AIAA-2002-1877

IP Multicast over Satellites - Technology Challenges

Z. Sun, H. Cruickshank, S. Iyengar and M. P. Howarth, University of Surrey, Guildford, Surrey GU2 7XH, UK,
Tel: +44 (0)1483 68 9493, Fax: +44 (0)1483 68 6011, z.sun@surrey.ac.uk

L. Claverotte, Alcatel Space Industries, Toulouse, France;

J. de la Plaza, Alcatel Espacio , Madrid

ABSTRACT[1]

This paper presents the research work carried out in the GEOCAST project, funded within the European 5th Framework IST programme. It describes the challenges when using satellites for IP multicast, concerning networking technologies, satellite communications payload, IP multicast protocols, the role of satellites in the network and, in particular, the paper focuses on security. There are various security standards such as DVB-S, DVB-RCS, ATM and IPSec that can be applied to satisfy some of the user and network requirements. The paper provides an overview of these issues and the possible interaction between them. Then it examines in detail the topic of securing very large multicast groups, where the group size and group dynamics have great impact on networks and network security. It also presents key management distribution systems and a satellite key distribution architecture.

1 Introduction

In recent years, significant research and development has been carried out in satellite networking technologies and applications such as ATM over satellite for broadband networks, IP over satellite for Internet access and interconnection, on-board processing and switching, and Digital Video Broadcasting – Satellite (DVB-S) and DVB interactive Return Channel via Satellite (DVB-RCS).

In addition to the traditional file and web page transfer with best-effort services in the Internet, research and development has been focusing on supporting real-time multimedia and multicast applications with quality of services (QoS).

Research has been carried out in the area of IP multicast over satellites, particularly over GEO satellites, within the European IST programme [IST000], Multicast Over Geostationary EHF Satellites (GEOCAST) project [GEOC00] supported by the EU 5th framework programme. This project is investigating the potential of satellites for IP multicast applications, due to the natural characteristics of satellites' wide coverage and broadcast capabilities. These characteristics have already led to the success of satellite applications in broadband access networks, broadband transit networks, and digital satellite broadcast services.

The challenge of security in GEO satellite environments is considered to be one of the main obstacles to the widespread deployment of satellite IP multicast and multimedia applications [CRUI98]. The main problem is that eavesdropping and active intrusion is much easier than in terrestrial fixed or mobile networks because of the broadcast nature of satellites. In addition, satellite channels experience long delays and high bit error rates, which may cause the loss of security synchronisation. This demands a careful evaluation of encryption systems to prevent Quality of Service (QoS) degradation because of security processing. Also the number of members in a multicast group can be very large and change dynamically.

This paper discusses these issues based on work from the GEOCAST project. First, in section 2 the paper discusses general satellite networking architectures and technologies including IP, ATM, DVB, and on-board processing and switching. Sections 3, 4 and 5 respectively discuss DVB, ATM and IP security systems. Section 5 discusses

[1] Copyright © 2002 University of Surrey. Published by the American Institute of Aeronautics and Astronautics, Inc., with permission.

multicast key management issues. Finally, section 6 concludes this paper.

2 Satellite IP networking and multicast

Satellite IP networking and multicast issues concern several related areas. These include services and applications and their QoS requirements and suitable network protocols. The discussion here is focused on IP multicast related issues and their relationship rather than a detailed description of these topics.

2.1 Network applications and services

Two main categories for broadband services have been specified from the network perspective: interactive services and distribution services. The interactive services are subdivided into three classes of services:

- Conversational services: Typical examples are video telephony, video-conferences, video/audio information transmission, high speed digital information, file and document transfer;
- Message services: Typical examples are video mail and document mail; and
- Retrieval services: Typical examples are video, high-resolution image, document and data.

The distribution services are subdivided into two classes:

- The class without user individual representation control, such as TV, multimedia video and audio distribution; and
- The class with user individual representation control, such as Pay TV (PTV).

From the user's perspective, satellite IP multicast should support existing multicast applications such as reliable file transfer, data distribution and multimedia streaming including video, voice and data.

All these services may have different QoS requirements such as jitter sensitive real time or loss sensitive transaction data.

The value added services provided by satellites include extended coverage and efficient delivery to a large number of users on a large scale. The satellite link can play different roles in the network:

- Last mile connections: End users are directly connected to the satellite to provide direct forward and return links. Traffic sources connect to the satellite feeder or hub stations through the Internet, tunnelling, dial-up links, etc.
- First mile connections: The satellite provides forward and return link connections directly to a large number of ISPs' or other service providers' gateways, which will deliver the IP packet onward to the end users. As with the last mile connections, traffic sources connect to the satellite feeder or hub stations through the Internet, tunnelling, dial-up links, etc.
- Transit connections: The satellite provides connections between Internet gateways or ISPs' gateways. The traffic is routed through the satellite links according to specified routing protocols and defined link metrics in the networks so as to minimise connection costs and to meet required QoS constraints for the given traffic sources.

Figure 1 gives an example how satellite can be used to support these types of connections, where Interior Gateway Routers (IGR) are used to route traffic within a single domain and Border Gateway Routers (BGR) are used between different domains.

2.2 Network protocols and internetworking

Internet protocols provide a uniform support to all the different services and applications across different technologies, such as LAN, MAN, WAN and satellite links. IP packets have to be encapsulated and transported across different networks. In a satellite environment, these can be traditional transparent data links, or broadband links based on ATM or DVB-S/DVB-RCS.

The Internet community has developed some mechanisms at the transport layer to provide a basic level of QoS. Traditionally, TCP is used for reliable connection oriented services and UDP for best effort connectionless services at transport level.

In addition to the best effort service provided by the IP network level protocol, new mechanisms such as DiffServ and IntServ have been developed to support QoS. In the DiffServ architecture, services are given different priority and resource allocations so that various types of QoS can be supported. In the IntServ architecture, resources have to be reserved for individual services. Given the large number of services that have to be supported in the network, resource reservation for individual services does not scale well in large networks.

Flow-based techniques such as Multi-Protocol Label Switch (MPLS) have also been developed to combine layer 2 and layer 3 functions to support QoS requirements.

Important network performance parameters include end-to-end delay, delay variation and packet loss. These have to be measured in an end-to-end reference path, where the propagation delay of satellite links has to be taken into account properly.

2.3 Satellite systems and technologies

Satellite systems and technologies concern two aspects: the ground segment and the space segment. In the ground segment, there are several constraints such as physical limitation, access, and trade-offs between transmission power, data rate and mobility. In the space segment, various types of payload can be used for communication links, such as transparent (bent-pipe), on-board processing, on-board packet switching (including ATM) and recently on-board DVB switching.

Transparent satellite links provide data link layer connections, where on-board signalling and control are minimal, but they may not provide optimised resource utilisation. On-board processing and switching satellites can provide optimised resource utilisation, but at the cost of complexity of on-board signalling and control. All these satellite systems can support IP protocols.

Future satellites with on-board DVB switching can integrate broadcasting and interactive services by combining DVB-S and DVB-RCS standards. Figure 2 shows a DVB regenerative payload, based on work conducted in the DOMINO-2 ESA programme. It performs the multiplexing of information from diverse sources into a standard DVB-S stream [LAMA01]. Another example of DVB on-board switching is the DILAN architecture for interconnecting of Local Area Networks (LANs) with IP over MPEG-2 encapsulation, using the regenerative STENTOR satellite payload [CLAV01].

The GEOCAST project can be based on either a transparent satellite system or a satellite system with on-board processing and switching capabilities. The forward link is based on DVB-S/MPEG-2 and the return link on DVB-RCS or ATM. The transparent satellite system provides a simple solution to support a mono-spotbeam star topology for networking. The on-board processing and switching satellite system has additional functionality, being capable of supporting multiple spotbeam star and mesh topology. It is also more flexible, with better utilisation of satellite bandwidth resources.

2.4 IP multicast over satellite

The development and investment in broadband communications and networks over satellite in recent years has been mainly based on three approaches: bent-pipe, ATM or ATM-like fast packet technology, and DVB for broadcasting. None of these were originally designed to support IP multicast, but they have now been adapted to support IP multicast over satellites.

Therefore, there are now several obvious options to support IP, depending on the available satellite systems and technologies: (1) IP over bent-pipe satellite, (2) IP over ATM, and (3) IP over DVB. The first option is based on simple technology and a large number of satellites in operation are available for IP connections. The second option will have to find solutions that enable ATM to support IP multicast and exploit the benefit of ATM. The third option will have to find solutions that support IP multicast over DVB;

these will explore the benefit of DVB technology, but may support only one-way communications or may have satellite return channels or terrestrial return channels.

If networks evolve towards an all-IP solution, a further option needs to be investigated: an all-IP satellite with on-board router. Such an option will need a significant amount of new system design, such as replacing the ATM and DVB switching with an on-board router, and will need to convince industry to develop and deploy satellite payload systems based on the new router technology instead of existing technologies. This may lose the benefits of ATM and DVB-S, which are already available. The benefit of an IP-router-in-the-sky approach is that the routing algorithm can be used to integrate the satellite links in an IP multicast routing tree at the source, trunk or end branch, as first mile connections, transit connections or last mile connections.

To reflect the requirements of different types of services and applications, IP multicast over satellite should address the topic of security, which is important for the widespread use of multicast and its commercial success. This subject is considered in the remainder of this paper.

3 Security systems in DVB-S and DVB-RCS

Security in general is intended to protect the user identity including its exact location, the signalling traffic to and from the user, data traffic to and from the user and the operator/user against use of the network without appropriate authority and subscription. In DVB, two levels of security can be applied:

- DVB common scrambling as described in section 3.1;
- Individual user scrambling in the forward and return link as described in section 3.2;

In addition, security can be applied in the application, transport and network layers. Application and transport layer security are not discussed in this paper. However, section 5 discusses IPSec in the context of network layer security.

Although the user/service provider could use its own security systems above the data link layer, it may be desirable to provide a security system at the data link layer so that the satellite link is secure without recourse to additional measures. Link level security is particularly desirable by satellite access network operators in order to secure satellite links and provide their clients (such as ISPs) with data confidentiality.

For DVB, the satellite interactive network forward link is based on the DVB/MPEG-TS Standard. The security concept is shown in Figure 3, which taken from [ETSI00].

3.1 Conditional Access in DVB-S

Conditional access (CA) is a service that allows broadcasters to restrict certain programming products to certain viewers. The CA does this by encrypting the broadcaster's programmes. Consequently, the programmes must be decrypted at the receiving end before they can be decoded for viewing.

CA offers capabilities such as Pay TV (PTV), interactive features such as video-on-demand (VOD) and games, the ability to restrict access to certain material (such as movies) and the ability to direct messages to specific set-top boxes (perhaps based on geographic region).

DVB Conditional Access (CA) originated as a broadcast security mechanism that allows a source to determine which individual receivers are able to receive particular broadcast programmes. CA requires two principal functions: (a) the ability to encode (or "scramble") a transmission and decode it (or "descramble") at the receiver, and (b) the ability to specify which receivers are capable of descrambling the transmission.

As Figure 4 shows, the transmission from a source to all receivers comprises a set of scrambled MPEG components (video, audio, data); Entitlement Control Messages (ECMs, session keys); and Entitlement Management Messages (EMMs, service keys). The ECMs identify the CA services, and for each CA service carry the control word (CW), in an encrypted form, and any other parameters required to access the service. The entitlement management messages (EMM) are a set of messages that identify the entitlements (permissions) of any individual user.

In addition, a Subscriber Management System (SMS) maintains and stores commercial aspects of customer relationship (registration, granting of entitlements, invoicing, and accounting), and the Subscriber Authorisation System (SAS) encrypts codewords and delivers them to the descrambler.

At the receiving end, it is the job of the Set-Top Box (STB) to descramble the CA encryption and decode the MPEG-2 streams for viewing. Each packet has associated with it (in its header) a program identifier (PID). The Conditional Access Table (CAT) has a well-known PID value = 1. This table can be used to identify the PID values of the transport packets containing the EMMs. The demux processor also constructs the Program Map Table (PMT) from non-encrypted packets; this gives the PID values of all the transport streams associated with a particular programme. Private data associated with the programme can also be included in this table - for example, the PID value of the packets that contain ECMs. All these tables (signalling messages) are transmitted in the clear, which is an inherent security weakness in DVB-S systems.

3.2 DVB-RCS security

The DVB-RCS standard provides much more advanced security procedures (in comparison to DVB-S CA) for satellite terminal authentication and key exchanges with the Network Control Centre (NCC).

DVB-RCS security can be divided into two phases: Phase 1 is the authentication during the logon procedure. During this phase a security session key is agreed between the satellite terminal and the NCC. The end user satellite terminal in the GEOCAST project is referred to as a User Earth Station (UES). In phase 2, the session key is used for the encryption of all subsequent messages between UES and NCC. The authentication is based on a long-term secret shared between NCC and UES, called a cookie. The cookie is 160 bits long and stored in non-volatile storage (such as smart cards). The NCC maintains a database of the cookie values of the UESs on its network. Cookie values can be updated occasionally as dictated by security policy, but they are less vulnerable than session keys. Anti-cloning measures can also be implemented using message sequence numbering. The DVB-RCS standard allows a Quick, Explicit and Main key exchanges. In the GEOCAST system, the Main key exchange has been chosen because it allows the UES cookie to be updated.

Figure 5 shows the message flows during logon. In summary, the messages are as follows:

- Logon: The UES indicates its intention to connect to the satellite network.
- Security sign-on: The NCC indicates which cryptographic algorithms it supports, as the initial stage of a security negotiation.
- Security sign-on response: The UES responds by specifying the specific algorithms and parameters it will use, chosen from the list presented by the NCC.
- Main key exchange: This message and the following enable the NCC and UES to use a public key algorithm to agree a shared secret.
- Main key exchange response: The second message enables the parameter values of the public key algorithm to be calculated.

A further consideration is security of the space segment. In satellite systems with DVB on-board switching such as DOMINO-2 [LAMA01], message integrity between the NCC and the OBP is important in order to make sure that configuration messages originate from the NCC. The major constraint in the OBP is its limited memory and computational power, since the computational cost of message integrity can be high. This depends on the type of algorithms used. For example, message integrity can be provided using public-key digital signatures, which are computationally heavy, or using MAC (Message Authentication Code) with secret keys, which is lighter. The use of secret keys implies the need for a key agreement, where keys can be stored in the OBP at installation time or agreed using the DVB-RCS key exchange mechanisms.

3.3 DVB-S and IP multicast security

DVB-S conditional access is used today for digital broadcasting over satellite and can be used to secure multicast communications over satellites at the MPEG-TS level. In DVB-S, IP packets are encapsulated in an Ethernet style header called Multi Protocol Encapsulation (MPE), where the IP address can be associated with the MPEG-TS PID. IP multicast can also be encapsulated with MPE. Descrambling in DVB-S is programme based, where a whole programme will be scrambled with the same CW. The programme may contain video, audio and data, each with a specific PID. The main drawback is that DVB-S scrambling system favours a centralised ECM and EMM and its use for securing dynamically changing IP multicast groups is limited.

On the other hand, the DVB-RCS standard provides more advanced security procedures for satellite terminal authentication and key exchanges with the satellite network operator. However it does not provide security procedures for terminal-to-terminal communications. The DVB-RCS standard allows the use of ATM cell transmission over satellites. Hence for satellite ATM networks, terminal-to-terminal communications and multicasting can be secured using the ATM security system as discussed in section 4.

4 Satellite ATM security systems

4.1 Technical challenges in GEO satellites

ATM security, as defined by the ATM Forum Security Working Group, is modelled after the ATM protocol reference model, which is divided into three planes: user, control, and management [ATMF01]. The ATM Forum security specification applies to virtual channel connections (VCCs) and virtual path connections (VPCs) for both point-to-point and point-to-multipoint connections. The ATM Forum defines the support of the following security services in the user plane:

- Entity authentication.
- Key exchange.
- Data confidentiality.
- Data integrity.
- Access control.

According to the ATM security specifications either the two-way or three-way security message exchange (SME) protocols may be used to establish the above mentioned security services. These SMEs can either be signalling or inband based. Security negotiation parameters can only be exchanged using the three-way SME. For unicast connections, either the three-way SME or two-way SME can be used to set up security associations. For the first “leaf” of a multicast connection, again, either the three-way or two-way SME can be used; for subsequent leaves, only the two-way SME can be used.

The ATM Forum security specifications state that for the data confidentiality service the ATM cell-level approach is used to encrypt the payload, and the header is left in the clear. The data integrity service is provided at the AAL level (rather than the ATM layer). Once a connection is established, keys for integrity and confidentiality services are negotiated using the three-way or two-way SME. However, when a key is used to provide confidentiality and integrity protection, the probability of successfully “cracking” the key increases with time. To prevent such an attack from being successful, keys must be changed periodically. To this end, a “session key update” procedure has been defined to support periodic key changeover. This procedure uses a master key, which is used to encrypt short-lived session keys; these in turn are used for a period of time for integrity and confidentiality services. The master key and first session key are exchanged during initial security negotiation. However, subsequent session keys must be transferred in the data channel so that the receiver may load them and start using them at the appropriate time.

The method for session key update, as described in the ATM security specification, consists of two processes: exchanging a new session key between the initiator and responder, and changing over from the old session key to the new session key. The first process is referred to as “session key exchange" (SKE) and the second process is referred to as "session key changeover" (SKC). The process of performing key updates is independent in each direction of data flow, for full duplex connections. It is the responsibility of the source (i.e. the encrypting side of the data confidentiality service) of each data flow to initiate the key update in its direction.

4.2 ATM and IP multicast security challenges

There are two important performance related considerations to be made when designing any ATM security system:

- ATM throughput: The encryption unit has to be fast and handle the full bi-directional data rates.
- Statistical multiplexing: Unique session keys are required for each VC. This requires that the cryptographic unit must be capable of changing the keys rapidly (a key agile system). Research in key agility has shown that one encryption unit for each direction can be sufficient.

Some challenges for IP multicast over ATM regarding key management are:

- Rekeying in ATM using SKC/SKE is performed in the data channel i.e. in the VC (in-band), while IP multicast systems often have a separate channel for key distribution e.g. using a different multicast address (out-of-band).
- The SKC/SKE protocols use a single ATM cell for rekeying. The size of the ATM cell restricts the use of sophisticated rekeying algorithms such as Logical Key Hierarchy [LKHW99], which are needed for scalability reason in large multicast groups. LKH is examined in section 5.
- There is no true provisioning for multicast connectivity in ATM.

4.3 Geocast satellite ATM system

In the GEOCAST project ATM satellite scenario, a typical connectivity example is that a UES establishes a connection with a Gateway Earth Station (GES). Each UES will use the three-way in-band SME to establish a secure unicast connection with the GES. After the satellite unicast ATM connection is set up, the user may try to join an existing or a new multicast group. In order to provide security services for the multicast group the ATM Forum security two-way signalling SME will be used. We assume that the GES generates the multicast session key $K_{SESSION\_MULTICAST}$ and master key $K_{CONTROL\_MULTICAST}$ and sends them to the UES. Moreover no security negotiation will take place since the GES will use a common cryptographic algorithm for data encryption. If the user is joining a new multicast group then the GES will generate the keys and send them to the UES. On the other hand, if the user is joining an existing group the GES only needs send the current multicast keys to the UES.

The rekey protocol is initiated by the GES, since the GES generates the initial session keys in both the unicast and multicast connections. The GES will use the SKC and SKE protocols to send the new session key ($K_{SESSION\_MULTICAST\_NEW}$) via multicast to the group. This key is encrypted with the control key ($K_{CONTROL\_MULTICAST}$) of the given multicast group.

5 Satellite IP multicast security systems

The security architecture of the Internet Protocol known as IP security (IPSec) is the most advanced effort in the standardization of Internet security. The IPSec protocol suite is used to provide inter-operable cryptographically based security services (i.e. confidentiality, authentication, integrity, and non-repudiation) at the IP layer [ATKI98]. It is composed of an authentication protocol: Authentication Header (AH), and a confidentiality protocol: Encapsulated Security Payload (ESP).

It is possible to use AH or ESP or combinations of both over satellites in transport or tunnel modes to provide network level security. This is in contrast to the DVB and ATM systems, which provide link layer security. The ESP tunnel mode provides the best security, however the addition of a new IP header (20 bytes) is a large overhead. The security key has to be agreed between the sender and recipient before using AH or ESP. For example this can be used with IP over MPEG-2 encapsulation in the DILAN architecture described in [CLAV01].

5.1 IP multicast security

In secure IP multicast, the group size and group dynamics have a great impact on the key management distribution system, especially for large groups. There are many architectures for key management, one of them is based on the IETF key management draft [HARD00]. In order to support multicast groups; the domain is divided into a number of administratively scoped "areas". A host-member of a multicast group is defined to reside within one (and only one) of these areas. The purpose of placing host-members in areas is to achieve flexible and efficient key management, particularly in the face of the problem of changes (joins and leaves) in the membership of a multicast group.

In [IYEN01] we investigated the idea of defining the satellite network as a single domain, which can be divided into administratively scoped areas. Each area could be mapped into a single spot beam. Area control keys are used to distribute session keys. However it seems the overheads of rekeying due to group membership changes are high in terms of satellite transmissions.

Therefore the remainder of this section discusses the alternative approach of the Logical Key Hierarchy [LKHW99]

5.2 Multicast rekeying issues

Confidentiality is ensured by encrypting traffic sent over the satellite links using a key, referred to here as the group key (this is identical in function to the session key defined in the ATM Forum specifications). Rekeying occurs for the following reasons:

(1) The group key is updated regularly (typically every few seconds or minutes) to reduce the probability of successful cryptanalysis of the encrypted traffic.

(2) The group key may also need to be changed on demand if it is determined that the key has been compromised.

(3) Rekeying may be required when a new user joins the multicast group. This ensures that the user cannot decrypt encoded traffic that was sent prior to their joining (this is called reverse secrecy).

(4) Rekeying may be required when an existing user departs from the multicast group. This ensures that the user cannot decrypt encoded traffic that is sent after they leave (this is called forward secrecy).

For large multicast groups that have frequent membership changes the cost of rekeying can be significant, since satellite resources are expensive. Scalable rekeying is therefore an important problem that needs to be considered in order to support secure communications for large dynamic groups. We now proceed to investigate rekey techniques for each of the four functions listed above.

Several techniques exist for rekeying (1) and (3) above: two options are for the new group key to be encrypted with either (a) the old group key, or (b) a separate "control" key negotiated during session establishment (this latter is the approach adopted by the ATM Forum, and described in section 4).

For (2) and (4) above a different rekeying approach is required since the old key is known by at least one user who is no longer to be a recipient of the multicast transmission. We assume that as each user joins, a unique pairwise key is shared between the source and the user. If the group key is then changed the new group key is encrypted with each user's unique pairwise key and then unicast to that user. Thus for *N* users a total of *N* encrypted keys are generated and transmitted across the satellite network (Figure 6a). The disadvantages of this approach are that it does not scale well for the large multicast groups that a satellite system can be expected to cater for, and it is expensive in its use of satellite network resources.

A hierarchical tree [LKHW99] provides a more scalable approach. Here a tree of keys is used (the keys are labelled A though O in Figure 6b). If a user departs from the group, say user 11, then it is only necessary to rekey keys F, K, N and the group key O. This requires seven encrypted keys to be sent: if the new keys are respectively F', K', N' and O' then the encrypted keys are $\{F'\}_{11}$, $\{K'\}_E$, $\{K'\}_{F'}$, $\{N'\}_{K'}$. $\{N'\}_L$, $\{O'\}_M$ and $\{O'\}_{N'}$, where $\{X\}_Y$ means key X encrypted using key Y. This represents a significant saving on the 16 keys that would need to be sent if the flat key domain of Figure 6a were used. In general for a departing user, (4) above, the rekey cost is reduced from N to $k\log_k(N)-1$ where k is the out-degree of the tree.

In the case of compromised keys, (2) above, all compromised keys must be rekeyed: The cost of this will vary between $k\log_k(N)-1$ (the cost of removing one user) up to $\frac{k(N-1)}{k-1}$ (assuming all keys in the hierarchy are compromised).

5.3 Rekeying and security policy

The security policy for each multicast group determines the frequency of group key regular updates, and whether or not rekeying is required for user joins and departs. As an example of this, there are a number of alternatives to rekeying on a user depart, and these are briefly discussed below. We assume that a user is connected to the satellite network via a UES:

- Do not rekey when a user leaves a group: if the UES is trusted not to forward data for a multicast group then this is the simplest option, involving no cost of either network traffic or key generation.
- Disable keys in the UES when it leaves the multicast group: the UES is trusted to actively destroy the keys it holds; once it has done this it is unable to decrypt the multicast group traffic.
- Rekey when a user departs from the multicast group: this is option (4) above. Although it is the most secure alternative, it has the disadvantage that when there are a large number of group members, changing the key on each departure may be a heavy processing load on the GES key server, and is unlikely to scale.
- Periodic rekeying: this is different from option (1) above, since here the intention is to bundle together a number of departing users and effectively rekey them simultaneously. This reduces the total rekey workload and increases the scalability of the multicast group, especially large dynamic groups, as has been illustrated by the Kronos system [SETI 00].

5.4 Applicability to satellites

A satellite system provides a further opportunity to reduce the rekey costs. Geostationary satellites transmit using a number of spotbeams. For a typical satellite currently under design there may be of the order of 50 to 300 such spotbeams. Let there be S spotbeams, and assume there is a different key hierarchy in each spotbeam (Figure 7). Then if a single user in one spotbeam departs from the group, the hierarchical tree only needs to be rekeyed in that spotbeam and, assuming the N users to be evenly spread over the spotbeams, the rekey cost is:

$$k\log_k\left(\frac{N}{S}\right)-1=k\log_k N-1-k\log_k S\ .$$

However, although the rekey cost is reduced significantly there is an S-fold increase in the volume of uplink traffic from the source, since each of the S spotbeams has a different group key (keys C, F and I in Figure 7). This is a major cost for a satellite system and would not be a worthwhile tradeoff. It also breaks the multicast paradigm that only a single copy of each packet is sent on any individual link.

However, an alternative that has the reduced rekey cost while retaining the multicast paradigm is to implement packet replication and re-encryption on-board the satellite. This option would be particularly appropriate for an IP-router-in-the-sky as described in section 2.4. A single copy of each packet is sent on the uplink to the satellite, encrypted with some group key. On the satellite S copies are made and each copy of the packet is re-encrypted with the group key for a single spotbeam. Each spotbeam then transmits the packets; they all have the same data but are encrypted with different group keys. Traffic is maintained at a minimum on each uplink and downlink, but at the cost of increased processing load on-board the satellite, and a small increase in the delay due to re-encryption. This delay would be negligible compared to the satellite's propagation delay.

6 Conclusions

This paper has presented multicast issues over satellites and has discussed satellite networking and technologies, including IP, ATM, DVB, and on-board processing and switching.

The research work in this paper has described the multicast and security challenges for GEO satellites, where there are various security standards that can be applied to satisfy some of the security requirements for such networks. DVB-S provides a conditional access system to control broadcasts such as pay-satellite-TV, but does not fit very well with IP multicast applications and architectures. On the other hand, DVB-RCS provides more advanced security procedures for satellite terminal authentication and key exchanges with the network operator. However it does not provide security procedures for communications between satellite terminals.

The DVB-RCS standard allows the use of ATM cell transmission over satellites. The ATM Forum has published the ATM security specifications, which mainly targets terrestrial ATM networks. However overlaps in authentication and key exchange exist between ATMSec and DVB-RCS, and duplication of these components should be avoided. This paper describes a satellite ATM system that provides authentication and key exchange protocols for master and session keys.

This paper also examines the issue of securing very large multicast groups, where the group size and group dynamics have great impact on the key management distribution system. This paper provides a hierarchical key distribution architecture together with policy options for re-keying when a member join or leave in addition to periodic re-keying.

7 Acknowledgements

The authors gratefully acknowledge the support from the European Union IST Programme [IST000] and the GEOCAST project (IST 1999 11754).

8 References

[AKYI97] I.F. Akyildiz, et al., ”Satellite ATM Networks: A Survey”, IEEE communications Magazine, July 1997.

[ATKI98] R. Atkinson, “Security Architecture for the Internet Protocol”, RFC – 2401, Nov 1998.

[ATMF01] ATM Forum, “ATMSec Specification Version 1.1”, March 2001.

[CLAV01] L. Claverotte et al., “DILAN: DVB PROC for the Interconnection of LANs using the STENTOR satellite”, 19th AIAA conference, Toulouse, France, 2001.

[CRUI98] H. Cruickshank et al., "Securing Multimedia Services over Satellite ATM Networks", International Journal of Satellite Communications, July-August 1998.

[GEOC00] GEOCAST project home page, http://www.geocast-satellite.com/

[HARD00] T. Hardjono, B. Cain, and I. Monga, “Intra-Domain Group Key Management Protocol,” IETF Internet draft (work in progress), Feb 2000.

[IST000] “Information Society Technologies Programme”, http://www.cordis.lu/ist/.

[IYEN01] S. Iyengar, H. Cruickshank, Z. Sun, “Security issues in IP Multicast over GEO Satellites”, 19th AIAA conference, Toulouse, France, 2001.

[LAMA01] M. Lamarca, J. Prat, et al., “DVB-Forward: a Digital Television / Internet Payload”, 19th AIAA conference, Toulouse, France, 2001.

[LKHW99] D. Wallner et al., “Key Management for Multicast: Issues and Architectures”, IETF RFC 2627, June 1999.

[ETSI00] ETSI EN 301790, “Digital Video Broadcasting (DVB) Interaction Channel for Satellite Distribution Systems”, 2000.

[SETI00] S. Setia, S. Koussih, S. Jajodia, E. Harder, “Kronos: a Scalable Group Re-keying Approach for Secure Multicast”, Proc. 2000 IEEE Symposium on Security & Privacy.

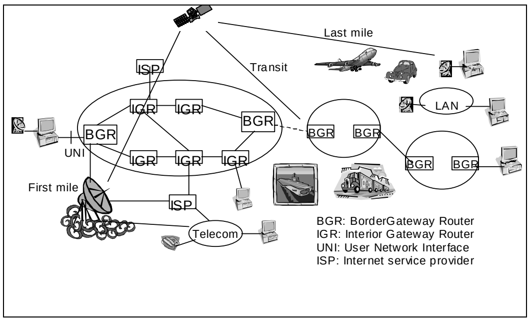
Last mile
Transit
ISP
IGR
IGR
BGR
BGR
BGR
BGR
BGR
LAN
UNI
IGR
IGR
IGR
First mile
ISP
Telecom
BGR: BorderGateway Router
IGR: Interior Gateway Router
UNI: User Network Interface
ISP: Internet service provider

Figure 1. Satellite IP multicast connections

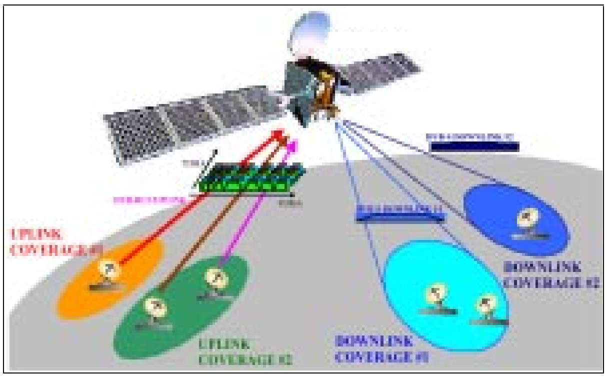

Figure 2 DVB with OBP network topology

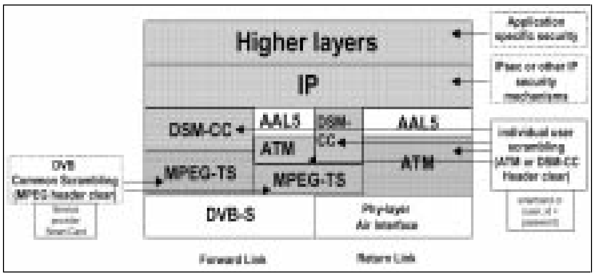
Higher layers
IP
DSM-CC
AAL5
DSM-CC
AAL5
ATM
ATM
MPEG-TS
MPEG-TS
DVB-S
Phy-layer
Air interface
Application specific security
IPsec or other IP security mechanisms
Individual user scrambling (ATM or DSM-CC Header clear)
DVB Common Scrambling (MPEG header clear)
Service provider Smart Card
Forward Link
Return Link

Figure 3. IP stack in DVB-RCS

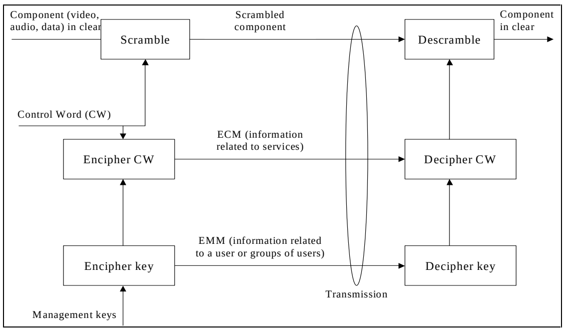

Figure 4. DVB Conditional Access

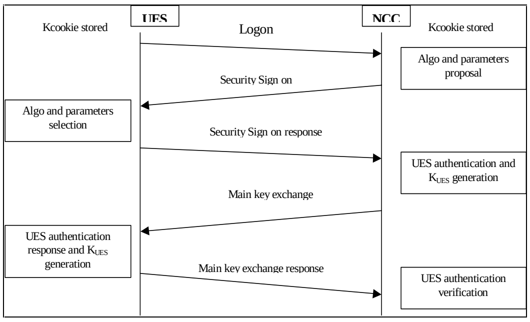
UES
NCC
Kcookie stored
Logon
Kcookie stored
Algo and parameters proposal
Security Sign on
Algo and parameters selection
Security Sign on response
UES authentication and K_{UES} generation
Main key exchange
UES authentication response and K_{UES} generation
Main key exchange response
UES authentication verification

Figure 5. DVB-RCS authentication

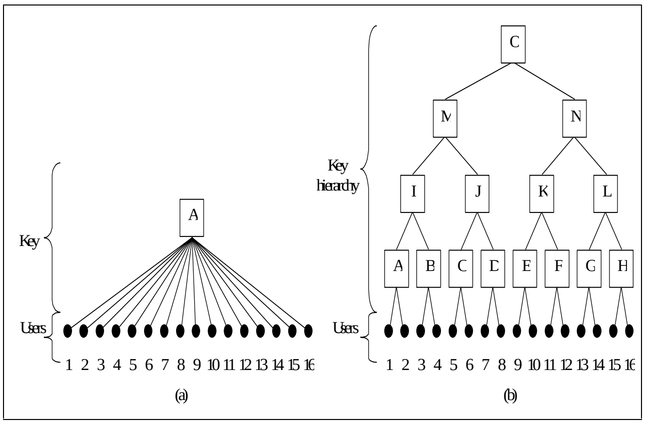

Figure 6 Key hierarchies: (a) N pairwise keys (left); (b) hierarchical tree (right)

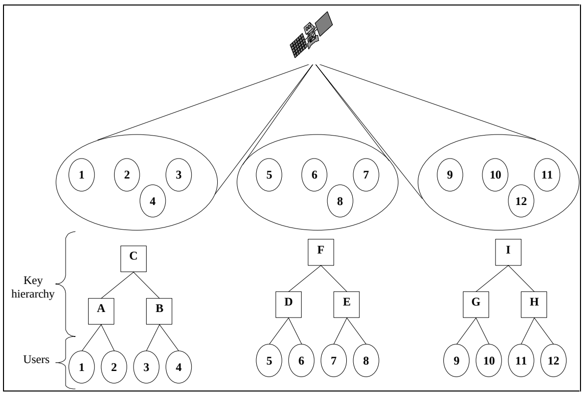

Figure 7. Hierarchical trees in satellite spotbeams