SATELLITE IP SEC: AN OPTIMIZED WAY OF SECURING MULTICAST WIRELESS COMMUNICATIONS

Sébastien Josset, Laurence Duquerroy
Alcatel Space, 26 avenue JF. Champollion- BP 1187, 31 037 Toulouse cedex 1 France

Abstract: The aim of this work is to introduce a new way of transparently securing both unicast and multicast services, optimised for satellite networks, named SatIPSec.

Key words: IPSec, SSL, satellite network, multicast, DVB-RCS

1. INTRODUCTION

The today 'de facto' generation of packet network technologies, which operates on the basis of 'no security by default', provides insufficient security support, especially in satellite networks with natural broadcast/multicast capability over large areas.

Some security protocols have been introduced such as SSL (Secure Socket Layer) or IPSec but they are dedicated to unicast communications.

In the Next Generation Networks (NGN), especially those integrating a satellite shared access, such as DVB-S/RCS, packet network technologies will have to support real-time multicast services (tele-conferences, pay per view videocasting, ... etc.) and will require improved Security support.

The aim of this work is to introduce a new way of transparently securing both unicast and multicast services, optimised for satellite networks, named SatIPSec.

2. SATELLITE SPECIFIC ISSUES

Satellite links are characterised by many specific properties. Some of the advantages and disadvantages of the satellite environment related to the subject of this work are:

- High delay: The end-to-end transmission delay is about 250 ms for a geostationary satellite (baseline in this paper).
- Broadcast and multicast capabilities: Satellites are the most natural and economical means for providing broadcast and multicast services.
- Extended coverage: The wide footprint provided by satellites allows the management of a large number of terminals depending from a single hub.
- Cost of the link: The satellite network infrastructure and the use of bandwidth can be more expensive than terrestrial alternatives.

These characteristics have impact on the design of the satellite system and on its performances. Future satellite systems will have to be more and more optimised for the transport and delivery of a wide range of IP services. In this frame, IP security is certainly one of the issues to be carefully addressed.

A study on the impacts of the delivery of IP packets over a broadband multimedia satellite network has been already performed in the IST-BRAHMS [1] project, where, in the specific field of the security, some solutions such as multi-layer IPSec have been proposed [2]. These concepts are now being further addressed in the frame of the IST-SatIP6 [3] project where the innovative SatIPSec concept presented in this paper will be developed.

The recent development of IPSec [4] in IETF is incompatible with a new set of networking paradigms that place more and more controls inside the network in intermediate nodes rather than in end nodes. For example, any service that requires knowledge of the TCP port number anywhere other than in the end host, cannot function if IP packets are encrypted.

Satellite specific high transmission delays introduce the need to customise algorithms each time a handshake protocol is used between two peers. TCP can use optional algorithms such as SACK, or Reno algorithms to enhance its performance. Throughput optimisations are possible thanks to proxy boxes that modify IP packets to change protocol classical behaviour by providing satellite specific Protocol Enhancement Proxies (PEP) functionalities (fig.1). Nethertheless, if the IP packets are protected by an end-to-end IP Sec ESP payload [5] or authenticated with an IPSec AH header, even the smartest satellite PEP becomes useless.

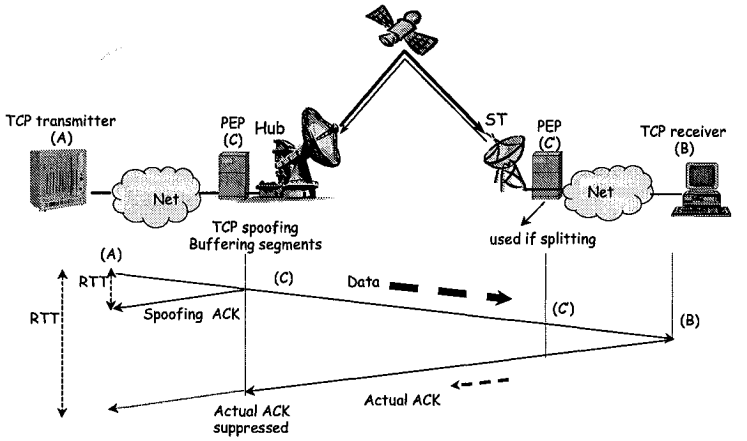


Figure 1. Satellite TCP PEP

IPSec data plane associated to IKE (Internet Key Exchange) [6] control plane permits to secure point-to-point communications, by offering four security services: confidentiality, integrity, message origin authentication, and entity authentication. It can be used in multicast environment, but in such a case, this solution is not optimised. Indeed, let us consider a group of satellite terminals, which wish to exchange securely multicast data by using the IPSec protocol. In order to protect all traffic, a secured bi-directional link has to be established between each satellite terminal pair. Consequently, each multicast packet has to be duplicated, and the copies have to be encrypted independently and sent on their respective satellite link (figure 2). This impacts the satellite system capacity and does not permit to take advantage of the natural broadcast capability of the satellite link. Moreover, if the number of receivers is equal to n, for each packet, the sender has to perform n-1 encryption computations.

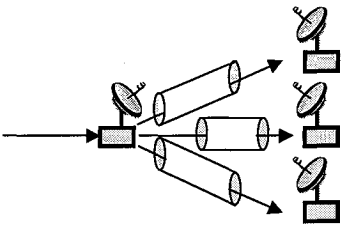


Figure 2. IP multicast over IPSEC/IKE: Duplication of the IP packets.

3. SAT IP SEC SOLUTION

SatIPSec aims at providing satellite systems with a security level comparable with the one of the IPSec protocol, but with an additional specificity: it is optimised with regard to the native multicast capacities of these systems. This part presents the SatIPSec advantages in comparison with IPSec, in particular in a satellite context.

SatIPSec aims at avoiding the duplication of multicast packets over the satellite link, while limiting the number of session establishment and the number of encryption computation, by replacing the IKE control plane and taking benefit from the IPSec uni-source multicast capabilities.

For that purpose, a centralised management solution is adopted (achieved by a central server), and the data plane and control plane are clearly separated.

SatIPSec control plane allows establishing a secured link between each terminal and the central server. Consequently, only one SatIPSec session establishment per terminal is needed. Moreover, SatIPSec imposes a common data security configuration, shared by all terminals. This configuration is sent securely to satellite terminals, by using the established secured links. A multicast IP packet is encrypted once, sent in multicast, and can be decrypted by all terminals.

Finally, SatIPSec mechanisms, when implemented at layer 3 are transparent to the satellite access and transmission definition: they can be implemented in overlay to existing standards.

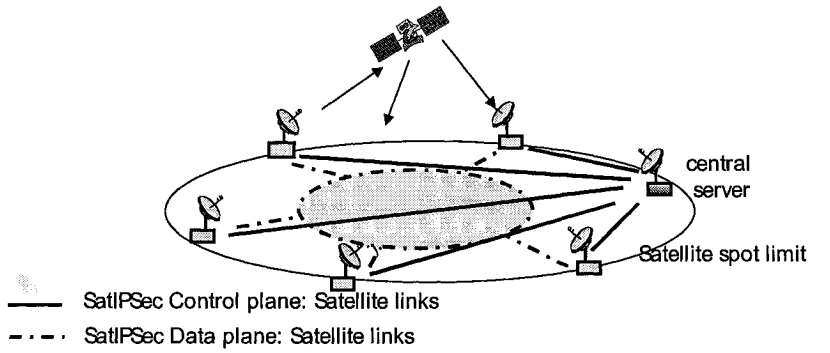


Figure 3. Use of SatIPSec for the exchange of secured multicast data

4. SYSTEM ARCHITECTURE

This solution is based on two main entities entitled SatIPSec client and SatIPSec Group Controller & Key Server (SatIPSec GCKS). The SatIPSec system architecture is thus formed of several SatIPSec clients and of one GCKS. SatIPSec clients are in charge of securing IP traffic flows during their transmission over the satellite links. For that purpose, they apply some security treatments (ciphering/deciphering, computation and checking of authentication values...) to IP datagrams. The GCKS centrally ensures the management of SatIPSec clients and the establishment of the security architecture. Its function is to configure SatIPSec clients, by supplying them with the necessary information for securing data transmissions according to the data security requirements.

The Fig. 2 presents the architecture. SatIPSec clients and GCKS are implemented in external boxes (independently of the other Satcom equipments) [1]. There is one SatIPSec client box behind each Satellite Terminal (ST), and the GCKS is located at the gateway side.

The location of SatIPSec clients allows to apply security mechanisms to IP traffic (if requested) so as to ensure its protection during its transmission over the satellite network (Fig. 3). In emission, the SatIPSec client can cipher each IP packet and compute an authentication value before transmitting it on satellite system. In reception, the SatIPSec client(s) can

[1] However SatIPSec mechanisms could also be implemented directly inside the satellite terminal IP stack.

decipher it and check the authentication value, before transmitting it on the terrestrial network it (they) is (are) connected to.

The implementation of the SatIPSec solution allows to protect any unicast or multicast IP flows transmitted on satellite links, from Hub to ST, from ST to Hub and from ST to ST.

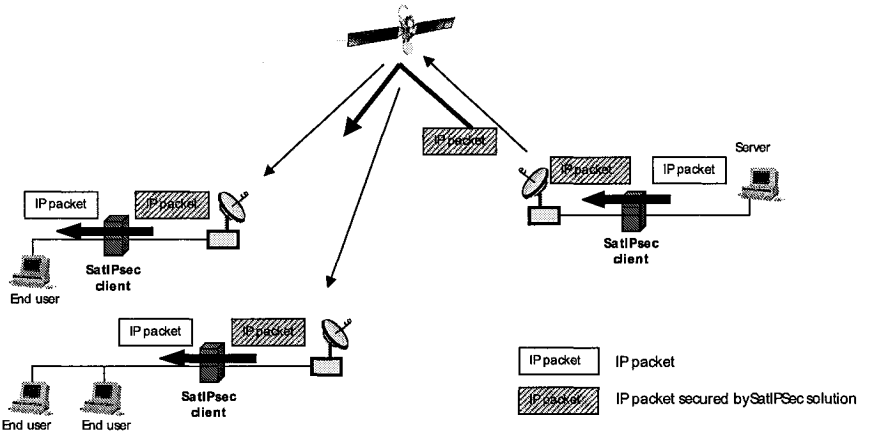


Figure 4. Protection of satellite IP transmissions by SatIPSec solution

5. CONTROL PLANE

The Flat Multicast Key Exchange (FMKE) protocol is a new group key management protocol, based on a centralized management achieved by the GCKS. Its objective is to manage securely Security Associations destined to protect multicast and unicast IP traffic, i.e. establish and update SAs in clients participating to Secure Multicast Groups and VPN. The FMKE protocol is in particular optimized for very large multicast groups in flat environment (i.e. no intermediate routers between the GCKS and a large amount of clients) like in satellite networks. In fact, FMKE is derived from the Group Domain Of Interpretation (GDOI) protocol [8] defined by the IETF Multicast SECurity (MSEC) group, and can be seen as a use case adapted to satellite networks and to the needs of the SATIP6 project. There are three main differences. First of all, FMKE manages SAs for group and unicast exchanges, contrary to GDOI, which manages only groups, and requires therefore to add external mechanisms to establish VPNs. Secondly, FMKE exchanges implement reliability mechanisms based on positive, negative acknowledgements... in order to guaranty a reliable key distribution (in unicast and in multicast). GDOI does not guaranty at all reliable key

distribution. At last, in GDOI, the client has to request to get access to a particular group in order to receive the corresponding SAs if it is authorized, while in FMKE, the client receives directly all SAs it is authorized to get access to, without having to send a request for each group. This way FMKE limits the consumed bandwidth. Indeed the client does not have to send a request for each group, and a FMKE message from the GCKS can contain SAs from different groups and VPNs. However, FMKE could be defined with a GDOI-like behavior.

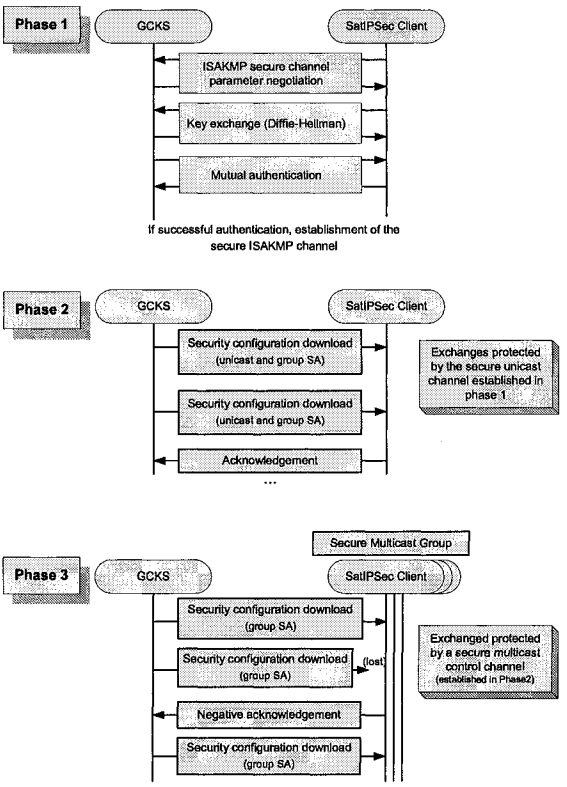
FMKE is thus used securely to configure SatIPSec clients with the necessary SAs to establish the required security architecture (i.e. VPNs, Secure Multicast Groups). Client configuration is achieved thanks to three different phases described in Ref. 4. The implementation achieved in the context of the SATIP6 project enables the two first ones.

The *first phase* is dedicated to the establishment of a secure ISAKMP [9] channel between the GCKS control plane and the client control plane. This establishment is preceded by a mutual authentication. In the SatIPSec implementation, the method which has been selected for this phase is the method called « Main-Mode with pre-Shared key for Authentication » defined in the IKE protocol [1](IKE phase 1). Authentication is based on a pre-shared secret.

The *second phase* is dedicated to the SatIPSec client configuration. The GCKS transmits to the client, SAs that it is authorized to receive. These SAs are sent securely in unicast, thanks to the secure ISAKMP channel established during the previous phase (confidentiality, data origin authentication and integrity are provided). SAs concerns VPN and Secure Multicast Groups.

The cryptographic methods and algorithms used in the SATIP6 demonstrator are Diffie-Hellman group 1 and group 2 for key exchange, DES, 3DES and AES for encryption, and HMAC-SHA1, HMAC-MD5 for integrity/source authentication.

The FMKE *third phase* is dedicated to the configuration of a Secure Multicast Group (i.e. of its group members). The GCKS transmits, in multicast, to all group members, SAs allowing to secure multicast flows. These transmissions are protected by a secure multicast control SA dedicated to the group, whose parameters have been previously transmitted to each group member thanks to phase 2.



5.1 Re-keying.

Keys used to protect data traffic (session keys) or management traffic have to be renewed regularly in order not to weaken the security of the system. The GCKS is in charge of distributing periodically these keys to the clients. Two re-keying modes are defined:

In the Nominal mode, the keys are sent in multicast, protected by the multicast control SA established during the second phase of the session establishment. The Control SA guarantees confidentiality, integrity and source authentication. The advantage of that solution is that only one message is needed to update keys in all clients belonging to the same group. It is therefore well adapted to large groups. This scheme is valid for the renewing of all group keys, i.e. keys of the Control SA and of Security Associations dedicated to protect user data traffic (session keys).

In the Alternative mode, the keys are sent in unicast, protected by the unicast secure channel established in the first phase of the session establishment (ensuring confidentiality, integrity and source authentication). This scheme can be used for all types of keys (keys of that channel, Control

SA keys, or Session keys). This solution is not considered the favourite one for group keys in large groups, as the re-keying message has to be sent as many times as the number of clients authorized to get access to these keys. However, these schemes may be implemented in groups with a small number of terminals (e.g. military applications).

5.2 Reliability.

SatIPSec requires reliable session establishment phases. The reliability mechanisms adopted in SatIPSec depend on the session establishment phase.

In the first phase, reliability mechanisms are based on unchangeable message order, on timers and on re-transmission. Each message sent on the satellite link is associated with a timer : when it expires, if the following message has not been received yet, the message is re-transmitted.

The second phase cannot be based on unchangeable message order as the number of configuration messages sent to the client module is different for each client. Reliability mechanisms are therefore based on positive acknowledgement (the client module will acknowledge each received message), retransmission of non acknowledged messages and selective acknowledgement (for optimisation). For that purpose, a sequence number is assigned to each message (mentioned in its fields).

The third phase cannot implement positive acknowledgement as the number of client modules receiving the configuration messages may be very large. So, reliability is based on negative-acknowledgement messages : when a client module determines that it has not received one or several messages, it asks for their retransmission by sending a Non-acknowledgement message. Retransmission is achieved in multicast. The time before sending a Non-acknowledgement message varies for each client module, in order to avoid the sending of too many Non-acknowledgements and the congestion at GCKS side : few client modules will be authorised to send a Non-acknowledgement at the beginning, and it is expected that these messages will be sufficient so that all client modules receive the configuration messages. As in the 2nd phase, a sequence number is assigned to each message..

6. DATA PLANE

6.1 Chaining.

SatIPSec aims at offering supplementary functions and services. These supplementary services are defined in the SA tables, and are considered as separate but chained functional blocks. The interest of block chaining is flexibility. During the SA utilisation, it is possible to modify all the parameters of the chain by adding, replacing, and withdrawing one or more functional blocks, such as IP Sec ESP, IP Sec AH, Encryption, Authentication, Tunnel, TCP Spoofer, IGMP proxy, packet filter...

6.2 Multicast Authentication

To authenticate packets in a stream, the source must add authentication information to the content, where the recipients use this information to ascertain the origin of the transmitted data.

In the case of two party communication (like in IPSec AH), the authentication is provided with symmetric cryptographic techniques using a MAC (Message Authentication Code) which relies on a secret key shared between the two communicating parties.

However, in the case of multiparty communication, authentication is divided into two categories :

Group authentication, where the recipient can verify that the received data is originated from a member of the group;

Source authentication, where the recipient can also verify the identity of the source of the data.

For group authentication, the techniques using MACs can also be applied in this case, where the secret key is shared between all the members of the group. In the case of source authentication, the existing solutions cannot be used because of the possibility that a member can impersonate the data while using MAC techniques. Several authentication schemes are proposed for resolving this problem.

The time based stream authentication scheme TESLA [11] provides source authentication with the requirement of secure clock synchronisation between the source and the recipients. It uses some MAC operations where the keys are declared after the data is sent. Some other hybrid approaches are proposed by Wong et al [12], Golle et al [13] , Perrig et al [14] and Pannetrat et al [15], where the use of asymmetric techniques are amortised with some hash chains: packets are linked together where some of them are digitally signed. These schemes are tolerant to packet losses.

In the case of SatIPSec, for the group authentication, the IP Authentication Header is sufficient. An optional module of source authentication can be added for this protocol, where one of the hybrid approaches can be used.

7. CONCLUSION

The SatIPSec protocol allows to flexibly set up large secure multicast networks in flat environment (no intermediate routers between the master and a large amount of clients). It is well adapted to satellite or terrestrial mobile systems that want to efficiently offer multicast secure services. This protocol is able to configure the well-known IPSec stacks and integrates possible functional extension that optimise the wireless bandwidth. The SatIPSec control plane reuses as far as possible the IKE/ISAKMP messages and some extensions proposed in IETF MSEC group.

8. REFERENCES

[1] http://brahms.tilab.com/

[2] M. Annoni, G. Boiero, N. Salis. Security issues in the BRAHMS system. *Proceedings of the IST Mobile & Wireless Telecommunication Summit 2002*

[3] http://satip6.tilab.com/

[4] "Security architecture for the Internet Protocol" , RFC 2401, S. Kent, R. Atkinson, IETF, November 1998 .

[5] "IP Encapsulating Security payload (ESP)", RFC 2406, S. Kent, R. Atkinson, IETF, November 1998

[6] "The Internet Key Exchange (IKE)", RFC 2409, D. Harkins, D. Carrel, IETF, November 1998.

[7] RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)

[8] C. K. Wong, M. Gouda, S.S. Lam. Secure group communications using keygraphs. *ACM SIGCOMM 1998.*

[9] D. M. Wallner, E.J. Harder, R. G. Agee. Key Management for multicast : Issues and architectures. Internet draft, Network working group,1998.

[10] S. Mittra. Iolus : A framework for scalable secure multicasting. *Proceedings of the ACM SIGCOMM'97.*1997.

[11] TESLA: Multicast Source Authentication Transform', draft-irtf-smug-tesla-00.txt, IRTF, Nov 2000

[12] C.K. Wong, S.S. Lam. Digital Signatures for flows and multicasts. *IEEE/ACM Transactions on Networking.* 1999

[13] P.Golle, N. Modagugu. Streamed authentication in the presence of random packet loss. *to appear in NDSS 2001.*

[14] A. Perrig, R. Canetti,J. Tygar, D. Song. Efficient authentication and signing of multicast streams over lossy channels. *IEE Symposium on Security and Privacy,* 2000.

[15] A. Pannetrat and R. Molva. Authenticating real time packet streams and multicasts. *The Seventh IEEE Symposium on Computers and Communications.* 2002.