteli információkat továbbítanak

(1) Forgalmi csatornák TCH: beszéd és adatforgalom továbbítása 26 keretes multikeret használatával, vagyis 26 TDMA keret szervezésében. Ebből 24 forgalmi, 1 lassú dedikált vezérlőcsatorna (SACCH) és 1 használaton kívüli csatorna.

(2) Vezérlő *CCH - Mindenkinek szóló vezérlő: broadcast control channels

- FCCH, Frequency Correction Channel, frekvenciakorrekciós csatorna: a mobil vevőjét a vivőfrekvenciához hangolja, és
- SCH, Synchronization Channel, szinkronizáló csatorna, a keretszerkezet szinkronizációjára, hálózat és BTS azonosító, mindkettő downlink és közös
- BCCH, Broadcast Control Channel, üzenetszóró vezérlőcsatorna (downlink, közös): folyamatos, rendszerinformációk, frekvenciakiosztás és frekvenciaugratási szekvencia információ

Moduláció: GMSK (Gaussian) BT = 0.3. CPFSK folytonos fázisú frekvenciakulcsolás, ahol a logikai nulla = f_1 , logikai egy = f_2 frekvencia. MSK a névleges bitidő alatt a fázistöbbség vagy fázishány $+\pi/2$. A Gauss-szűrés hatása: ISI csökkentése, spektrumszélesség nő

GPRS Rádiós interfész

Moduláció: GMSK

Csatornák: a GSM frekvenciasávok használat. Az átvitel alapegysége a rádiós blokk (456 bit). 52 keretes multikeret. Időrések összevonása egy felhasználó számára. Időrések dinamikus szétosztása a felhasználók között. aszimmetrikus DL/UL forgalom. változatos csatornakódolási lehetőségek.

EDGE

Rádió alapú nagysebességű mobil adat szabvány. 8 időrés használatával 384 kbps érhető el. Moduláció: 8PSK automatikusan alkalmazkodik a rádió környezethez, a bázisállomáshoz közelebb, jó terjedési viszonyok mellett nagyobb sebesség érhető el. EDGE adóvevőket kell a cellákba építeni.

ÓRÁN VOLT, VIZSGÁN KÉRDEZHETŐ:

	WLAN	GSM/GPRS	UMTS
multiplexálás	TDD	FDD	FDD
közeghozzáférés	PCF, DCF	TDMA	CDMA

A multiplexálás azt a folyamatot jelöli, amikor egy központi helyről a beérkező **közös jelfolyamot** a felhasználók között **szétosztjuk**. A többszörös hozzáférés esetén pedig a földrajzilag szétszórt állomások igyekeznek **ugyanahhoz a közeghez hozzáférni**.

FDD = adási és vételi irány eltérő frekvenciasávban biztosítják

TDD = ua. csak eltérő időrésekbe

GSM vegyes (TDMA/FDM/FDD/CDM):

- FDM: a frekvenciatartományt 200kHz-es sávokra bontják
- TDMA: minden sávot 8 időosztásos csatorna között osztanak fel (7 ember kommunikálhat, mert 1 védősáv)
- FDD: az adási és vételi irányokat 45 MHz távolságra helyezték egymástól
- CDM: opcionális frekvenciaugratási sorozat is rendelkezésre áll

sebességek:

GSM: 14,4 kbps (valójában 9,6)

HSCSD: 4 időrés összevonása -> 4xGSM

EDGE: moduláció váltás 8PSK-ra -> gyorsabb lett -> 484 kbps/slot

TA – Timing Advance (pár bit szolgál erre)

- milyen messze van a mobil a bázisállomástól (20-30 km a max)

GPRS vs. GSM adatsebesség:

- felhasználó szemszögéből semmi (ua. időréseket használja)
- de van olyan hibajavító kódolás, ami jobb, mint a GSM-ben, de ez 1:1-ben redundáns nem gyorsabb a GSM-nél
- csomagkapcsolt a GPRS
 - !! kaput nyitott a csomagkapcsolt világ felé és az lényeg !!

20. UMTS rádiós interfész, QoS osztályok, HSDPA, HSUPA továbbfejlesztések

Cél:

- (1) Minden korábbi mobil szolgáltatás támogatása.
- (2) Fix hálózatok minőségi paramétereinek elérése
- (3) Kapacitásnövelés
- (4) Kihasznátltság javítás
- (5) Olcsó kisméretű kézi készülékek kifejlesztése
- (6) Sokféle szolgáltatás, szolgáltatás multiplexálás
- (7) Aszimmetrikus forgalom támogatása
- (8) Együttélés a 2G rendszerekkel (pl. GSM)

Strukturális felépítés:

1. **Felhasználói készülék (UE):** 2 rész: (1) *UMTS Service Identity Module (USIM)* (2) *Mobile Equipment (ME)*
Universal Terrestrial Radio Access Network (UTRAN): rádiós hozzáférést biztosító hálózat, amelyeket rádiós alrendszerekre osztunk (*Radio Network Subsystem, RNS*). Az UTRAN feladata a rádiós hozzáférés biztosítása a CN és az UE között. EDGE alkalmazásánál a hozzáférési hálózat neve GERAN (GSM/EDGE RAN)
2. **RNS:** Egy RNS tartalmaz egy RNC-t, ami a rádiós hálózatvezérlő és az általa felügyelt bázisállomásokból (Node B) az I-xx az interfészek.
3. **RNC:** GSM BSC-hez hasonló: I-xx interfészen csatlakozik a gyökérhálózathoz. Egy RNC BS-ek csoportját vezérli és adatokat továbbít a bázisállomásokhoz (kapcsoló funkció)
4. **Node B:** GSM BTS-e, csak más a moduláció, közeghozzáférés, frekvenciasávok és sűrűbben kell elhelyezni. Feladata az OSI fizikai réteg megvalósítása a rádiós interfészen. Uu fizikai megvalósítása, I-xx kommunikáció.
5. **Core Network (CN):** Gyökérhálózat

QoS osztályok:

- (1) **párbeszéd osztály:** beszéd és videotelefon. késleltetés érzékeny, kevés adatvesztést tolerál.
- (2) **streaming osztály:** netrádió, VoD, késleltetés ingadozásra érzékeny
- (3) **interaktív osztály:** web böngészés, játék, késleltetés, tolerancia, adatvesztést nem tolerál.
- (4) **háttér osztály:** email, fax, ftp. maradék erőforráson, nagy késleltetés, adatvesztést nem tolerál.

Rádiós interfész:

5Mhz csatorna távolság, 200 kHz raster, 1 szolgáltatónak legalább 3-4 csatornára van szüksége.

2 rádiós interfész technológiát támogat az UMTS (ETSI SMG döntése szerint):

1. W-CDMA
2. W-TDMA/CDMA: Cellás rendszerekben WCDMA/FDD, ad-hoc hálóban WTDMA/CDMA/TDD és lehetőség van az OFDMA technológia alkalmazására is.

WCDMA rendszer alapkövetelmények:

Direct Sequence spreading technique. FDD/TDD duplexing lehetőség, 10ms keret. 3,840 Mcchip/sec (7,680 vagy 15,360). Flexibilis vivő kijelölés (4,4 – 5,2 MHz, 200 kHz-es lépésekben)

Bázisállomások közötti szinkronizálás (FDD nem pontos, TDD pontos). Változtatható szórási faktor. Forward error correcting (CRC, konvolúciós kódoló, turbó kódoló). Nagy és változtatható adat sebesség. Beépített frekvencia diversity. A rendszer teljesítőképességének növelése szempontjából opcionálisan alkalmazható további lehetőségek (adaptív antenna, multiuser detection, transmitter diversity, antenna diversity, OFDM technology)

A fizikai csatornák főbb karakterisztikái:

- (1) Főbb struktúra: 10 msec frame, 15 slots (0,667 msec), power control time interval. Idő multiplexálás downlink és kód multiplexálás uplink csatornában. QPSK moduláció 0,22-es roll-off paraméterrel.
- (2) Kód típusok: Channelization code, variable spreading factor, orthogonal codes
- (3) Forward error correcting csatorna kódolás (FEC): Cyclic redundancy check (CRC) $\frac{1}{2}$ vagy $\frac{1}{3}$ konvolúciós kód. $\frac{1}{3}$ turbo kód. Interleaving. Sebesség igazítás a konvolúciós kódoló lyukasztásával
- (4) Hozzáférés típusai: Véletlen hozzáférés réselt ALOHA módszerrel (preamble code assigned to a base station, matched filtering). Frequency reuse factor 1. Soft vagy hard handover. Egyidőbeni kommunikáció két bázisállomással. Csomag kommunikációs mód

Moduláció:

- (1) GSM GMSK: 1 bit/Ts. Gauss szűrővel konvolvált MSK moduláció. Robusztus
- (2) Fázis moduláció: QPSK. 2 bit/Ts. Emelt koszinuszos jelformálás 0.22 roll-off faktoral

Csatorna kódolás:

- $\frac{1}{2}$ vagy $\frac{1}{3}$ konvolúciós kód,
- kényszerhossz = 9
- $\frac{1}{3}$ turbo kód,
- nincs kódolás
- Interleaving

HSDPA

High Speed Downlink Packet Access (HSDPA) 8-10 Mbps (20 Mbps MIMO használata esetén).

HSDPA újdonságok:

- Adaptív moduláció és kódolás (AMC),
- Multiple-Input Multiple-Output (MIMO),
- Gyors ütemezés (RNC helyett BTS)
- Gyors ARQ (RNC helyett BTS)

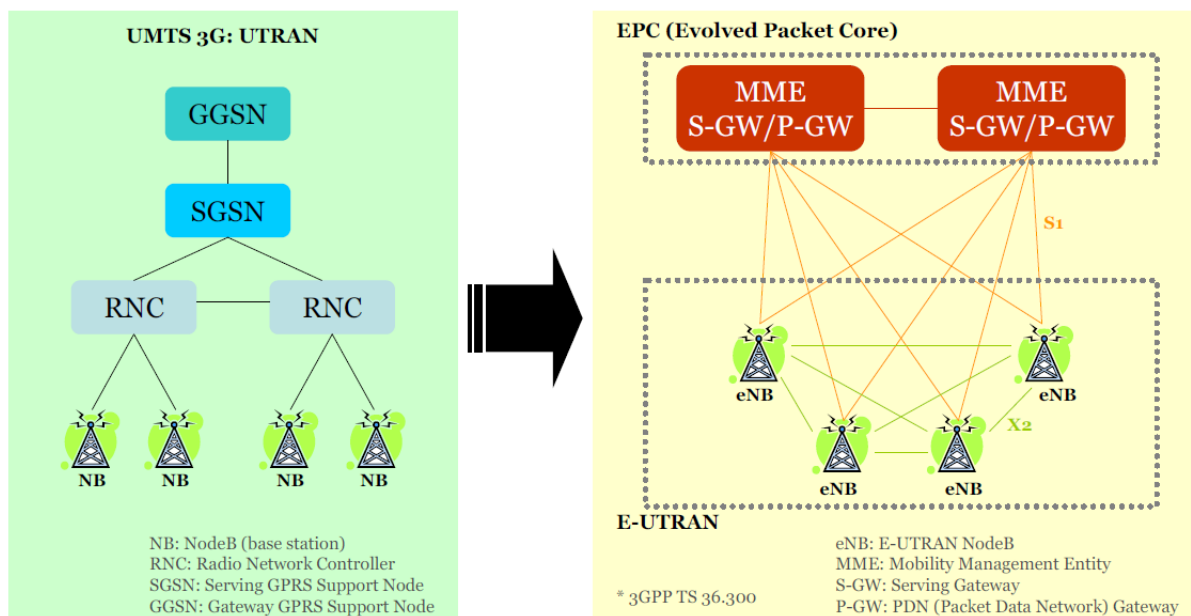
HSUPA

A HSUPA a használt eszközöktől függően 0,7-1,4-2-5,7 Mbit/s maximális feltöltési sebességű adatátvitelre képes.

A feltöltés sebességét több tényező befolyásolja:

- Bázisállomás konfigurációja, átviteli kapacitása
- Rádiós környezet minősége (interferencia, jel-zaj viszony stb.)
- Felhasználók száma az adott cellában
- Felhasználó által használt eszköz típusa
- Felhasználó távolsága az adótoronytól, illetve a felhasználó sebessége (áll, vagy mozgásban van a mobil terminál)

21. Az LTE rádiós interfész fontosabb jellemzői, képességei



LTE rádiós követelmények

- legalább 100 Mbps DL és 50 Mbps UL átviteli csúcsebesség, 20 MHz használatával
 - nagyobb sávszélességeken arányosan nagyobb
- FDD és TDD támogatása
- kis csomagkésleltetés a rádiós hozzáférési hálózatban (max. 5 ms alacsony terhelésnél)
 - kis méretű IP csomag késleltetése egy irányban, ha csak 1 terminál kommunikál
- 5 MHz-en egyszerre legalább 200 előfizető kiszolgálása egy cellában
 - nagyobb sávszélességen legalább 400
 - nem aktív mobilok számára nincs explicit követelmény, de tipikusan jóval nagyobb
- többféle sávszélesség támogatása

LTE alapvető rádiós jellemzők

- OFDM alapú rádiós interfész
 - downlink: **OFDMA** (Orthogonal Frequency Division Multiple Access)
 - uplink: **Single Carrier-FDMA** más néven DFTS-OFDM (Discrete Fourier Transform Spread OFDM)
--- ez is OFDM alapú
 - lehetővé teszi a rugalmas sávhasználatot
 - frekvencia szelektív fading hatása elleni védekezés
 - a megvalósítása egyszerű IFFT-vel
- számos sávszélességet és átviteli sávot támogat
- FDD és TDD támogatás
- adaptív moduláció és csatornakódolás
- gyors második rétegbeli újraküldés (HARQ)
- többantennás támogatás (max. 4x4)

LTE Rádiós Hozzáférési Hálózat (Radio Access Network, RAN) követelményei

- rádiós interfész és eNodeB-k hálózata, protokollok és interfészek
- egyféle RAN architektúra
- csomagkapcsolt, de valós idejű szolgáltatásokat támogatnia kell
- robusztusság: hálózati leállást okozó pontok (single point of failure) számának minimalizálása
- interfészek egyszerűsítése, számuk minimalizálása
- rádióhálózat és transzport hálózat kooperációja lehetséges
- vég-vég szolgáltatási minőség (QoS) biztosítása

22. Cellás hálózati architektúra fejlődése (ugyanaz, mint 17-18.)

23. SAE hálózati architektúra

Többféle hozzáférési hálózat támogatása

- 3GPP és nem 3 GPP
- fix hozzáférési rész

Roaming

Mobilitás a különféle hozzáférési hálózatok közt

Any service IP alapon támogatása

Interworking: PS és CS szolgáltatások közt

Rendszer architektúra:

- a működéshez szükséges funkciók logikai csomópontokhoz rendelve
- interfészek a csomópontok közt
- két fő blokk:
 - maghálózat (Core Network, CN): **EPC, Evolved Packet Core**,
 - rádiós hozzáférési hálózat (Radio Access network, RAN): **E-UTRAN**

Funkciók:

- rádióhálózat menedzsment
- számlázás
- hitelesítés
- vég-vég kapcsolat menedzsment
- gerinchálózati funkciók és rádióhálózati funkciók
- mobilitás menedzsment

RAN funkciók

- kódolás, interleaving, moduláció, más fizikai réteg funkciók;
- ARQ, fejléc tömörítés, ütemezés, stb. egyéb második réteg funkciók;
- rádiós erőforrás menedzsment, handover stb., más rádiós erőforrás kontroll funkciók
- biztonsági funkciók: titkosítás, adat integritás megőrzése

Core funkciók

- számlázás
- előfizető menedzsment
- mobilitás menedzsment (a mobil helyzetének követése)
- hordozó szolgáltatások kezelése, szolgáltatási minőség kezelése
- előfizetők adatfolyamain végrehajtandó eljárások (policy) kezelése
- kapcsolódás külső hálózatokhoz
 - más szolgáltató LTE SAE
 - más hálózat (GSM, 3G, Internet)

24. Ismertesse az IMS architektúrát és az IMS szerepét az NGN koncepcióban.

NGN 3 szintű architektúra:

(1) Application serverek: független szolgáltatási réteg

(2) Session szerverek: hívásvezérlés, soft switchek, SIP protokoll.

(3) Routerok: jelzésüzenetek és a tartalom (média) szállítása. Média gateway és média szerverek: a call szerverek irányításával adatfeldolgozás, konvertálás

Miért szükséges az IMS, ha az Interneten a szolgáltatások nagy része ma is elérhető?

- QoS
- számlázás
- szolgáltatásintegrálás
- Fix mobil konvergencia
- Internet alkalmazás fejlesztési elv bevezetése

IMS előnyei:

- Egyszerű szolgáltatásfejlesztés
- egységes megjelenés
- látványos szolgáltatások
- fejlett QoS és számlázás támogatás
- közös IP mag
- session felépítés, vezérlés
- roamingtámogatás
- új szolgáltatás képességek

IMS (IP Multimedia Subsystem)

- Egyszerű új szolgáltatásokat bevezetni: nyílt API-k és alkalmazásfejlesztési platformok. Mobilitás támogatás. Újrahasznosítható komponensek. Szélessáv.
- Költségcsökkentés: Konvergencia a hálózatban.
- Az IMS kombinálja az Internet és a mobil kommunikáció előnyeit. Lehetővé teszi, hogy két mobil terminál az IP hálózaton keresztül érje le egymást.
- Bevezeti az IP alapú szolgáltatásokat a mobil világba.
- Az IMS a mobil terminálok közötti kapcsolat felépítésre a **SIP**-et használja. Az IMS azonban nem egyszerűen protokollok összessége, hanem egy architektúra.
- Az IMS nem csak két mobil terminál között képes kapcsolatot teremteni, hanem point-multipoint kapcsolatra is képes, valamint a mobilt képes számítógéppel vagy egyéb más Internetre kapcsolódó géppel összekötni.

Lényeg:

Csomagkapcsolt rendszerekben, ahol nagy lehet a késleltetés-ingadozás, csomagvesztés stb., az IMS segítségével le tudjuk foglalni az erőforrásokat, így megbízható(bb) átvitel jöhet létre.

IMS alkalmazások:

- (1) **videó átvitele beszéd közben:** hang videó beszéd képek átvitele egyszerre, egy kapcsolaton belül. interaktív alkalmazások pl.: játékok.
- (2) **Push To Talk:** egy személy vagy személyek egy csoportja egyetlen gombnyomással felhívható. A CB rádióhoz hasonlít, egyszerre csak egy ember beszélhet. Előny hogy a hálózaton csak, akkor van tényleges forgalom, ha beszél is valaki.
- (3) **Presence:** kijelezhetővé válik, hogy valaki éppen mit csinál. (msn-hez skyphoz hasonlóan) Ráér vagy nem ér rá a kommunikációra, milyen az érzelmi állapota. Mikor lesz elérhető stb.
- (4) **Media Push:** A tartalom csak akkor jut el a felhasználóhoz, amikor a felhasználó akarja. A tartalom lehet: szöveg, kép, videó, hang... Működés pl.: a felhasználó letölti a media push alkalmazást, majd megnézi annak tartalmát (ennek tartalma természetesen frissíthető), kiválasztja, hogy mit szeretne megnézni, majd beállítja a küldés paramétereit. Ezek után megkapja a kívánt szolgáltatást.
- (5) **Instant messaging (chat)**
- (6) **Web audió/videó konferencia**

Az IMS architektúra:

Alapelvek:

Nem definiálnak konkrét szolgáltatásokat csak enabler-eket. Beépített támogatást nyújt multimedia over IP, VoIP, IM, presence szolgáltatásokhoz. Flexibilis multimedia átvitel támogatás IP felett. Laza vertikális integráció a hálózatok és szolgáltatások/alkalmazások közt.

Rétegek:

- (1) **Szállítási és végpont réteg:** SIP jelzési folyamatok kezelése. gatewayek kezelése PSTN felé
- (2) **Kapcsolat vezérlési réteg:** CSCF: végpontok regisztrációja, SIP jelzésüzenetek útvonal irányítása. HSS, Média gatewayek-ek kezelése
- (3) **Alkalmazási réteg:** végfelhasználók felé nyújtott szolgáltatások, egységes API-k használata.

25. Sorolja fel és elemezze, hogy általánosságban milyen problémák jellemzik a vezeték nélküli hálózatokat biztonsági szempontból + WLAN eredeti megoldásainak tanulságai!

Vezeték nélküli hálózatok problémái:

Rádiós hozzáférés:

- kis sávszélesség
- nagy késleltetés lehet
- könnyebben lehallgatható, módosítható
- ezek miatt rövid és újragondolt protokollok szükségesek (pl. kihívás-válasz hitelesítés)
- nem minden szakasz rendelkezik ugyanolyan védelemmel

Felhasználói eszközök széles palettája

- – Kis számítási kapacitás (igen eltérő lehet eszközönként)
- – Nehéz, vagy lehetetlen szoftverfrissítés, algoritmus csere széles körben

Szolgáltatáshatárok, adminisztráció

- rosszul szabályozott lehet
- elérhető lehet a szolgáltatás a szolgáltatási területen kívül is
- a felelősség kérdése sokszor nem tisztázott

Törvényi szabályozás

- gyenge algoritmusok (+ export tilalmak)
- lehallgathatóság

Főbb problémák WLAN környezetben:

A fizikai közeg nem biztosít már védelmet:

- Bárki hozzáférhet (olcsó HW)
- Észrevétlen/nyom nélküli hozzáférés
- Az infrastruktúra kiterjedése nehezen korlátozható (pl. épületen kívülre is kijuthat a WiFi jele)

Támadási lehetőségek:

- Passzív támadások észrevétlenül, egyszerűen
- Aktív támadások
- Közbeékelődés (pl. AP megszemélyesítés)
- DOS: csomag elárasztással
- Kihívás-válasz hitelesítési módok veszélye

Megoldás: WEP (Wired Equivalent Privacy)

Céljai:

- Bizalmasság
- Hitelesség
- Felhasználó hitelesítése

WEP Paraméterek:

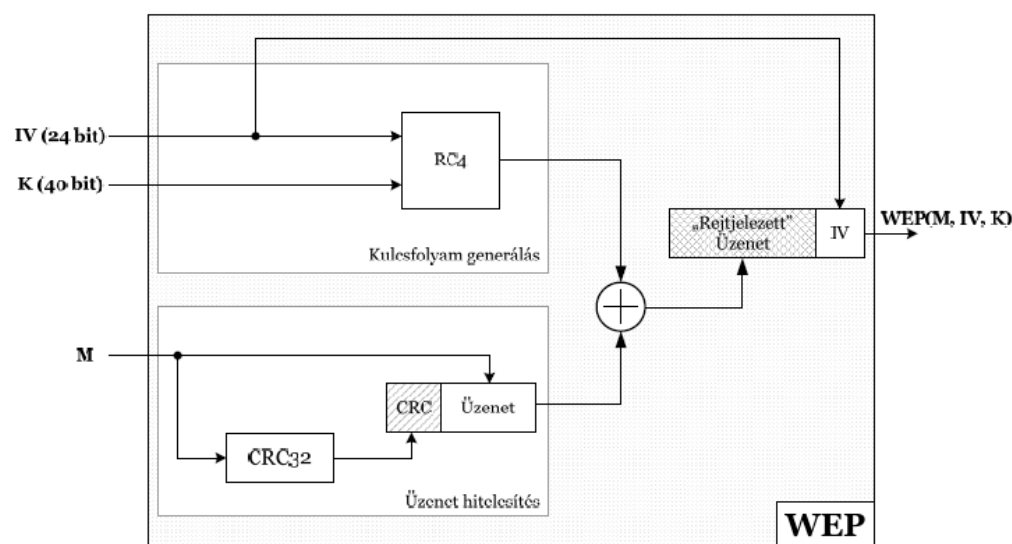
- IV – inicializáló vektor (24 bit)
- K – titkos kulcs (40 vagy 104 bit)
- M – a kódolandó üzenet

Egyszerű elemeket használ:

- RC4 kulcsfolyam generálásra (OFB módban)
- CRC-32 a hitelesség garantálására (Cyclic Redundancy Check)

A kulcsfolyamot és a CRC-vel ellátott üzenetet XOR művelettel egyesíti.

– $WEP(M, IV, K) = \{IV, [M, CRC(M)] \oplus RC4(IV, K)\} = C$



Gyengeségek:

1. Állapotmentes protokoll
2. CRC alkalmazása a hitelesség védelmére
 - Független a kulcstól
 - Lineáris: $CRC(A \oplus B) = CRC(A) \oplus CRC(B)$
3. Egyirányú hitelesítés
 - AP hitelesítésének hiánya
 - A szolgáltatás hitelesítésének hiánya
4. Kulcs körüli problémák
 - Rövid kulcsok
 - IV + kulcs miatt 40 és 104 bit
 - A csomagkulcs tér csak 224 méretű (IV!)
 - Csomagkulcsok újra felhasználása
 - A szabvány nem foglalkozik a kulcsmenedzsment kérdéskörével
 - Támogatja több kulcs használatát, de az eszközök általában nem (jelszavak állomásonként)
 - A kulcsosztás kézzel történik (de facto szabvány)
 - Hosszú élettartamú kulcsok
 - A megjegyezhetőség miatt általában nem jó minőségű kulcsok („alma123”), vagy hexa szavak („CODE CODE CODE CODE”)

WEP – mi a megoldás?

- Biztonságérzet illúziója
 - Ingyenes szoftverek érhetőek el, amelyek WEP hálózatok törésére is alkalmazhatóak (pl. Aircrack-ng)
- Bővítések
 - 128 (256) bites kulcs: WEP-104 (WEP-232)
 - Nehezíti a statisztikai analízist
 - Nincs „erősebb” biztonság – nem a kulchosszal volt a baj
- Új módszerre van szükség!
 - Kiegészítés: WPA-TKIP
 - Teljesen új: WPA-CCMP (WPA2)!

26. Válaszolja fel a mobil rendszerekben alkalmazott hitelesítés és titkosítás menetét! Mi az egyes algoritmusok szerepe és hogyan jellemezné azokat?

Általános problémák

- (1) Rádiós hozzáférés jellemzői: kis sávszélesség, nagy késleltetés, könnyen lehallgatható, módosítható üzenetek és nem minden szakasz rendelkezik ugyanolyan védelemmel. Emiatt rövid és újragondolt protokollok kellenek.
- (2) Felhasználói eszközök széles palettája: kis számítási kapacitás előfordulhat, nehézkes, lehetetlen szoftverfrissítés, algoritmus csere széles körben.
- (3) Szolgáltatáshatárolók, adminisztráció: rosszul szabályozott lehet, elérhető lehet a szolgáltatás a szolgáltatási területen kívül is, felelősség meghatározása nehézkes több szolgáltató esetén.
- (4) Törvényi szabályozás: gyenge algoritmusok (és export tilalmak), lehallgathatóság.
- (5) Észrevétlen vagy nyom nélküli hozzáférés.
- (6) Infrastruktúra kiterjedése nehezen korlátozható
- (7) Aktív, passzív támadások, közbeékelődés (AP megszemélyesítés), DOS: csomag elárasztással.
- (8) Privátszféra: anonimitás lehetősége

GSM

Célkitűzések:

- (1) Gyakori azonosítás: bekapcsoláskor és híváskor
- (2) Forgalom titkosítása a hozzáférési hálózatban
- (3) Hitelesítés az előfizető és a szolgáltató közös titka alapján (128 bites kulcs, Ki) AuC és SIM ismeri csak.
- (4) Security through obscurity: A3, A5, A8 titkos algoritmusok használata

A3, A8: Szolgáltató választja meg. A3: kihívás-válasz hitelesítéshez egyirányú függvény egy véletlen számból (Rj) és a közös titokból (Ki). A8: kulcsgeneráló algoritmus (egyirányú fv)

A5: Álvéletlen sorozat generátor. OFB módú folyamkódoló. A8 által generált kulccsal dolgozik. 3.5 órás periódusidő. Európa: A5/1, export A5/2 (nem nyilvánosak a részletek)

Problémák

Nem nyilvános részletek. Gyorsan körbeforduló kulcsfolyam. Általában a Kc utolsó 10 bitjét 0-ra állítják. Csak a hozzáférési hálózati van titkosítás. Nincs hálózathitelesítés. A5/1 és A5/2 is támadható. 500 000 SIM lekérdezéssel törhető.

UMTS

Célkitűzések

- (1) Gyakori azonosítás
- (2) Forgalom titkosítása a hozzáférési hálózatban
- (3) Hitelesítés az előfizetői és szolgáltató közös titka alapján
- (4) **Új:** Kölcsönös hitelesítés, hitelesítés gerinchálózaton is. Integritásvédelem a hozzáférési hálózaton. Algoritmusok: f1...f5, f8, f9. Nyilvános és elérhető leírás. Bővíthetőség. Erősebb kriptográfiai algoritmusok.

f1...f5: Csak az USIM és az AC-n vannak implementálva, szolgáltató választása.

SQN: Dinamikus, USIM tárolja. Az SQN kezelés operátorfüggő lehet. Ellenőrizni kell, hogy inkrementális legyen a használata (ne használják fel újra)

További eltérések

UTRAN szakaszon is titkosítás

Kulcs mellett használnak még: számlálót, különböző vivők, adatfolyam iránya, hossz

	GSM	UMTS
<i>Hitelesítés</i>	Felhasználó	Kölcsönös
<i>Titkosítás</i>	Rádiós interfészen	Gerinchálózaton is
<i>Algoritmusok</i>	Titkos	Nyilvános
	Gyengített	Megfelelő
	Fix választék	Bővíthető
<i>Integritás védelem</i>	-	Hozzáférési hálózat