Az IEEE 802.16 szabvány közeghozzáférési (MAC) rétege

SZALAY MÁTÉ, GÓDOR GYŐZŐ, IMRE SÁNDOR

Budapesti Műszaki és Gazdaságtudományi Egyetem, Híradástechnikai Tanszék
{szalaym, godorgy, imre}@hit.bme.hu

Kulcsszavak: WiMAX, MAC, közeghozzáférés, IEEE 802.16

Cikkünkben az IEEE 802.16 szabvány közeghozzáférési rétegét mutatjuk be. A referenciamodell bemutatása után részletesen kitérünk a szolgáltatás specifikus alrétegre, a közös alrétegre és a biztonsági alrétegre. A cikk a 802.16-2004 szabvány alapján készült [1].

1. Bevezetés

1.1. A 802.16 szabvány

Az IEEE 802.16 szabvány egy nagysebességű, nagy hatótávolságú, vezeték-nélküli telekommunikációs protokoll BWA (Broadband Wireless Access) fizikai és közeghozzáférési szintjeinek definícióját tartalmazza.

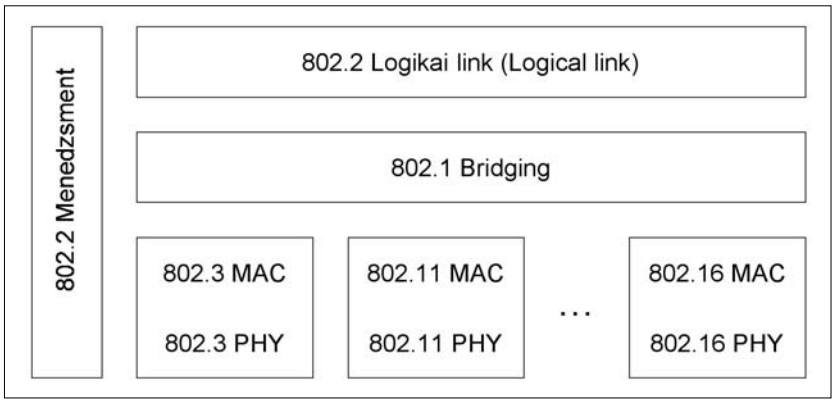
A 802.16 ugyanúgy közeghozzáférési és fizikai rétegeket definiál, mint a 802.3 (Ethernet), a 802.5 (Token ring) vagy a 802.11 (WLAN). A 802.16 szabvány helyét a többi IEEE 802 szabvány között az *1. ábra* mutatja.

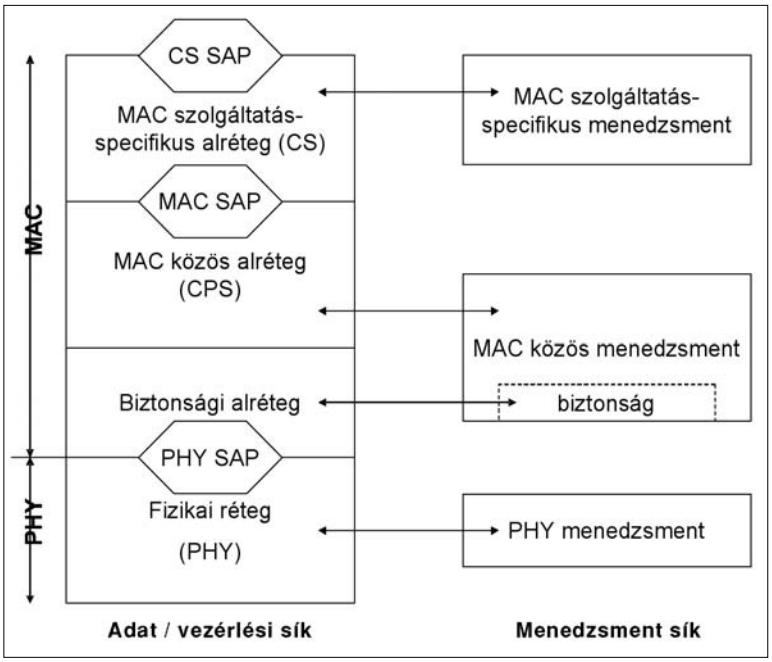
1.2. Referenciamodell

A 802.16 szabvány referenciamodelljét a *2. ábra* mutatja. A modell adat/vezérlési és menedzsment síkra osztható. A 802.16 szabvány csak az adat/vezérlési síkot definiálja, a menedzsment síkkal nem foglalkozik.

Az adat/vezérlési sík két rétegből áll: a fizikai (PHY) rétegből, és a fölötte elhelyezkedő közeghozzáférési (MAC) rétegből. Ez a cikk a közeghozzáférési réteget mutatja részletesen. A fizikai réteg a PHY SAP-on (Service Access Point, szolgálat-elérési pont) keresztül nyújt szolgáltatásokat a közeghozzáférési réteg számára.

1. ábra IEEE 802.16 helye az IEEE 802 szabványok közt





2. ábra A 802.16 referenciamodell

1.3. A MAC réteg felépítése

A közeghozzáférési réteg tovább bontható három alrétegre. Ezek: a legfelül elhelyezkedő szolgáltatásfüggő konvergencia-alréteg (CS), a közös-alréteg (CPS), és a biztonsági-alréteg (Security).

A szolgáltatás-függő konvergencia alréteg a CS SAP-on keresztül, felsőbb rétegektől érkező külső adatokat képezi le MAC SDU-kra, amelyeket a közös alréteg kap meg a MAC SAP-on keresztül. Különböző protokollokhoz különböző konvergencia alréteg specifikáció tartozik, tehát különböző formátumú MAC SDU-k keletkeznek. A közös alréteg nem értelmezi a kapott MAC SDU-kat, hanem PDU-ként (Protocol Data Unit) tekint rájuk. A közös alréteg olyan feladatokat lát el, mint sávszélesség allokálás, kapcsolat-felépítés és kezelés, ütemezés.

A MAC réteg legalul elhelyezkedő alrétege a biztonsági alréteg, amely kulcskezelési és adattitkosítási funkciókat valósít meg.

Az alrétegeket a következőkben részletesen fogjuk tárgyalni.

2. A szolgáltatás-specifikus konvergencia alréteg

A szolgáltatás-specifikus konvergencia alréteg közvetlenül a MAC közös-alréteg (MAC CPS) fölött helyezkedik el, és a MAC-SAP-on keresztül a közös-alréteg által nyújtott szolgáltatásokat használja. A konvergencia alréteg a következő feladatokért felel:

– fogadja a magasabb rétegből érkező PDU-kat;
– osztályozza a magasabb rétegekből érkező PDU-kat;
– ha az osztályozás alapján szükséges, akkor feldolgozza a magasabb rétegből érkezett PDU-kat;
– a CS-PDU-kat eljuttatja a megfelelő MAC-SAP-hoz (szolgálat-elérési ponthoz);
– fogadja a CS rétegbeli partner entitásoktól érkező CS-PDU-kat.

Eddig két konkrét konvergencia-alréteg definíciót tartalmaz a szabvány, de ez természetesen bővülhet a jövőben. A jelenleg definiált két CS a következő:

– ATM (aszinkron átviteli mód) konvergencia-alréteg
– Csomag (packet) konvergencia-alréteg

Ezt a két közös-alréteget mutatjuk be röviden a következőkben.

2.1. Az ATM konvergencia-alréteg

Az ATM konvergencia-alréteg (CS) egy logikai interfész, amely a különböző ATM szolgáltatásokat a MAC-CPS SAP-hoz rendeli. Az ATM-CS a fölötte elhelyezkedő ATM-rétegtől ATM-cellákat fogad, osztályozza azokat, esetleg fejléc-tömörítést hajt végre, és az így keletkezett PDU-t eljuttatja a megfelelő MAC-SAP-hoz. Az ATM-CS egyaránt képes SVC, PVC és soft-PVC ATM kapcsolatok kezelésére.

Mivel az ATM virtuális kapcsolatok az ATM szabványnak megfelelően épülnek fel, a 802.16 szabvány nem definiál szolgáltatási primitíveket az ATM konvergencia alréteghez.

A jobb sávszélesség-kihasználás érdekében egyrészt lehetőség van a szállított ATM cellák fejlécének tömörítésére, másrészt egy MAC PDU szállíthat több, ugyanahhoz a kapcsolathoz tartozó ATM cellát.

2.2. A csomag konvergencia-alréteg

A csomag konvergencia-alréteg a következő feladatokat látja el:

– osztályozza a felsőbb rétegből érkező PDU-kat;
– megállapítja, hogy melyik kapcsolathoz tartoznak az érkezett PDU-k;
– ha szükséges, fejléc-tömörítést hajt végre;
– az így keletkezett CS-PDU-kat eljuttatja a megfelelő MAC-SAP-hoz;
– fogadja a más MAC-SAP-októl érkezett CS-PDU-kat;
– visszaállítja az esetlegesen elhagyott fejléc-mezőket.

A csomag konvergencia-alréteg használható tetszőleges csomagkapcsolt protokoll továbbítására, úgy mint IP, PPP, vagy 802.3 Ethernet.

Ugyanúgy, mint az ATM konvergencia-alréteg esetében, itt is lehetőség van a szállított csomag fejlécének tömörítésére.

2.3. A MAC SAP

A konvergencia-alréteg és a közös-alréteg közötti interfész egy logikai interfész, az itt definiált protokoll-primitívek informatívak, azt mutatják meg, hogy milyen információk átadására van szükség a két alréteg között. A két réteg határán helyezkedik el a MAC-SAP (lásd 2. ábra).

A MAC SAP-on a szabvány a következő protokoll-primitíveket definiálja:

```
MAC_CREATE_SERVICE_FLOW.request
MAC_CREATE_SERVICE_FLOW.indication
MAC_CREATE_SERVICE_FLOW.response
MAC_CREATE_SERVICE_FLOW.confirmation
MAC_CHANGE_SERVICE_FLOW.request
MAC_CHANGE_SERVICE_FLOW.indication
MAC_CHANGE_SERVICE_FLOW.response
MAC_CHANGE_SERVICE_FLOW.confirmation
MAC_TERMINATE_SERVICE_FLOW.request
MAC_TERMINATE_SERVICE_FLOW.indication
MAC_TERMINATE_SERVICE_FLOW.response
MAC_TERMINATE_SERVICE_FLOW.confirmation
MAC_DATA.request
MAC_DATA.indication
```

A MAC_CREATE_... primitíveket egy új kapcsolat felépítésekor használjuk. A MAC_CHANGE_... primitíveket egy kapcsolat paramétereinek megváltoztatására használjuk, a MAC_TERMINATE_... primitíveket pedig a kapcsolat lebontására. A változtatást és lebontást szintén kezdeményezheti a bázisállomás és az előfizetői állomás is. Adatáramlás a MAC_DATA... primitívek segítségével történhet.

3. Közös-alréteg

Egy hálózatnak, mely megosztott közeget használ, szüksége van egy hatékony közeghozzáférési mechanizmusra. A 802.16 szabvány kétirányú pont-multipont (PMP) és Mesh topológiájú vezeték nélküli hálózatokat definiál. Ebben az esetben a közeg maga a tér, melyben a rádióhullámok terjednek.

PMP esetben a downlink irány a bázisállomástól (BS) az előfizetői állomás (SS) felé mutató irány, a másik pedig az uplink irány. A 802.16 szabvány vezetéknélküli kapcsolatot definiál, ahol középen a bázisállomás helyezkedik el, illetve szektor-antennák segítségével párhuzamosan szolgálja ki a független szektorokat. Egy

adott frekvencia csatornát és egy antenna szektort tekintve az összes előfizetői állomás ugyanazt az adást veszi. Egyedül csak a bázisállomás adhat ebben az irányban, így nem kell szinkronizáljon más állomásokkal, egyedül csak az esetleges idő osztású duplexálást (TDD) kell figyelembe vegye, mely meghatározza, hogy egy időszeletet milyen módon kell továbbosztani uplink és downlink adási periódusokra. Downlink irányban tehát általában broadcast üzenettovábbítás történik.

Uplink irányban az előfizetői állomások igény alapján osztoznak a kapacitáson, melyet az adott szektoron belül a bázisállomás oszt szét köztük. A bázisállomás lekérdezi az egységeket, hogy mekkora uplink irányú sávszélességre van szükségük. Az előfizetői egység sávszélességet kérhet a bázisállomástól, mire az sávszélességet oszt ki neki.

Az egy címzetthez szóló üzeneteken kívül lehetőség van címzettek egy csoportjához címzett (multicast) és mindenkinek címzett (broadcast) üzenetek küldésére is.

A szabvány definiál egy másik topológiát is, a Mesh topológiát. Ennek megvalósítása opcionális a 802.16 szabvány alapján. A fő különbség a PMP esethez képest az, hogy míg PMP módban a forgalom csak a bázisállomás és az előfizetői egységek között zajlik, addig Mesh módban a forgalom más előfizetői állomásokon is keresztülhaladhat, illetve közvetlen kommunikáció is lehetséges két előfizetői egység között.

A MAC összeköttetés alapú. A rendszerhez kapcsolódott előfizetői állomások minden forgalma úgynevezett kapcsolatokon keresztül történik. Egy felépített kapcsolat a típusától függően több-kevesebb karbantartást igényelhet. Az IP-alapú kapcsolatoknak például magas a karbantartás igénye, mert tipikusan burst-ösek, és a csomagok szétdarabolását és összerakását (fragmentation) is kezelni kell. A kapcsolatok paramétereiben történő változást, valamint a kapcsolatok befejezését a bázisállomás és az előfizetői állomás is kezdeményezheti.

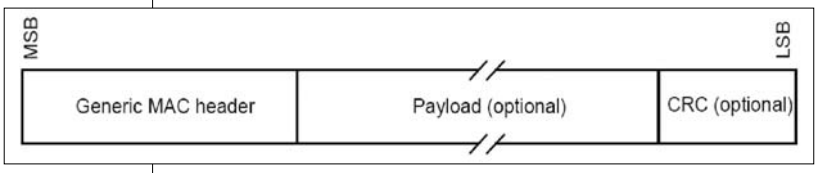
3.1. Címzés

Az IEEE 802-2001 szabványnak megfelelően minden előfizetői állomásnak van egy 48 bites, globálisan egyedi azonosítója (MAC address). PMP esetben ezt az egyedi azonosítót a regisztrációs folyamatnál, az előfizetői egységgel való kapcsolat kiépítéséhez használják. Szerepet játszik még a hitelesítési folyamatnál is, ahol a bázisállomás és az előfizetői állomás egymás identitását ellenőrzik. Mesh módban ezt a címet a hálózatba való belépés folyamán, illetve az adott csomópont és a hálózat közötti kölcsönös hitelesítési folyamat során használják.

A kapcsolatokat egy 16 bites kapcsolat-azonosító (CID) azonosítja. Az előfizetői állomás inicializálásakor irányonként három kapcsolat épül fel a bázisállomás és az előfizetői állomás között. A három különböző kapcsolatra azért van szükség, mert különböző menedzsment-üzeneteknek különböző QoS-re van szükségük. Az előfizetői állomás és a bázisállomás az alap-kapcsolaton (basic connection) rövid és késleltetés-érzékeny üzeneteket váltanak egymással, az elsődleges menedzsment-kapcsolaton (primary management connection) hosszabb, és késleltetés-tűrőbb üzeneteket, a másodlagos menedzsment-kapcsolaton (secondary management connection) pedig késleltetés-tűrő, valamilyen külső szabványnak megfelelő üzeneteket. A harmadik csoportba tartozhatnak például a DHCP vagy SNMP üzenetek.

Mesh mód esetén az egyik előfizetői állomás bázisállomásként viselkedik a többi előfizetői állomás felé. Ezt az előfizetői állomást nevezzük „Mesh-BS”-nek. Ha a hitelesítés megtörtént, a többi előfizetői állomás kap egy 16 bites csomópont azonosítót (Node ID) válaszként a Mesh BS-hez küldött kérésre. A csomópontok azonosítása a normál működés folyamán a Node ID-k segítségével történik. A Node ID a Mesh alfejlécben továbbítódik, mely az általános MAC fejlécet követi mind az unicast, mind pedig a broadcast üzenetek esetén.

A szomszédos csomópontok címzésére egy 8 bites link azonosítót (Link ID) kell használni. Minden egyes csomópontnak ki kell jelölnie egy azonosítót minden összeköttetéshez, mely valamelyik szomszédjával létesült. A Link ID-k a teljes kapcsolatlétesítési folyamat alatt továbbítódnak, mindaddig, míg a szomszédos csomópontok új összeköttetéseket alakítanak ki egymással. A Link ID unicast üzenetként továbbítódik a CID részeként az általános MAC fejlécben.

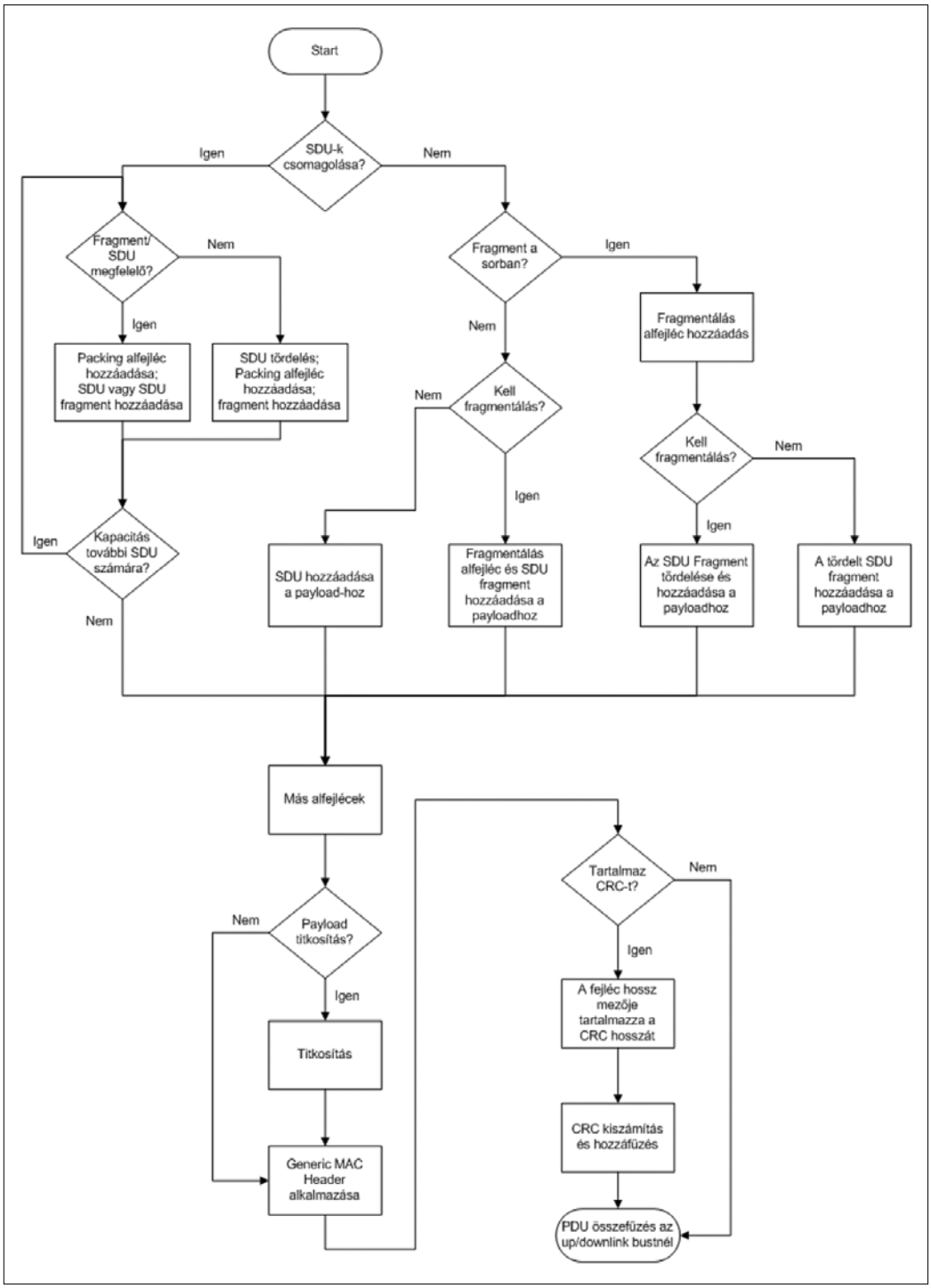


3. ábra A MAC PDU formátum

3.2. A MAC PDU formátum

Minden MAC PDU a *3. ábrán* látható struktúrájú. Minden egyes PDU egy fix hosszúságú általános MAC fejléccel (Generic MAC header) kezdődik. A fejlécet a MAC PDU Payload mezője követheti. Ha ez létezik, akkor a Payload nulla vagy több alfejlécből, nulla vagy több MAC SDU-ból és/vagy azok részeiből kell álljon. A payload információ változó hosszúságú lehet, így egy MAC PDU bájtok változó számát reprezentálhatja. Ez teszi lehetővé, hogy a MAC alagút technikával továbbítson különféle magasabb szintű forgalmi típusokat ezen üzenetek formátumainak, vagy bit-mintáinak ismerete nélkül. A MAC PDU végül tartalmazhat egy CRC mezőt is.

A szabvány kétféle MAC header formátumot definiál. Az első az általános MAC fejléc (Generic MAC Header), mely minden MAC PDU legelején található és MAC vezérlési üzeneteket vagy CS adatokat tartalmaz. A második header formátum a sávszélesség kérés fejléc (Bandwidth Request Header), melyet további sávszélesség igényléskor használnak. Azt, hogy éppen melyik típusú fejlécről van szó, a fejlécben található HT (Header Type) bit jelzi: ha a bit 0 értékű, akkor Generic Header, ha 1 értékű, akkor Bandwidth Request Header.



4. ábra
A MAC PDU szerkesztésének folyamata

Mind az uplink, mind pedig a downlink irányban egy egyszerű átvitelbe összefűzhetőek összetett MAC PDU-k. Egy uplink burst átvitel esetén az összetett MAC PDU-t az *5. ábra* ismerteti.

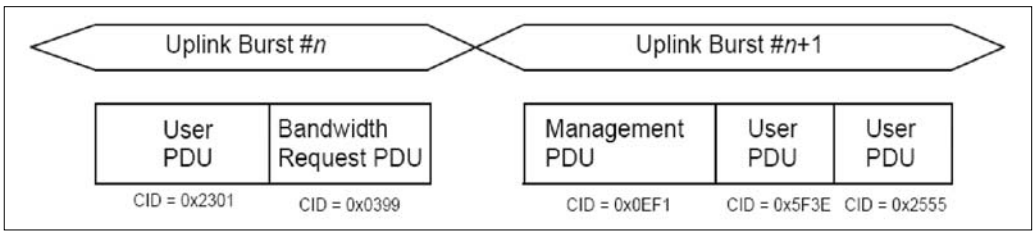
Minden egyes MAC PDU egy egyedi CID (Connection Identifier) azonosítóval van ellátva, amely azt jelzi, hogy melyik kapcsolathoz tartoznak. A CID alapján a vételi oldalon a MAC entitás össze tudja állítani a MAC SDU-t a fogadott MAC PDU-kból, és továbbítani tudja a felsőbb rétegek felé.

3.3. Fragmentáció

Fragmentációnak azt a folyamatot nevezzük, amikor egy MAC SDU egynél több MAC PDU-ba van szétosztva. Így a rendelkezésre álló sávszélesség hatékonyabb kihasználására, illetve egy adott kapcsolat esetén a QoS paraméterek biztosításának elősegítésére nyílik lehetőség. A szabvány a fragmentáció és a visszaállítás funkciókat kötelezően írja elő, vagyis minden eszközben implementálva kell, legyen.

Egy összeköttetésen a töredék forgalom (fragment traffic) engedélyezés akkor történik meg, mikor a MAC SAP felépíti a kapcsolatot. A fragmentációt downlink irányban a BS, míg uplink irányban az SS kezdeményezi.

A fragmentek egy toldalékkal (Fragmentation Control) jelzik helyzetüket az éppen aktuális SDU-ban, az *1. táblázatnak* megfelelően.



5. ábra
MAC PDU összefűzés

Fragment	Fragmentation Control (FC)
Első fragment	10
További fragmentek	11
Utolsó fragment	01
Fragmentáció nélkül	00

1. táblázat Fragmentálási szabályok

Ütemezési mechanizmus	PiggyBack kérés	Sávszélesség „lopás”	Lekérdezés
UGS	Nem lehetséges	Nem lehetséges	A PM bit segítségével kérhet unicast lekérdezést nem-UGS folyamok számára. Egyébként nincs lekérdezés.
rtPS	Lehetséges	Lehetséges	Csak unicast lekérdezés
nrtPS	Lehetséges	Lehetséges	Átviteli/kérési stratégián keresztüli unicast lekérdezés esetén korlátozható egy szolgáltatás folyam; máskülönben minden típusú lekérdezés lehetséges.
BE	Lehetséges	Lehetséges	Minden típusú lekérdezés lehetséges

2. táblázat
Ütemezési mechanizmusok uplink irányban

3.4. Ütemezés

Minden egyes kapcsolathoz társul egy egyszerű adatszolgáltatás, illetve minden adatszolgáltatáshoz QoS paraméterek egy halmaza kapcsolódik, mely meghatározza az adatok viselkedését. Ezen paraméterek kezelése a DSA (Dynamic Service Addition) és a DSC (Dynamic Service Change) üzenetek segítségével történik. A 802.16 szabvány négy különböző ütemezési mechanizmust definiál: Unsolicited Grant Service (UGS), Real-time Polling Service (rtPS), Non-real-time Polling Service (nrtPS) és Best Effort Service (BE).

Unsolicited Grant Service (UGS)

Ennél az ütemezési mechanizmusnál az előfizetői állomás kérés nélkül fix méretű engedélyt (grant) kap előre definiált szabályos időközönként. A lekérdezések megtakarításával ez a mechanizmus meghatározott időközönként fix méretű adatcsomagot igénylő szolgáltatásokhoz megfelelő. Ilyenek például a T1/E1 vagy a VoIP, ha nem alkalmazunk csend-elnyomást.

Real-time Polling Service (rtPS)

Ez a mechanizmus a real-time, de változó bitsebességű adatfolyamokhoz megfelelő. Ilyen például az MPEG videó-folyam. Az előfizetői állomás előre definiált fix időközönként igényelhet grant-et, melynek méretét minden alkalommal az előfizetői állomás határozhatja meg. Ennek az ütemezési mechanizmusnak valamivel nagyobb a jelzési overheadje, mint az UGS mechanizmusnak.

Non-real-time Polling Service (nrtPS)

Ez a mechanizmus a nem valós idejű, változó sávszélesség-igényű adatfolyamok számára megfelelő. Ilyen például az FTP fájl-átvitel. Az nrtPS osztályhoz tartozó CID-ket a bázisállomás tipikusan egy másodpercenként (vagy gyakrabban) kérdezi le. Ez az időköz valós idejű folyamok számára nem lenne megfelelő.

Best Effort Service (BE)

Ez a mechanizmus a best-effort típusú forgalomhoz illeszkedik. Az uplink, vagyis felfelé-irányú ütemezés célja a poll/ grant mechanizmus hatékonyságának növelése. Például nyilván nem hatékony a hosszú ideig inaktív előfizetői állomás folyamatos, gyakori lekérdezése (polling). A megfelelő ütemezés, és a hozzá tartozó megfelelő QoS paraméterek beállításával elérhető, hogy a felfelé irányú forgalom késleltetése és sávszélessége megfeleljen az elvárásoknak, és a lekérdezések (polling) és engedélyezések (grant) a megfelelő időben érkezzenek. A *2. táblázat* ismerteti az uplink irányú ütemezési megoldásokat.

3.5. Sávszélesség allokálás

Ahogy már írtuk, a hálózatba való belépés során, illetve inicializáláskor minden előfizetői állomáshoz az előfizetői állomás és a bázisállomás között irányonként három kapcsolat épül fel. Ezen kapcsolatok vezérlési üzenetek fogadására és továbbítására szolgálnak. A kapcsolat-párok QoS szintek segítségével vannak elkülönítve egymástól, ezáltal lehetővé téve, hogy a különböző kapcsolatok más-más MAC vezérlési forgalmat bonyolítsanak.

Ha egy kapcsolaton a sávszélesség növelésére van szükség, akkor ezt az igényt az előfizetői állomásnak valamilyen módon jeleznie kell a bázisállomás felé. Az ilyen sávszélesség kérések lehetnek inkrementálisak (incremental) vagy aggregáltak (aggregate). A sávszélesség kérés fejlécének Type mezője tartalmazza, hogy milyen fajta kérés érkezett. Az inkrementális kérés azt tartalmazza, hogy az előfizetői állomás mekkora sávszélesség növelést/csökkentést szeretne a kapcsolat eredeti sávszélességéhez képest. Aggregált kérés esetén az üzenet azt tartalmazza, hogy mekkora legyen a kapcsolat sávszélessége (a régi sávszélesség helyett). Hogy a mechanizmus önkorrigáló legyen, az előfizetői állomások kötelesek bizonyos időközönként aggregált sávszélesség-kérést küldeni.

A sávszélesség kérésre (request) a bázisállomás sávszélességet ad (grant) az előfizetői állomásnak. A sávszélesség-kérések kapcsolatra vonatkoznak, míg a sávszélességet az előfizetői állomás egyben kapja (tehát nem kapcsolatonként). Előfordulhat, hogy az előfizetői állomás kisebb sávszélességet kap, mint amit kért. Ennek oka például az ütemező döntése, vagy a kérés üzenet (request) elveszése lehet. Fontos azonban, hogy ha az előfizetői állomás kisebb sávszélességet kapna a kértnél, akkor nem ismeri ennek okát. Ha kisebb sávszélességet kapott, akkor vagy újabb kéréssel próbálkozik, vagy eldobja a feldolgozás alatt lévő SDU-t.

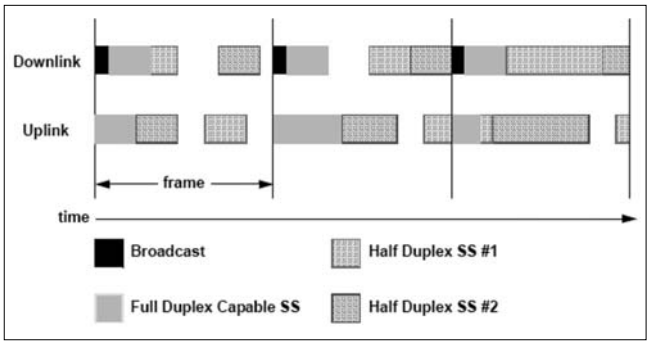
A lekérdezés (polling) tulajdonképpen az a mechanizmus, amikor a bázisállomás sávszélességet allokál az előfizetői állomásnak azzal a céllal, hogy sávszélesség igényt (request) küldhessen. A lekérdezés címezhető egy konkrét előfizetői állomásnak, de sávszélesség-hiány miatt előfordulhat, hogy a lekérdezést a bázisállomás egyszerre egy előfizetői-állomás csoporthoz (multicast), vagy a szektor összes előfizetői állomásához (broadcast) intézi.

3.6. A PHY réteg MAC rétegbeli támogatása

A MAC protokoll számos duplexálási technikát támogat. A duplexálási technika megválasztása hatással lehet bizonyos PHY paraméterekre.

FDD

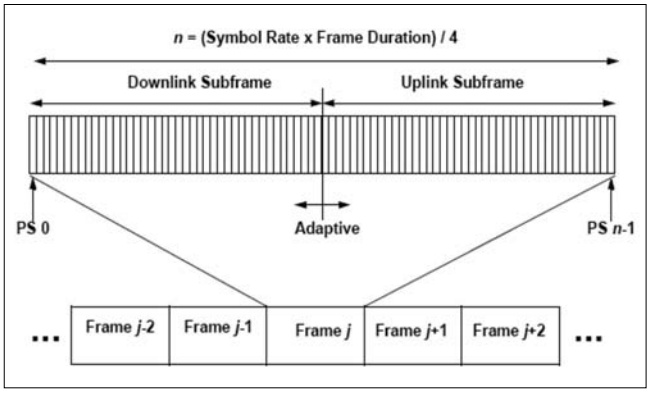
Ebben az esetben az uplink és a downlink csatornák különböző frekvenciákra vannak szétválasztva. A burst-ökben való adattovábbítás lehetővé teszi az egy rendszeren belüli különféle modulációs technikák alkalmazását, illetve engedélyezi a rendszernek a full-duplex SS (adás és vétel történhet egyszerre is) és a half-duplex SS (egyszerre csak az egyik történhet) átvitel együttes alkalmazását. A *6. ábra* példát mutat az FDD keretre.



6. ábra Példa a frekvencia osztásos duplexálásra

TDD

Ebben az esetben az uplink és a downlink átvitel azonos frekvencián történik, de időben szét vannak választva, mint ahogy ez a *7. ábrán* látható. A TDD keretnek egy fix időtartam van definiálva, ami tartalmaz egy downlink és egy uplink alkeretet.



7. ábra Egy TDD keret felépítése

A downlink burst és a következő uplink burst között található rés, a TTG (transmit/receive transition gap), mely időt biztosít arra, hogy a BS át tudjon kapcsolni adási üzemmódból vételibe, illetve az SS át tudjon kapcsolni vételiből adási módba. Ez alatt az idő alatt nincs modulált adatátvitel a BS és az SS között. A TTG befejeztével a BS vevő figyelni fogja, mikor jön az uplink burst első szimbóluma.

Az RTG (receive/transmit transition gap) résnek hasonló a szerepe, mint a TTG résnek. Ezen időrés alatt a BS átkapcsol vételi üzemmódból adásiba, illetve az SS adásiból vételibe. Az időrés alatt szintén nem megy modulált adat, és az időrés befejeztével az SS vevők figyelik a QPSK modulált adat első szimbólumát a downlink burst-ben.

Keretszervezés

Ez a PHY specifikáció keretszervezéses csomagtovábbítással működik. Minden egyes keretben található egy downlink és egy uplink alkeret. A downlink alkeret a keretszinkronizáció és a vezérlés számára elengedhetetlenül szükséges információkkal kezdődik. TDD esetben a downlink alkeret az első, ezt követi az uplink alkeret. FDD esetében az uplink adattovábbítások egyidejűleg történnek a downlink kerettel. Minden egyes SS meg kell próbálja venni a downlink keret összes részét, kivéve azon burst-öket is, melyek burstprofilja vagy nincs implementálva az SS-ben, vagy kisebb robosztussággal bír, mint az SS épp működésben lévő burstprofilja. A half-duplex SS-eknek nem kell megkísérelni a downlink részeit hallgatni, ha az egybeesik a kiosztott uplink adatátvitelükkel.

4. A biztonsági alréteg

A biztonsági alréteg, a 802.16 szabvány MAC rétegének legalsó alrétege kettős feladatot lát el. Egyrészt biztosítja az adatok titkosságát a bázisállomást és az előfizetői állomást összekötő linken. Ezáltal az előfizető biztos lehet, hogy forgalma nem kerül jogosulatlan harmadik fél kezébe. Másrészt a megszemélyesítéses támadások (szolgáltatás lopás, „service theft") ellen is véd. Ez mind az előfizetőnek, mind pedig a szolgáltatónak az érdeke.

Ha az előfizetői állomás a képességek egyeztetésekor azt közli, hogy nem támogatja a 802.16 biztonsági mechanizmusokat, akkor a bázisállomás a beállításainak megfelelően vagy a hitelesítési lépés kihagyásával hitelesítettnek tekinti az előfizetői állomást (nyitott rendszer), vagy megtagadja a szolgáltatást az előfizetői állomástól. Egyik esetben sincs a linken se kulcscsere, se titkosítás.

4.1. Biztonsági protokollok

A biztonsági alréteg két protokollból áll:

– Egy encapsulation (beágyazó) protokollból, amely adattitkosító- és hitelesítő-algoritmusokból, valamint az ezek alkalmazására vonatkozó szabályokból áll.

– Egy kulcsmenedzsment protokollból (PKM, privacy key management), amely a kulcsok bázisállomástól az előfizetői állomáshoz való eljuttatására, valamit egyéb kulcskezelési feladatok ellátására szolgál.

4.2. Csomagtitkosítás

A csomagok titkosítása a biztonsági alréteg feladata. A MAC fejléc tartalmaz a titkosítással kapcsolatos mezőket, tehát nincs külön – a titkosítással kapcsolatos – fejléc.

A csomagtitkosítás a MAC PDU-ra vonatkozik, a MAC-fejléc nincs titkosítva, a MAC menedzsment üzenetek tehát titkosítás nélkül kerülnek továbbításra. A csomag-

titkosítás DES vagy AES algoritmussal történik, de a szabvány „nyitott” olyan értelemben, hogy csomagtitkosításra használt algoritmusok köre a jövőben bővülhet.

4.3. Kulcsmenedzsment

A kulcsmenedzsment protokoll segítségével vizsgálja meg a bázisállomás, hogy az előfizetői állomás jogosult-e a szolgáltatás igénybevételére, valamit elvégzi a kulcs eljuttatását az előfizetői állomáshoz. Lehetőség van adott időközönként a jogosultságok újra-ellenőrzésére, és a kulcsok frissítésére.

A kulcsmenedzsment protokoll az IETF RFC 3280-ban [2] definiált X.509 tanúsítványokat, RSA nyilvános kulcsú titkosítást, és más erős szimmetrikus-kulcsú titkosító eljárásokat (3DES, AES) használ. Az algoritmusoknak ez, a kulcsmenedzsmentben használt köre is bővülhet a jövőben.

A PKM kulcsmenedzsment protokoll kliens-szerver architektúrát követ. A bázisállomás, a kliens, kulcs-anyagot (keying material) kér a szervertől, vagyis a bázisállomástól. A PKM kulcsmenedzsment protokoll MAC-menedzsment üzeneteket használ.

A PKM protokoll úgy működik, hogy első lépésben nyilvános kulcsú kriptográfiai algoritmusok segítségével egy osztott titkot (shared secret) generál a bázisállomás és az előfizetői állomás, majd a forgalom-titkosító kulcsokat (TEK, traffic encription key) ennek az osztott titoknak a felhasználásával, szimmetrikus kulcsú algoritmusok használatával cserélik ki. Ennek a megoldásnak az az előnye, hogy a forgalom-titkosító kulcsokat a rendkívül számításigényes nyilvános kulcsú algoritmusok használata nélkül tudják frissíteni.

A bázisállomás az előfizetői állomást a kezdeti jogosultság-ellenőrzéskor hitelesíti. Minden előfizetői állomásnak van egy X.509 tanúsítványa, amelyet a gyártója bocsátott ki, és programozott bele az eszközbe. Ez a tanúsítvány tartalmazza, vagyis egymáshoz rendeli az előfizetői állomás MAC-címét és nyilvános kulcsát. A hitelesítés úgy történik, hogy az előfizetői állomás elküldi a tanúsítványát a bázisállomásnak. A bázisállomás a tanúsítvány ellenőrzése után a tanúsítványban található nyilvános kulccsal eltitkosít egy „authorization key”-t (AK), és elküldi az előfizetői állomásnak. Ezután a bázisállomás hozzárendeli a már hitelesített identitást azokhoz a szolgáltatásokhoz, melyeket jogosultságai alapján az előfizető elérhet. Ezzel a módszerrel azt is elkerüljük, hogy egy támadó egy jogos felhasználó nevében lépjen fel (megszemélyesítéses támadás), és azt is, hogy egy jogos felhasználó hamis identitással próbáljon meg fellépni a hálózat felé.

Minden előfizetői állomásnak vagy a gyártó által előre beprogramozott RSA titkos/nyilvános kulcspárja van, vagy egy mechanizmussal maga képes kulcspárok generálására. Ha előre beállított kulcspárral rendelkezik, akkor előre megkapja a nyilvános kulcsot tanúsító X.509 tanúsítványt a gyártótól. Ez a megoldás biztonsági problémákat vet fel, mert a gyártó ismerni fogja a titkos kulcsokat is, tetszőleges tanúsítványt ki tud állítani, és bármelyik eszközt meg tudja személyesíteni. Ha maga generálja a kulcspárt, akkor ezt az első hitelesítési lépés előtt meg kell tennie, és utána valamilyen mechanizmus segítségével egy X.509 tanúsítványt kell beszereznie, amely igazolja a generált kulcsok hitelességét.

4.4. Security Association (SA)

Az SA biztonsággal kapcsolatos információk egy csoportja, amely egy bázisállomás és a hozzá tartozó egy vagy több előfizetői állomás közötti biztonságos kommunikációt segíti elő, a paramétereket, algoritmusokat írja le. A 802.16 szabvány háromféle SA típust definiál: elsődleges (primary), statikus (static) és dinamikus (dynamic). Az elsődleges SA-t az előfizetői állomás az inicializációs folyamatban építi ki. A statikus SA-kat a bázisállomás megtartja, a dinamikus SA-k pedig menet közben keletkeznek és szűnnek meg a különböző adatfolyamok keletkezésével és megszűnésével. Mind a statikus, mint a dinamikus SA-k tartozhatnak egyszerre több előfizetői állomáshoz is.

Az SA-kat SAID-k azonosítják. Minden előfizetői állomás, kapcsolódáskor felépít egy darab elsődleges SA-t, melynek SAID-je megegyezik az alap-kapcsolat (basic connection) CID-jével.

A további SA-khoz az előfizetői állomás kér kulcs-anyagot (például DES kulcs és inicializáló vektor (IV)) a bázisállomástól. A kulcs-anyagnak korlátozott élettartama van, amelyet a bázisállomás a kulcs-anyaggal együtt eljuttat az előfizetői állomásnak. A kulcs-anyag élettartamának lejárása előtt az előfizetői állomásnak új kulcs-anyagot kell kérnie a bázisállomástól.

Hogy a titkosítás folyamatos maradjon, mindig két érvényes forgalom-titkosító kulcs van, melyek nem egyszerre járnak le, hanem átlapolódva. Mikor az egyik lejár, újat generálnak helyette, de addig a másik kulcsot lehet használni, így a szolgáltatás folyamatossága biztosított.

5. Összefoglalás

Cikkünkben áttekintettük az IEEE 802.16-2004 szabvány közeghozzáférési (MAC) rétegét. Alrétegenként haladva felülről lefelé, először bemutattuk a szolgáltatás specifikus alréteg ATM-hez illeszkedő és csomag típusú forgalomhoz illeszkedő változatait, majd a közös alrétegnél kitértünk a címzésre, MAC PDU felépítésére, az ütemezésre, illetve a fizikai réteg támogatására. Végül a biztonsági alréteg tárgyalásánál leírtuk, hogy hogyan működik az adattitkosítás és a kulcsmenedzsment.

Irodalom

[1] IEEE Standard for local and metropolitan area networks, Part 16:
Air Interface for Fixed Broadband Wireless Networks, URL: http://ieee802.org/16/pubs/80216-2004.html

[2] 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, URL: http://www.faqs.org/rfcs/rfc3280.html