MMXVI. IV. ÉVFOLYAM III. SZÁM

NEMZETBIZTONSÁGI SZEMLE

KÜLÖNLENYOMAT

NEMZETI KÖZSZOLGÁLATI EGYETEM
NEMZETBIZTONSÁGI INTÉZET
BUDAPEST

Műholdas felmenő hívások detektálása Winrádióval

Szűcs Péter[1]

Absztrakt:

Kutatási témám a „Műholdas személyi távközlési rendszerek felderíthetősége, a felderítés végrehajtásának metodikája, a keletkezett információk felhasználása Magyarország biztonsága érdekében”. A „Haza Szolgálatában 2014” konferencián bemutattam kutatási témám első eredményét, az Iridium rendszer felmenő hívásainak felderíthetőségét. Folytatva kutatásaimat második cikkemben jelentést teszek a Thuraya rendszerben indított telefonhívások detektálhatóságáról. A sorozat folytatásaként bemutatom, hogyan lehet felderíteni egy Inmarsat telefonról kezdeményezet hívást. Mindhárom rendszerben a detektáláshoz Winrádiót használtam, ezért jelen cikkemben, e rádiók felépítését, felhasználási sokoldalúságát kívánom bemutatni.

Kulcsszavak: szoftverrádió, vevőkártya, spektrumkép, moduláció, demoduláció, IQ.

Abstract:

My research topic is the detection of personal satellite communication systems, method of detection procedure and use of acquired information in order to protect the security of Hungary. ”In the service of my country 2014” conference presented the first results of the research topic, the Iridium system calls to the ascending detectable. Continuing my research in my article I launched a report on the Thuraya system calls reconnaissance. As a continuation of the series shows how to detect an Inmarsat phone to make a call. All three detection system to Winradios were used, so in this article I build this radio, I intend to present the versatility of use.

Keywords: Winradio, SDR, softvware defined radio, IQ

[1] *NKE KMDI doktorandusza, szucs.peter@nbsz.gov.hu ORCID: 0000-0001-8033-6230*

Bevezetés

A szoftvervezérlésű rádió, rövidebb elnevezésével a szoftverrádió Software Derfined Radio (SDR) definíciója szerint: „*olyan rádiótechnológia, amely szoftveres úton lehetővé teszi a modulációs eljárások széles körének kiválasztását, a széles, vagy keskenysávú üzemmódokat, a forgalmazás különböző eljárásokkal való rejtését, titkosítását, az adott hullámsávban jelenleg, vagy akár a jövőben használatos szabványok, eljárások rugalmas beépítését, alkalmazását. A szoftverrádió technológia olyan funkcionális moduloknak szoftveres eszközökkel egy rádiórendszerbe való összekapcsolása, mint például:*

- *oszcillátor (jelgenerátor);*
- *modulátor /demodulátor;*
- *kódoló (kapcsolati réteg protokollok);*
- *sokszorozók/osztók, stb.”*[2]

Az SDR technológia lehetővé teszi a programozható hardver modulok összekapcsolását és ennek a nyílt architektúrának a felhasználó igényeinek leginkább megfelelő szoftverrel való együttműködését. A rádiókészülékek alapvető paramétereit meghatározó oszcillátorok, modulátorok, demodulátorok, kódolók, dekódolók, titkosítók és az együttműködést meghatározó kapcsolati réteg protokollok működését és jellemzőit a szoftver határozza meg, így szükség esetén az egész rendszer egy szoftverfrissítéssel újabb szabványok alkalmazására tehető alkalmassá, vagy akár egy újabb berendezés típussá alakítható át. Ezáltal az egész berendezés a hardverelemek cseréje nélkül is modernizálható.[3]

Winrádió bemutatása

A WINRADIO WR-G39DDC rádióvevő két verzióban érhető el:

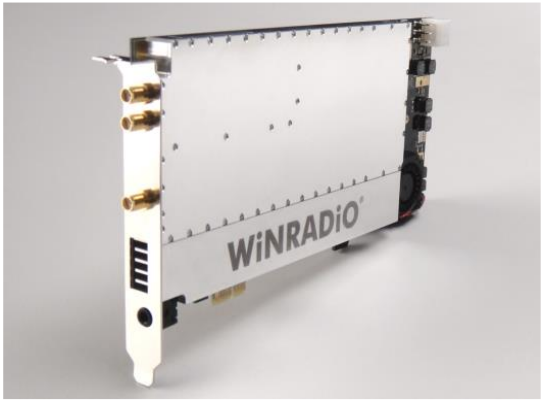
- külső eszközként WR-G39DDCe USB (Universal Serial Bus) csatlakozóval
- alaplaphoz integrálva WR-G39DDCi

A két eszköz rádiófrekvenciás egységében nincs különbség, de a WR-G39DDCe eszköznél a második vevőegység DDC (Digitally Down Converted) sávszélessége 2 MHz-ben van maximalizálva, az USB adatátviteli kapacitásának limi-

[2] *Dr. Ványa László: Út a szoftverrádiók és szoftver rádiózavaró állomások felé. Kommunikáció 2006, Zrínyi Miklós Nemzetvédelmi Egyetem konferencia kiadvány, ISBN: 978-963-7060-18-2, pp. : 76–83*

[3] *Uo.*

táltsága miatt. Méréseim során végig a WR-G39DDCe rádiót használtam. Mindkét berendezés alkalmas a spektrum vizsgálatára 0-tól 3,5 GHz-ig.



1.ábra: A WR-G39DDC Excelsior szoftvervezérelt rádióvevő fizikai felépítése[4]

Használatához vezérlő számítógépre van szükségünk, amelynek a következő minimum paraméterekkel kell rendelkeznie:

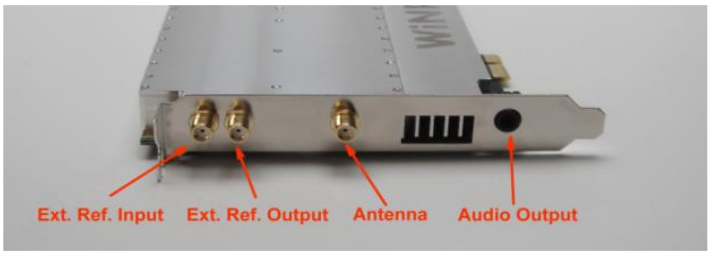
- CPU: 2 GHz Quad Core
- RAM: 2 GB RAM
- monitor: SVGA
- HD szabad terület: 20 MB
- Hangkártya: bármely Windows-kompatibilis kártya
- Csatlakozó: PCI Express (G39DDCi)
- Operációs rendszer: Windows XP, Vista, 7
- kártya feszültség igénye: 12V DC (+/- 1 V)
- kártya áramigénye: 2A

Látható, hogy nincs komoly gépigénye a vevőkártyának, ami a költségek szempontjából nem elhanyagolható. Egy kimenete van a hangnak (mini jack típusú) és egy SMA[5] típusú antennabemenet az elektromágneses jeleknek.

---

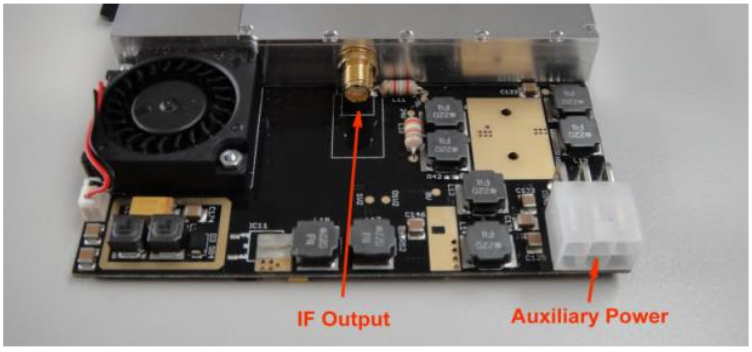
[4] WiNRADiO G39DDC User's Guide - Ver. 1.01.pdf

[5] Kicsi, 5 watt alatti teljesítményű VHF, UHF és SHF miniatűr kézirádiók esetén, illetve mikrohullámú berendezésekben, előszeretettel használják ezt a csatlakozótípust antenna csatlakoztatására.



2.ábra: G39DDCi PCIe kártya csatlakozói[6]

Alapesetben a vevőkártya a PCIe[7] busz rendszeren keresztül kapja az áramot, de amennyiben több vevőkártyát is integrálunk a számítógépbe, a megnövekedett áramigény kielégítésére egy külön 6 lábas áramcsatolási lehetőség is van. A vevőkártyában opcionálisan van egy KF középfrekvenciás kimenet is (70 MHz).



3.ábra: IF kimenet és külső tápcsatlakozó[8]

Beszerelés és telepítés a meghatározottak szerint egyszerűen elvégezhető. A szoftver a telepítés után egyszerűen futtatható, az asztalra kitett WiNRADiO ikonnal megnyitható. A szoftver automatikusan elindul, nem kell több másodpercet várni (mint több más berendezésnél), amíg az eszköz üzemkész lesz.

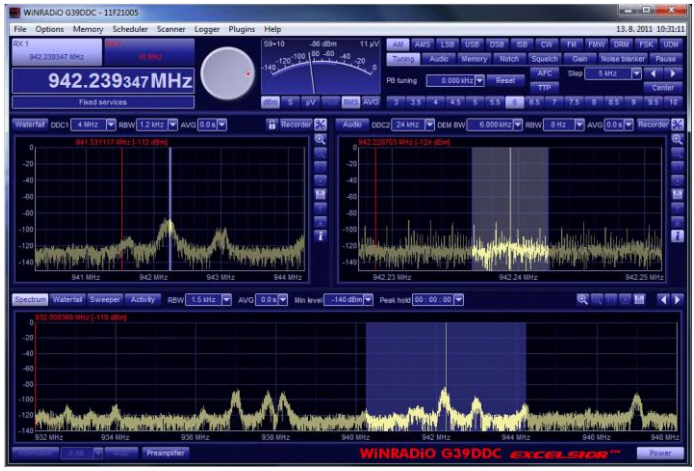
---

[6] *WiNRADiO G39DDC User's Guide - Ver. 1.01.pdf*

[7] *A PCIe a PCI-hoz hasonlóan az OSI modell alsó négy rétegét implementálja (fizikai, adatkapcsolati, hálózati és szállítási réteg). A legfelső réteg megvalósítása a két sín esetén kompatibilis, így az alkalmazások mindkét esetben ugyanazt a folytonos címzési modellt használhatják.*

[8] *WiNRADiO G39DDC User's Guide - Ver. 1.01.pdf*

A megnyitáskor a következő virtuális vezérlő panel jelenik meg a számítógép kijelzőjén:



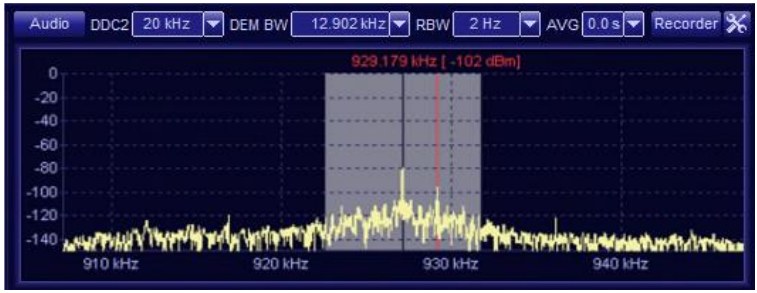
4.ábra: A virtuális vezérlő panelen a rádiós spektrum kép jelenik meg.[9]

5.ábra: Spektrum kijelzése a DDC1 felületen.[10]

A sávtartomány alapértelmezésben 20 KHz – 4 MHz közötti -, de amennyiben kiválasztjuk a széles sáv funkciót, akkor 20 KHz – 6 MHz között állítható. A frekvencia kiválasztott tartományon belül 26 lépésben állítható a minimum és ma-

[9] *WiNRADiO G39DDC User's Guide - Ver. 1.01.pdf*
[10] *Uo.*

ximum értékek között. Az idő 0 és 2 másodperc között állítható 21 lépésben 0,1 másodperces időközönként. A felderített frekvencia rögzíthető.



6.ábra: DDC2 panelen kijelezhető a rádióspektrum és az audiospektrum.[11]

A sávtartomány 20 KHz – 320 KHz között 13 lépésben állítható a minimum és maximum értékek között. Az idő 0 és 2 másodperc között állítható 21 lépésben 0,1 másodperces időközönként. A figyelt frekvencia itt is rögzíthető.

Az eszközzel egy időben két rádióállomás is lehallgatható, amennyiben 16 MHz-es sávon belül sugároznak. Ilyenkor engedélyeznünk kell az RX 2-es virtuális vevőegység alkalmazását, amivel párhuzamosan a DDC1-es panel sávtartományát 4 MHz-es maximális kijelzési sávszélességre „rontjuk" le.

7.ábra: RX1 és RX2 virtuális vevő kijelzője[12]

Az RX1-es és az RX2-es virtuális vevőegységre kell beállítani a kívánt frekvenciákat. Ezzel az opcióval két különböző frekvenciájú kommunikációt egy időben figyelhetünk. Nem kell folyamatosan hangolni a rádióvevőnket. Vett jeleket lehet külön-külön lehallgatni vagy egyszerre, és mindeközben a vett anyagok rögzítésére is van lehetőség.

8.ábra: Beállított rádiós frekvenciák ellenőrzése[13]

[11] *WiNRADiO G39DDC User's Guide - Ver. 1.01.pdf*
[12] *Uo.*

Lehetőség van előre elkészíteni olyan feladatot, amelyekben beállítjuk a figyelni kívánt frekvenciákat a hozzájuk tartozó paraméterekkel. Erre lehet példa, hogy beállítjuk egy feladatnak a 446,00625MHz-es és 446,100 MHz-es sáv közé eső analóg PMR[14] frekvenciák szkennelését. A feladat alkalmazásának elindításával a berendezés folyamatosan lépteti a fix frekvenciákat és a beállítások alapján megáll az adás folyamán, majd miután az adásnak vége, tovább lépteti a figyelt frekvenciákat. Az ily módon felfedett adásokat rögzíteni is tudjuk.

Lehetőség van egy meghatározott feladaton belül különböző modulációs módot használó jelek figyelésére is. Erre lehet példa a PMR frekvenciák és a DPMR[15] frekvenciák egyidejű beállítása.

A berendezés gyárilag a következő demodulátorokkal van felszerelve:

- AM Amplitúdó Moduláció
- AMS Amplitúdó Moduláció (Szinkron Demoduláció)
- LSB Alsó Oldalsávos
- USB Felső Oldalsávos
- ISB Független Oldalsávos
- DSB Két Oldalsávos
- CW Continuous Wave (Morse)
- FM Frekvencia Moduláció
- FMW Széles Sávú Frekvencia Moduláció
- DRM "Digital Radio Mondiale" (HF Digital Radio) „FM-szerű" minőségben, nagy távolságból vehető AM rendszerű műsorsugárzás leváltása.
- FSK Frekvenciabillentyűzés
- UDM Felhasználó által definiált működés

A vett jelek demodulálása egy gombnyomásra történik a kívánt demodulátor ikonjának lenyomásával. Amennyiben nem sikerült a jelet az elsőnek kiválasztott alkalmazással demodulálni, akkor a demodulátorok változtathatóak az ikonok

[13] *WiNRADiO G39DDC User's Guide - Ver. 1.01.pdf*

[14] *Personal Mobile Radio – személyi mobil rádió*

[15] *Digital Personal Mobile Radio – digitális személyi mobil rádió. A rendszer részére 446,100 – 446,200 MHz között 16 db 6,25 kHz-es csatorna van kiosztva, ezáltal az analóg változat 8 csatornája helyett itt kétszer annyi valódi csatornán folyhat majd hangátvitel.*

egymás utáni lenyomásával. Abban az esetben, ha a vett jel nem alakítható át a beépített modulokkal, akkor a vezérlő számítógépre telepített segédszoftverek lehetnek segítségünkre.

Az RF spektrumban folyamatosan jelennek meg új modulálási és titkosítási eljárásokat alkalmazó jelek, amelyekkel csökkenteni szeretnék a lehallgatás valószínűségét. Ezek az adások nem alakíthatóak vissza régi (nem szoftveres) rádióvevő készülékekkel oly módon, hogy a kezelő kinyerhesse belőlük a hang, a kép, vagy az adattartalmat. Ebben az esetben szükség van a vevőkészülékhez csatlakoztatott egyéb berendezésekre. amelyek a rádióhoz csatlakoztathatók.

A WiNRADiO WR-G39DDC vevőkártya alkalmazásakor nem feltétlenül kell további hardvereket alkalmaznunk, elég lehet a vezérlő számítógépre telepített a kívánt képességekkel rendelkező szoftver. Így viszonylag gyorsan és egyszerűen (és persze kis költséggel) lehet a berendezésünk demodulálási képességeit továbbfejleszteni, így annak tudása nem korlátozódik a gyári alapbeállításokra.

A rádió nem alkalmas vizualizációra, így nem képes videó jelek és adatfolyamok megjelenítésére. Amennyiben videó jelek „képét”, vagy például rövidhullámon sugárzott kódtáviratok adatsorait szeretnénk látni, akkor a vezérlő számítógépre telepített további segédprogramokra, vagy újabb hardverekre van szükség.

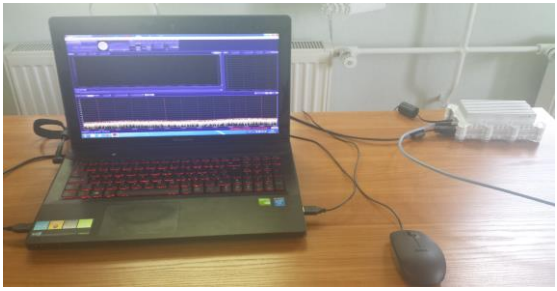
A vevőkártya sajnos csak egy antennabemenettel rendelkezik. Abban az esetben, ha ki szeretnénk használni a berendezésünk által venni képes teljes sávtartományt (0 – 3,5 GHz), akkor szélessávú antennát kell használnunk. Erre megoldás lehet egy antennamátrix. Ebbe az antennamátrixba kell bekötni a különböző sávokra optimalizált antennákat (V4R, Logper, Discone, Yagi, stb.). A mátrixból kijövő kábel van bekötve a vevőkártya antenna bemenetére, és mindig az éppen vizsgált sávtartományhoz választjuk ki a megfelelő érzékelőt.

Iridium műholdas felmenő hívások winrádióval

Elvégeztem a tesztelésre megkapott 3 különböző típusú műholdas telefon (Inmarsat, Thuraya, Iridium) technikai elemzését. Jelen cikkemben az Iridium telefon felmenő hívásainak mérési eredményeit mutatom be. A mérésemhez a következő eszközöket használtam:

- L –sávú FLAT antenna, beépített LNA (Low Noise Amplifier) és L-Band Uplink Filter
- Winradio Power Injector (tápfeladó az antenna erősítőjéhez, 12 V – 200 mA.)

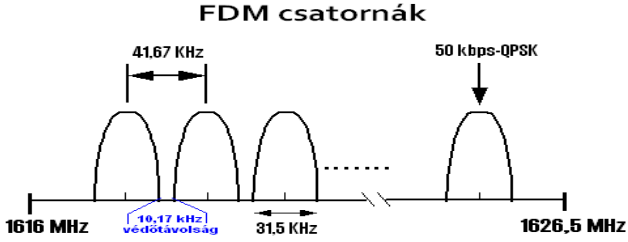
- Winradio G39DDCe (a G39DDC külső változata, mely USB 2.0 porton keresztülkapcsolódik a számítógéphez)
- Vezérlő számítógép



9. ábra Mérési összeállítás (készítette: szerző)

A tesztelés során rögzített IQ felvételeken elvégzett technikai elemzés, illetve spektrumképek vizsgálata során az Iridium műholdas rendszerrel kapcsolatos tapasztalataim a következők:

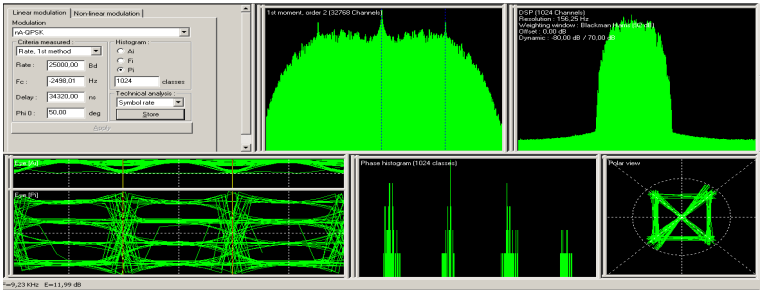
Az Iridium rendszer az 1616-1626,5 MHz sávtartományban dolgozik, mely tartomány csatornakiosztása egymástól 41,67 kHz távolságra lévő 31,5 kHz széles FDM kommunikációs csatornák sorozatából épül fel.



10.ábra: Iridium rendszer csatorna kiosztása[16]

[16] *IRIDIUM® Subscriber License Information http://marine.rutgers.edu/~kerfoot/pub/slocum/RELEASE_6_32/src/doco/specifications/iridium-phone/IR_Lband.doc.rtf (Letöltve: 2013. 10. 11.)*

A technika elemzés során mért modulációs paraméterek:
szimbólumsebesség: 25000 Bd (50 kbps adatsebesség)
moduláció: QPSK /DEQPSK (Differentially Encoded QPSK)/



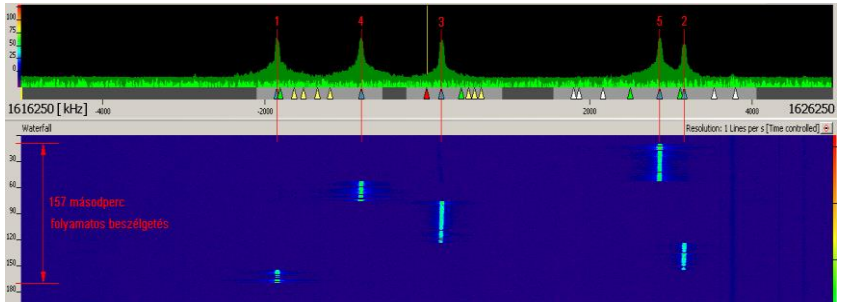
11.ábra: Iridium rendszer mért modulációs paraméterei (készítette: szerző)

A nagysebességű rádiókommunikációs eszközöknél fellépő Doppler effektus hatására a csatornák „egymásba csúszásának" megelőzése érdekében a rendszer tervezői az egyes csatornák között 10,17 kHz „védőtávolságot" hagytak. Így a frekvencia eltérési értéket meghaladva a rendszer a folyamatos és zavarmentes adatátvitel érdekében egy véletlenszerűen kiválasztott éppen szabad csatornára vált át.[17]

Egy 157 másodperces folyamatos beszélgetés alatt végrehajtott csatornaváltást mutat a lenti ábra, melyen jól látható, hogy ezen idő alatt a rendszer 5 alkalommal vált csatornát, továbbá hogy az egyes – éppen aktív – csatornák hosszai változó értéket mutatnak, annak függvényében, hogy az adott csatorna mikor éri el Doppler-határt.[18]

[17] *IRIDIUM® Subscriber License Information http://marine.rutgers.edu/~kerfoot/pub/slocum/RELEASE_6_32/src/doco/specifications/iridium-phone/IR_Lband.doc.rtf (Letöltve: 2013. 10. 11.)*

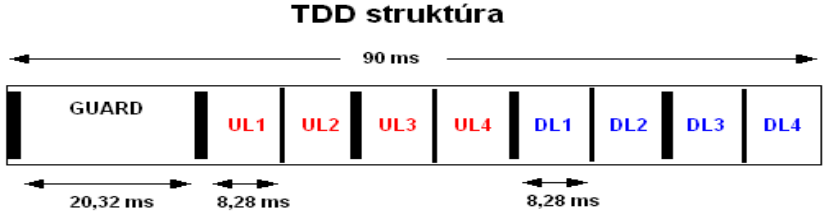
[18] *IRIDIUM® Subscriber License Information http://marine.rutgers.edu/~kerfoot/pub/slocum/RELEASE_6_32/src/doco/specifications/iridium-phone/IR_Lband.doc.rtf (Letöltve: 2013. 10. 11.)*



12.ábra: 157 másodperces beszédkapcsolat spektrum ábrája (készítette: szerző)

Az adatátvitelhez a rendszer a TDD módszert (Time Domain Duplex – időosztásos kettőzést) alkalmazza, azaz egy keretrendszerben kiosztott időrésekben ad és vesz ugyanazon a frekvenciasávban. FDMA/TDMA (Frequency Division Multiple Access/ Time Division Multiple Access) módszerrel rendelik hozzá 1-1 előfizetőhöz az általa használható csatornát, ami a frekvenciából és az időrésből tevődik össze az adott cellán. A csatorna hozzárendelést a műhold vezérli a cellák határain.[19]

A TDD struktúra 90 ms-os keretekből áll, ami egy 20,32 ms-os (Guard) védőidővel kezdődik, melyet 4-4 db, egyenként 8,28 ms-os uplink (UL) és downlink (DL) időrés követ.[20]



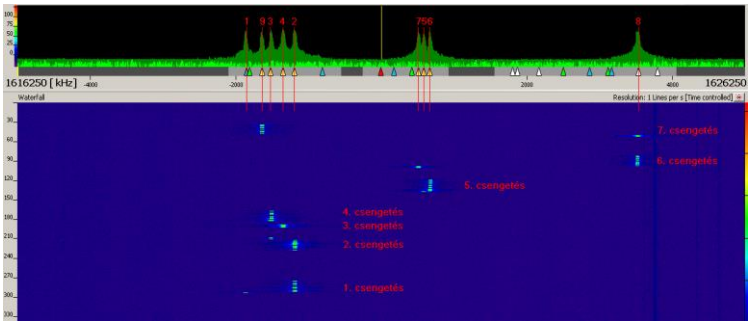
13.ábra: Az időkeret felépítése[21]

[19] *IRIDIUM® Subscriber License Information http://marine.rutgers.edu/~kerfoot/pub/slocum/RELEASE_6_32/src/doco/specifications/iridium-phone/IR_Lband.doc.rtf (Letöltve: 2013. 10. 11.)*

[20] *Uo.*

[21] *Uo.*

Az Iridium 9555 készülékkel 7-szer kezdeményezett hívás jellegzetességei az alábbi ábrán láthatók:



14.ábra: Felmenő hívások spektrum képe és esőábrája (készítette: szerző)

A lejövő adatforgalmat csak egy - kifejezetten erre a sávtartományra méretezett – FLAT antennával mértem. Az elemzés során megállapítható, hogy a felmenő jelekkel megegyező modulációt és TDD (Time Domain Duplex) struktúrát használ. A többi csatornához képest ezeken a csatornákon – a tesztelés során – nem látható folyamatos adatátvitel, csak az esőábrán látható rövid kommunikáció.

Következtetések

Kérdés, hogy a közeljövőben a műholdas távközlési rendszerek csak a földi rendszerek kiegészítései, meghosszabbításai maradnak, esetleg visszaszorulnak. Az is elképzelhető, hogy a technológia fejlődésével, a műholdas eszközök miniatürizálásával, a robotika eredményeinek felhasználásával átveszik a földi infrastruktúrák szerepét, és a földön a műholdas kommunikáció lesz a kizárólagos kommunikációs szolgáltatási forma. Ezt még nem tudom, de az biztos, hogy napjainkban is és a közeljövőben is működni fognak, szolgáltatásaik igénybe vehetők, ezért indokolt, hogy foglakozzunk velük, megismerjük képességeiket, működésüket.

Méréseim során bebizonyosodott, hogy a Winradio G39DDCe rádió kiválóan *alkalmas* az ilyen típusú műholdas telefonok jeleinek detektálására és felvételek készítésére, melyekből utólagos elemzéssel megállapítható, hogy milyen típusú műholdas telefonnal történt a forgalmazás. A gyári szoftverével ez csak úgy te-

hető meg, hogy egy operátor kezeli az eszközt és manuálisan végzi a felderítést és a felvételek készítését. A gyártó biztosít az eszközhöz SDK-t (Software Development Kit), amelynek segítségével egy tapasztalt programozó, aki rendelkezik némi rádiófelderítési ismerettel, viszonylag könnyen készíthet olyan alkalmazást, amely ezt a feladatot automatikusan is el tudja végezni.

Iridium telefonkészülékről indított rádióforgalmak a felhasznált frekvenciatartomány, a technikai elemzés során kinyert paraméterek, illetve az adás jellegzetességei alapján a továbbiakban *technikai elemzés nélkül is könnyen megkülönböztethetőek más műholdas rendszerektől.* Az elvégzett mérésekből megállapítható, hogy az Iridium telefonkészülékek csak *aktív kommunikáció alatt* (hívás felépítés, beszélgetés, SMS) *deríthetők fel,* készenléti állapotban nem.

Célom, hogy olyan automatizált, a szabadba kihelyezhető, távolról menedzselhető mérőrendszert építsek, amely képes a műholdas felmenő hívások felderítésére. Kutatásaimat ebbe az irányba folytatom tovább.

Felhasznált irodalom:

- NAGY Lajos, FARKASVÖLGYI Andrea: Műholdas szolgáltatások. Magyar Tudomány 2007/7 ISSN 0025 0325 pp. 899–902.
- Roman BERESIK, Milos SOTAK, Frantisek NEBUS, Jozef PUTTERA: Satellite communication system's detection. Electrical Review, ISSN 0033-2097, NR 7/2011
- VÁNYA László: Út a szoftverrádiók és szoftver rádiózavaró állomások felé. Kommunikáció 2006, Zrínyi Miklós Nemzetvédelmi Egyetem konferencia kiadvány, ISBN: 978-963-7060-18-2, pp. 76–83.
- Komplex IQ jelek feldolgozása http://forum.xham.org/index.php?topic=292.0 (Letöltve 2015. 08.10)
- IRIDIUM Subscriber License Information http://marine.rutgers.edu/~kerfoot/pub/slocum/RELEASE_6_32/src/doco/specifications/iridium-phone/IR_Lband.doc.rtf (Letöltve: 2013. 10. 11.)
- WiNRADiO http://www.winradio.com (Letöltve 2015. 08. 10.)
- WiNRADiO G39DDC User's Guide - Ver. 1.01.pdf