Detection of the uplink of the Inmarsat satellite phone calls

Péter Szűcs[1]

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 a 2. cikkemben jelentést teszek a Thuraya rendszerben indított telefonhívások detektálhatóságáról. A sorozat folytatásaként bemutatom, hogyan lehet felderíteni egy Inmarsat telefonról kezdeményezet hívást.

Kulcsszavak: műholdas kommunikáció, műholdas távközlés, műholdas személyi kommunikációs rendszerek, felderítés, detektálás, TDD, FDMA, TDMA, uplink, downlink, WiNRADiO.

Absztrakt*:* 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.

Keywords: satellite communication, satellite personal communication systems, detection, TDD, FDMA, TDMA, uplink, downlink, WiNRADiO.

[1] *szucs.peter@nbsz.gov.hu*

Introduction

Our society is the information society; people, the government and the manufacturer/productive sector suffers from information dependency therein. This fact – which is very well-known by nearly everybody – has an emphasized role due to the fact that it means dependency from info-communication systems and information infrastructures. Technologies of our days are present in almost every area of our lives, from the workplaces to the entertainment. The duration of reaching information has an emphasized role as well, people in our time – be anywhere in the world – intends to reach every information without delay.[2] The continuous availability and safe operation are basic requirements from the information infrastructures. Safe operation has many interpretations, in my essay – because of the subject of my PhD thesis – I examine "safety" from the prospect of society and nation. My intention is to support and intensify this safety – at least one segment thereof – with my measuring, and the determination of detection modus operandi.

The detection ability of the initiated calls in Iridium and Thuraya systems are the results of an earlier started measuring series. My first manual measuring was started in connection with the Iridium platform, and I shared my results on the conference, "In the service of the country" in 2014.[3] As a sequence, I presented the detection manner of the initiated calls from Thuraya system, which is available for an interested reader in the Nemzetbiztonsági Szemle 2015/3.[4] In this essay, I present the detection manner of the initiated calls from an Isatphone, which belongs to Inmarsat system.

Detection of uplinks of initiated calls in the INMARSAT system

The Inmarsat provide reliable, safe, global voice and data transfer services (except in North and the South Pole on the Earth). This company has been functioning on the satellite market since 1979, and they have determining role thereon. Now they operate 11 satellites on GEO orbit to provide perfect voice and data

[2] *Haig Zsolt: Információs társadalom biztonság Budapest, 2015, ISBN:978-615-5527-08-1*

[3] *Szűcs Péter: Műholdas személyi távközlési rendszerek felderíthetősége, a felderítés végrehajtásának metodikája, a keletkezett információk felhasználása Magyarország biztonsága érdekében, Társadalom és honvédelem, Nemzeti Közszolgálati Egyetem XVII. Évfolyam, 3-4. szám, ISSN 1417-7293 pp.:256-264*

[4] *Szűcs Péter: Műholdas telefonok felmenő hívásainak közeltéri felderítése Nemzetbiztonsági Szemle 2015/3, HU ISSN 2064-3756, pp.: 20-30. http://www.satellitephone.hu /muholdas-telefon-thuraya (letöltve 2015. 08. 10.)*

communication services. As a matter of fact only three of them are at service of users; the other satellites are in standby or have special purposes.

For my measuring, I used the Isatphone2 satellite phone, which can be used in the Inmarsat system. Presently this device has the largest storage battery capacity, and its standby period with one charge can be 160 hours in ideal circumstances.[5]

figure 1. ISatphone2 [5]

I carried out the technical analysis of Isatphone 2 satellite phone (1st figure). I used the following devices for the measuring:

- L band FLAT antenna, built-in LNA (Low Noise Amplifier) an L-Band Uplink Filter,
- Winradio Power Injector (power injector to the amplifier of the antenna, 12V-200 mA),
- Winradio G39DDCe (outside version of G39DDC, which interlocks to the computer through USB 2.0 port),
- management computer.

In the course of technical analysis of IQ records (collected during tests) and the examination of rainfall diagrams, my experience was the followings:

I initiated calls with Isatphone2 satellite phone from different distances, and I tried to detect them with Winradio, which had 1 GHz/s frequency sweep time. The frequency sweep range was from 1620 MHz to 1670 MHz, with 1,5 kHz resolution.

[5] *INMARSAT http://www.satellitephone.hu/muholdas-telefon-inmarsat (letöltve 2015-11-20)*

When the sign appeared on the spectrum image, I turn down the frequency sweeping and I tuned the device to the percept frequency. After tuning on, I had opportunity to specify the frequency on the 16 MHz bandwidth panoramic pictures, which turned up straight on DDC-1 spectrum picture. On the DDC-1 pictures, I fixed IQ sign from the sign, which I put under analysis with offline devices.

I placed the directed antenna of the detection device in the window on the first floor, which was on 4-5 meter height from the ground. Next to the window there was a big tree, and because of the treetop there was no free visibility – not even in the case of the closest measuring – to the transmitter. I did my measuring turns per 100 meter, descend to 1000 meter. The surface was woody and bushy one after the other, and the effects to the communication thereof was presented connected to my Thuraya test (in my previous article).

The Isatphone remains on one frequency during one call. The amplitude of the sign showed flutter even in the case of close measuring. This can be caused by the adverse effect of multi-path or the device is able to control its efficiency (I did not find any information concerning to that the device can control its outgoing efficiency).

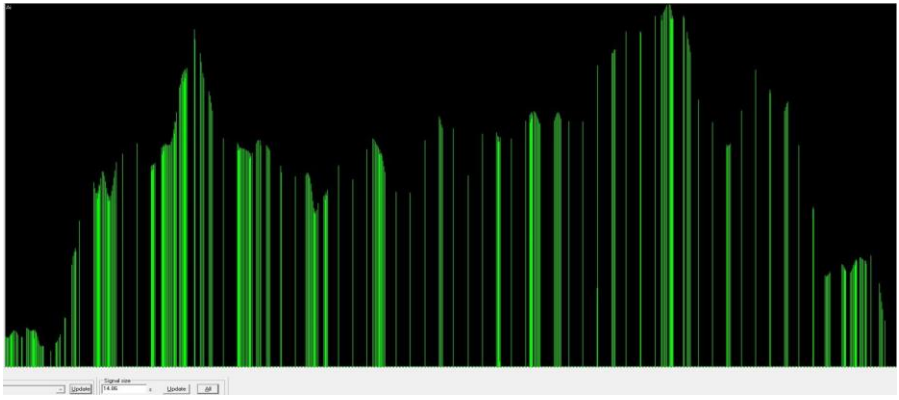

figure 1. fluttering sign during measuring close to the amplitude [own picture]

The sign was not continuous, but it showed burst system. The duration of one burst was 2.2.ms, of two burst was 16.26 ms:

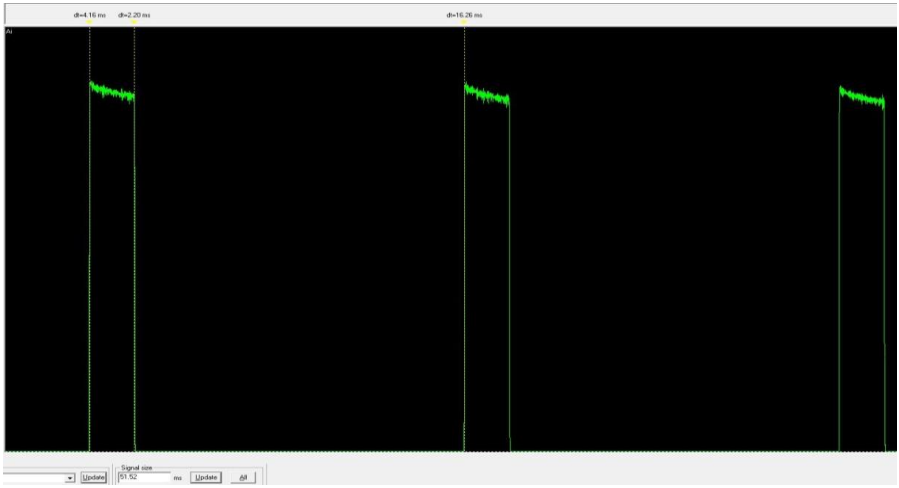

figure 2. Burst sign [own picture]

The Isatphone system uses GMSK modulation toward uplink and downlink as well. In the next test, I measured the uplink only.

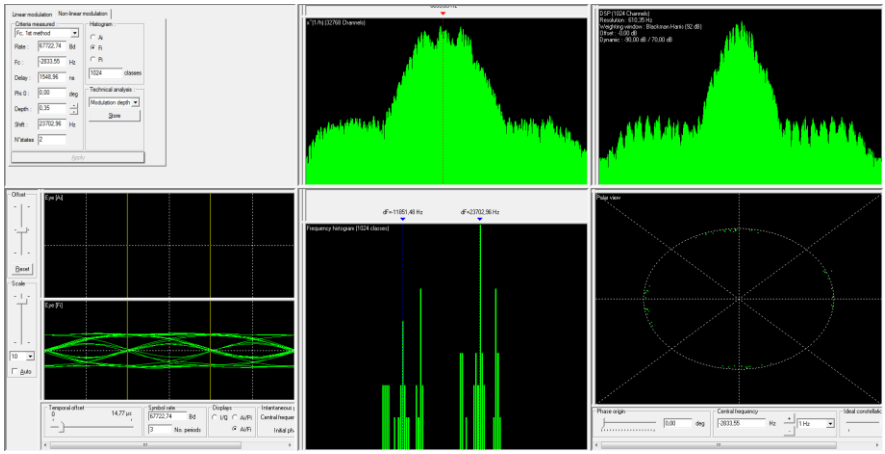

figure 3. Modulation declaration [own picture]

The speed of GSMK modulation 67722 symbols per seconds, the index of the modulation is 0,35. In the case of GSM modulation, the demodulator did not

provide figure in connection with the bit error percentage, and this mode cannot be demodulated perfectly with synch FSK demodulator device.
Sign spectrum and sign-noise relation

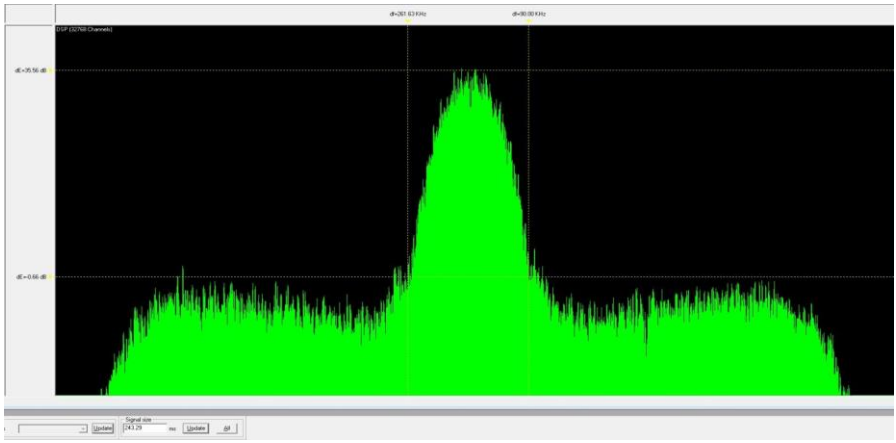

figure 4. measuring from close when the sign-noise relation is 35 dB

In 500 meter distance, the sign-noise relation still reached the 34 dB figure.

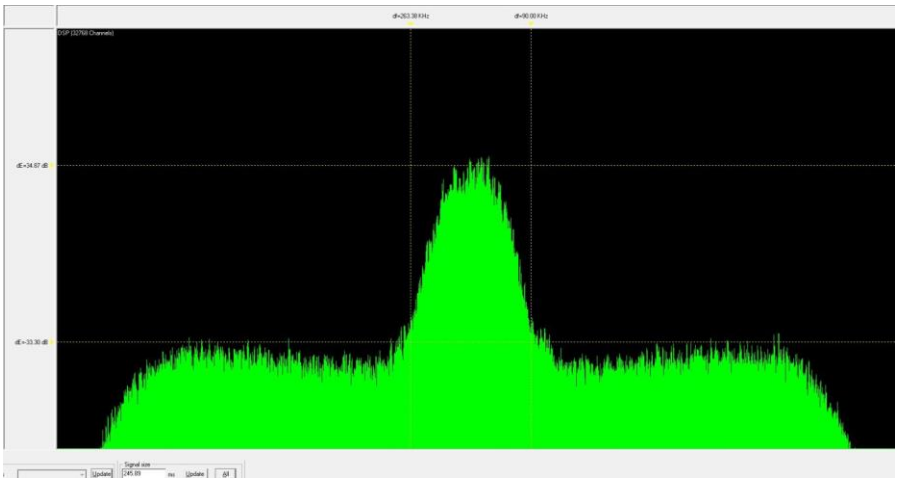

figure 5. 500meter distance the sign-noise relation is 34 dB [own picture]

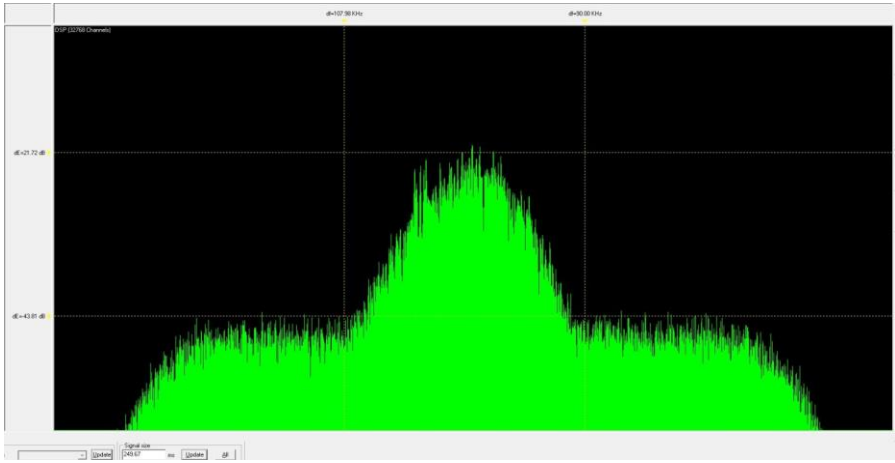

figure 6. 1000meter distance the sign-noise relation is 21 dB [own picture]

We can declare that the phone is easily recognizable and its sign can be demodulated from 1000 meter distance.

Conclusion

The question is that whether the satellite telecommunication systems will hold on their supplementary manner or they will lose their role, or – thanks to the technological development, miniaturization of satellite devices, and results of robotics – they will take the place of the terrestrial infrastructures and the satellite communication will be the sole communication service. I do not know the answer yet, but it is a fact that they will operate now and in the near future, their services will be available, so it is a reasonable idea to examine them to get to know their capacity, power and function.

Winradio G39DDCe is perfectly suitable for detection and recording the signs of these satellite phones, and from these signs – through posterior examination – the type of the used satellite phone is identifiable. With the original software this can be realized when the operator operates the device and he does the detection manually and take recording. The manufacturer provides SDK (Software Development Kit) to the devices. With this, an experienced programmer who has a little knowledge in the field of radio intelligence, will be able to make an application relatively effortlessly, which application can do this task automatically.

A phone call initiated from an Isatphone – unlike Thuraya phone – has no beacon neither turning it on, nor turning it down and due to this fact that the

device can only be detected if there is a real communication thereon (voice, SMS).

The radio communication initiated from an Isatphone2 is easily separable – because of the used frequency, data got to know from technical analysis, and the specialties of the transmission – from other radio systems. With the used methodology, it is unambiguously determinable that the call was initiated from Inmarsat satellite phone. Finally, it is declarable – because of the results of the analysis – the Isatphone can be detected only during an active communication (construction of the communication, conversation, SMS).

References:

- Szűcs Péter: Műholdas személyi távközlési rendszerek felderíthetősége, a felderítés végrehajtásának metodikája, a keletkezett információk felhasználása Magyarország biztonsága érdekében, Társadalom és honvédelem, Nemzeti Közszolgálati Egyetem XVII. Évfolyam, 3-4. szám, ISSN 1417-7293 pp.:256-264
- Szűcs Péter: Műholdas telefonok felmenő hívásainak közeltéri felderítése Nemzetbiztonsági Szemle 2015/3, HU ISSN 2064-3756, pp.: 20-30. http://www.satellitephone.hu/muholdas-telefon-thuraya (letöltve 2015. 08. 10.)
- Haig Zsolt: Információs társadalom biztonság Budapest, 2015, ISBN:978-615-5527-08-1
- Bruce R Elbert: The Satellite Communication Applications Handbook, Artech House 2004 ISBN 1-58053-490-2
- INMARSAT http://www.satellitephone.hu/muholdas-telefon-inmarsat (letöltve 2015-11-20)
- Roman BERESIK, Milos SOTAK, Frantisek NEBUS, Jozef PUTTERA: Satellite communication system's detection. Electrical Review, ISSN 0033-2097, NR 7/2011
- Nagy Lajos-Farkasvölgyi Andrea: Műholdas szolgáltatások. Magyar Tudomány 2007/7 pp. 899-902. ISSN 0025 0325