Security Enhancement for Internet Communications over Satellite DVB using Chaos

Daniel Caragata, Bassem Bakhache, Safwan El Assad, Ion Tutanescu

***Abstract* - Satellite connections are expected to play an important role in providing Internet Protocol services as a complement of the next generation terrestrial network. DVB-S is one of the most widely used standards to transmit video, audio and data over satellite.**

This paper proposes a security system for IP over DVB-S that satisfies all the security requirements while respecting the characteristics of satellite links, such as the importance of efficient bandwidth utilization and high latency time. The usage of chaos is proposed both for the generation of new keys and for the data encryption.

A theoretical analysis of the system and a simulation of FTP and HTTP traffic are presented and discussed to show the cost of the security enhancement and to provide the necessary tools for security parameters setup.

***Index Terms* - Chaos, DVB, Internet, satellite, security.**

I. Introduction

Nowadays the Internet is the most important communication network as it has become very widespread (more that 20% of world population is using it [1]) and the services it may support are very diverse: news, shopping, bank accounts access, money transfer, video and audio conferencing etc.

Satellites have some very important characteristics: accessibility in isolated places (top of mountains, deserts, oil platforms, isolated villages etc.), easy implementation in disaster stricken zones (areas affected by earthquakes, fire, war etc.) or an alternative to land infrastructures. These are the reasons why the satellites have their place in the next generation Internet architecture.

DVB-S (Digital Video Broadcasting – Satellite) [14] is an open standard ratified by ETSI (European Telecommunication Standard Institute) in 1994. It is a part of the DVB standards family along with DVB-C (DVB – Cable), DVB-T (DVB – Terrestrial) and DVB-H (DVB – Handled). DVB-S2 was proposed in 2003 as the next generation of DVB-S [15]. It uses the advances made in coding and modulation technology. The DVB-RCS (Digital Video Broadcasting, Return Channel via Satellite) standard was developed in 1999 and its main feature is that it enables a two-way communication, the forward channel being similar to that of DVB-S.

DVB standards were initially proposed to offer video and audio services. Later, some encapsulation methods were proposed to enable IP links over DVB. The Unidirectional Lightweight Encapsulation (ULE) has proven to be the most successful. Even though the ULE standard is in its mature state, the optimal security solution remains to be studied.

This paper is organized as follows. In Section II we present how Internet over satellite works and what are the security requirements for it. In Section III we propose a security mechanism that uses: a multilevel key management technique, a simplified extension header, and chaotic functions for key generation and data encryption. In Section IV we analyze the data overhead and the period of Master Key usage in order to study the cost of security and to provide the necessary tools for the correct setup of the security parameters. We also simulate the system using real HTTP and FTP data. In Section V we present our conclusion.

II. Internet over DVB-S

A. General overview

The general structure of the communication system that allows Internet access over satellite DVB is presented in Figure1. The Internet Service Provider (ISP) has access to the Internet and sends IP packets to his clients (satellite terminals) using the satellite link. The IP packets need to be encapsulated and are carried by a MPEG-2 stream.

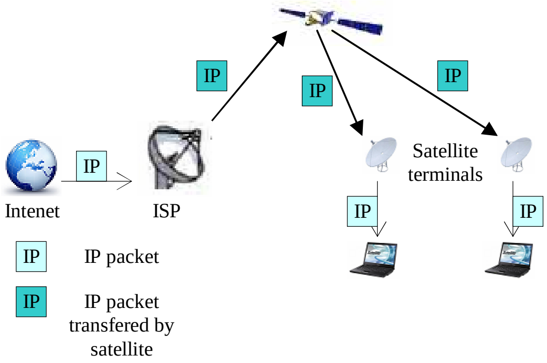


Fig. 1: Satellite IP communication.

A MPEG-2 TS (Transport Stream) is created after the multiplexing of several MPEG-2 ES (Elementary Streams)

Manuscript received July 1, 2009.

D. Caragata and S. El Assad are with IREENA, Ecole Polytechnique de l'Université de Nantes, France (e-mail {daniel.caragata, safwan.elassad}@univ-nantes.fr).

B. Bakhache is with the Electronics and Communications Department of the Faculty of Engineering – Lebanese University

I. Tutanescu and D. Caragata are with Electronics, Communications and Computers Faculty of University of Pitesti, Romania.

and is made up of a continuous stream of data frames with a fixed length of 188 bytes. Each frame has a header of at least 4 bytes and a payload of maximum 184 bytes. The only field of the header that is of interest for our paper is the Packet Identifier (PID). It is a 13 bits field that is used to determine to which ES the payload of the frame belongs.

We propose a security mechanism for the data link layer connection between the ISP and the satellite terminals.

B. ULE Encapsulation

Network level Packet Data Units (PDU) must be encapsulated in order to be transported over the satellite link. There are two possible encapsulation methods, MPE [2] and ULE [3]. It has been shown in [4], [5] and [6] that ULE has many advantages over MPE such as improved efficiency and native support for a wide range of network protocols. It is therefore becoming the predominant method of encapsulation in DVB-S/DVB-RCS.

The standard ULE encapsulation method is presented in Figure 2.

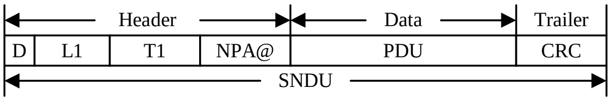


Fig. 2: Standard ULE encapsulation

ULE creates a Sub Network Data Unit (SNDU) by adding a header and a trailer to the network level PDU. The header is formed of:

- *D*: a one bit field indicating the presence or absence of the optional field NPA (see below).
- *L1*: a 15 bits field indicating the length of the SNDU starting from the first byte after the *T1* field and including the CRC trailer. The length is expressed in bytes.
- *T1*: a 16 bits field indicating the type of network PDU being carried by the SNDU. Its values are assigned by the Internet Assigned Numbers Authority (IANA).
- *NPA@*: Network Point of Attachment address is a 48 bits optional field that can carry the destination address of the SNDU. Usually it is a MAC address.

The SNDU data is represented by the network level PDU and the SNDU trailer is a CRC-32 code applied to the whole SNDU.

If no additional information about the PDU is required then the standard ULE header will be used. This adds very little additional information. If other services are to be provided, such as security, ULE allows a flexible mechanism for the extension of the SNDU header. Its format is presented in Figure 3.

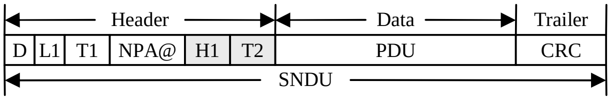


Fig. 3: ULE extension header

The field *T1* does not indicate the type of network PDU that is carried, but the type of extension header. Its values are also assigned by IANA.

The field *H1*is the extension header and its structure is determined by the type *T1*. There are predefined extension headers (such as the format for a bridged payload [3]) and unassigned values of extension header types that can be used for new extension headers.

T2 indicates the type of PDU that is being carried, similar to the field *T1* of the ULE without the extension header.

C. Security requirements

IP over satellite DVB is a wireless communication protocol and thus susceptible to several attacks. They have been studied in [7] and [8]. The security requirements that have been derived in order to counter these attacks are:

- *Data confidentiality*: is the most important security requirement because any unauthorized receiver can access the PDU that are being transmitted.
- *Data integrity and authentication*: are required to counteract active threats.
- *Protection against replay attacks*: sequence numbers are suggested to prevent replay attacks.
- *Link layer terminal authentication*: it is required as part of the key management protocol.

Trying to respond to these security requirements, two security systems have been proposed, one in [9], [10] and the other in [11]. We have used the advantages of both in order to present a novel and improved security system for satellite Internet.

III. Proposed System

A. General description

The security system that we propose responds to the security requirements and takes into consideration the characteristics of satellite communications. In order to achieve the required properties, an extension header is used that contains a 32 bit Packet Number (PN). This field provides protection against replay attacks and is used as a nonce in the key deriving process.

In order to provide data integrity and authentication, we propose that the CRC trailer of the SNDU be replaced by a MAC (Message Authentication Code).

All the PDU are encrypted. We propose a key derivation system that allows the encryption of each PDU with a different key and we also propose the encryption of the MAC trailer for more security.

The link layer terminal authentication is realized by the multilayer key management system. It is based on a private key that has been previously exchanged between the ISP and the terminals by other means of communication than the satellite link.

B. SNDU structure

The structure of the SNDU is presented in Figure 4: *T1* is the type of the extension header. As mentioned above, IANA must assign a value for it. *T2* carries the type of the encapsulated PDU.

In order to enhance the security of the MAC code, and to broaden the range of choices for it, it will also be encrypted. The MAC will not protect just the PDU that is encapsulated but also the ULE header, thus providing protection against a wider range of active attacks.

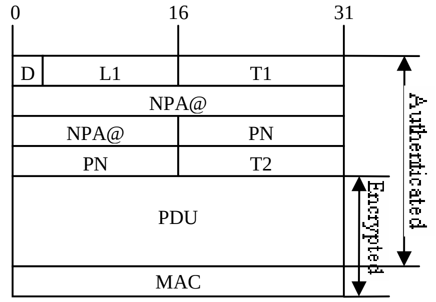


Fig. 4: SNDU secured.

C. *Key management system*

We propose the use of a multilayer key management structure [19], [20]:

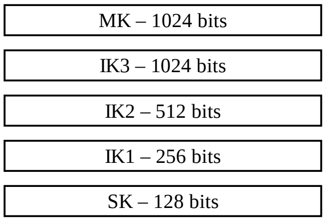


Fig. 5: Multilayer key management system.

The number if Intermediary Keys (IK) and the size of keys can be chosen by the ISP as it sees fit, taking into account the particular security requirements and the bit rate of the protected connection. However, we can choose them at the initialization stage. Once fixed, they cannot be modified.

The current key, Session Key (SK), is used to derive the encryption and the authentication keys. We consider that a length of 128 bits provides the required security level for most applications.

SK will be used for a limited amount of data, SKTh (Session Key Threshold). When SK needs to be changed, a new SK will be generated by the ISP and it will be sent encrypted using IK1 to the terminal. IK1 will also be used a limited number at times, IK1Th (Intermediary Key 1 Threshold). When IK1 needs to be changed a new value for it will be generated and it will be sent encrypted with the next level key, IK2. IK2 and IK3 are treated in a similar manner.

MK (Master Key) is the top level key of the structure. It is agreed upon between the ISP and the terminal at a previous stage, using a smart card. The MK cannot be changed using the satellite communication.

D. *Proposed chaos generator*

We propose the use of chaotic functions, both for key generation and data encryption.

The proposed chaotic generator [17] consists of two cascaded generators. Each one is looked at as a recursive filter containing in addition a non-linear function. Different non-linear functions FNL(x) were tested: *xLnx*, *x×exp[cos(x)]*, *pwlcm*, etc.

If the *x×exp[cos(x)]*, is used as non linear function, the equations of every layer are:

$$x_1(n) = \mathrm{mod}[k_{u1}(n) + c_{11} \times e_{u1}(n-1) + c_{12} \times e_{u1}(n-2) + c_{13} \times e_{u1}(n-3), 2^N]$$

$$e_{u1}(n) = \mathrm{mod}[x_1(n) \times \exp\{\cos[x_1(n)]\}, 2^N] \qquad (1)$$

$$x_2(n) = \mathrm{mod}[e_{u1}(n) + c_{21} \times e_{u2}(n-1) + c_{22} \times e_{u2}(n-2) + c_{23} \times e_{u2}(n-3), 2^N]$$

$$e_{u2}(n) = \mathrm{mod}[x_2(n) \times \exp\{\cos[x_2(n)]\}, 2^N] \qquad (2)$$

All coefficients C_{11}, C_{12}, C_{13}, C_{21}, C_{22}, *and* C_{23} are equal to 1. The structure of the generator is presented in Figure 6.

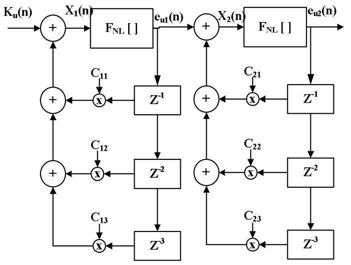


Fig. 6: Proposed chaotic generator.

It has been proven that this generator allows to expand the periodicity of its outputs and passes the randomness NIST tests.

Our proposed security enhancement for the ULE communications can support different algorithms for data encryption, and has a mechanism that allows a very frequent change of the encryption algorithm. We recommend that one of the supported algorithms to be the CCMSTI algorithm from [18].

E. *Encryption and authentication*

The encryption and authentication of each PDU are realized with a different key, which will be derived from the current SK, the NPA address and the PN with the aid of a any hash function, as shown in Figure 7. Using a 32 PN bits as a nonce guarantees that a new key is obtained for each packet. This approach is similar to the security solution in Wi-Fi, WPA (Wireless Protected Access) protocol that uses TKIP (Temporal Key Integrity Protocol) [13].

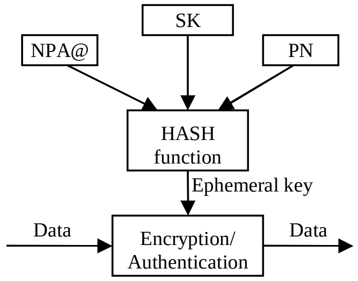


Fig. 7: Key derivation system.

We provide a mechanism that allows algorithm agility for the hash function, the encryption algorithm and MAC algorithm, thus increasing the overall security of the system.

F. *Security PDU*

The system must be able to provide a way to transport the new secret keys. This will be a new type of PDU, the Security

PDU (SPDU). The structure of the SPDU will be analogous with the structure of a normal network PDU. It will contain a header that will carry information about the current security association, and a payload that will carry the new keys. Its structure is depicted in Figure 8.

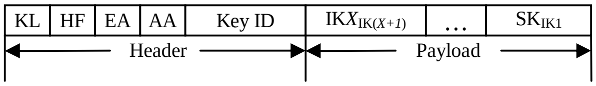


Fig. 8: The SPDU.

The header will contain the following fields:

- *KL, Key Level:* a 2 bit field indicating what keys are being transported by the SPDU: just the SK, the IK1 and SK, the, IK2, IK1 and SK or, IK3, IK2, IK1, and SK.
- *HF, Hash Function:* a 2 bit field that indicates the hash function used in the key derivation from fig. 7.
- *EA, Encryption Algorithm:* a 2 bit field indicating the encryption algorithm that will be used.
- *AA, Authentication Algorithm:* a 2 bit field indicating the authentication algorithm.
- *Key ID:* an 8 bit field identifying the security association that is being created.

The payload of the SPDU carries the new keys. $IKX_{IK(X+1)}$ means one of IK1, IK2 or IK3 encrypted with IK2, IK3 or MK respectively. Finally, this SPDU will be encapsulated and transported like any other network PDU.

G. *The alarm message*

Under certain circumstances, such as high noise, hardware error, active attack, power failure, the terminal may loose the key synchronization with the ISP. In this case it is unable to decrypt any messages or to recover any new keys. In order to recover the key synchronization the terminal will send an alarm message. We will not discuss its exact structure because it is a function of the return channel that will be used. However, it will always carry the Key ID of the last valid keys that were used by the terminal.

IV. System analysys and symulation results

A satellite can cover a very wide area, so the number of possible users is very large. In the same time the bandwidth of a certain satellite link is limited at 40 MHz for most applications. This is why one of the key characteristics of IP over satellite DVB is the importance of using the spectrum resource in an efficient way, thus maximizing the number of clients for a certain ISP, or the available bit rate.

Our system uses a hierarchical key management system. The choice of the exact structure of the system (number of intermediary keys and security parameters) must be done taking into account the systems particularities. One of these particularities is the frequency of MK usage, FMK. It is very important to analyze this parameter because it is easy to obtain systems that use the MK very often (many times in one day) or systems that almost never use MK (one time at more than 2 years). If the optimum value of the frequency of MK usage may be chosen by the ISP and his client, the extreme cases must always be avoided.

We have analyzed 5 sets of parameters (see Table I):

Table I - The sets of analysed parameters.

	I	II	III	IV	V
IK4Th	50	100	200	500	1000
IK3Th	50	100	200	500	1000
IK2Th	50	100	200	500	1000
SKTh	256 kb	512 kb	1 Mb	2 Mb	4 Mb

The studies we have performed have showed us that these sets of parameters can cover a wide range of applications.

A. *Theoretical data overheads*

The Data Overhead, DO, is the expression of the added quantity of data that needs to be sent using the satellite link in order to provide the security services. It is expressed as the ratio between the added information and the total information sent. It can be expressed in percentage:

$$DO = \frac{AI}{TI} \cdot 100$$

where *AI* is Added Information and *TI* is Total Information.

For our system the *DO* has two components: the key management component and the extension overhead component. We calculate the *DO* for a complete cycle of key management, between two successive utilizations of MK.

The key management component, DO_{KM} is made up of all the SPDU that need to be sent to carry the key management information. Therefore, it is a function of the security parameters SKTh, IK2TH, IK3Th and IK4Th.

The extension header component, DO_{EH} is made up of the extra bytes of the ULE header, the fields *T1* and *PN*. Because the same amount of data, 6 bytes, is sent with each packet, the value of this component is a function of the medium packet length.

$$DO = DO_{KM} + DO_{EH} = \frac{KMI + EHI}{TI} \cdot 100$$

where:

- *KMI* – Key Management Information, is the number of bytes in the totality of SNDU that are sent over the satellite carrying key management information; these SNDU will be supposed to have standard header.
- *EHI* – Extension Header Information, is the total number of extension header bytes.
- *TI* – Total Information, is the number of bytes in the totality of SNDU sent over the satellite link.

The extension header component will be applied also on the SNDU that carry the key management information. In order to calculate the DO_{EH} component of the SNDU that carry key management information only once, we will suppose that these SNDU have the standard header when we calculate DO_{KM}.

We will calculate DO_{KM} using the following formula:

$$DO_{KM} = \frac{KMI}{TI} \cdot 100$$

where:

- DO_{KM} is the calculated data overhead;
- *KMI* (Key Management Information) is the number of bytes in the totality of SNDU that are sent over the satellite carrying key management information; these SNDU will be supposed to have standard header.
- *TI* (Total Information) is the number of bytes in the totality of SNDU sent over the satellite link.

$KMI = \mu(IK3)+(IK3Th-1)\cdot\mu(IK2)+ IK3Th\cdot(IK2Th-1)\cdot\mu(IK1) + IK3Th\cdot IK2Th\cdot(IK1Th-1)\mu(SK)$,

$TI = KMI' + \nu(IK3Th\cdot IK2Th\cdot IK1Th\cdot SKTh)$,

where

- $\mu(X)$ is the length of the SNDU frame, with standard ULE header, that carries key management information about key X.
- $\nu(D)$ is the total length of the SNDU that carry the data D. It is a function of the length of the PDU.
- *KMI'* is the total length of the SNDU that carry key management information, but using the extension header.

We will calculate DO_{EH} using the formula:

$$DO_{EH} = \frac{EHI}{TI} = \frac{N \cdot EH}{N \cdot l(SNDU)} \cdot 100 = \frac{EH}{l(SNDU)} \cdot 100$$

where:

- *N:* is the total number of SNDU frames.
- *EH:* is the length of the extension header, which is 6 bytes.
- *l(SNDU):* is the medium length of the SNDU frames.

B. *Analysis of the data overhead*

We have simulated the DO_{EH} and DO_{KM} for the five sets of security parameters we studied and for average packet lengths between 50 bytes and 1500 bytes. The obtained results are presented in Fig. 9:

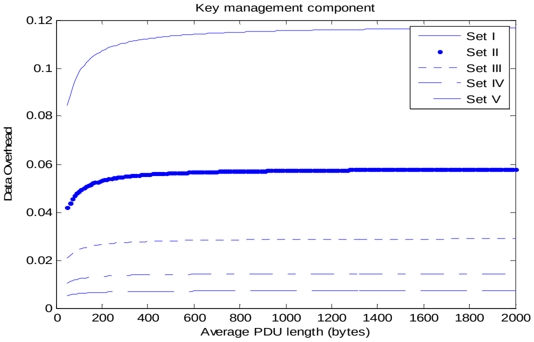


Fig. 9: Key Management component of Data Overhead.

Because of the fact that we have doubled the value of the security parameters from one set to another, the value of the DO_{KM} doubles also from one set of parameters to another. When the length of the packets increases, the number of the SNDU frames that transport the data decreases. Thus, the added information by the ULE header decreases and, together with it, *TI* decreases also. The result of a decreasing *TI* is an increasing DO_{KM} (see Figure 10).

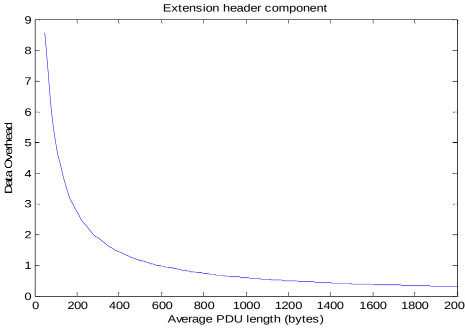
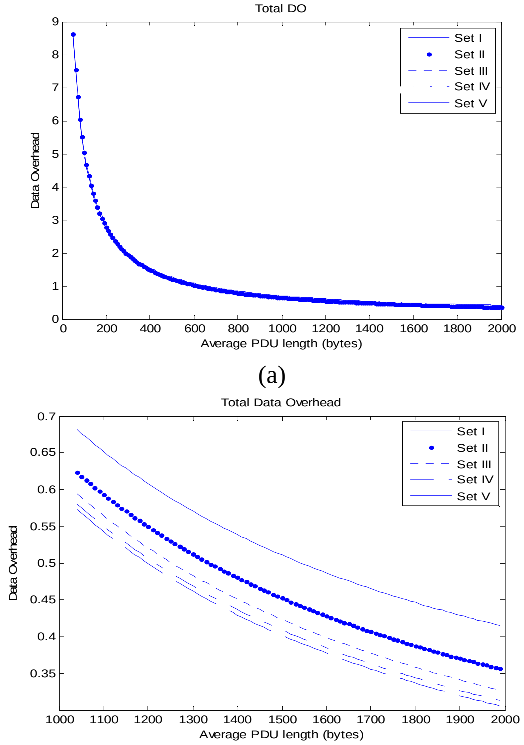


Fig. 10: Extension Header component of Data Overhead.

The DO_{EH} is not influenced by the set of security parameters that are used. It expresses the quantity of added information by the use of an extension header. Thus it is only a function of the IP packet length, because there are always added 6 bytes regardless of the length of the IP packet.

We have noticed that for small values of packet length, the value of DO_{EH} is much more important that the value of DO_{KM}. DO could be approximated with DO_{EH}. However, when the length of IP packets becomes more important, DO_{EH} and DO_{KM} have values of the same magnitude and the influence of the chosen set of parameters becomes important (see Fig. 11).



(a)

(b)

Fig. 11: Total Data Overhead (a) for packet length values between 50 and 2000 bytes; (b) for packet length values between 1000 and 2000 bytes.

The analysis of DO is very important also from the perspective of the response time. The propagation time for a round trip is around 0.5 seconds. Compared to this, the time added by the encryption, authentication and key management processing can be neglected. However, when we consider large file downloads, the time needed to send the extension header and key management information can be important and it is a given by the DO.

C. *Period of MK usage*

The period of MK usage (TMK) must be studied in order to avoid the undesired extreme values and to be able to set the frequency of MK changing, in function of the security policy that is agreed upon between the ISP and the client.

The formula of TMK is:

$$TMK = \frac{TI}{Bitrate}$$

where *Bitrate* is the channel bitrate.

The Table II shows the MK usage frequency for the analyzed sets of parameters and channel bit rate. The values are expressed in days. the values smaller than 0.25 days (6 hours) and greater than 730 days (2 years) have been ignored:

Table II - MK usage frequency.

	256 kbps	1 Mbps	5 Mbps	20 Mbps	90 Mbps
I	1,52	0,38			
II	23,68	5,92	1,18	0,29	
III	372,6	93,17	18,63	4,66	1,04
IV				144,1	32,04
V					510,9

D. Simulation results

We have used Wireshark 1.0.6 to capture the data and Matlab to simulate the transmission over satellite of both standard ULE and the proposed secure ULE in order to calculate the practical value for DO (see Figure 12).

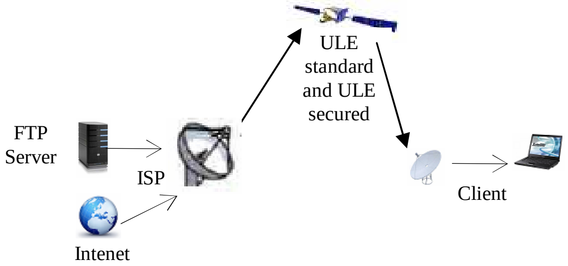


Fig. 12: Simulated network architecture.

We have simulated two communication protocols FTP and HTTP, thus covering two possible applications of the system: file transfer and Internet browsing. For the FTP communication we have used two transfer speeds: 256 kbps and 90 Mbps. We have tried to cover the entire interval of download speeds used in real systems. The results are presented in Tables III, IV and V.

Table III - Simulated extension header component of DO.

	FTP 90 Mbps	FTP 256 kbps	HTTP
Data Overhead	0.454	0.668	0.773

Table IV - Simulated key management component of DO.

	I	II	III	IV	V
FTP 90 Mbps	0.110	0.055	0.028	0.014	0.007
FTP 256 kbps	0.112	0.056	0.028	0.014	0.007
HTTP	0.114	0.057	0.028	0.014	0.007

Table V - Simulated total DO.

	I	II	III	IV	V
FTP 90 Mbps	0.562	0.507	0.479	0.465	0.458
FTP 256 kbps	0.776	0.719	0.692	0.678	0.671
HTTP	0.882	0.826	0.798	0.784	0.777

We can notice the correspondence between the theoretical data overhead and the simulated data overhead. HTTP traffic is characterized by smaller packet length and thus has the highest data overhead. The FTP download is characterized by longer packet length. The higher is the bit rate, the longer are the packets and, thus, the lower is the DO.

V. Conclusions

In this paper we have proposed a novel security enhancement for TCP/IP over DVB-S/RCS that respects the security requirements for this type of communications. It uses chaotic sequences for key generation and data encryption and the key management is based on a multilayer protocol.

We provide all the necessary information and formulas to allow an ISP to correctly choose the security parameters of a certain connection taking into account the security policy and channel characteristics.

References

[1] http://www.internetworldstats.com/stats.htm, June 2009.

[2] EN 300 468 “Digital Video Broadcasting (DVB); Specification for Data Broadcasting”

[3] G. Fairhurst, B. Collini-Nocker “Unidirectional Lightweight Encapsulation (ULE) for Transmission of IP Datagrams over an MPEG-2 Transport Stream (TS)”, IETF RFC 4326, December 2005

[4] C. N. Bernhard, F. Godred, “ULE versus MPE as an IP over DVB Encapsulation”, in *Performance modeling and evaluation of heterogeneous networks*, West Yorkshire, U.K., July 2004.

[5] C. H. The, T.C. Wan, R. Budiarto, “A comparison of IP Datagrams Transmission using MPE and ULE over MPEG/DVB Networks”

[6] Zul Hilmi Zulkifli, “Analysis of IP Encapsulation Methods over DVB Satellite”, [Online]. Available at: http://member.wide.ad.jp/draft/wide-draft-dvbrcs-hilmi-00.pdf, June 2009.

[7] H. Cruickshank, P. Pillai, M. Moisterning, S. Iyengar, “Security requirements for Unidirectional Lightweight Encapsulation (ULE) protocol”, IETF work in progress

[8] S. Iyengar, H. Cruickshank, P. Pillai, G. Fairhurst, L.Duquerroy, “Security requirements for IP over satellite DVB networks”, *Mobile and wireless Communications Summit*, 16th IST, July 2007.

[9] P. Pillai, Y-F Hu, “Design and Analysis of Secure Transmission of IP over DVB-S/RCS Satellite Systems”, *Wireless and Optical Communications Networks*, 2006.

[10] H. Cruickshank, S.Iyengar, S. Combes, L. Duqueroy, “A secure extension for the Unidirectional Lightweight Encapsulation (ULE) protocol”, IETF Internet draft, work in progress.

[11] D. Caragata S. El assad, I. Tutanescu, E. Sofron, “Secure TCP/IP Communications over DVB-S/DVB-RCS Using Chaotic Sequences”, The 4th International Conference for Internet Technology and Secured Transactions, November 2009, accepted paper.

[12] G. Bouchard, “Directives pour la mise en réseau des trames de transport”, *Revue des technologies de Radio-Canada*, Number 3, January 2007.

[13] A. Géron, *WIFI, Déploiement et* sécurité, Dunod, 2006, p. 303-340.

[14] EN 300 421, “Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for 11/12 GHz satellite services”, ETSI, 1997.

[15] EN 302 307, “Digital Video Broadcasting(DVB):Second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broadband satellite applications”, ETSI, 2005.

[16] “Digital Video Broadcasting, Return Channel via Satellite (DVB-RCS) Background Book”, Nera Broadband Satellite AS, 2002.

[17] S. El Assad, H. Noura, I. Taralova, “Design and Analyses of efficient chaotic generators for crypto-systems”, Lecture Notes in IAENG Transactions on Electrical and Electronics Engineering, vol 1, 2008, 10 pages (to appear)

[18] A. Awad, S. El Assad, D. Caragata, “A robust Cryptosystem Based Chaos for Secure Data”, in *4th International Symposium on Image/Video Communications over Fixed and Mobile Networks*, Bilbao, Spain, 2008.

[19] W. Fumy, P. Landrock, “Principles of key management”, *IEEE Journal on selected areas in communications*, vol 11, No. 5, June 1993.

[20] A. Menezes, P. van Oorshot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996, pp. 506-515.