Securing Satellite Communications

H. Cruickshank, S. Iyengar, M. P. Howarth and Z. Sun,

University of Surrey, Guildford, Surrey GU2 7XH, UK, Tel: +44 (0)1483 68 6007, Fax: +44 (0)1483 68 6011,
email: h.cruickshank@surrey.ac.uk

ABSTRACT

This paper presents securing satellite communications using link level security (such as ATM security) or network level security (such as IPSEC), where both can be applied to military satellite communications. The paper examines the topic of securing very large multicast groups over satellites, where the group size and group dynamics have great impact on networks performance and network security.

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 [AKYI97], 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) [ETSI00].

In addition, satellites are ideally suited for delivery of multicast applications, including multimedia content distribution. GEO satellite systems are particularly well suited to multicast, where the duplication of packets is performed on board the satellite and all terminals can receive a single transmission. If these systems can be optimised to simultaneously support multicast down-load of bulk content and streaming of real-time multicast content, they will provide a flexible and economic IP multicast delivery platform.

The challenge of security in GEO satellite environments is considered to be one of the main obstacles to the widespread deployment of satellite multimedia applications [CRUI98]. This is particularly important in the case of military satellites. 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.

Security can be applied in the application, transport and network layers. This paper discusses link layer and network layer security systems in the context of satellites. Application and transport layer security are not discussed in this paper.

2 Link layer security systems

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 with data confidentiality. One good example is satellite ATM systems.

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.

For satellite ATM networks, the above security specifications can be used. In hybrid systems such as the DVB-RCS specification ATM is used in the return link. For DVB-RCS satellite terminals with ATM capabilities, the security recommendations are to use the ATM Forum recommendations for providing data confidentiality.

3 Network level security: IPSEC

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 [IETF, RFC 2401]. It is composed of an authentication protocol: Authentication Header (AH) [IETF, RFC 2402], a confidentiality protocol: Encapsulated Security Payload (ESP) [IETF, RFC 2406]. These security protocols are designed for both IP version 4 (IPv4) and IP version 6 (IPv6) environments.

Securing IP multicast is an interesting and a difficult topic. In principle, the security system should be decoupled from the underlying multicast routing protocols, to allow differing security models and architectures to be deployed, without affecting the multicast distribution tree, which delivers the multicast data end-to-end. Therefore implementing IP level or application level security can achieve this goal. This paper focuses on IPSEC which is IP level security system.

There are several interrelated factors or aspects of IP Multicast that influence the approaches and mechanisms used to secure it. Of these, some broad and most relevant factors include:

- Multicast application type;
- Group dynamics; □
- Scalability issues; □
- Underlying trust model.

Since these factors and others are interrelated, it is difficult to portray their specific relationships and influences. This can have great impact on security key updating or sometimes called re-keying.

4 Rekeying secure satellite group communications

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. This is called periodic rekeying.

(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 and 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 1).

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 (or key controller) 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 1a). 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.

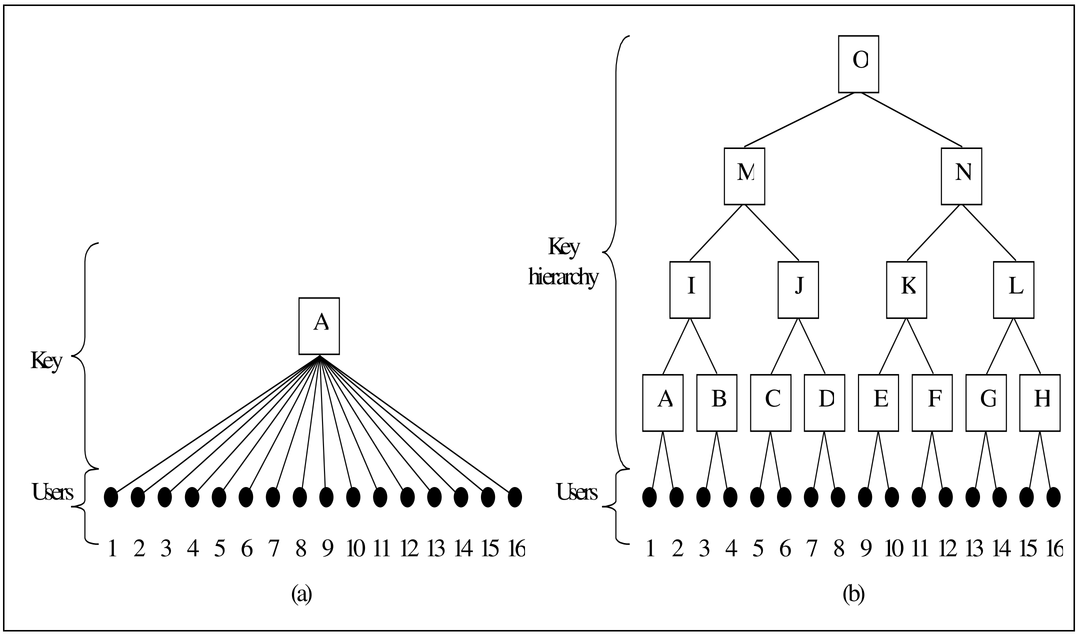

Figure 1 Key hierarchies: (a) N pairwise keys (left); (b) hierarchical tree (right)

A hierarchical tree [IETF, RFC 2627] provides a more scalable approach. Here a tree of keys is used (the keys are labelled A though O in Figure 1b). 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 1a were used. In general for a departing user, cast (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 Multi layer IPSEC for securing satellite group communications

IPSEC encrypts the transport headers (such as TCP or UDP) and transport payload. Therefore IPSEC will not work with satellite entities that need access to the transport header information to enhance transmission rates or reliability of delivering IP packets. This can be solved by modify IPSEC and using Multi-Layer IPSEC (ML-IPSEC) [MAHC02]. In ML-IPSEC, two keys can be used: one for the transport header and one for the transport payload. This ensures that the user data is protected end-to-end. It also provides satellite proxies access to the transport header.

It is possible to have an interworking solution between ML-IPSEC and LKH, where the end users are put into one branch of the LKH tree and the satellite terminals are put into another branch. The root key in the LKH tree will be used for the securing the transport header and a branch key for the end users. The proposed scheme is scalable, in that the rekey effort varies with $\log N$, and efficient, in that the number of rekeys required is half that of two separate tree hierarchies.

6 Conclusions

The research work in this paper has described the 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 such as ATM and IPSEC. The ATM Forum has published the ATM security specifications, which mainly targets terrestrial ATM networks. Such system can be adapted for satellite environment.

This paper also examines network level security and using IPSEC. Also it presents the research issues in securing very large multicast groups, where the group size and group dynamics have great impact on the key management distribution system.

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 Comms Magazine, July 1997.

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

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

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

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

[IETF] home: http://www.ietf.org/ or RFCs: http://www.rfc-editor.org/rfcsearch.html

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

[MAHC02] M. Annoni et al., “Interworking between Multi-Layer IPSEC and secure multicast services over GEO satellites”, COST 272 meeting in Thessaloniki, Greece June 2002.