

Műholdas telefonok felmenő hívásainak közeltéri felderítése

Szűcs Péter

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 a kutatási témám első eredményét, az Iridium rendszer felmenő hívásainak felderíthetőségét. Folytatva kutatásaimat cikkemben jelentést teszek a Thuraya rendszerben indított telefonhívások detektálhatóságáról.

Kulcsszavak: műholdas kommunikáció, műhold pályák, műholdas távközlés, műholdas személyi kommunikációs rendszerek

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.

Keywords: satellite personal communication systems, MEO, GEO, LEO, felderítés, detektálás, TDD, FDMA, TDMA, uplink, downlink.

1. Bevezetés

Örök kérdés, hogy amivel éppen foglalkozunk, mennyire modern, mennyire van helye a mai kommunikációban, bele tartozik-e a védendő információs infrastruktúrák közé. Ezt a műholdas kommunikációra kivetítve – a feldolgozott irodalom alapján – megállapíthatjuk, hogy egyre nagyobb szerep hárulhat a műholdas technológiákra, ha sikerül megoldani a műholdak árának csökkentését, a pályára állítási költségeket minimalizálni és növelni a pályán tartás idejét, tehát olyan hajtóművek kifejlesztése, amelyek jelentősen megnövelik a kommunikációs műholdak élettartamát. A piko- és mikro műholdas fejlesztések erre tesznek kísérletet, tovább növelve a műholdas technológiák létjogosultságát. Természetesen továbbra is igaz az, hogy a Föld nagy részén - az információs társadalom embere számára - nincs megfelelő földi kommunikációs infrastruktúra. A műholdas rendszereknek ezért van még létjogosultságuk, ezért folynak még a fejlesztések. Doktori témám kiválasztásakor elsőként a fenti tényeket vizsgáltam és döntöttem, hogy ezzel a technológiával érdemes foglalkozni, rejlenek még benne új lehetőségek. Az általam választott kutatási területem egyik részeredményét kívánom bemutatni jelen cikkemben. A Thuraya rendszerben indított felmenő hívások felderíthetősége már egy megkezdett mérési sorozat második állomása. Az első méréseimet az Iridium rendszerű platformon kezdtem és eredményeimet a 2014. évi „Haza szolgálatában” konferencián ismertettem. Publikációm a konferencia kiadványban lehet elolvasni, a most ismertetett gyakorlati mérések leírásánál is fogok hivatkozni az ott leírtakra.¹

2. A Thuraya rendszer

A Thuraya arab kifejezés, melynek jelentése: az égbolt. A Thuraya céget 1997-ben alapították az Egyesült Arab Emírátsban, részvénytársasági formában működik. A Thuraya távközlési vállalat mobil műholdas telefon és adatátviteli szolgáltatásokat kínál három kontinens, Európa, Ázsia és Afrika nagy területén. A Thuraya szolgáltatási területén a szolgáltatásokat kombinált (műhold/GSM/GPS) készülékekkel vehetjük igénybe.

Kutatásaim során egy tesztelésre kapott Thuraya XT PRO műholdas telefon (1. ábra) technikai elemzését végeztem el. A telefon rendelkezik GPS funkcióval is, melynek segítségével meghatározhatjuk pillanatnyi helyzetünket, illetve Waypoint-ok, fordulópontok tárolásával konkrét helyekre is egyszerűen navigál-

¹ Szűcs Péter: *Műholdas személyi távközlési rendszerek felderíthetősége, a felderítés végrehajtásának metodikája, a keletkezett információk felhasználása Magyarország biztonsága érdekében*, In: *Társadalom és honvédelem, Nemzeti Közszolgálati Egyetem XVII. Évfolyam, 3-4. szám, pp. : 256-264*

hatunk.² A Thuraya a geoszinkron pályás – úgynevezett GEO (Geostationary Earth Orbit) – műholdas rendszerek közé tartozik, vagyis a műholdak mindig az Egyenlítő ugyanazon pontja felett helyezkednek el. Ezért geoszinkron műholdak esetén, fixen beállított, nagynyereségű antennákat alkalmazhatunk a műhold jeleinek vételére (downlink), illetve a felhasználói terminál adás-irányú jeleinek műholdra juttatására (uplink).



1. ábra. Thuraya XT PRO készülék³

A Thuraya maroktelefonok roamingra is használhatóak. A szolgáltatás képes a helyi GSM rendszert használni, majd annak megszűnése esetén automatikusan átlép a műholdas kapcsolatra. A műholdak által lefedett területeken lehetőség van telefonhívásokat indítani, fogadni a Föld bármely pontjáról. A műholdak által nem fedett területeken a GSM roaming lehetséges.

Méréshez alkalmazott eszközök:

- 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 keresztül kapcsolódik a számítógéphez)
- Vezérlő számítógép

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

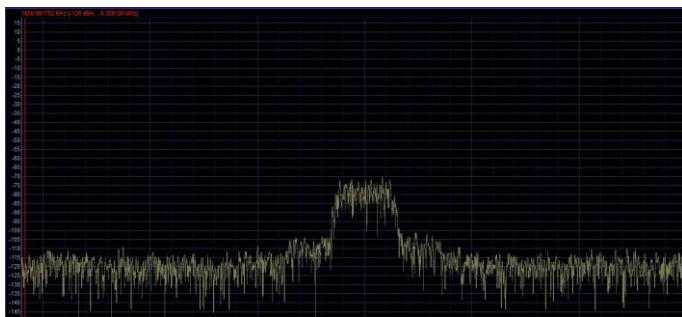
² *satellitephone* <http://www.satellitephone.hu/muholdas-telefon-thuraya> Letöltve: 2015. 08. 10.

³ Uo.

A Thuraya telefonkészülékkel különböző távolságokból hívásokat kezdeményeztem, melyet megpróbáltam detektálni a Winradio eszközzel, melynek frekvenciasöprési ideje 1 GHz/s. A söprési frekvenciatartomány 1620 MHz-től 1670 MHz-ig terjedt 1.5 kHz-es felbontással. Amikor a spektrumképen megjelent a keresett jel, akkor leállítottam a frekvenciasöprést és lehangoltam a készüléket az észlelt frekvenciára. Lehangolás után a készülék 16 MHz sávzélességű panoráma ablakában lehetőségem volt pontosítani a frekvenciát, mely rögtön megjelent a DDC-1 spektrumképén. A DDC-1 ablakban IQ jelet rögzítettem a jelről, melynek elemzését offline eszközökkel végeztem.

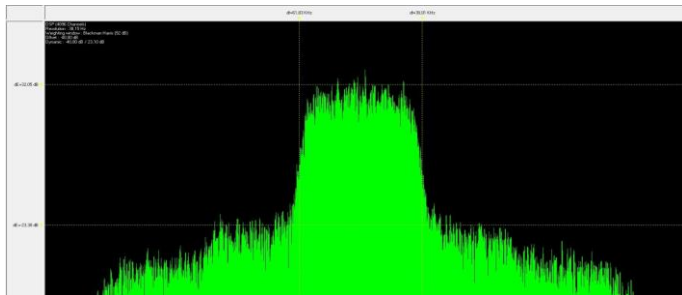
A felderítő eszköz irányított antennáját az épület első emeleti ablakában helyeztem el, mely a földfelszínhez képest kb. 4-5 m magasságban volt. Közvetlenül az épület mellett egy nagy fa található melynek lombjától nem volt szabad rálátás az adóra még a legközelebbi mérésnél sem.

Az első mérést 400 m távolságból végeztem és 100 méterenként növeltem a távolságot. Ekkor az észlelt jel jel/zaj viszony elérte a 40 dB-es értéket. (2. ábra)



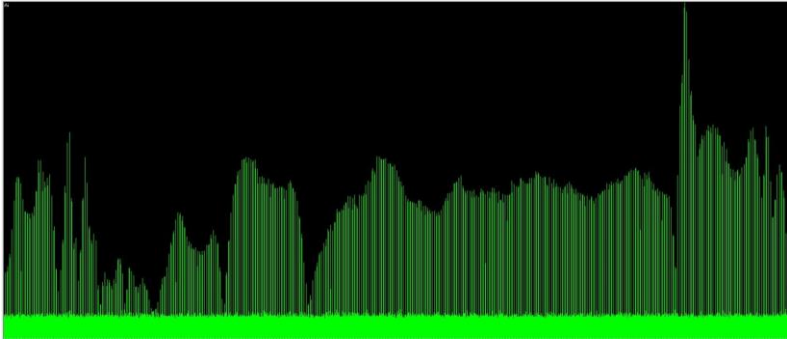
2. ábra. DDC1 spektrum képe (saját rögzített kép)

Tovább haladva a következő mérést 700 m távolságból végeztem A jel/zaj viszony itt is még elérte a 32 dB-t. (3. ábra)



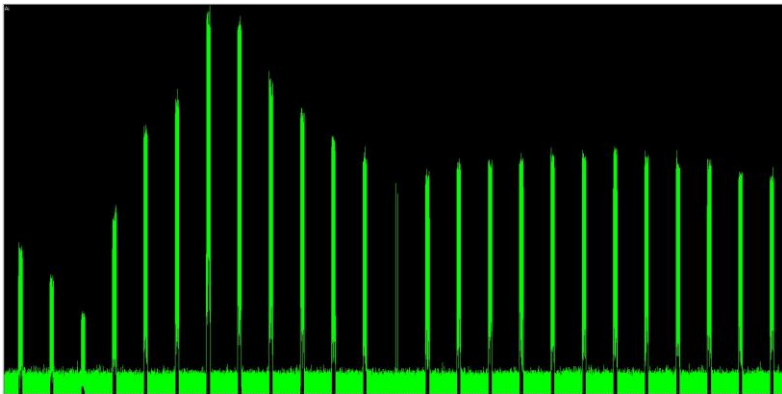
3. ábra. 32 dB jel/zaj viszony 700 m-en (saját rögzített kép)

Ennél a mérésnél megvizsgáltam a jel amplitúdójának az időbeli változását és a demodulálhatóságának a minőségét. A 4. ábrán a jel amplitúdó hisztogramja látható 15 s időtartamban nézve. Jól látszik rajta, hogy a terepviszonyok és a dús növényzet függvényében (a növényzet csillapítása jelentős) mennyire ingadozik a jel erősségének a mértéke, de a vizsgált időtartam nagy részében még elegendően erős volt detektáláshoz és a demoduláláshoz.

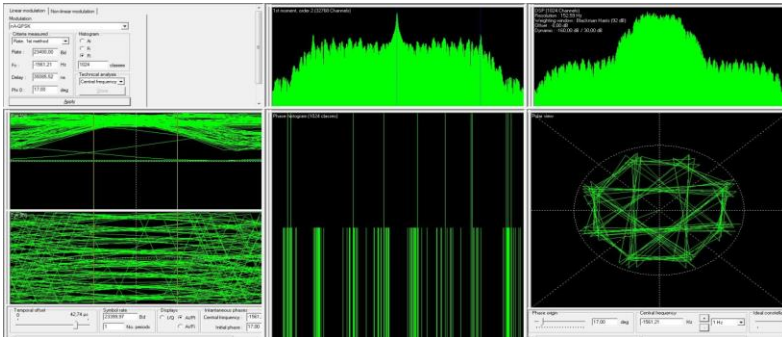


4. ábra. 700 m-en a növényzet csillapítása 15 s intervallumban (saját rögzített kép)

A IQ rögzítményből az 5. ábrán a jel amplitúdójának ingadozása látható 1 s időtartamra nézve.

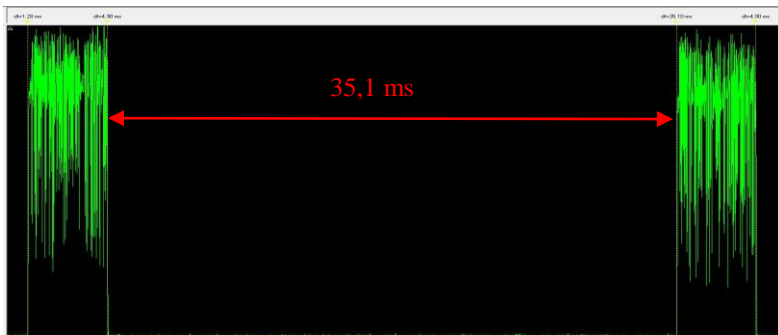


5. ábra. A jel amplitúdója 1 s időtartamra nézve (saját ábra)



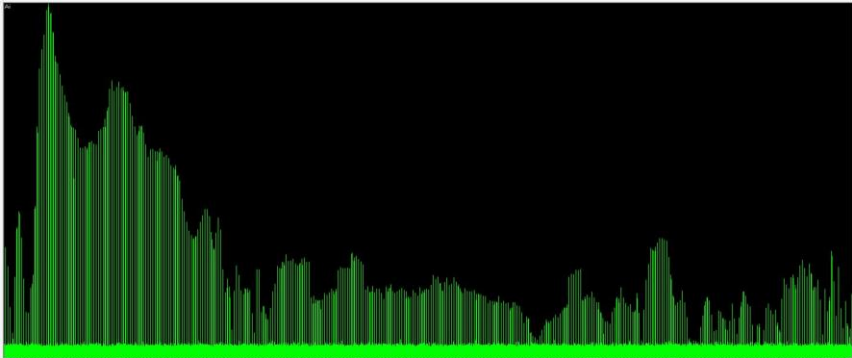
6. ábra. A jel moduláció típusa: $\pi/4$ DQPSK és szimbólumsebessége: 23400 (saját ábra)

A Thuraya jel 4.9 ms hosszúságú „burst”-okból áll és a köztük lévő szünetek 35.1 ms hosszúak. (7. ábra)



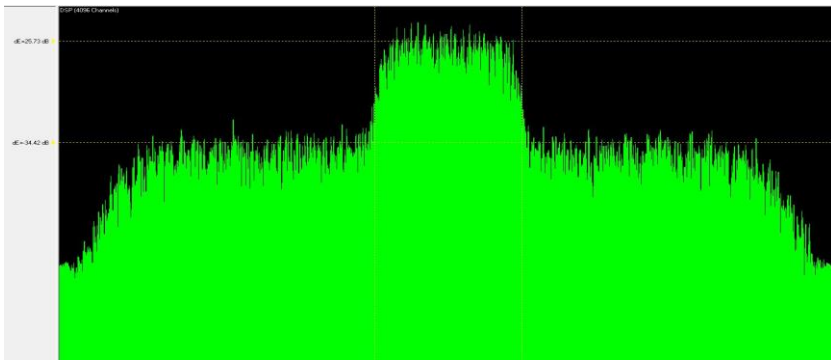
7. ábra. A burst-ök távolsága (saját ábra)

A jelet 1000 m távolságból vizsgálva azt tapasztaltam, hogy néhány burst amplitúdója elérte a 35 dB jel/zaj viszony értéket. Ebben az esetben (néhány ms ideig) valószínűleg kedvezőbb volt a vevőantenna rálátása az adóantennára, mint a 700 m távolság esetén, de ha 15 s intervallumban nézzük a jelet, akkor azt lát-hatjuk, hogy sokkal kevesebb ideig vannak nagy energiájú burst-ök, mint a 700 m távolságból történt mérés esetén. (8. ábra)



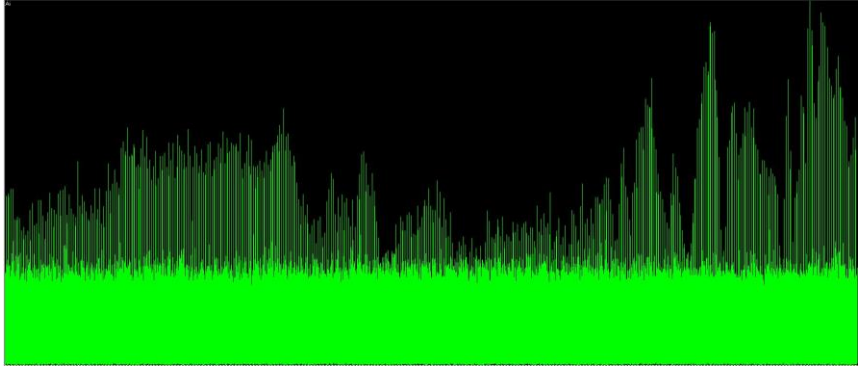
8. ábra. A jel amplitúdó változása 1 km távolságra (saját ábra)

1500 m távolságból történt mérés esetén még jobban csökkent azon burst-ök száma, amelyek alkalmasak a detektálásra és a kommunikációs eszköz azonosítására, de az erősebb burst-ök itt is elérik a 25 dB-es értéket. (9. ábra)



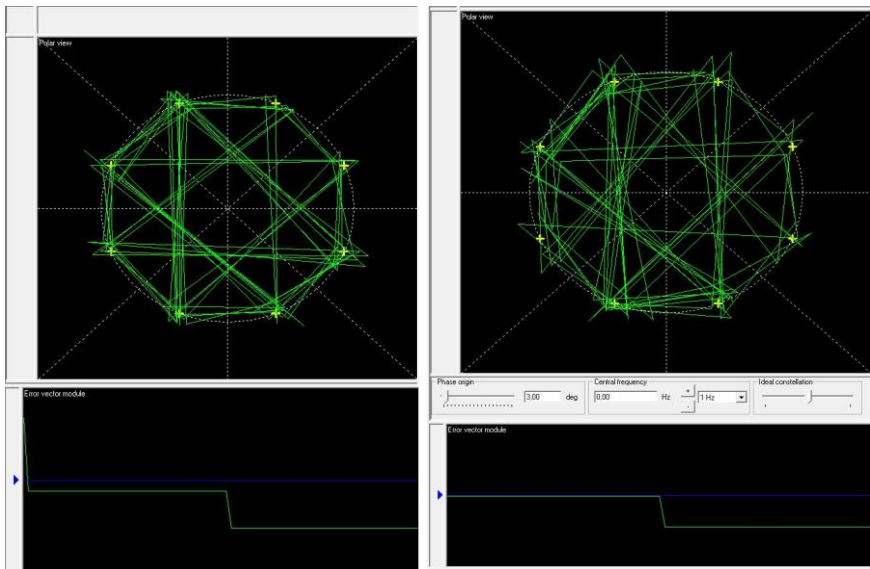
9. ábra. A jel amplitúdó változása 1,5 km távolságra (saját ábra)

A legtávolabbi mérést 2000 m távolságból végeztem, ahol az amplitúdó ingadozás hasonló volt az 1500 m történt méréshez, de itt a legerősebb burst jel/zajviszonya 20 dB volt.



10. ábra. A jel ingadozása 2 km-en (saját ábra)

A demodulálhatósági minőséget igen nehéz mérni olyan eszközzel, amely nem az ilyen rövid burst alapú átvitelre készült. Az alkalmazott offline demodulátor is folyamatos jelek demodulálására készült és a jel elején több hibával dolgozik, mint a későbbi szakaszban. A 11. ábrán szemléltettem a demodulálási minőség különbségét a 700 m-es és a 2000 m-es mérés esetén:



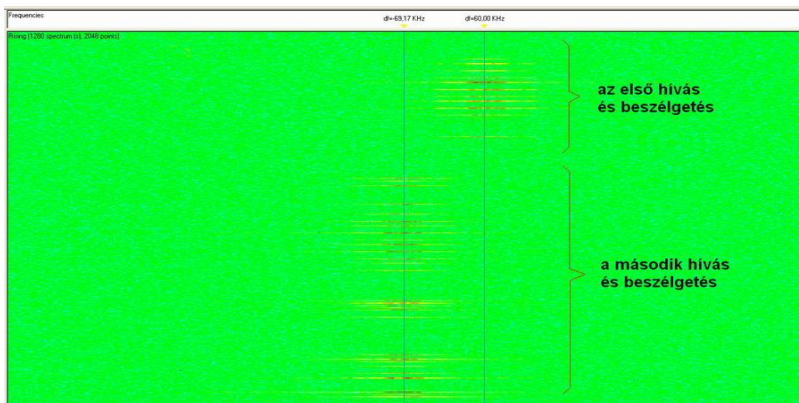
11. ábra. A jel demodulálási minősége 700 m-en (bal) és 2 km-en (jobb) (saját ábra)

3. Következtetések

Kérdés, hogy a közeljövőben a műholdas távközlési rendszerek csak a földi rendszerek kiegészítései, meghosszabbításai maradnak, esetleg visszaszorulnak, vagy a technológia fejlődésével, a műholdas eszközök miniatürizálásával, a robotika eredményeinek felhasználásával átveszik a földi infrastruktúrák szerepét, és 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 foglalkozzunk velük, megismerjük képességeiket, működésüket.

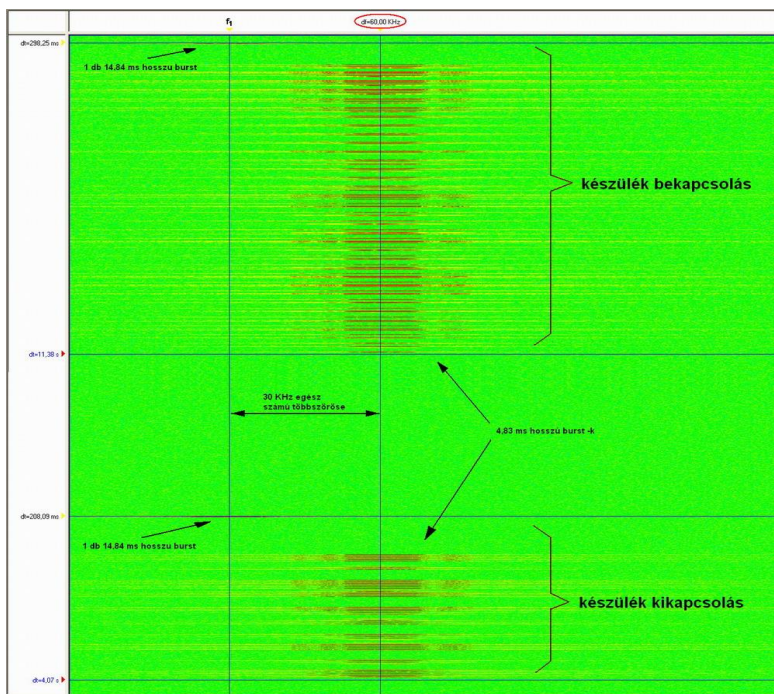
A Winradio G39DDCe rádió kiválóan alkalmas az ilyen típusú műholdas telefonok jeleinek detektálására és felvételek készítésére, melyekből utólagos elemzéssel megállapítható, hogy milyen típusú műholdas telefonnal történt a forgalmazás. A gyári szoftverével ez csak úgy tehető meg, hogy egy operátor kezeli az eszközt és manuálisan végzi a felderítést és a felvételek készítését. A gyártó biztosít az eszközhöz SDK-t (Software Development Kit). Ennek segítségével egy tapasztalt programozó, aki rendelkezik némi rádiófelderítési ismerettel, viszonylag könnyen készíthet olyan alkalmazást, amely ezt a feladatot automatikusan is el tudja végezni.

A Thuraya készülékkel kezdeményezett hívást, az adott felmenő sáv tartományban a hívás elejétől (kicsengéstől) egészen a kapcsolat bontásáig ugyanazon a frekvencián bonyolítja le. Az alábbi esőábrán is jól megfigyelhető, hogy a készülék 2 egymás után lefolytatott beszélgetés során 2 különböző frekvencián dolgozik:



12. ábra. A készülék felmenő hívásai az esőábrán (saját ábra)

Mivel a Thuraya készüléknek – az Iridiummal ellentétben – be-, illetve kikapcsoláskor is van kisugárzása, ezért ezen eszköz úgy is felderíthető, ha azon tényleges (fónia, SMS) kommunikáció nem történik. Az alábbi esőábrán látható, hogy az adás mindig először egy 14,84 ms hosszú burst-el kezdődik egy adott (f_1) frekvencián, majd az információt hordozó 4,83 ms-os burst-sorozat ettől 30 kHz egész számú többszörösére kiosztott frekvencián jelenik meg. Ez a sajátos adás-módszer minden üzemmódra (beszélgetés, SMS) jellemző.



13. ábra A készülék bekapcsolása és kikapcsolása az esőábrán (saját ábra)

Az elvégzett mérések alapján megállapítottam, hogy a Thuraya telefonkészülékről indított rádióforgalmak a felhasznált frekvenciatartomány, a technikai elemzés során kinyert paraméterek-, illetve az adás jellegzetességei alapján a továbbiakban technikai elemzés nélkül is könnyen megkülönböztethetők más rádiós rendszerektől. Az alkalmazott mérési módszerrel egyértelműen meghatározható, hogy a felmenő hívást Thuraya rendszerű telefonkészülékről kezdeményezték. Az elvégzett mérésekből megállapítható, hogy az Thuraya telefonkészülékek nem csak aktív kommunikáció alatt (hívás felépítés, beszélgetés, SMS) deríthetők fel, hanem bekapcsolt készenléti állapotban is.

Felhasznált irodalom:

- BERESIK Roman, SOTAK Milos, NEBUS Frantisek, PUTTERA Jozef: Satellite communication system's detection. Electrical Review, ISSN 0033-2097, NR 7/2011
- BRUCE R. Elbert: The Satellite Communication Applications Handbook, Artech House 2004 ISBN 1-58053-490-2
- VÁNYA László: Út a szoftverrádió és szoftver rádiózavaró állomások felé. Kommunikáció 2006 ZMNE 2006 ISBN: 978-963-7060-18-2. pp.: 47-84
- NAGY Lajos-FARKASVÖLGYI Andrea: Műholdas szolgáltatások. Magyar Tudomány 2007/7 pp. 899-902. ISSN 0025 0325
- SZÜCS Péter: Műholdas személyi távközlési rendszerek felderíthetősége, a felderítés végrehajtásának metodikája, a keletkezett információk felhasználása Magyarország biztonsága érdekében ISSN 1417-7293
- <http://www.satellitephone.hu/muholdas-telefon-thuraya> (letöltve 2015. 08. 10.)
- Thuraya <http://Thuraya.com> (letöltve: 2015. 08. 11.)
- MIKKO Valkama: Advanced I/Q signal processing for wideband receivers: Model and Algorithms, Tampere 2001, ISBN 952-15-0715-2
- Társadalom és honvédelem, Nemzeti Közszolgálati Egyetem XVII. Évfolyam, 3-4. szám, ISSN 1417-7293 pp.:256-264