Secure IP over Satellite DVB Using Chaotic Sequences

Daniel Caragata, Safwan El Assad, Bassem Bakhache, 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 (Digital Video Broadcasting – Satellite) 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 – **Chaotic functions, DVB, Internet Protocol, satellite, security.**

I. INTRODUCTION

One of the most impressive prophecies of the 20th century was made by Arthur C. Clarke in 1945 in an article published in *Wireless World* [25]. The scientist and fiction novel writer presented the concept of using extra terrestrial satellites that would rotate around the earth with a 24-hours orbit to provide communication services.

"An artificial satellite at the correct distance from the earth could make one revolution every 24 hours, i.e., it would remain stationary above the same spot and would be within optical range of nearly half of the earth's surface. Three repeater stations, 120 degrees apart in the correct orbit, could give television and microwave coverage to the entire planet". Although this statement made little impact at the time, it can be considered the birth of modern extra-terrestrial communication systems.

The first operational space communication system was used by the U.S. Navy. They began bouncing radio signals off the Moon in 1954 and were able to provide a link between Hawaii and Washington DC from 1959 to 1963 using the Communications by Moon Relay (CMR) system [26].

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 gained a very important place in today's communication systems and are supposed to be a very important part of the next generation Internet architecture.

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.

DVB-S [14] is an open standard ratified by European Telecommunication Standard Institute, ETSI, in 1994. It is a part of the DVB standards family along with Digital Video Broadcasting – Cable, DVB – C, Digital Video Broadcasting – Terrestrial, DVB – T, and Digital Video Broadcasting – Handled, DVB-H. 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 Digital Video Broadcasting, Return Channel via Satellite, DVB-RCS, 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.

In recent years, the study of chaos has attracted great interest in many fields of scientific research. One of the fields where the theory of chaos finds practical implementation is the field of telecommunications. Thus, properties such as high sensitivity to initial conditions and non-periodic deterministic behaviour of chaotic maps can be harvested in order to realise chaos based crypto-systems or new communication systems, to name just a few.

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 a simplified version of the security system we propose, one that does not use the extension header. The

Manuscript received January 14, 2010.

D. Caragata and S. El Assad are with IREENA, Ecole Polytechnique de l'Université de Nantes, rue Christian Pauc, BP 50609, 44306, Nantes, France (e-mail {daniel.caragata,_ safwan.elassad}@univ-nantes.fr, tel: + 33 6 76 32 28 36, fax : + 33 2 40 68 32 32).

B. Bakhache is with the Electronics and Communications Department of the Faculty of Engineering – Lebanese University, Beirut, Liban. (bakhache@hotmail.com).

I. Tutanescu and D. Caragata are with Electronics, Communications and Computers Faculty of University of Pitesti, str. Targu din Vale, nr. 1, 110040, Pitesti, Romania. (ion.tutanescu@upit.ro).

advantages and drawbacks of this approach are studied. In section VI 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 Figure 1. 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.

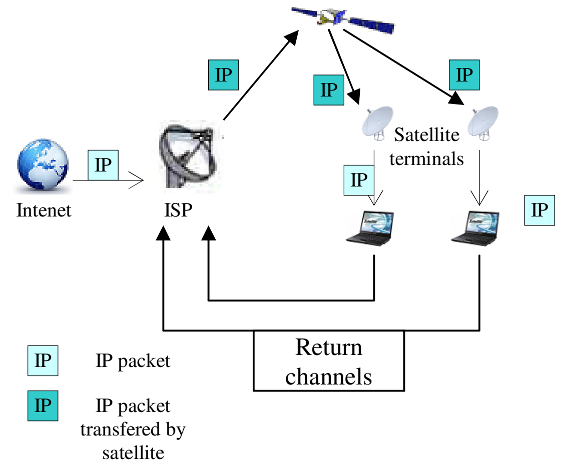


Fig. 1: Satellite IP communication.

A MPEG-2 Transport Stream, MPEG-2 TS, is created by multiplexing several MPEG-2 Elementary Streams, MPEG-2 ES, and it consists 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.

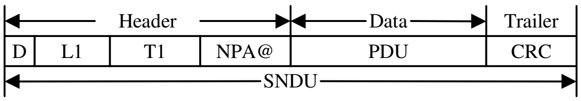


Fig. 2: Standard ULE encapsulation.

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.

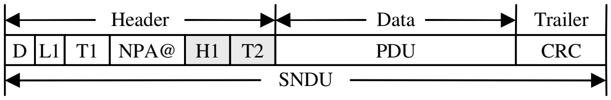


Fig. 3: ULE extension header.

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. Transmitter and receiver base station

A typical architecture of a transmission base station that allows the transmission of IP datagrams through DVB-S, also named provider or ISP, should comprise a router with access to Internet, an IP encapsulator, a MPEG 2 multiplexer, a modulator and a satellite antenna as shown in Figure 4.

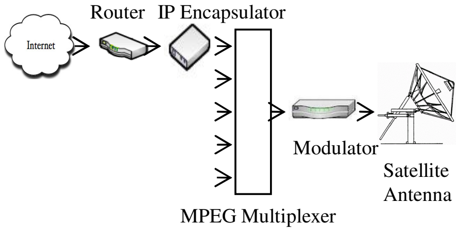


Fig. 4: Transmission base station or provider.

The receiver base station, Figure 5, contains a satellite antenna, a demodulator, a MPEG 2 demultiplexer, an IP

Packet Recovery Unit, IPPRU, a router and the final user which may be a computer or a Local Area Network, LAN, if the router uses Network Address Translation, NAT.

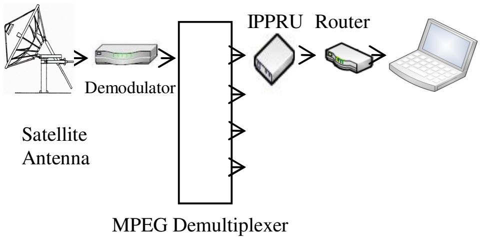


Fig. 5: Receiver base station, or user.

D. *The return channel*

Opposed to TV broadcasting, TCP/IP communications need a return channel in order to work properly. A key characteristic of most TCP/IP communications is the high asymmetry between the forward and the return channel. This is not the case for all TCP/IP applications, the exceptions are e-mails, chat or heavy AJAX based pages. However, it is common practice for systems that provide Internet access via satellite to use different channels for forward and reverse communications. There is no special condition for the reverse channel. Depending on users' requirements, it may be Dial Up ISDN, GPRS, other satellite data systems, etc.

E. *Security requirements*

IP over satellite DVB is a wireless communication protocol and thus susceptible to several attacks [7], [8]. The existing threats can be devised in two categories: passive and active. Passive attacks are considered the major threats for our communication system. Examples of passive threats are: the attacker is monitoring the transmission to extract the traffic between the IP endpoints, the attacker is monitoring the traffic to obtain information about the communicating parties. This information may be the amount of traffic, the time the parties are active, different statistics about the traffic associated with a certain NPA/MAC address. Due to the ease of interception this threat is of particular interest for DVB broadcasting networks.

Active attacks require that the intruder injects his own messages into the bitstream or modifies the bitstream. Examples of active attacks are:

- *Masquerading*: when the attacker pretends to have a different identity.
- *Repudiation*: when the originator of a message denies having sent that message or when the receiver denies having received the message.
- *Replay attacks*: when the attacker sends multiple copies of an authentic message.
- *Denial of service*: when the attacker prevents an entity from performing its proper function.

Active threats are considered major threats for the Internet community where masquerading or modification of IP packets are relatively easy to perform. This motivates the mandatory use of sequence number in IPSec. However, active attacks are much more difficult to perform in a MPEG-2 broadcasting environment.

Based on the topology of the systems using IP over DVB, the security threats have been divided into three categories:

- *Monitoring*: in this case the attacker monitors the ULE broadcast to gain information about the ULE data, about the communicating parties or even access the transmitted information. For this case, measures must be taken to protect the ULE payload and the identities of the communicating parties.
- *Locally conducting active attacks on the MPEG*-TS *multiplex*: in this case, the attacker is presumed to modify the original transmission of the ISP and provide his own version of the transmission to an isolated ULE receiver or a small group of receivers (e.g. a company site). The ISP may not be aware of these attacks. The measures that must be taken to prevent this kind of attack are data authenticity and data integrity as well as the prevention of old message replay.
- *Globally conducting active attacks on the MPEG*-TS *multiplex*: in this case the attacker is presumed sophisticated enough to override the entire MPEG-TS transmission multiplex. The provider is normally aware of this attack and the measures that must be taken are similar to the case of the local active attack.

The active attacks described above can be divided into two classes:

- *Insider attacks*: the attacks are performed by adversaries from the network and that have access to the secret materiel.
- *Outsider attacks*: the attacks are performed by adversaries without access to the secret materiel.

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.

Other general requirements are:

- ULE key management functions must be decoupled from ULE security services such as encryption or authentication.
- Algorithm agility must be supported in order to allow upgrading the encryption and authentication algorithm if they become obsolete
- The security extension header must be compatible with other ULE extension headers.

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 [33].

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. A 32 bit extension header, called Packet Number, PN, is used. This field provides protection against replay attacks and is used as a nonce in the key deriving process.

We propose that the CRC trailer of the SNDU be replaced by a Message Authentication Code, MAC. This will provide data integrity and data authenticity.

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 in order to have improved 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 6: *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.

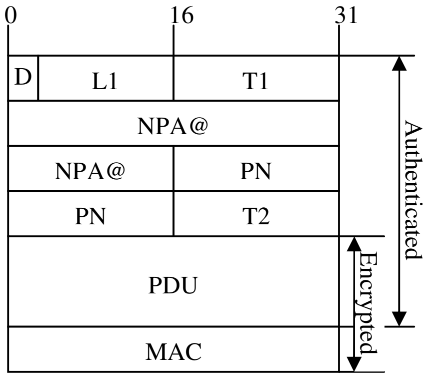


Fig. 6: SNDU secured.

C. Proposed key management system

We propose a key management system that takes into consideration the security requirements for IP over satellite DVB, stressed out in [7] and [8], as well as the characteristics of IP satellite communications in order to provide an efficient implementation.

The system for which we propose the security enhancement is characterized by a high asymmetry in bandwidth between the forward and the return paths. However both paths must be used to have proper Internet browsing and key management. Our proposed security enhancement takes these considerations into account and uses the return path only to allow users to send alarm messages if they have lost the key management information.

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

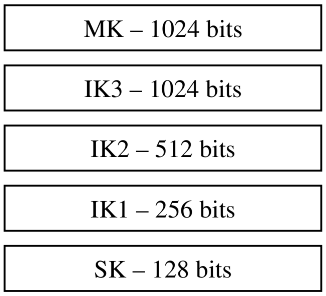


Fig. 7: Multilayer key management system.

The Master Key, MK, 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 can only be changed using other means of communication, not the satellite link.

The number of 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, they can be chosen at the initialization stage. Once fixed, they cannot be modified. We propose and analyze a system that has 3 intermediate keys: Intermediary Key 1, IK1, with a length of 256 bits, Intermediary Key 2, IK2, with a length of 512 bits and Intermediary Key 3, IK3, with a length of 1024 bits:

All data is encrypted and authenticated using an Ephemeral Key, EK. This key is derived from the Session Key, SK, the NPA address and the Packet Number, PN.

The requirements for the two keys, SK and MK, are very different. SK must be changed as frequently as possible, while MK should be changed only in case of compromise or periodically at long time intervals. The SK should have a length that would balance good security and cost of processing. We recommend a length of 128 bits. On the other hand, MK should have a much longer length because the security of the whole system depends on it. We recommend a length of at least 1024 bits.

The SK will be used for a limited amount of data. In order to decide whether the SK will be changed or not, the provider will count the total number of bytes encrypted and authenticated with the current SK. When the counter reaches a certain threshold, Session Key Threshold, SKTh, a new SK will be generated by the ISP and will be sent encrypted using IK1 to the terminal.

The 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. The values of SKTh, IK1Th, IK2Th, and IK3Th are the parameters of the key management protocol.

D. Proposed key generator

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

The proposed chaotic generator [17], [21] for the generation of the keys consists of two parallel generators as seen in Figure 8. Each one is looked at as a non linear recursive filter (non linear IIR Filter). Different non-linear functions FNL(x) were tested: *Skew Tent map, xLnx, x×exp[cos(x)]*, *pwlcm*, etc.

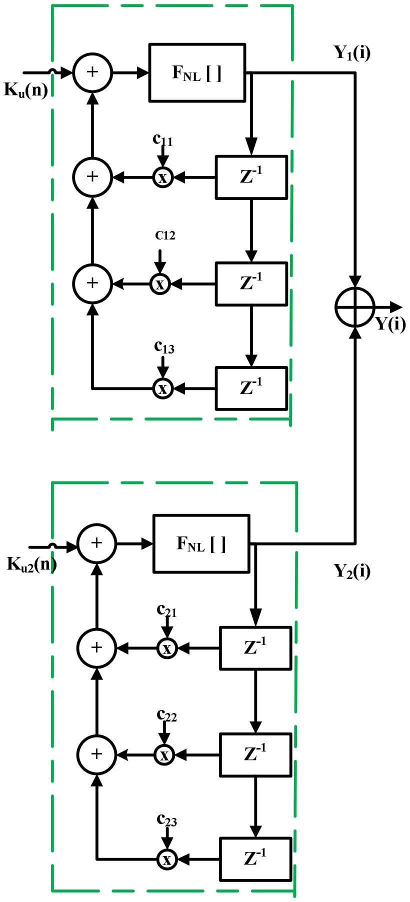


Fig. 8: Proposed chaotic generator.

All coefficients c_{11}, c_{12}, c_{13}, c_{21}, c_{22}, and c_{23} can take values ranging from 1 to $2^N - 1$, where N is the number of bits used to represent the value of the coefficients. The general equation for this generator is defined by the following equations:

$$Y_1(n) = FNL(k_{u1}(n) + \sum_{i=1}^{3}[c_{1i} \times Y_1(n-i)] \qquad (1)$$

$$Y_2(n) = FNL(k_{u2}(n) + \sum_{i=1}^{3}[c_{2i} \times Y_2(n-1)] \qquad (2)$$

$$Y(n) = Y_1(n) \oplus Y_2(n) \qquad (3)$$

Our experiments have shown that the best properties, in terms of cryptographic characteristics and ease of implementation, are obtained when the Skew Tent map is used. The Skew Tent map is a non linear ergodic function and it has uniform invariant density function in its definition interval. The Skew Tent map is composed of two linear segments and is given by:

$$y(n) = F[y(n-1)] =$$
$$= \begin{cases} \dfrac{y(n-1)}{p} \; if \; 0 \le y(n-1) < p \\ \dfrac{1-y(n-1)}{1-p} \; if \; p \le y(n-1) < 0.5 \end{cases} \qquad (4)$$

We have quantized the chaotic map in order to make it run over the integer set, as follows:

$$Y(n) = F[Y(n-1)] =$$
$$= \begin{cases} \left\lfloor 2^N \times \dfrac{Y(n-1)}{P} \right\rfloor if \; 0 \le Y(n-1) < P \\ \left\lfloor 2^N \times \dfrac{2^N - Y(n-1)}{2^N - P} \right\rfloor if \; P \le Y(n-1) < 2^N \end{cases} \qquad (5)$$

Where $\lfloor Y \rfloor$ denotes the biggest integer, not bigger than *Y*, *Y(n)* is the discrete state ranging from 0 to $2^N - 1$ and P is the discrete control parameter with $0 < P < 2^{N-1}$.

In order to quantify the performances of the proposed generator we have realized some simulations which we present in Figures 9, 10 and 11. The mapping, of the proposed generator, shown in figure 9, indicates clearly that the generated sequences are random. Also, we found that the auto and cross correlation functions in figure 10 are noise-like. Moreover, for each test (among 188 NIST tests) we compute the proportion of sequences that pass. The obtained result, given in figure 11, indicates that the produced chaotic sequences exhibit randomness properties.

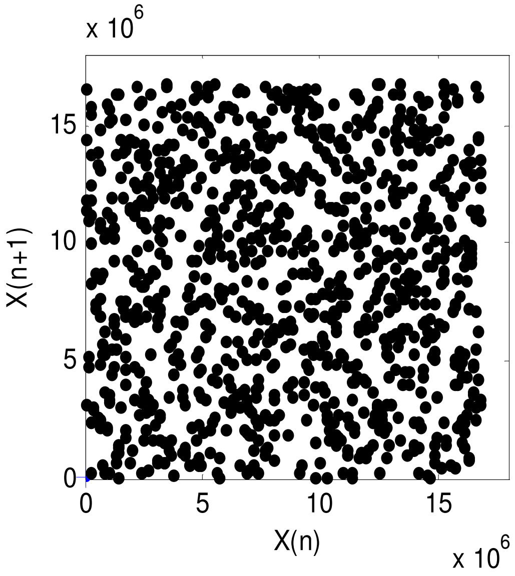


Fig. 9: Mapping result.

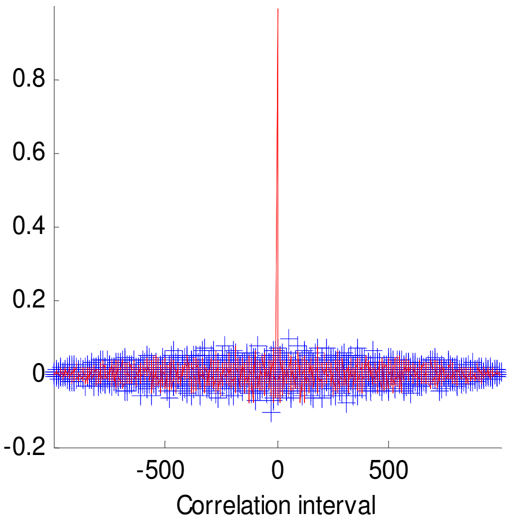


Fig. 10: Auto and cross correlation functions.

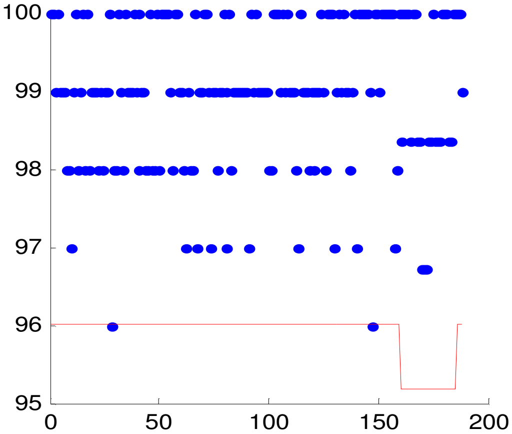


Fig. 11: Proportion value of NIST Test.

E. Proposed encryption algorithm

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 be the CCMSTI algorithm from [18], [22]. The other 3 algorithms should be public algorithms that are considered robust encryption algorithms, e.g. AES (Advanced Encryption Standard) [23].

The CCMSTI, Figure 12, was originally designed for image encryption, but can be easily modified to encrypt the PDU flow. It is a block cipher, it breaks up the plaintext messages to be transmitted/received into blocks of fixed length and encrypts/decrypts one block at a time. The algorithm uses a key length of 128 bits and a perturbed Piecewise Linear Chaotic Map, PWLCM, for its improved statistical properties. It also uses pseudo-random permutation generator, *P*-box, and complex substitution box, *S*-box, in order to add diffusion to the system. The algorithm performs *r* rounds of the *SP*-network on each block of data.

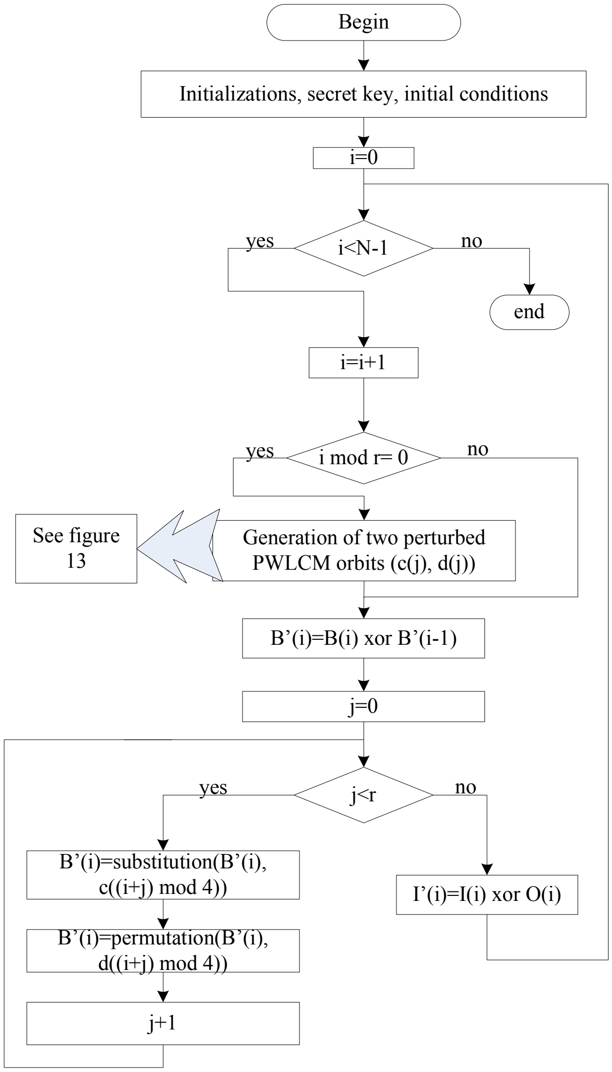

Begin
Initializations, secret key, initial conditions
i=0
yes
i<N-1
no
end
i=i+1
yes
i mod r= 0
no
See figure 13
Generation of two perturbed PWLCM orbits (c(j), d(j))
B'(i)=B(i) xor B'(i-1)
j=0
yes
j<r
no
B'(i)=substitution(B'(i), c((i+j) mod 4))
B'(i)=permutation(B'(i), d((i+j) mod 4))
j+1
I'(i)=I(i) xor O(i)

Fig. 12: The encryption algorithm.

The perturbation of the PWLCM orbit is depicted in Figure 13. Once every δ iterations of the PWLCM, a pseudo random numbers generator, LFSR, is iterated and the obtained value, *l*, is used to perturb the chaotic orbit.

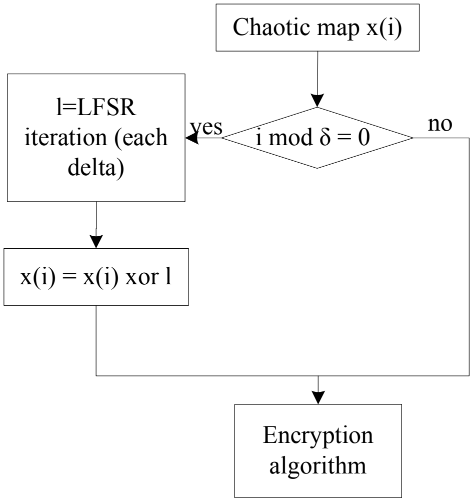


Fig. 13: The generation of the perturbed PWLCM orbits.

The decryption algorithm differs slightly from the encryption one. To decrypt the encrypted data the sequence of inverse transformations must be performed.

F. Ephemeral key derivation

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 hash function, as shown in Figure 13. Using PN as a nonce guarantees that a new key is obtained for each packet. This approach is similar to the security solution in Wi-Fi, Wireless Protected Access WPA protocol that uses Temporal Key Integrity Protocol, TKIP [14].

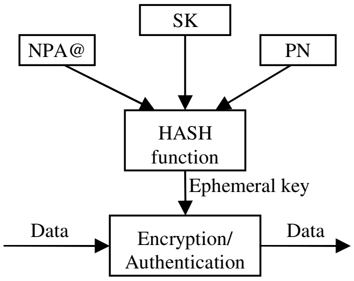


Fig. 14: Key derivation system.

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.

G. Security PDU

A new type of PDU, the Security PDU, SPDU, is needed so that the system is able to provide a way to transport the new secret keys and to choose the algorithms that will be used for encryption, authentication and key deriving. The structure of the SPDU will be similar 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 15.

KL	HF	EA	AA	Key ID	$IKX_{IK(X+1)}$	…	SK_{IK1}
← Header →					← Payload →		

Fig. 15: 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.

H. The IP Encapsulator structure

The encryption and key management functions are realized by the IP Encapsulator block at the provider, while the decryption is realized by the IPPRU block at the user. A standard IP encapsulator can be represented as in Figure 16.

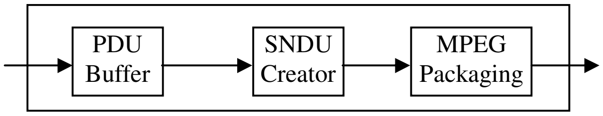


Fig. 16: Standard IP encapsulator.

The *PDU Buffer* is a block that memorizes the PDUs that wait to be encapsulated and transmitted.

The *SNDU Creator* adds the ULE header and trailer to the PDU, hence creating the SNDU that is ready to be packed into MPEG-TS frames and to be transmitted. It calculates the length of the SNDU, the type of the PDU, the destination address, if needed, and the CRC code.

The *MPEG Packing* block creates the MPEG-TS packets that will carry the SNDU to the destination. The *SNDU Creator* and *MPEG Packaging* must respect the standard [3].

The structure of the *IP Encapsulator* must be upgraded in order to support the presented ULE security enhancement. The structure of the *Secure IP Encapsulator* is presented in the Figure 17.

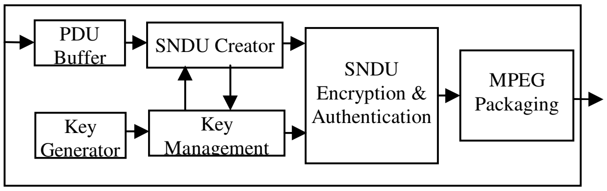


Fig. 17: Secure IP encapsulator

The *PDU Buffer* and *MPEG Packaging* blocks remain unchanged.

The *Key Management* block becomes the core of the Secure IP Encapsulator. It commands the *Key generator* block, it works with the *SNDU Creator* block to help create the SPDUs and to receive PN nonce and it provides the *Ephemeral key* to the *SNDU Encryption & Authentication* block

The *SNDU Encryption & Authentication* block performs the authentication of the SNDU header and PDU and the encryption of the PDU packet and of the MAC trailer. It receives the secret keys and the encryption and authentication algorithms from the *Key Management* block.

I. 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. The key synchronization between the client and the ISP will be restored after the client sends the ISP an alarm message. We will not discuss the exact structure of the alarm message because it must take into account 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 a very 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, key lengths and security parameters) must be done taking into account the characteristics of the system. One of these characteristics 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 analyzed 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 overhead

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:

$$DO = \frac{AI}{TI} \times 100 \qquad (6)$$

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.

$$DO = DO_{KM} + DO_{EH} = \frac{KMI + EHI}{TI} \cdot 100 \qquad (7)$$

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 total number of bytes that are 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 $\mathrm{DO_{KM}}$ using the following formula:

$$DO_{KM} = \frac{KMI}{TI} \cdot 100 \qquad (8)$$

where:

- DO_{KM} is the calculated data overhead.
- *KMI* – Key Management Information is the number of bytes that are sent over the satellite carrying key management information. We will suppose that the ULE standard header is used in this case.
- *TI* – Total Information is the number of bytes sent over the satellite link.

$$\begin{aligned} &KMI = \mu(IK3) + (IK3Th - 1) \times \mu(IK2) + \\ &IK3Th \times (IK2Th - 1) \times \mu(IK1) + \\ &IK3Th \times IK2Th \times (IK1Th - 1) \times \mu(SK) \end{aligned} \qquad (9)$$

$$TI = KMI' + \nu(IK3Th \times IK2Th \times IK1Th \times SKTh) \qquad (10)$$

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 key management data D.
- *KMI'* is the total length of the SNDU that carry key management information using the extension header.

We will calculate $\mathrm{DO_{EH}}$ using the formula:

$$DO_{EH} = \frac{EHI}{TI} = \frac{N \cdot EH}{N \cdot l(SNDU)} \cdot 100 = \frac{EH}{l(SNDU)} \cdot 100 \qquad (11)$$

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 $\mathrm{DO_{EH}}$ and $\mathrm{DO_{KM}}$ 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 Figures 18, 19 and 20:

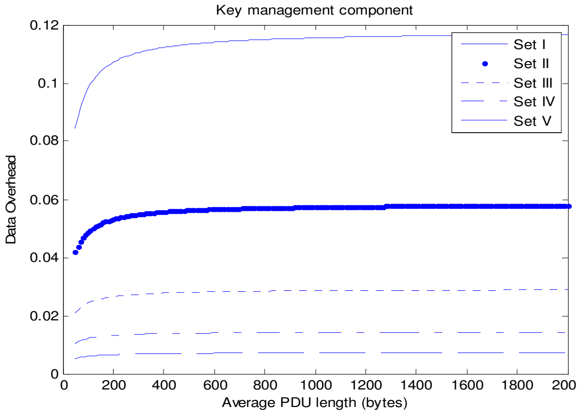


Fig. 18: Key Management component of Data Overhead.

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} also doubles 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 18).

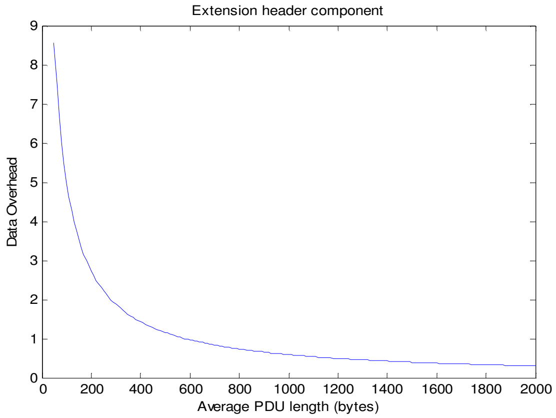
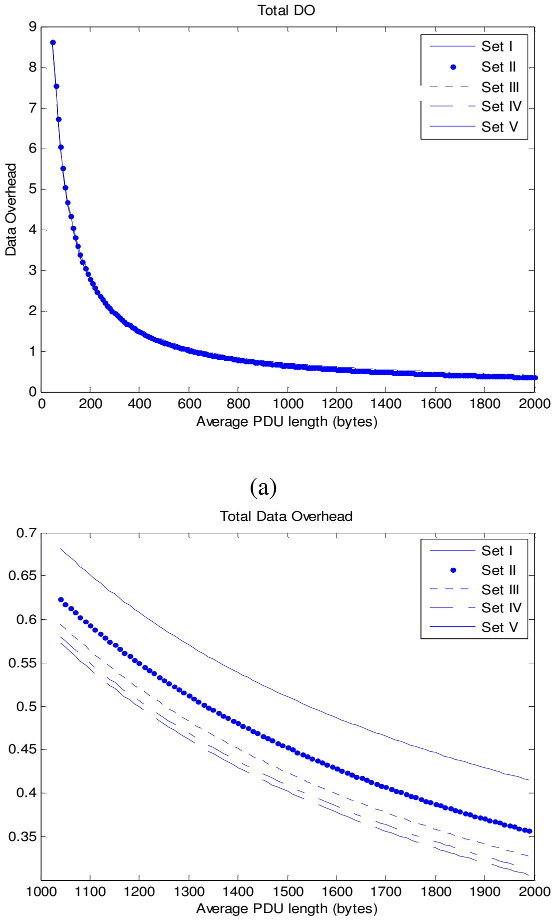


Fig. 19: Extension Header component of Data Overhead.

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 a fixed number of bytes, 6, is added to the frame regardless of the length of the IP packet. Figure 19 represents the DO_{EH}.

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 Figure 20a, b).



(b)

Fig. 20: 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 study of the period of MK usage, TMK, is important because it provides a tool that will allow the ISP to choose the correct security parameters. This means that the security parameters will ensure that the security policy is respected with optimal cost.

The formula of TMK is:

$$TMK = \frac{TI}{Bitrate} \qquad (12)$$

where *Bitrate* is the channel bitrate.

Table II shows the MK usage frequency for the analyzed sets of parameters and channel bit rates. 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 calculated the practical value of DO using Wireshark 1.0.6. We have captured real IP traffic and we have used Matlab to simulate its transmission over satellite using both standard ULE and the proposed secure ULE (see Figure 21).

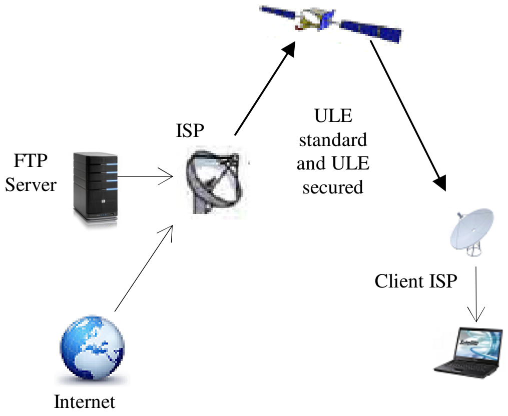


Fig. 21: Simulated network architecture.

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. SIMPLIFIED SYSTEM

The security system we have proposed offers confidentiality, authenticity and data integrity. This is almost a complete package of security services as we could not influence the availability of the communications. However, the security requirements for ULE communications over satellite clearly demonstrate that confidentiality is more important than the other security services, see Section *II.E.* It is very expensive for an attacker to modify the data that is carried by the satellite or to inject its own data.

This is why we also propose a simplified version of the security enhancement, one that does not use the ULE extension header. The main drawback of this system is that the SK will be used as the encryption key. Without the PN field of the extension header it is impossible to derive a fresh EK for each PDU being secured.

Data authenticity and data integrity could be provided by this security system also if the CRC trailer of the SNDU were replaced by a MAC code. This decision is up to the provider for a given implementation or up to the standardization body (IETF) for a standard modification.

A. Theoretical analysis

For the simplified version of the security enhancement we will calculate the data overhead using the following formula:

$$DO = \frac{KeyManagementTS}{TotalTSSent} * 100 \qquad (13)$$

where:

- DO is the calculated data overhead;
- *KeyManagementTS* is the number of MPEG TS frames carrying key management information;
- *TotalTSSent* is the total number of MPEG TS frames sent.

KeyManagementTS = μ(L2K) + L2KTh*μ(L3KTh) + (L2KTh + 1)*L3KTh*μ(L4K) + (L2KTh + 1)(L3KTh + 1)*L4KTh*μ(SK),

TotalTSSent = *KeyManagementTS* + ν((L2KTh + 1)(L3KTh + 1)(L4KTh +1)*SKTh),

where:

- μ(*X*) is the number of MPEG TS frames needed to carry the key management information about key *X*.
- ν(*D*) is the number of MPEG TS frames needed to carry the useful information *D*.

In the relation above, we have supposed that a new TS frame will be sent for each security message and that that TS frame will contain only that security message. In practice, because of the small size of most security SNDU they will be sent in a TS containing also data SNDU, thus the practical data overhead will be smaller that the theoretical data overhead we have calculated.

The obtained overhead for each set of parameters is represented in Table VI:

Table VI - Theoretical DO for the simplified system

I	II	III	IV	V
0.5584%	0.28%	0.1402%	0.0701%	0.035%

The frequency of MK usage is calculated as a function of the security parameters and the bit rate of the communication:

$$FMK = \frac{DataMaxMK}{Bitrate} \tag{14}$$

where:

- *FMK* is the calculated MK usage frequency.
- *DataMaxMK* is the maximum amount of data that can be encrypted without using the MK.
- *Bitrate* is the channel bit rate.

We want to use the MK as rarely as possible.

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

Table VII - Theoretical FMK for the simplified system

	256 kbps	1 Mbps	5 Mbps	20 Mbps	90 Mbps
I	1,54	0,39			
II	23,92	5,98	1,2	0,3	
III	376,4	94,12	18,82	4,71	1,05
IV				145,6	32,37
V					516,1

B. Simulation results

We have used the same simulation methodology as the one described in Section *IV.D* and depicted in Figure 21. We have studied two types of MPEG transmission: with padding and with packing. MPEG transports variable length SNDU packets using fixed length packets. It is normal that at most times the MPEG frame carrying the last part of the SNDU is not completely used: there are a number of bytes that are free. If these bytes are set to 1 and the packet sent like this, then padding is used. If these bytes carry the begging of next SNDU frame, then packing is used.

We have analyzed 4.4 Gb of Internet HTTP traffic which was sent using 2.688.800 MPEG2 TS frames with packing and 3.202.481 frames with padding. The ULE data overhead was 15.02% when padding was used and 3.09% when packing was used. We have obtained the following results when we have simulated each of the five proposed sets of parameters:

Table VIII – Simulated DO for Internet browsing

	I	II	III	IV	V
Security PDU size	3.19 Mb	1.99 Mb	0.56 Mb	0.35 Mb	0.25 Mb
Satellite Overhead for ULE with padding	0.38%	0.24%	0.069%	0.044%	0.030%
Satellite Overhead for ULE with packing	0.071%	0.044%	0.012%	0.0079%	0.0055%

We have also analyzed an FTP client-server communication for two different bit rates: 256 kbps and 90 Mbps. The total amount of data transferred was 5.8 Gb for the 90 Mbps connection and 4.6 Gb for the 96 kbps connection. The 90 Mbps connection was transferred using 3.685.902 TS frames and a data overhead of 11.42% with padding and 3.335.487 TS frames and a data overhead of 2.72% with packing, while the 256 kbps connection used 4.685.244 TS frames and data overhead of 12.25% with padding and 4.246.833 TS frames and a data overhead of 3.04% with packing.

The satellite data overhead for the two systems using the analyzed sets of parameters are depicted in Table IX and Table X:

Table IX – Simulated DO for 90 Mbps FTP

	I	II	III	IV	V
Security PDU size	4.23 Mb	2.64 Mb	0.74 Mb	0.47 Mb	0.33 Mb
Satellite Overhead for ULE with padding	0.4%	0.25%	0.071%	0.045%	0.031%
Satellite Overhead for ULE with packing	0.070%	0.045%	0.012%	0.008%	0.0055%

Table X – Simulated DO for 256 kbps FTP

	I	II	III	IV	V
Security PDU size	3.35 Mb	2.08 Mb	0.58 Mb	0.37 Mb	0.26 Mb
Satellite Overhead for ULE with padding	0.4%	0.25%	0.071%	0.045%	0.031%
Satellite Overhead for ULE with packing	0.071%	0.044%	0.012%	0.008%	0.0055%

It can be noticed that the practical overhead for simulated traffic is smaller than the theoretical overhead. This can be easily explained by the fact that when we have calculated the number of necessary TS frames needed to transport the useful data we have supposed that all TS frames will be full, because this is the worst case scenario. When we have simulated the transport of real PDU over satellite, we have calculated the number of necessary TS frames for each individual PDU, thus increasing the *TotalTSSent*. Also, when packing is used, most of the security PDU are included in TS frames containing also traffic PDU, hence there is no need for new TS frames.

The theoretical analysis and simulation results have shown that the simplified version of the security enhancement comes with a cheaper cost than the complete version. It is up to the provider to decide whether the cost of DO is justified or not depending on the security policy that needs to be implemented.

VI. 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.

The complete security system offers data confidentiality, which is the main security objective for TCP/IP over DVB-S, data integrity, data authenticity, link layer terminal authentication and protection against replay attacks. For improved security a fresh key is generated for every packet that is encrypted or authenticated. The cost of using this system in terms of data overhead is small and has been attentively studied.

We have also proposed a simplified security system that offers data confidentiality and can offer data authenticity or data integrity, but that offers limited protection against replay attacks. This version of the system comes at a lower cost and it is up to the provider to choose what system best suites a particular connection.

We have also provided 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, the reference site for Internet usage statistics, June 2009.

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

[3] G. Fairhurst and 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 and 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 and 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 and S. Iyengar, “Security requirements for Unidirectional Lightweight Encapsulation (ULE) protocol”, IETF work in progress

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

[9] P. Pillai and 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 and 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 and 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.

[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 and 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 and 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 and 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 and S. Vanstone, *Handbook of Applied Cryptography,* CRC Press, 1996, pp. 506-515.

[21] H. Noura, “PhD Thesys, work in progress”, 2009.

[22] A. Awad, S. El Assad, D. Caragata and H. Noura. Rapport RNRT, projet ACSCOM "Etude comparative de deux algorithmes de chiffrement/déchiffrement chaotique vis-à-vis de la cryptanalyse et des erreurs" , Juin 2008, 31 pages.

[23] National Institute of Standards and Technology – “Anouncing the Advanced Encryption Standard”, FIPS-197, November 2001.

[24] H. Cruickshank, M.P. Howarth, S. Iyengar and Z. Sun, “A comparison between satellite DVB Conditional Access and secure IP multicast”, 14th IST Mobile and Wireless Communications Summit, Dresden, Germany, June, 2005.

[25] A. C. Clarke, “Extra-Terrestrial Relays”, *Wireless World*, 1945.

[26] D. K. Van Keuren, “Moon in their eyes: Moon communication Relay at the Naval Research Laboratory, 1951-1961”, *Beyond the Ionosphere: Fifty years of satellite communication*, Washington DC: NASA: pp. 9-18. NASA Pub. SP-4217.

[27] A. Rukhin, “A statistical test suite for random and pseudorandom Number Generators for Cryptographic Applications”, *NIST Special publication 800-22*, 2001

[28] DVB project homepage: www.dvb.org. Access date December 2009.

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

[30] S, Kent and K. Seo, “Security architecture for Internet Protocol”, IETF RFC 2401, December 2005.

[31] C. Kaufman, “Internet Key Exchange (IKEv2) Protocol”, IETF RFC 4306, December 2005.

[32] S. Bellovin, “Problem Area for IP Security Protocols”, *Computer communications review* 2:19, pp 32-48, april 1989.

[33] D. Caragata, B. Bakhache, S. El Assad and I. Tutanescu, “Security Enhancement for Internet Communications over Satellite DVB using Chaos”, *Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2009,* WCECS 2009, 20-22 October, 2009, San Francisco, USA pp. 419-424.