Securing multicast in DVB-RCS satellite systems

H. Cruickshank[1], M.P. Howarth[1], S.Iyengar[1], Z. Sun[1], and L. Claverotte[2]

[1] Centre for Communication Systems Research, University of Surrey, Guildford, UK
[2] Alcatel Space, Toulouse, France

Abstract – Whilst TV broadcasting is probably the best-known application of satellite technology, satellite service providers are now expanding their services to include Internet data transmission. Consequently, security of satellite data is becoming an important issue. This article examines the current DVB-RCS security standard and identifies the principal gaps in the provision of secure multicast over DVB-RCS. The main contribution of this article is a proposal for adapting the current DVB-RCS two-way satellite standard to provide secure multicast services over satellites.

Index terms – Security, satellite, key exchange, multicast, DVB-RCS.

I. INTRODUCTION

There probably exists no other application of satellite technology that is as well known as satellite broadcasting. The mere existence of satellite dishes is a constant reminder that there are systems in orbit that are used for television and radio transmission. However, the service providers of these satellite systems are now looking to expand their services to include data and interactivity. These new broadcasting and data applications, such as pay-per-view, home shopping, electronic commerce, and online and data delivery services, require a return path from the user to the central broadcast or information server. Some applications require only a low data rate return path and limited sophistication, and typically a phone line can be used in this case. However, future applications, more oriented towards multimedia and two-way communications, will require higher and more flexible data rates.

The advent of Ka-band satellites has made possible small, low cost user terminals and has thus spurred on the expansion of multimedia satellite networks. The range of users now includes small and medium-sized businesses and residential users. One promising type of satellite system that uses these terminals is called Digital Video Broadcasting (DVB) Return Channel System (DVB-RCS) [1], and was standardised by ETSI [2] in early 2000. This two-way satellite system consists of a gateway station (or hub), one or more satellites in the forward direction, a user terminal called a Return Channel Satellite Terminal (RCST), and a satellite for return traffic (as shown in Figure 1). A Network Control Centre (NCC) is responsible for monitoring and control. The satellite systems used for DVB may either be transparent (containing no on-board switching or routing) or use on-board processing (OBP). Transparent satellites support limited services since traffic can only be directly passed between the hub and the RCSTs; OBP satellites on the other hand contain on-board switching that allows traffic to flow from one RCST to another without passing via the ground hub. However, the issues and their proposed solutions discussed in this article are applicable both to transparent and OBP satellite systems.

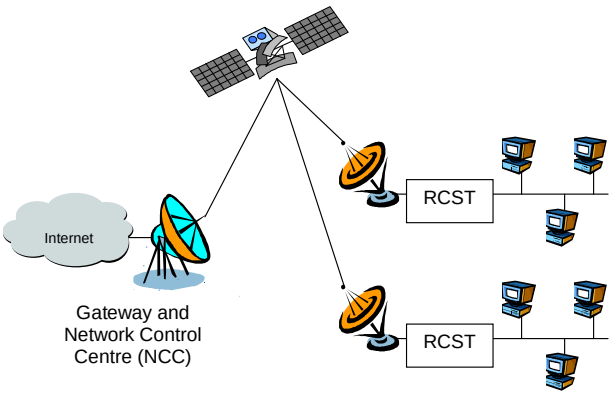

Figure 1: DVB-RCS architecture (single satellite)

One type of data transmission for which a large satellite demand is foreseen is IP multicast [3], [4]. This allows a source to send data simultaneously to multiple clients whilst transmitting only a single copy to the network. The network then replicates packets as necessary and forwards them to all recipients. Multicasting

originated as an audio/visual streaming service, but has recently started to experience broader interest and deployment [3]. Its applications include high-speed distribution of large scientific data sets, content distribution, and file push. There are two major components in multicast: group management using a protocol such as Internet Group Management Protocol (IGMP) [5], and multicast routing protocols. These two network layer (IP) components can be configured in a variety of ways over satellite systems.

A key issue for the future success of multicast over DVB-RCS systems is ensuring that it can be implemented securely, for example to prevent eavesdropping. There is currently no provision in the DVB-RCS specification for securing multicast traffic, and it is the objective of this article to propose mechanisms that enable this.

Security in DVB-RCS is implemented at the data link layer, and consequently from a security perspective the satellite DVB link can be considered transparent to multicast's network layer group management and routing protocols. These IP multicast components are therefore not discussed further in this article; instead, our focus is on securing data transmission, and for this we consider authentication and privacy. This article also does not consider security of OBP satellite signalling traffic, such as bandwidth allocation or satellite configuration messages, since this is usually implemented using proprietary mechanisms.

An alternative security mechanism, IPSEC, implemented at the network layer, can be used to secure multicast services over DVB satellite networks. Whilst IPSEC is widely implemented in IP routers and hosts on the terrestrial Internet, there are significant overheads in using IPSEC directly to protect satellite links. A major advantage for the data link layer security approach of DVB-RCS is its protection of the complete IP packet including IP addresses and user identity hiding [6]. The approach we adopt in this article is to use DVB-RCS security to provide basic privacy over the satellite link; IPSEC can then optionally be used to provide additional end-to-end security between end hosts, independent of the satellite security afforded by DVB-RCS.

In this article, we focus on the two-way security procedures in DVB-RCS, and propose modifications to enable it to support secure multicast services over satellites. In the next Section we provide an overview of the current DVB-RCS security procedure. This is followed by a Section that presents our proposed modifications to the DVB-RCS security system to enable it to support multicast services efficiently.

II. THE CURRENT DVB-RCS SECURITY SYSTEM

The DVB-RCS specification [1] defines the return (or "interaction") channel for communication between a Return Channel Satellite Terminal (RCST) and a Gateway/hub ground station. The term RCST simply refers to a satellite terminal, the term gateway refer to a large ground station that is connected to other networks such as the Internet, and the hub is the entity that is responsible for multiplexing data destined to multiple RCSTs onto the satellite broadcast channels. The gateway and hub station are typically co-located in satellite systems. The satellite network is monitored and controlled by the NCC. Signalling is transmitted between the NCC and the RCSTs over the forward link [1]and the return link.

The DVB-RCS security specification currently supports the authentication of each RCST to the NCC, and the encryption of both forward and return link traffic, and these functions are described in the following sub-sections.

A. DVB-RCS Authentication

Each RCST holds a shared secret key, called a cookie, known only to the given RCST and the NCC. This cookie is used during key exchanges [1], [7] as will now be described.

A logon is initiated by a RCST, for example when the first user of the RCST wishes to use the satellite link for data transfer. This is followed by an initial handshake between the NCC and the RCST to agree the security profile (i.e. the cryptographic algorithms and key sizes to be used): this is performed by the Security Sign-On and Security Sign-On Response messages[1] (Figure 2). The current DVB-RCS specification supports a single session key per RCST, this key being used to encrypt data traffic in both directions on the

[1] The current range of security profiles available is limited and, by current security standards, weak. We consider that these profiles should be strengthened.

satellite link. In the process of authentication, the specification then allows one of three key exchange mechanisms to occur. The objectives of these key exchange messages are firstly to authenticate the RCST and secondly for the RCST and NCC to agree the session key to be used. The three key exchanges and their principal features are as follows:

- Main Key Exchange (MKE): this uses the Diffie-Hellman algorithm [8] to develop a shared secret between the NCC and RCST, known only to these two entities; it also uses the cookie (secret key) held in the RCST to authenticate the RCST to the NCC; optionally it can use the newly developed shared secret to update the cookie; and finally it derives a session key from the newly developed shared secret.
- Quick Key Exchange (QKE): this uses the cookie to authenticate the RCST to the NCC; and derives a session key from the cookie.
- Explicit Key Exchange (EKE): this transmits (encrypted) a key from the NCC to the RCST; this key is then used as the session key.

Following logon, the NCC can initiate further key exchanges as required to update the session key.

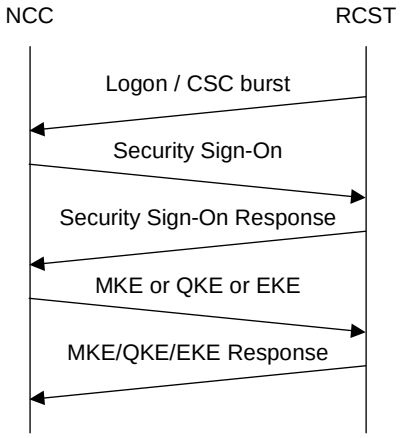

Figure 2: DVB-RCS security establishment

B. DVB-RCS Encryption

The session key obtained during authentication is used in DVB-RCS to encrypt IP datagrams in both forward and reverse directions, and this is shown in Figure 3 as "individual user scrambling." This allows data destined for different RCSTs to be encrypted with different keys. The Figure also shows an alternative encryption approach, "Common Scrambling," used to encrypt traffic in DVB Conditional Access (CA) systems. CA is typically used for encryption of broadcast traffic such as TV transmissions. Although it could be used for IP traffic, CA relies on a single key to encrypt all IP datagrams and thus encrypted traffic destined for one RCST could be decrypted by any other RCST.

The DVB satellite specifications support two data link layer platforms: DVB/MPEG2 and ATM. Encryption is performed differently in the two cases:

- In DVB Multi Protocol Encapsulation (MPE), two scrambling control fields are defined: these are the payload_scrambling_control field and the address_scrambling_control field. MPE is placed within the DSM-CC - Digital Storage Media Command and Control(DSM-CC) section in Figure 3.
- The DVB-RCS specification requires that the payload and/or address may be scrambled, but the MAC address must not be encrypted. As defined in [7] Section 7, the payload includes the IP datagram.

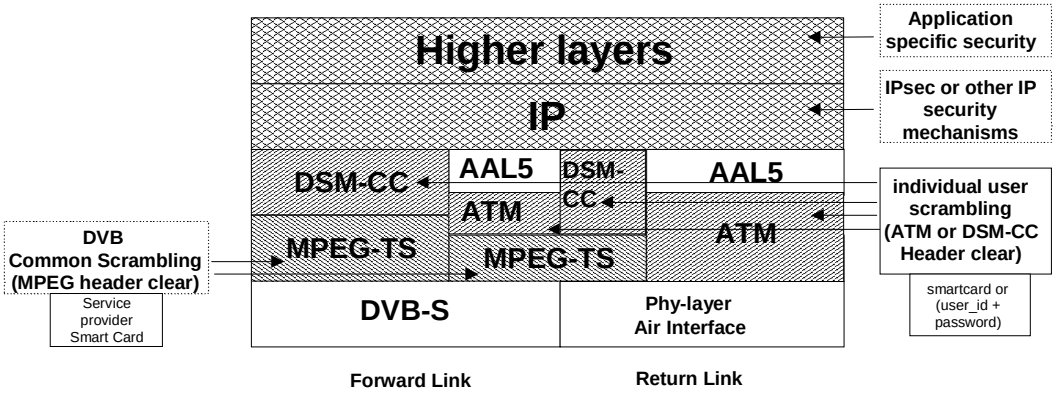

Figure 3: Security layers for satellite interactive network (example), from [1]

- In an ATM stream, the 48-byte cell payload is encrypted using the session key, but the 5-byte ATM header is not encrypted. If a single ATM VPI/VCI is used to carry traffic on the forward or return link then no information is given away to an eavesdropper by the ATM address.

The principal advantages of individual user scrambling compared to MPEG-TS common scrambling are:

- Encrypted traffic sent to or from one RCST can not be decrypted by any other RCST;
- There are no fixed relationships between IP addresses, the MPEG-TS program identifier (PID) and session key used for encryption, thus making eavesdropping more difficult;
- Data decryption at the RCST does not have to be performed on all the packets in MPEG-TS stream, but only on the individual unicast or multicast packets that are required by the given RCST, identified by the MAC address in each MPE Section header. This simplifies the RCST design.

However, as we shall see in the following Section, DVB-RCS does not support different session keys for different purposes, such as different multicast groups. If DVB-RCS were to support multiple session keys then different security protection could be provided for different multicast groups and this could even allow different security profiles to be implemented for different countries in the satellite beam.

III. PROPOSED AMENDMENTS TO THE DVB-RCS SECURITY SPECIFICATION

A. Security requirements

We thus see from the preceding Section that DVB-RCS currently supports the following security requirements:

- Enables RCST authentication to NCC, by means of a logon phase;
- Maintains the forward and return uplinks and downlinks secure from eavesdropping, either by unauthorised persons or by other users of the satellite system, provided “individual user scrambling” is implemented;
- Supports separate keys for unicast traffic to each RCST so that no RCST can decrypt unicast traffic intended for a different RCST;
- Supports periodic rekeying of unicast channels using the EKE messages;
- Supports logout.

The security procedure in the current DVB-RCS standard (as presented above) has several gaps. The most important gap is the lack of support for multicast security. The standard currently mentions the use of Explicit Key Exchange (EKE) for multicast ([1] paragraph 9.4.6.1). However it is not clear how a particular key exchanged with EKE can be linked to multicast in general or to a particular multicast service, since only one key is used per session and this key needs to support all unicast and multicast traffic through the RCST. This shortcoming is addressed in this Section. In particular, in order to support multicast security the following additional requirements can be stated:

- Support separate keys for each multicast channel;

- Transmit multicast keys efficiently to RCSTs;
- Support different security profiles (i.e. a specific set of cryptographic algorithms and parameters) for each channel's keys, both unicast and multicast;
- Support periodic rekeying of multicast channels – this is usually performed at regular intervals to reduce the probability of successful cryptanalysis of the encrypted traffic;
- Support rekeying to perform ejection of a compromised member of a multicast group.

We now proceed to consider how to modify the DVB-RCS specification to meet the requirements described above.

B. DVB-RCS security specification implications

In order to support multiple keys per RCST, the Main Key Exchange (MKE), Quick Key Exchange (QKE) and EKE messages need to both support multiple keys and also identify which unicast or multicast channel uses a given key. These messages therefore need extending to allow this. One of the following two mechanisms could be adopted to enable the NCC to send the keys for each multicast group to an RCST:

- At logon: keys for all multicast groups are distributed to each RCST, at the same time as the RCST's individual (unicast) session key. This mechanism is suitable where there are a small number of multicast groups. The advantage of this mechanism is its simplicity, but the disadvantage is that if there are a large number of multicast keys and each RCST is only expected to join a small number of groups then a large amount of network capacity is wasted in sending unwanted keys.
- On demand: keys for multicast groups are issued on demand, when the RCST joins a multicast group. This mechanism is scalable and suitable for systems with a large number of multicast groups, and requires new message types to enable a RCST to request the key(s).

In addition, in order to provide periodic rekeying and existing member ejection, the MKE/QKE/EKE messages can be used. However, key management architectures exist that are highly scalable to large multicast groups; one particularly promising mechanism which is receiving a high degree of interest is Logical Key Hierarchy (LKH) [9], [10]. LKH requires that multiple keys be unicast to each RCST when it joins a multicast group, and that some further keys be multicast to the group when rekeying takes place. LKH therefore requires two new extensions to the EKE message, which we call Extended EKE and Rekey EKE.

We therefore proceed to consider four sets of DVB-RCS security specification amendments, as follows:

- Support for multiple keys per RCST, to enable unicast and multicast traffic to use separate keys;
- Transmission of multicast keys at logon;
- RCST on-demand request for keys, to provide a scalable mechanism for multicast group joining;
- Extensions to EKE to support multicast rekeying, to enable key updates in case an RCST is compromised (Extended EKE and Rekey EKE).

C. Support for multiple channel keys per RCST

If we permit different security profiles for each channel (unicast or multicast), then such a profile has to be individually negotiated or specified for each channel. Different multicast channels could have different security profiles, for example to meet individual country security requirements. It should be noted that for a multicast channel all RCSTs must have the same profile to allow the traffic to be decoded: in this case the NCC therefore has to specify the security profile to each RCST. The Security Sign-On and Security Sign-On Response messages (Figure 2) need to be exchanged once for each channel, and the current message formats need to be amended so that the channel can be specified. This approach differs from the current security standard, in which security profile selection is global across all users of a given RCST ([1] Section 9.4.9.1).

We therefore propose that a field such as the payload stream ([1] Section 9.4.6.1) be explicitly included in the Security Sign-On and Security Sign-On Response messages. This could be based on the 48-bit MAC address, or use the low 23 bits of the multicast Class D address [11] or use the 24-bit ATM VPI/VCI. A new field, Payload_Stream_ID (PSID) is thus introduced into the Security Sign-On and the Security Sign-On

Response messages, and the message structures for these therefore become modified. Backwards compatibility with the current version of the DVB-RCS specification of this and all other messages can be implemented by for example setting the first bit of the existing Reserved field to indicate the new message structure. It should be noted that at the time of writing this article, a proposal has been made to ETSI to implement modifications to the existing MKE, QKE and EKE messages that are similar to and based on our proposals.

A unicast channel could, as allowed in the current DVB-RCS specification, use any of MKE, QKE or EKE. A multicast channel would normally use EKE, because all RCSTs need to be given the same session key (valid across the particular multicast group and known to all its members), and only EKE provides this function. It is expected that for consistency EKE will be used for both unicast and multicast (although EKE does not allow the NCC to instruct the RCST to update its cookie value; this can only be done using MKE). A single RCST would therefore in general conduct multiple key exchanges: one for each unicast channel and one for each multicast channel. To enable this, we propose that the new Payload_Stream_ID field be introduced in each of MKE, QKE and EKE messages and their responses. This field can then be used to specify the payload stream for the required key exchange.

We propose that such key exchanges be allowed at any time, not simply at logon. This is in accordance with the current DVB-RCS security specification, but here we make this point explicitly.

D. Transmission of multiple channel keys at logon

Two mechanisms were described in Section B above that could be adopted to enable the NCC to send the keys for each (or several) multicast group to a RCST: these were transmission at logon, and on-demand requests. In this Section, we consider transmission at logon, where either of two options could be adopted:

- A simple modification of the DVB-RCS specification, that allows multiple sets of Security Sign-On and Key Exchange messages for each key: this has the disadvantage that there is a large time delay in sending many messages over the satellite link;
- A new multiple explicit key exchange message that allows many keys to be downloaded in a single message and response pair.

Multiple sets of Security Sign-On and Key Exchange message pairs

This is implemented simply by a set of *N* key exchange messages for each of *N* keys that are to be transmitted. We therefore propose that the number of key messages remaining to be sent, *N*, is a new field "Number of Key Messages Remaining" in the Security Sign-On message. Each key exchange message could be any one of the MKE, QKE or EKE pairs (i.e. a message and its corresponding response).

Corresponding sets of messages (Security Sign-On, Security Sign-On Response, and the Key Exchange and its Response) are matched up by having a common Payload_Stream_ID (PSID).

As with the current DVB-RCS security establishment ([1] 9.4.7) a failure during Security_Sign-On or Security_Sign-On_Response causes the NCC to revert to non-secure interaction with the RCST, and a failure during MKE, QKE or EKE causes the RCST to be logged off.

Thus, as an example, if the NCC wishes to transmit one unicast channel key and two multicast channel keys to an RCST at logon, then one Main Key Exchange and two Explicit Key Exchanges occur as shown in Figure 4.

New Multiple Explicit Key Exchange messages

In this option we propose a new set of messages that allow multiple explicit key exchanges, allowing multiple multicast channel keys to be transmitted in one message. These messages are the Multiple Security Sign-On and Multiple Explicit Key Exchange (MEKE). The message structures contain the following features:

- A Count of EKE Sets, *M*, field contains the number of keys that are being transmitted in this message;
- All *M* keys are encrypted using the same temporary key; this is derived from the RCST's cookie using the same algorithm as the Explicit Key Exchange message ([1] 9.4.4).

Figure 5 illustrates the message exchanges required to transmit one unicast channel key and two multicast channel keys to an RCST. A further modification would be to allow a mix of main key exchanges and explicit key exchanges, but to simplify the discussion in this article we have not considered this further.

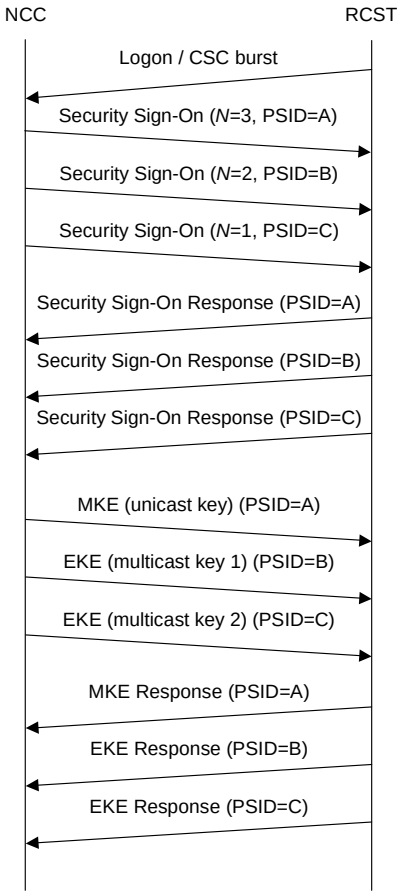

Figure 4: Example of multiple key transmissions at logon

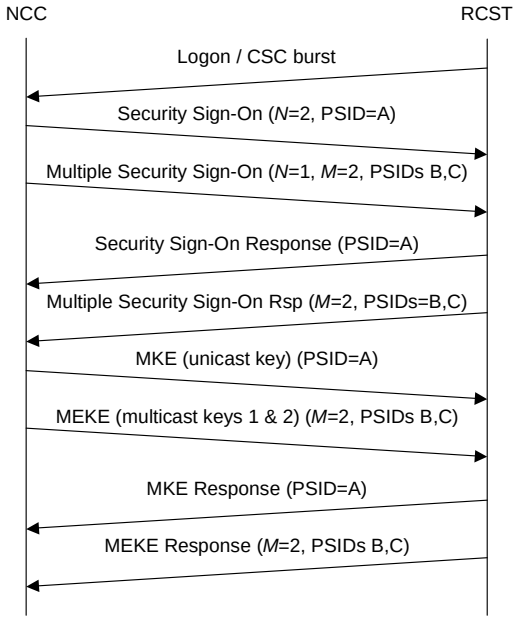

Figure 5: New Multiple Explicit Key Exchange (MEKE) at logon

E. On-demand requests by RCST for multicast channel keys:

This Section considers the second mechanism discussed in Section B for the NCC to send the keys for a multicast group to a RCST: on-demand request.

The NCC can transmit MKE/QKE/EKE messages at any time to update session keys on the fly ([1] Section 9.4.7). In the current DVB-RCS standard, the NCC initiates such session key updates. We propose that to support multiple multicast keys the RCST can additionally initiate a request to agree a security profile and obtain a key. This allows keys to be requested dynamically when a user joins a multicast group. Since this mechanism is not included in the current security specification, we propose that a new Security Key Exchange Initiate (SKEI) message be specified.

The security policy implemented at the NCC may either allow or not allow a particular RCST to access a particular multicast channel. If the connection is to be refused, one of two approaches could be adopted:

- The NCC transmits a new Security Key Exchange Reject message; or
- The NCC remains silent (i.e. does not transmit a Security Sign-On message).

The choice of which of these two approaches is taken would depend on the particular security policy for the satellite system. Figure 6 illustrates a successful on-demand key exchange.

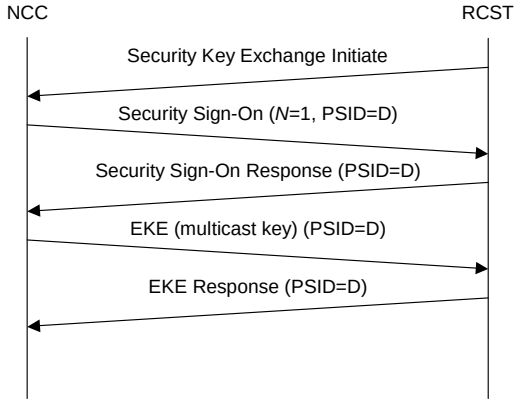

Figure 6: Example on-demand request for a channel key

The Security Key Exchange Initiate message would be re-transmitted if the RCST does not receive a response (i.e. either a Security Sign-On message or a Security Key Exchange Reject message) within a given time interval. If the number of transmissions exceeds three, the protocol fails (this proposed approach matches that in [1] 9.4.8.1). A protocol timeout value will be required (e.g. 1000ms, preferably configurable by the RCST and notified to the NCC).

We further propose that the SKEI message include both join and depart options, allowing an RCST to transmit a message indicating when it has finished receiving a multicast channel and no longer has any interest in the channel.

F. Extended EKE and Rekey EKE to support rekeying of multicast keys.

The existing EKE and EKE Response message pair satisfactorily support unicast transmission of a single given session key from the NCC to an RCST. However, they do not support multicast transmission of a key to all RCSTs, because the temporary key that is used to encrypt the given session key is derived from the RCST cookie, and this temporary key can therefore only be calculated by the one RCST.

A further modification to the DVB-RCS specification would be to introduce messages that support multicast and unicast transmission of multiple keys using a mechanism such as Logical Key Hierarchy (LKH) [9]. LKH is an approach that reduces the number of keys transmitted on rekeying from O(R) to O(log R) where R is the number of multicast receivers in the group. Thus LKH is particularly useful for rekeying in dynamic multicast groups with large number of members and membership changes. An implementation of LKH requires two types of messages:

- A unicast message sent to a RCST when it joins a particular multicast group: this message delivers to the RCST all the keys it needs to decrypt traffic and future key downloads, all encrypted with a key derived from the RCST's cookie;
- A multicast message transmitted to all group members whenever a rekey is required (e.g. due to eviction of a group member): this rekey message consists of the set of encrypted keys that allows the departing members to be securely removed from the group.

In the case of this DVB-RCS security specification, we propose that the unicast message be implemented using an Extended EKE message (EEKE) and that the multicast message be implemented using a Rekey EKE message (REKE). The message structures can be derived from and improve upon those specified in Group Secure Association Key Management Protocol (GSAKMP) [12]

The REKE fields that are encrypted use the encryption algorithm defined in the Security Sign-On and the key whose LKH ID is specified in the REKE message. In general a REKE message will contain keys encrypted using several different encrypting keys, with each key encrypted using the same encryption algorithm. Each RCST responds with an REKE Response.

The REKE and REKE Response message pair maintain the DVB-RCS specification paradigm of confirming every transmission from the NCC. However, at large scales the REKE will result in a large number of REKE responses back to the NCC. Even with the retention of the Response message to ensure reliability, LKH provides a benefit: to expel a group member with LKH would entail multicasting one LKH set of O(log *R*) keys and receiving *R* Response messages, whereas without LKH it would entail unicasting O(*R*) copies of the session key and receiving *R* Response messages.

G. Comparison of approaches

We can illustrate the efficiency of using the different message types to pass keys between the NCC and the RCSTs. Our proposals for modifications to the existing messages (Security Sign-On, MKE, QKE, EKE and all their corresponding responses) can be implemented within the existing Reserved fields of these messages and hence these messages are not increased in length. The number of messages transmitted in each of the different mechanisms discussed above are compared in Table 1. The table is constructed for an illustrative case of one unicast channel and two multicast channels.

We note that the multiple key transmissions at logon (A) involve the fewest changes to the current DVB-RCS specification. The table shows that MEKE (B) is the most efficient in terms of requiring the fewest number of messages and the smallest total length in bytes. Finally, whilst the on-demand key exchanges (C) require the most messages and channel capacity, they provide the most flexibility, being able to respond to ad-hoc user requests to join multicast channels. (A) and (B), by comparison, require all keys for all supported multicast channels to be transmitted at logon irrespective of whether or not the user wishes to use any of the channels.

	Message type	**Number of messages**	**Total bytes**
A	Multiple key transmission at logon (modified MKE and EKE messages) (see Fig. 4)	13	482
B	New Multiple Explicit Key Exchange (MEKE) at logon (see Fig. 5)	9	457
C	On-demand multiple key exchanges (modified MKE and EKE messages) (see Figs 2 and 6)	15	494

Table illustrates message count and total byte count for 1 unicast and 2 multicast channels.

Table 1: Efficiency of different message types

IV. CONCLUSION

Many satellite service providers are now looking to expand their TV broadcast service offerings to include Internet services, making use of DVB standards. A key issue for the future success of these DVB systems is thus security. This article has reviewed the security procedures in DVB-RCS satellites' two-way system.

The main contribution of this article is in adapting the current DVB-RCS standard procedures to provide secure multicast services over satellites. We have proposed updating the current security key exchange messages MKE, QKE and EKE with new messages that enable distribution of individual keys for each unicast channel and multicast group in operation; the changes to these existing messages are minimal. We have also proposed options for new messages that provide key updates at logon (MEKE), on demand (SKEI) and for rekeying multicast groups in the case of user expulsion or key compromise (EEKE, REKE).

V. ACKNOWLEDGEMENT

This work was supported by the EU Information Society Technologies SATLIFE project, IST-2004-507675 and the GEOCAST project, IST-1999-11754.

VI. REFERENCES

[1] ETSI, "Digital Video Broadcasting (DVB); interaction channel for satellite distribution systems," ETSI EN 301 790 V1.3.1 (2003-03).

[2] ETSI home page: http://www.etsi.org/

[3] I. Brown, J. Crowcroft, M. Handley and B. Cain, "Internet Multicast Tomorrow", *Cisco Internet Protocol Journal*, Vol. 5, No. 4, 2002.

[4] Z. Sun, M.P. Howarth, H. Cruickshank, S. Iyengar and L. Claverotte, "Networking issues in IP multicast over satellite," *International Journal of Satellite Communications and Networking*, Vol. 21, No. 4-5, pp.489-507, Jul.-Oct. 2003.

[5] B. Cain, S. Deering, I. Kouvelas, B. Fenner and A. Thyagarajan, "Internet Group Management Protocol, Version 3," IETF RFC3376, Oct. 2002.

[6] P. Karn, et al, "Advice for Internet Subnetwork Designers", IETF RFC3819, July. 2004.

[7] ETSI, "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP Interworking over satellite IP over satellite - security aspects", TR 102 287 (2003-11).

[8] B. Schneier, "Applied Cryptography", second edition, ISBN 0-471-12845-7, 1996.

[9] D. Wallner, E. Harder and R. Agee, "Key management for multicast: issues and architectures," IETF RFC2627, June 1999.

[10] M.P. Howarth, S. Iyengar, Z. Sun and H. Cruickshank. "Dynamics of key management in secure satellite multicast," *IEEE Journal on Selected Areas in Communications*, Vol. 22, No. 2, pp.308-319, 2004.

[11] S. Deering, "Host extensions for IP multicasting," IETF RFC1112, Aug. 1989.

[12] H. Harney, U. Meth, A. Colegrove and G. Gross, "GSAKMP: Group Secure Association Group Management Protocol", IETF Internet-Draft, draft-msec-gsakmp-sec-10.txt, May 2005.