A Location Privacy Extension for DVB-RCS

Aggelis AGGELIS, Emmanuel T. SARRIS, Vasilios KATOS

Dept. of Electrical and Computer Engineering, Democritus University of Thrace,
Kimeria University Campus, 67100 Xanthi, Greece

aaggel@ee.duth.gr, sarris@ee.duth.gr, vkatos@ee.duth.gr

Abstract. *In this paper we studied the DVB-RCS (Return Channel through Satellite) standard from a privacy perspective and proposed an approach to incorporate a location privacy enhancing mechanism into the standard. Offering location based privacy in DVB-RCS communication is a challenge as the location of a satellite terminal must be revealed to the network operator of the DVB-RCS network for technical and administrative reasons. We proposed an approach of cloaking the location by intentionally compromising its accuracy whilst maintaining the operability and integrity of the communications system. In addition we implemented a proof of concept technique utilizing the theoretical findings of this work on a real DVB-RCS system, presenting the methodology along with the tools used and the experimental results.*

Keywords

DVB-RCS security, location privacy, satellite communications, data cloaking, spatial accuracy.

1. Introduction

The Digital Video Broadcasting (DVB) Project was founded in 1993 by the European Telecommunications Standards Institute (ETSI) with the goal of standardizing digital television services [6]. This initial standard for satellite delivery of digital television was named DVB-S (Digital Video Broadcasting-Satellite) [7].

The DVB-S infrastructure used to carry television services via (Geosynchronous) satellite can be used to provide Internet services to subscribers. Internet over satellite is a competitive technology to DSL technology, having the advantage of serving even the most remote areas. DVB-S provides only the downlink. A reverse communications channel is also needed to enable interactivity in applications such as web browsing. Symmetric uplink and downlink is not a necessity, because most Internet services require a faster downlink.

Initially telephone modems were used for the uplink, but this approach has several disadvantages such as slow data rates, not always on service and telephone lines may not be an option in remote areas. An alternative solution is for the subscriber equipment to transmit the uplink signal back to the satellite over the same antenna used for signal reception (hence the name DVB-RCS Return Channel Satellite).

Throughout the bibliography [3], [9] security in DVB-RCS networks adopts a traditional view such as confidentiality and integrity of data and source authentication. In addition due the particular nature of satellite communications there is an effort to secure the physical layer against Jamming, Detection/Interception, Traffic Analysis, Denial of Service and Replay attacks [3]. However privacy concerns such as location based privacy have received little attention and relied only on scrambling the forward and return link to prevent unwanted leakage of information ([9] p.23). However for reasons that will be explained in the following paragraphs the exact location of the RCST's (Return Channel via Satellite Terminal) is still known to the Network Operator.

Usually, location based privacy enhancing techniques can be based on purpose built technologies, or by using false location data without affecting the operation of the underlying system information. Representative technologies involve MIXes [2], [11] or data perturbation. Grutester et al. [10] employed data cloaking by reducing spatial accuracy in order to offer location based privacy. A similar concept was followed by Kido et al. [12] where false ("dummy") location data is submitted by a user in order to conceal their location.

Location information in the context of satellite communications is vital for synchronization purposes in the Return Link of an RCST in a DVB-RCS network. Its location (latitude, longitude and altitude) must be known to the operator of the network, assuming accuracy of the location of no more than a few kilometers [8]. Concealing location is a challenging exercise since in practice this means that an RCST cannot synchronize with the Hub station and provide connectivity to the end user unless it is configured with the coordinates of the installation location. It is thus the fundamental part of the design philosophy of a DVB-RCS network that force the user to provide (and disclose) the RCST physical location with an accuracy of a few kilometers. For certain users and sectors (such as government, law enforcement and military for example) this can be viewed as an unacceptable leakage of information security event.

The main research goal of this work is to find out if the fundamental design principles of the DVB-RCS standard would allow a user to bypass location accuracy restrictions and employ data cloaking in order to enhance location based privacy. The methodology adopted to meet this goal involves a theoretical analysis of the DVB-RCS standard, development of a privacy enhancing extension to the standard and finally validation via a proof of concept "attack" on a real DVB-RCS system. In addition we present the results along with the methodologies and tools used.

This paper is structured as follows. In section 2 we outline the main aspects of DVB-RCS specification for the benefit of the reader. In section 3 we develop the privacy preserving approach and investigate its integration within the DVB-RCS specification. Section 4 describes the proof of concept used for empirically validating the proposed approach, and finally section 5 contains the conclusions.

2. The Privacy Lacking DVB-RCS Specification

For the benefit of the reader in the next paragraphs we present an introduction to the design principles that the DVB-RCS standard is based on. Radio communications can generally be classified as unidirectional or bi-directional. In unidirectional communications such as broadcasting (e.g. TV services) a station solely uses its assigned frequency bandwidth. In bidirectional radio communications (full duplex) stations monopolize their allocated resources during transmission time. Unfortunately satellite frequency capacity and power is both limited and expensive. With the exception of dedicated use such as TV program delivery, transponder bandwidth has to be shared among many users. Therefore almost all satellite communications systems employ techniques to permit Multiple Access (MA) to the satellites limited resources. Classical methods for MA such as TDMA (Time Division Multiple Access) and FDMA (Frequency Division Multiple Access) are used in current DVB-RCS networks.

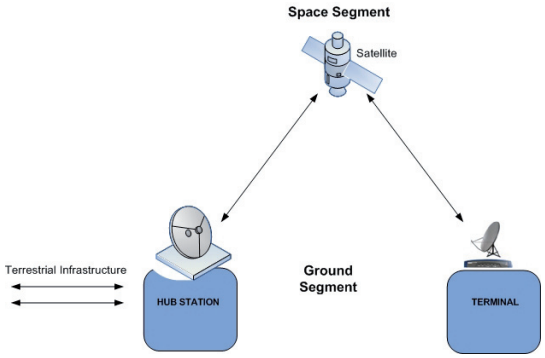

Fig. 1. Typical Satellite Communications System.

In general principle all satellite communications involve at least three stations, two placed on the earth surface and a repeater station on the satellite (Fig. 1):

- **Space segment:** Satellite and the transmission paths.
- **Ground segment:** Stations communicate via satellite, and
- **Interconnection to the terrestrial networks:** e.g. connection to a terrestrial ISP.

Communication between any two Terminals depends on the network topology. Satellite, being usually a "passive" relay (mirror in the sky) does not enforce a specific network topology. Although Mesh networks provide advantages such as half the latency in Terminal-to-Terminal communications their traffic handling requirements increase with the number of installed Terminals. For this reason, in large installations, all DVB-RCS are configured as stars (Fig. 2) where all Terminals communicate via base stations called Hubs. The terms "Hub" and "Gateway" can be used interchangeably to designate the major station (having full control over its Terminals) in a satellite communications system, carrying terrestrial network services to and from Terminals. In the case of VSAT (Very Small Aperture Terminal) particularly, the term "Hub" is used to identify the central station of a star network configuration (Fig. 2).

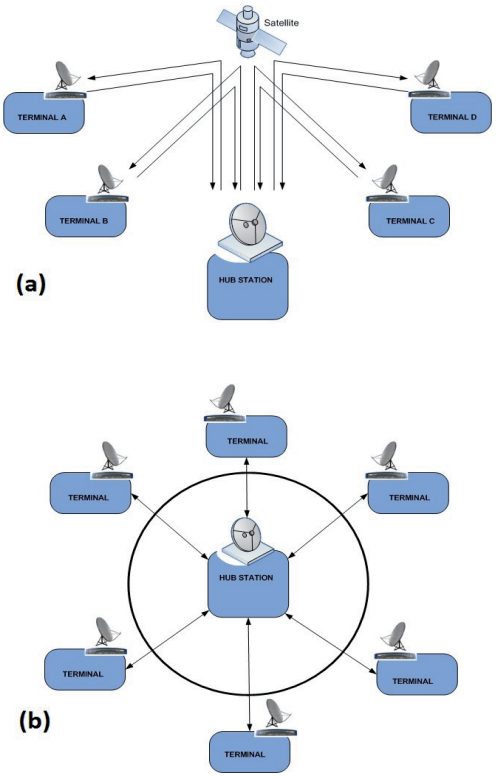

Fig. 2. Typical Star Satellite network. Physical (a) and Logical (b) architecture is depicted.

DVB-RCS systems support bi-directional communications by means of:

- **Forward channel:** Transmission from Hub station to many terminals.
- **Return channels:** Transmission from the Terminals to the Hub station.

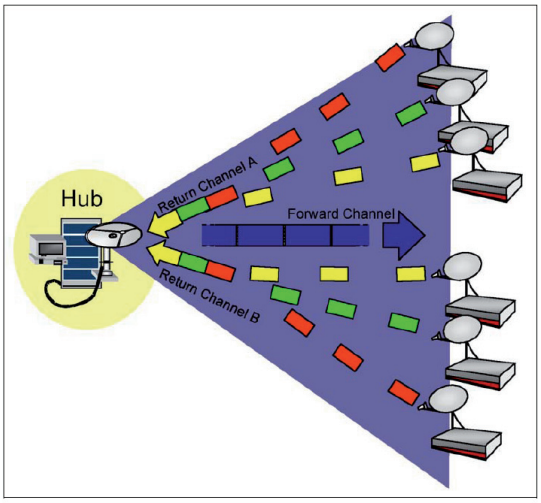

Fig. 3. Bi-directional communications via Forward and Return channels. (adapted from [14]).

Forward channel provides the "point-to-multipoint" service. It has a single carrier which may utilize the full bandwidth of a transponder and it is identical to a DVB-S broadcast channel. Forward link resources sharing by the RCST's, is accomplished through the use of different time slots in the TDM carrier.

Return channel capacity, of one or more satellite transponders, is shared among Terminals by transmitting in bursts, using MF-TDMA (Multiple Frequency-TDMA). This means that there is a number of return channel frequencies, each divided into time slots. These time slots then can be assigned to Terminals permitting simultaneous transmission to the Hub Station (Fig. 3). A Common clock for all terminals is provided via timing information (NCR Network Clock Reference) embedded in the Forward Link.

In a satellite network, the Hub and the satellite are located at fixed points on the earth's surface and on the geostationary orbit respectively, keeping the uplink and downlink transmission times between the Hub and the satellite very nearly fixed. Terminals on the other hand can be spread throughout the satellites footprint, having different signal transit times between them and the satellite. This variation is unimportant to the forward link due to its broadcast nature.

However on the uplink the Terminals transmit in bursts that share a common return channel. These bursts are spaced from each other in time. Those small variations in Terminal-to-Satellite transit times can disrupt transmission since, as illustrated in Fig. 4, a burst from one Terminal may collide with a neighboring burst sent by a Terminal having a longer signal transit time to the satellite.

Differences in Terminal-to-Satellite transmission times might be compensated for by using time slots sufficiently longer than the bursts emitted by the terminals, so that before and after a burst there is a guard time (Fig. 5) sufficiently long to prevent collisions or power leakage from switch-off transients with the bursts in neighboring slots in the TDMA frame.

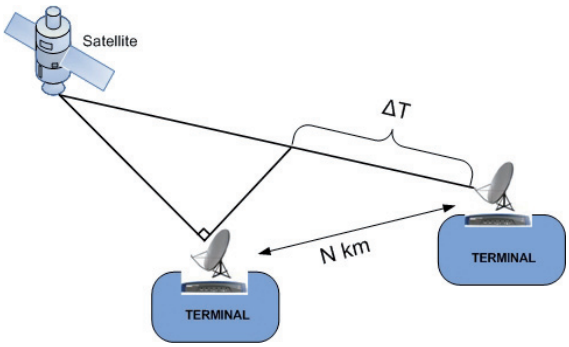

Fig. 4. Terminals located at different places in satellite footprint. Uplink transmission times to and from them vary.

"The one-way delay time between a Hub and a Terminal varies from 250 to 290 milliseconds, depending on the geographical location of the Terminal with respect to the Hub. So the time differential, ΔT, might be as large as 40 milliseconds. Consequently, the round-trip time differential might be as large as 80 milliseconds. Thus, the total guard time associated with a slot would have to be at least 80 milliseconds. This is excessive, particularly as the guard time does not carry information and wastes satellite resources" ([14] p.37). Minimizing guard in most TDMA systems involves various means of timing adjustments to compensate for these Terminal-to-Satellite path differences. DVB-RCS has two built-in methods of pre-compensating the burst transmission time of each Terminal [14]:

- Each terminal is configured with its local GPS coordinates and therefore can calculate its own burst transmission time.
- The Hub monitors the arrival time of bursts and can send timing correction information to Terminals if need be.

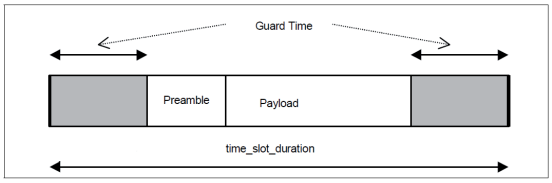

Fig. 5. Time slot in a DVB-RCS system (adapted from [8]).

3. A Location Privacy Preserving DVB-RCS Approach

From the basic operational theory of a DVB-RCS network, presented in section 2, it is obvious that the necessity of providing the exact location to the RCST and consequently to the network operator, is only needed for the calculation of the range (distance) between the specific RCST and the satellite. This range is then used by the RCST to synchronize its transmission bursts (calculate appropriate delays) in a TDMA frame of the Return Channel. We can also see that the calculation of this range can be within some tolerances which can be "absorbed" by

the system through the mechanism of the guard time between consequent bursts of the RCST's.

So let us now assume that we have an RCST *R*, whose real geographical position lies in the footprint of satellite S, and has (true) LLA (Latitude, Longitude, Altitude) coordinates (*LatR, LongR, AltR)*. The geosynchronous satellite *S* locates at longitude *LongS*. The range between satellite *S* and RCST *R* ($Distance_{R\text{-}S}$) is given by the following equation:

$$Distance_{R-S} = F(LatR, LongR, AltR, LongS) \quad (1)$$

where *F* is the function that provides the range (distance) in meters between the RCST and the satellite.

Now let us consider some other coordinates *LatR', LongR', AltR'* different than the true ones that satisfy the following equation:

$$Distance_{R-S} = F(LatR', LongR', AltR', LongS) . \quad (2)$$

If (2) is satisfied then we can provide the RCST with the new "fake" *LatR', LongR', AltR'* coordinates and the system would continue to operate without any loss of availability or QoS reduction in general, having effectively hidden the real location of our RCST from the network operator.

From a theoretical standpoint, the locations on Earth (assuming a spherical earth) which are equidistant from the specific satellite *S*, lie on the intersection of two spheres. The first sphere is the earth (*Sph01*). The second sphere (*Sph02*) has center the position of the satellite *S* and radius the distance ($Distance_{R\text{-}S}$) between the satellite and the RCST. This concept is depicted in Fig. 6.

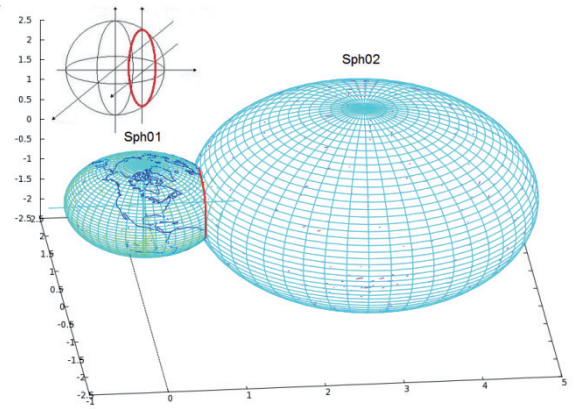

Fig. 6. Intersection of two spheres where *Sph01* is the Earth and *Sph02* has center the position of Satellite S and Radius=$Distance_{R\text{-}S}$..

We also have to note that not all points that belong to the intersection of the above spheres can be used to hide our true location. This is due to satellite footprint which may not cover the total of the intersection. Although we could use from a physical standpoint any location on the intersection, this would raise suspicion on the network operator because an RCST would be located in a place where there is no satellite coverage.

So we can only use the points that belong both to the satellite footprint AND the intersection of two spheres in order to effectively hide our RCST without raising any kind of suspicion.

3.1 Incorporating the Privacy Preserving Method into the DVB-RCS Procedures

In the DVB-RCS standard for an RCST to be able to join the network it has to get into various states following specific procedures. Initially the RCST is at the **Receive Sync state**, which is reached following the **Initial synchronization procedure** (described later). Then the entry of an RCST into the system is achieved through the following four phases [5]:

- **Logon procedure:** the RCST requests initial access to the network and gets initial logon information from the network.
- **Acquisition coarse synchronization procedure (optional):** the RCST improves its physical synchronization (frequency, time, and power adjustments).
- **Fine synchronization procedure:** the RCST completes its physical synchronization.
- **Synchronization maintenance procedure:** the RCST maintains its physical synchronization during the entire session.

Corresponding to the *procedures*, the RCST can be in one of the following *states* [5]:

- **Hold:** the RCST is in hold mode. In this state the RCST is instructed by the NCC (Network Control Center) to cease transmission until it is told differently.
- **Inactive Off/Stand-by:** the RCST is not powered or on a stand-by mode or has lost synchronization.
- **Receive sync:** the RCST has acquired the forward link.
- **Ready for coarse sync:** the RCST has been detected by the NCC, and may initiate a coarse synchronization procedure.
- **Ready for fine sync:** the RCST has been detected by the NCC, and may initiate a fine synchronization procedure.
- **Fine sync:** the RCST is synchronized and can send traffic.

Especially important is the initial synchronization procedure which is followed by the RCST in order to enter the Receive sync state. This procedure is executed immediately after the power-up of the RCST and is described below [5]:

- The RCST receives all necessary control information related to the operation of the DVB-RCS network

through the forward link. This includes NCR (Network Clock Reference) synchronization, through which the RCST initiates its internal clock.

- The RCST then calculates the satellite ranges for both forward and return links using the satellite ephemeris data contained within the Satellite Position Table (SPT, acquired through the Forward link signaling) plus a knowledge of its own location (latitude, longitude and height above sea level). It uses then these ranges to calculate the corresponding satellite to RCST and RCST to satellite propagation delays. In case the NCC does not transmit an SPT the nominal satellite position can be used, which can be found in the NIT (Network Information Table acquired also through the Forward link signaling).
- The RCST continues to receive the NCR throughout the session. In the event that NCR synchronization is lost, the RCST ceases transmission and re-starts the initial synchronization procedure. Similarly, any failure of the RCST during one of the later procedures takes the RCST back to the initial synchronization procedure.
- The RCST receives the burst time plan transmitted by the NCC at regular intervals. The BTP is contained in the Forward link Signaling, and is made of the Superframe, Frame and Timeslot Composition Tables.

Coarse and Fine synchronization procedures which are optional are used only in cases where timing errors are above "coarse sync thresholds" and "fine sync thresholds".

Initial burst time errors can be low when the satellite and terminal position are known. Provided that the NCC/gateway receivers can cope with these errors, which are small for a satellite maintained in a tight "box", there is no requirement for the RCST to perform the ranging process of the coarse synchronization procedure. Therefore if we use as "fake" coordinates those that produce the same $Distance_{R\text{-}S}$ as the true coordinates (measured with a GPS device) of the RCST the whole synchronization-logon procedure would be carried out successfully in both cases.

The DVB-RCS standard states that "an RCS system can be designed assuming accuracy of the location (latitude, longitude and altitude) of the RCST of no more than a few kilometers" [8]. Let us be conservative enough in our calculations, by using an accuracy of 2 km. The area A_t of a circle with center in the true location of the RCST and a radius of 2 km is:

$$A_t = \pi \cdot r^2 = \pi \cdot 2^2 \cong 12.56 \text{ km}^2. \quad (3)$$

This means that the NCC assumes that the location of the RCST lies in this specific area A_t (by reading the RCST coordinates).

If we modify (2) relaxing the equality restriction we have

$$D1 = Distance_{R-S} - 1000m,$$

$$D2 = Distance_{R-S} + 1000m, \quad (4)$$

$$D1 < F(LatR', LongR', altR', LongS) < D2.$$

Equation (4) transforms the intersection of the two spheres of Fig. 6, from a line into a ribbon with an area of A_I. We then keep the part of the ribbon that lies within the footprint of the satellite, having an area of A_{IF} ($A_{IF} < A_I$). Then we can define a metric for the improvement of location privacy (LP_I) of the specific RCST:

$$LP_I = \frac{A_{IF}}{A_t}. \quad (5)$$

In the next section we present a proof of concept of the above theory, tested in a real DVB-RCS system, along with experimental results.

4. Proof of Concept and Experimental Results

In order to test the theoretical findings presented in the previous section, we developed a practical method, tested in a real DVB-RCS network. Also we had to take into account the following restrictions:

- A normal user usually does not have access to the ephemeris data of the satellite (necessary for obtaining the best accuracy in the range calculations).
- Guard time between time slots is network dependent and it is not announced to the users of the DVB-RCS service.
- A normal user does not have easy access to expensive equipment, such as DVB-RCS analyzers.
- Earth is not an ideal sphere.

It was our intention to keep the validation approach as simple as possible, the equipment to be the absolute minimum and the necessary data to be freely available, in an effort to prevent unnecessary leakage of user information through other channels (e.g. through the purchase of non-free high accuracy Earth surface elevation data). For the specific practical method that was carried out during this work, we used:

- One SatNet 4100 satellite modem (DVB-RCS) from Advantech Wireless, Canada.
- Subscription to the DVB-RCS network of Hellenic Aerospace Industry (1024down/256up kbps).
- PC with a core2duo at 3.33GHz cpu, 4GB ram and 1TB hard drive. The operating system was Fedora Linux. The necessary software was developed in C/C++ using development tools provided by the distribution.
- The Digital Elevation Model, for the footprint of the satellite used by our DVB-RCS provider, was

acquired from the Advanced Spaceborne Thermal Emission and Reflection Radiometer (ASTER) instrument of the Terra satellite (freely available covering 99% of the globe) [1].

- The footprint of the satellite (Fig. 7) was acquired from LyngSat Maps [13].
- The DVB-RCS network operator uses the Hellas Sat 2 satellite located at 39°E.

For the purpose of our tests, we used a DVB-RCS terminal (SatNet 4100) [15] located at the premises of Democritus University of Thrace (DUTH). The RCST was initially fully functional, obviously configured with the correct (acquired through the use of a common GPS device) coordinates:

$$\begin{aligned} Lat_{DUTH} &= 41.142445^{o}, \\ Long_{DUTH} &= 24.890225^{o}, \\ Alt_{DUTH} &= 79 \text{ m}. \end{aligned} \quad (6)$$

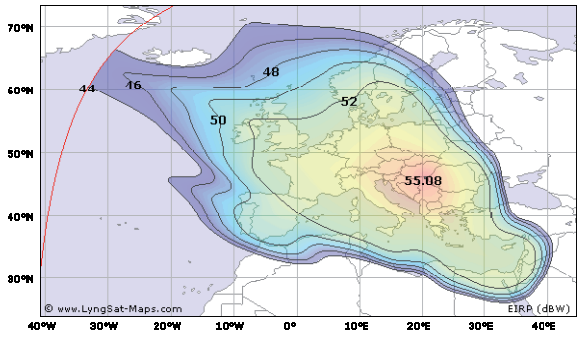

Fig. 7. Footprint of Hellas Sat 2 satellite (adapted from LyngSat Maps [13]).

A Digital Elevation Model (DEM) – also sometimes called a Digital Terrain Model – generally refers to a representation of the Earth's surface (or a subset of this), excluding features as vegetation, building, bridges, etc. DEM data usually come in the form of raster images holding surface elevation data along georeferencing (e.g. latitude, longitude) information. There are various sources for obtaining free DEM data, one of them being the ASTER instrument of the Terra Satellite covering the globe at a 30meter resolution (1 arcsecond) [1]. Terrain Elevation data from ASTER can be downloaded from their site, in the form of GeoTIFF [16] files where embedded in the header are geographic information and the value of each pixel represents its Altitude. Combining these pieces of information we can compute the latitude, longitude and altitude information (in the World Geodetic System 84 (WGS84) reference frame [4], for every pixel on the raster.

Based on Fig. 7 (satellite footprint) and for the needs of our experiment, we have downloaded from ASTER website the Digital Elevation Model (in GeoTIFF format) for the region which is depicted in Fig. 8. Using these files we calculated for every point i (having Lat_i, $Long_i$, Alt_i coordinates) on the terrain the distance ($Distance_{i\text{-}S}$) from Hellas Sat 2 satellite. Hellas Sat 2 is located (latitude, longitude and altitude coordinates) at:

$$Lat_S = 0^{o}, Long_S = 39^{o}E, Alt_S = 35{,}786.2 \text{ km}. \quad (7)$$

Fig. 8. Digital Elevation Model for the area of interest (lies inside Hellas Sat 2 footprint). Color represents the altitude above sea level.

The distance between the Hellas Sat 2 satellite and the location of our RCST in DUTH was calculated and found to be:

$$Distance_{DUTH-S} \cong 37{,}749 \text{ km}. \quad (8)$$

For every point i of the Digital Elevation Model of Fig. 8 we calculated the distance $Distance_{i\text{-}S}$. The points that their distance from Hellas Sat 2 satisfies the following equation (9):

$$\begin{aligned} D1 &= Distance_{DUTH-S} - 1000m, \\ D2 &= Distance_{DUTH-S} + 1000m, \\ D1 &< Distance_{i-S} < D2 \end{aligned} \quad (9)$$

can be considered that are equidistant to Hellas Sat 2

$$Distance_{i-S} \cong Distance_{DUTH-S} \quad (10)$$

and that their latitude, longitude and altitude (Lat_i, $Long_i$, Alt_i) coordinates can be used on the RCST instead of the true ones (Lat_{DUTH}, $Long_{DUTH}$, Alt_{DUTH}). The geographical location of the points that satisfy (9) along with the real location of the RCST are depicted in Fig. 9 (thin grey line and red X mark respectively).

Fig. 9. The gray line denotes the geographic location of the points of the terrain that satisfy (9). The true location of the RCST is denoted with a red X.

Fig. 10. Coordinates of Locations P1-P12 were used instead of the real ones (DUTH) and the RCST continued to synchronize to the Hub station.

The next step was to configure our RCST through its web interface with the latitude, longitude and altitude (Lat_i, $Long_i$, Alt_i) coordinates of various points that lie in the "equidistant" grey zone (Fig. 9), while our RCST was still located in DUTH premises. For every set of coordinates that we provided, we rebooted the RCST and watched if it could still synchronize and connect with the Hub station. This procedure takes about 4 minutes and obviously we could not perform this test for all the points that lie in this "equidistant" zone (for the 30m grid of Fig. 9 the grey "equidistant" zone included 3,096,855 points). The above procedure was repeated for a large number of points that were spread throughout this "equidistant" zone and the RCST synchronized and connected to the hub as expected. A sample of those points is depicted in Fig. 10 and their coordinates are presented in Tab. 1.

Point	Latitude [°]	Longitude [°]	Altitude [m]	RCST Sync. (YES/NO)
P1	39.2181061	19.5055362	0	YES
P2	39.4347330	20.0060191	70	YES
P3	39.6999143	20.6409601	312	YES
P4	39.9016014	21.1377080	1505	YES
P5	40.1331681	21.7689140	820	YES
P6	40.3834096	22.4934937	149	YES
P7	40.6934102	23.4048208	33	YES
P8	40.9810011	24.3198828	50	YES
P9	41.2237726	25.1415711	467	YES
P10	41.4553393	26.0043438	398	YES
P11	41.6981109	26.9978397	138	YES
P12	41.9296776	28.0286851	69	YES

Tab. 1. Coordinates of Locations P1-P12 and synchronization results.

In the previous section we developed a metric (5) for the level of improvement on location privacy for an RCST. For the RCST located at DUTH, the area that is covered by the "equidistant" zone (excluding sea areas) of Fig. 9 was:

$$A_{IF} \cong 1650 \text{ km}^2 \tag{11}$$

and location privacy was improved by a factor of ~131 times:

$$LP_I = \frac{A_{IF}}{A_t} \cong \frac{1650 Km^2}{12.56 Km^2} \cong 131. \tag{12}$$

The same test procedure was repeated successfully for an RCST physically located at:

$$\begin{aligned} Lat_{TEST2} &= 37.962939^o, \\ Long_{TEST2} &= 23.690662^o, \\ Alt_{TEST2} &= 28 \text{ m}. \end{aligned} \tag{13}$$

The "equidistant" zone for this location along with the successfully tested "fake" locations, are presented in Fig. 11a, 11b.

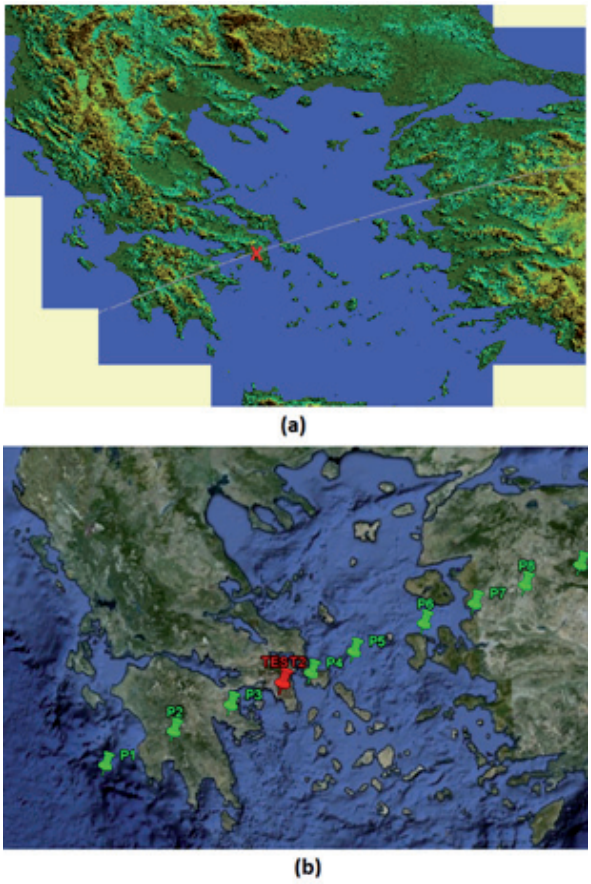

Fig. 11. Physical location of TEST2 RCST (red X mark) and respective "equidistant" zone (grey line) (a). P1-P9 coordinates were used instead of the true ones (TEST2) and the RCST continued to synchronize to the Hub station.

5. Conclusions and Areas of Future Research.

In this work we presented that by exploiting the physics that govern the DVB-RCS return link synchronization we can significantly improve the location privacy level of an RCST. This paper also presented a methodology, using the least possible equipment, free software and freely distributed terrain elevation data for the calculation

of the geographic area where the user can effectively "hide" his/her terminal. The theoretical findings and the utilized methodology were tested on a real system with successful results. Although the location privacy was greatly improved, the restrictions we set on "equidistancy" (1 km) were really conservative. It is our intent to explore, in a following work, the limits of this methodology in order to maximize the area that a user can effectively "hide" his/her terminal.

Acknowledgements

The authors would like to thank the staff at Satellite and Space Applications Department of Hellenic Aerospace Industry S.A. for their invaluable help.

References

[1] ASTER Global Digital Elevation Model (ASTER GDEM) data. Collaborative project of Trade and Industry of Japan (METI) and the National Aeronautics and Space Administration (NASA). Data available at http://www.gdem.aster.ersdac.or.jp/.

[2] BERESFORD, A. R., STAJANO, F. Mix zones: User privacy in location-aware services. In *Proc. Pervasive Comput. Commun. Security (PerSec)*, 2004, p. 127–131.

[3] ESA, European Space Agency. *Final Report: Security for DVB-RCS at Management and Control Planes*. [Online] Cited 2010-05-27. Available at http://telecom.esa.int.

[4] EUROCONTROL, European Organization for the Safety of Air Navigation. *WGS 84 Implementation Manual*. [Online] Cited 1998-02-12. Available at http://www2.icao.int.

[5] European Telecommunications Standards Institute, ETSI. *Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems. ETSI EN 301 790 V1.5.1*. [Online] Cited 2009-05. Available at http://www.etsi.org.

[6] European Telecommunications Standards Institute, ETSI. *Digital Video Broadcasting; Implementation guidelines for Data Broadcasting. ETSI TR 101 202 V1.2.1*. [Online] Cited 2003-01. Available at http://www.etsi.org.

[7] European Telecommunications Standards Institute, ETSI. *Digital Video Broadcasting; Framing structure, channel coding and modulation for 11/12 GHz satellite services. ETSI EN 300 421 V1.1.2*. [Online] Cited 1997-08. Available at http://www.etsi.org

[8] European Telecommunications Standards Institute, ETSI. *Digital Video Broadcasting (DVB); Interaction channel for Satellite Distribution Systems; Guidelines for the use of EN 301 790. ETSI TR 101 790 V1.4.1*. [Online] Cited 2009-07. Available at http://www.etsi.org.

[9] European Telecommunications Standards Institute, ETSI. *Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); IP Internetworking over satellite; Security aspects. ETSI TR 102 287 V1.1.1*. [Online] Cited 2004-05. Available at http://www.etsi.org.

[10] GRUTESER, M., SCHELLE, G., JAIN, A., HAN, R., GRUNWALD, D. Privacy-aware location sensor networks. In *Proceedings of the 9th conference on Hot Topics in Operating Systems (HotOS 2003)*. Lihue (HI), May 2003, vol. 9.

[11] JIANG, J., HE, C., JIANG, L. A novel mix-based location privacy next term mechanism in Mobile IPv6. *Computers & Security*, 2005, vol. 24, no. 8, p. 629-641.

[12] KIDO, H., YANAGISAWA, Y., SATOH, T. Protection of location privacy using dummies for location-based services. In *Proceedings of the 21st International Conference on Data Engineering Workshops*. Tokyo (Japan), 2009.

[13] LyngSat Maps. Website providing standardized footprint maps for more than 600 satellite beams in the world. Available at http://www.lyngsat-maps.com/

[14] NBS, Nera Broadband Satellite AS, Norway. *Digital Video Broadcasting, Return Channel via Satellite (DVB-RCS) Background Book*. [Online] Cited 2002-11-25. Available at http://www.dvb.org/documents/white-papers/RCS-backgroundbook.pdf

[15] Advantech Wireless, Canada. *SatNet SIT Series S4120 IDU datasheet*. [Online] Cited Rev.2 2009-07. Available at: http://www.advantechwireless.com/file/product_sheets/Product_Sheet_VSAT_S4120.pdf.

[16] GeoTIFF project. *GeoTIFF Format Specification; Specification Version: 1.8.2*. [Online] Cited 2000-12-28. Available at http://www.remotesensing.org/geotiff/spec/geotiffhome.html.

About Authors ...

Aggelis AGGELIS obtained his BSc in Electrical and Computer Engineering, and MSc in Telecommunications, both from Democritus University of Thrace, Greece. He is currently a PhD candidate in Electrical and Computer Engineering in the same university. Aggelis is currently working as a Telecommunications Engineer at the Hellenic Aerospace Industry. His research interests include DVB-RCS, embedded computing and signal processing.

Emmanuel T. SARRIS is Professor of Electrodynamics at the Department of Electrical Engineering of the University of Thrace and Director of the Space Research Laboratory, 1977-present. Physics Diploma, U. of Athens (1967). PhD in Space Physics, U. of Iowa (1973, w. J.A. Van Allen). Experience: Space Plasma Electrodynamics; Design, Construction and Testing of Space Instruments and Systems; Satellite Communications. Co-I or P-I of experiments on the spacecraft: Ulysses, Geotail, Interball-Aurora, Interball-Tail, Cluster, Spektr-R. Over 300 refereed publications and 1700 citations. Member COSPAR Council. Corresponding Member of the Academy of Athens, 2003. ESA and/or NASA Awards for outstanding contributions to the Ulysses, Geotail and Cluster Missions.

Vasilios KATOS is Assistant Professor of Information and Communications Systems Security at the Department of Electrical and Computer Engineering of Democritus University of Thrace in Greece. Prior to his current post he was Principal Lecturer at the School of Computing at the University of Portsmouth where he participated in the development of the interdisciplinary Masters course MSc in Forensic IT. He has worked in the industry as a security consultant and expert witness in information systems security. His research interests are in information security, privacy, digital forensics and incident response.