TECHNICAL RESEARCH REPORT

Security Issues in Hybrid Satellite Networks

by Ayan Roy-Chowdhury, Michael Hadjitheodosiou, John S. Baras

CSHCN TR 2004-17
(ISR TR 2004-33)

The Center for Satellite and Hybrid Communication Networks is a NASA-sponsored Commercial Space Center also supported by the Department of Defense (DOD), industry, the State of Maryland, the University of Maryland and the Institute for Systems Research. This document is a technical report in the CSHCN series originating at the University of Maryland.

Web site http://www.isr.umd.edu/CSHCN/

Security Issues in Hybrid Satellite Networks

Ayan Roy-Chowdhury
Electrical and Computer Engineering
and Institute for Systems Research
University of Maryland
College Park, Maryland 20742
Email: ayan@umd.edu

Michael Hadjitheodosiou
Institute for Systems Research
University of Maryland
College Park, Maryland 20742
Email: michalis@isr.umd.edu

John S. Baras
Electrical and Computer Engineering
and Institute for Systems Research
University of Maryland
College Park, Maryland 20742
Email: baras@isr.umd.edu

***Abstract*— Satellites are expected to play an increasingly important role in providing broadband Internet services over long distances in an efficient manner. Future networks will be hybrid in nature - having terrestrial nodes interconnected by satellite links. Security is an important concern in such networks, since the satellite segment is susceptible to a host of attacks including eavesdropping, session hijacking and data corruption. In this paper we address the issue of securing communication in satellite networks. We describe the different kinds of hybrid network topologies considered for deployment. We discuss various security attacks that are possible in these networks, and survey the different solutions proposed to secure communications in the hybrid networks. We point out important drawbacks in the various proposed solutions, and suggest a hierarchical approach to add security to the hybrid networks.**

I. Introduction

Satellites have become increasingly important as a bridge for communications in various network scenarios. With the rapid growth of the Internet, satellite networks are being put to use to deliver Internet services to the consumers. The primary advantage of satellite networks is that a satellite can reach users in remote areas where terrestrial connectivity is not possible. Satellite networks are also easily deployed, and can be cheaper than laying ground fiber networks.

Although satellite networks show great promise, they also present significant security challenges.

- Satellite channels are wireless broadcast media, which makes it easy for an unauthorized user to eavesdrop on the communication.
- Without proper security mechanisms, any sufficiently well-equipped adversary can send spurious commands to the satellite and disrupt the communication, even take over the satellite, which is a single point of failure.
- Satellite channels can have high bit-error rates that result in packet loss, and also suffer from long propagation delays (e.g., geostationary satellites), therefore security systems should add minimal delays to the communication and have mechanisms to recover from loss in security information.

In this paper, we consider the important security issues in hybrid satellite networks that involve both terrestrial and space components. Most satellite networks are moving to IP-based routing, hence we limit ourselves to IP networks. We focus on end-to-end network layer security for commercial networks, though we also consider scientific space networks, since the security issues are similar. We do not deal with military networks, where the security approach can be significantly different. Our discussion covers both unicast and multicast (group) communication.

The rest of the paper is organized as follows. In section II we briefly describe the various types of hybrid networks in scientific and commercial use. Section III discusses some important security attacks that are possible in the hybrid networks discussed in section II. We survey the various security solutions that have been proposed in section IV, and highlight our approach in section V. We conclude the paper in section VI.

II. Hybrid Satellite Network Architectures

In the following we briefly describe the common hybrid satellite network architectures for scientific and commercial use that enable IP-based communication.

A. Scientific Space Networks

The National Aeronautics and Space Administration (NASA) has undertaken a lot of research work focussed on enabling IP support for scientific space communications. There are multiple IP network architectures being considered that involve different types of spacecraft [1]. A generic IP space network would have IP addresses assigned to all the space entities, e.g., space shuttles and satellites. The different scientific networks can be classified under *near space* networks and *deep space* networks.

One near space network architecture is the experimental setup defined by the *Operating Missions as Nodes in the Internet* (OMNI) activity from NASA [2]. The spacecraft(s) communicate via satellite to the ground stations. From the ground station the data flows over NASA's private IP network to the control center and principal investigators. The private network is protected from the open Internet using firewalls. However, some of the data might available to other users, such as collaborative scientists and educational institutions, who access the data via the open Internet.

Deep space networks require a relay of high-altitude spacecraft to transmit information from space vehicles to the earth.

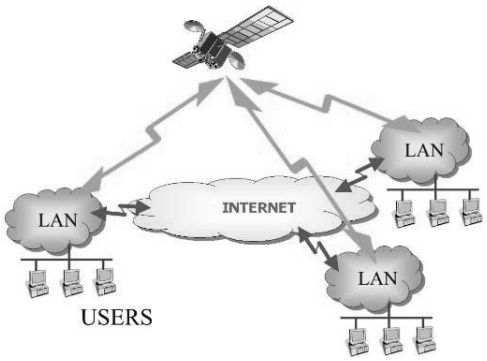


Fig. 1. Commercial Backbone Hybrid Network Topology

There would be point-to-point links between various spacecraft; the ones that are in transmission range of the ground stations would have communication with terrestrial nodes.

B. Commercial Networks

We consider two types of commercial networks - satellite Backbone networks, and satellite Direct-To-Home (DTH) networks [3]. In both topologies, we assume that there is one regional satellite in geostationary orbit that connects the users to the Internet. The satellite has multiple spotbeams covering a large geographical area. Each spotbeam covers a subset of the total user set. We assume that the satellite has an IP stack on board and is capable of on-board processing (OBP) of the data, and can switch the data between the different spotbeams that it supports. The satellite therefore acts as an *IP router-in-the-sky*. A dedicated high-speed link connects the satellite to the ground station or satellite gateway. The ground station is connected to the Network Operations/Control Center (known as NOC or NCC) through terrestrial links. The NOC is connected to the open Internet through a firewall which sits at the boundary between the closed satellite network and the open networks beyond.

In the backbone network (fig. 1), the users are located in multiple local area networks (LANs), each LAN being served by one or more satellite terminals. The satellite interconnects the different LANs. The LANs might have alternate communication paths via terrestrial links. Here the satellite offers simpler one-hop end-to-end communication.

In the DTH network topology we consider, the users can be stand alone machines, each with its own satellite terminal (fig. 2(a)). The satellite terminals have both downlink and uplink capabilities. The return channel from the user to the Internet is through the satellite uplink.

Alternatively, in the DTH topology, the users can be located in terrestrial LANs, each LAN being connected to the satellite through one or more satellite terminals (fig. 2(b)). The satellite terminals at the customer permises have both uplink and downlink capabilities. Data from the Internet is received by the satellite terminals via the satellite, and subsequently transmitted to the end users over the terrestrial LAN. The return channel from the user is via satellite uplink through the local satellite terminal. There is no terrestrial connectivity between the LANs.

The terrestrial LANs can be either static or dynamic. In the static case, the users are connected to Ethernet-based LANs as described above. In the dynamic case, the users are mobile and use wireless channels, for example cellular networks or IEEE 802.11x wireless networks to access the Internet.

Usually, in commercial satellite networks that transfer Internet traffic a split connection TCP Performance Enhancing Proxy (PEP) is implemented to reduce the negative effects of the satellite link on the Internet connection [4]. In the network topologies considered here, we assume that there is a TCP PEP at the satellite gateway that buffers the data, and provides a local acknowledgment to the remote server in the Internet. The satellite gateway is then responsible for reliably transferring the data to the peer application. To do performance optimization effectively, the satellite gateway PEP needs to have the ability to view and modify the IP and TCP packet header and possibly some of the application data. This functionality has important implications for security of the data transmission, as discussed in section IV.

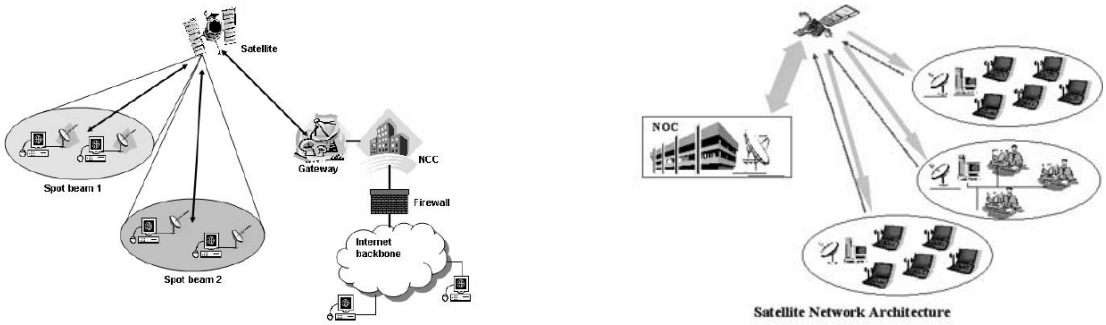
III. Security Threats

Similar security attacks can be launched against different hybrid satellite network topologies, but the impact of attacks would differ depending on the type of network, and the applications supported by the network scenario. In the following, we list some of the important security threats in the hybrid networks described above, and highlight the importance of the threats for the different network scenarios.

Confidentiality of information: For networks that require information privacy, a primary threat is unauthorized access to confidential data or eavesdropping. Since the satellite is a broadcast medium, any entity on the ground with the right equipment can receive the satellite transmission. If the data is broadcast in the clear, then adversaries who are listening to the transmission using their own equipment can be privy to the information that is flowing in the network. This can lead to loss in revenue for commerical services, or leakage of classified information for scientific or military applications.

Data confidentiality is an end-to-end requirement, therefore security measures taken to ensure privacy of communication should include the terrestrial segments of the network also. In many hybrid network scenarios, efficient solutions for data confidentiality would apply different measures to the space segment and the ground segment, and have mechanisms to integrate the two. We discuss such solutions in sections IV and V.

Data confidentiality can be achieved by message encryption. This requires coordination between the senders and the receivers so that they are concurrently aware of the correct cryptographic keys used in the encryption/decryption operations. This is a two-fold problem: the problem of selecting suitable cryptographic algorithms for doing encryption so that overall network performance is not affected, and the problem of coordinating keys between users, i.e., *key management*.



(a) Case I

(b) Case II

Fig. 2. Commercial Direct-to-Home Network Topology

Sending spurious commands: It is essential that the control of the spacecraft (e.g., the satellite) at all times be maintained by the proper control center. An adversary with the right equipment, can send spurious control and command messages to the spacecraft, making the spacecraft perform operations different from their intended use. This can disrupt legitimate operations and communication in the network, and can lead to hijacking of the session or even the actual spacecraft.

This attack can be prevented if the sources of the messages are properly authenticated by every receiver. This would require suitable mechanisms for authentication, such as digital signatures, which should be appended by the source to every message it sends. The exact algorithm used depends on the network infrastructure and node capabilities, amongst other factors. Also, the level of security required would dictate the authentication policy, for example, whether only the end users should authenticate each other, or whether authentication should happen on a per-hop basis. The latter might be needed in scenarios where the satellite should not broadcast spurious information. If the satellite authenticates the source of every message it receives, it will transmit only those messages for which source authentication happens correctly. However, verification of authentication by the satellite can lead to other attacks, as discussed later.

Message modification attack: When the traffic goes over open networks, an adversary who is listening on the path can intercept both control and data messages. The adversary can modify the messages and send them to the destination, which can be the spacecraft or the ground terminals or the end users. Here the adversary need not masquerade as a legitimate node in the network, unlike the previous attack. When the message reaches the intended destination, it would think that the corrupt message is coming from the true source, but the message content might be different from expected or required for normal network operation. This can lead to abnormal behavior of the nodes, and cripple the network.

Message modification can be prevented by appending message integrity check mechanisms to every message, for example, Message Authentication Codes (MACs) or digital signatures. Use of MACs would require that the sources and destinations share the same cryptographic keys required to generate and validate the MACs, which is a key management problem. Again, network infrastructure and node capabilities might dictate which mechanism will be used. Also, security requirements and policies can dictate whether message authentication should happen only at the communication end points, or whether intermediate nodes should also verify the integrity of every message.

Denial of service attack: Some attacks on security can be facilitated if strong security mechanisms are put in place for performing message integrity checks or authenticating users. Consider the case where the satellite does authentication and integrity check on all messages before broadcasting. An adversary can send a large number of spurious messages to the satellite, making the satellite spend significant computational cycles processing the spurious messages, which could be better spent broadcasting legitimate messages. Since the satellite has limited processing power, such an attack can be very effective, especially if strong cryptographic mechanisms such as digital signatures are used for authentication and message integrity. This is a denial of service (DOS) attack. Although this DOS attack can be launched against any node in a network, a satellite network can be particularly susceptible to such an attack since the satellite is a single point of failure and can be easily overwhelmed if made to perform too much computation. It should be noted that the primary requirement of any communication network is *availability*, and the DOS attack described above can compromise network availability.

Insider attacks: An adversary can gain access as a legitimate node in the operation of the network, possible if there is weak access control, or if the adversary is successful in password sniffing of some other legitimate node in the network. Once the adversary has access to the closed network, it can carry out a host of attacks, depending on its permission levels. At the very least, it will be able to read confidential data and can leak them to the outside. This is similar to an insider attack, and can also be carried out by a legitimate user if it turns malicious.

The steps outlined above to defend against attacks on privacy, integrity and source authentication, should normally prevent such an attack. However, if an attack is successful, then detecting the malicious node requires *intrusion detection* mechanisms that are beyond the scope of this discussion.

Traffic analysis: In some network scenarios requiring very high security, it might be necessary to make sure that no outsider can know which parties are taking part in the communication. This would require that traffic analysis of the data flowing in the network be prevented. Traffic analysis attacks are difficult to prevent even if the network is secured for data confidentiality and data integrity and source authentication. An adversary only needs to "sniff" the packet headers for the source and destination information to do successful traffic analysis. This can be prevented by additional mechanisms, such as masking the actual source/destination headers, etc.

IV. Proposed Security Approaches for Satellite Networks

Significant research has been done on secure communication in general, some of which can be applied to satellite networks. More recently, there have been several proposals to secure communication specifically in satellite networks. In this section we discuss in brief the various proposals that have been made for satellite networks. Discussion of general security issues as applied to satellite networks can be found in [5].

Research on satellite security in the academia and industry has focussed on using existing, standardized technology originally designed for terrestrial networks, to fix well-known security holes in satellite networks. Several proposals for data confidentiality and authentication in satellite networks call for use of the Internet Security Protocol, IPSEC [6], which has been widely adopted by the Internet Engineering Task Force (IETF) for security at the network layer. IPSEC has two variants: the Authentication Header (AH) [7], which provides integrity protection to data packets, and the Encapsulating Security Payload (ESP) [8] that provides encryption and optional integrity protection. Use of IPSEC requires establishment of a *Security Association* (SA) between the source and destination end points. The SA specifies the various security attributes for the particular session, such as the cryptographic algorithms to be used, the session keys for performing cryptographic operations on the data, etc. IPSEC AH adds an authentication header to each data packet, which can be verified only at the end points, since the intermediate nodes do not know the session key for the SA between the end points. IPSEC AH does not provide data privacy. IPSEC ESP provides data confidentiality, and it can also provide for authentication in the "tunnel" mode of operation. Before either IPSEC AH or ESP can be used, the SA has to be established, which is done using the Internet Key Exchange (IKE) protocol [9]. IKE requires the end points to have some *pre-shared* secret or public key pairs, for the key exchange to be initiated.

IPSEC provides strong security for data confidentiality and authentication, but it has a heavy byte overhead - in the ESP mode, IPSEC adds 10 bytes overhead to every data packet. NASA and its allied agencies have proposed a variant of IPSEC, called the Space Communications Protocol Specification - Security Protocol (SCPS-SP) [10] to be used for data confidentiality and authentication in space missions. SCPS-SP adds 2 bytes of overhead per IP packet. The NASA publication [11] discusses various security issues for space missions. It recommends use of SCPS-SP for encryption on the space segment, and IPSEC ESP on the ground segment, where the nodes are expected to have more resources and bandwidth is less constrained. The report describes the requirement for, and the design of, a SCPS gateway to interoperate the SCPS-SP protocol with the IPSEC protocol The report also recommends the use of a lightweight version of IKE for key establishment that offers less overhead. The recommendations of [11] are specifically for unicast communications for civilian or scientific space networks. They do not address many security problems, such as securing communication amongst groups, or authentication of different users in the group.

Although IPSEC has been considered favorably by the space community, it can be used only for point-to-point communication; it does not support security for group communication. IPSEC also does not allow for authentication at intermediate nodes, as mentioned earlier, but this might be useful in some security situations. Establishment of SAs using IKE can be complex and expensive. If network entities do not have pre-shared secrets, then IKE requires public key pairs, which means a public key infrastructure will be needed. This brings into question infrastructural issues related to the use of Certificate Authority (CA) for public key management. Public key cryptography involves heavy computation for signature generation and verification, and the keys can be large in size, so nodes will need to have sufficient processing power and storage. This can be a serious issue if the satellite is one of the end points in the communication. IKE requires an elaborate "handshaking" mechanism to set up the SA between two endpoints, based on which the secure channel between the endpoints is established. This requires a minimum of 3 messages exchanged between the endpoints (in the *aggressive* mode of IPSEC), and can require a 6-message exchange in the *main* mode of IPSEC. The overhead due to the message transmission over high-delay satellite links is not insignificant.

Another widely-researched problem with using IPSEC in satellite networks is its inability to co-exist with PEPs. In ESP mode, IPSEC encrypts the full IP payload.The TCP header is encrypted as part of the payload, and only the end points who know the encryption key, can recover it. A PEP, which is an intermediate node on the path, will not be able to read the encrypted TCP header and therefore cannot apply its TCP performance improvement mechanisms on the message stream. This can lead to significant performance degradation.

Two solutions using gateways located at different points in the network, to overcome the drawbacks of implementing IPSEC in the hybrid environment, have been proposed in [4]. One is to use a secure gateway and an enhanced gateway at each end of the link. The enhanced gateway proxies the TCP sessions to add TCP performance optimizations such as large

windows, large buffers and modified TCP start algorithms. The data is subsequently secured by the secure gateway. This is preferable for users who want direct control over network performance and security, and are unwilling to trust intermediate nodes. But this leads to performance problems in the event of transmission errors, and can be expensive to implement on a per-user basis. The second solution is to split the secure connection into two at the satellite gateway, which would be responsible for packet decryption and re-encryption. This creates two secure connections, and require placing trust on the satellite gateway, which would usually be a third party node outside direct control of the end users initiating the secure channel.

The problem arising in the performance of TCP PEPs due to use of IPSEC has also been addressed by splitting IPSEC into *layers*, which has been proposed independently by Zhang [12] and Karir et al. [13]. We describe Zhang's solution, which is the Multilayer IP-security protocol (ML-IPSEC). ML-IPSEC is modeled on IPSEC and the two have most features similar so that the use of ML-IPSEC in an IPSEC environment can be achieved with minimal changes. The crucial difference is that ML-IPSEC breaks an IP datagram into multiple *security zones*, with cryptographic operations being performed with different keys in different zones. The TCP payload is a different security zone from the TCP header, and encrypted with a different key. The key for encryption of the TCP payload is shared only by the end parties, so that no intermediate entity in the path can read the data. But the key for encrypting the TCP header is shared with trusted intermediate nodes, such as the gateway PEP, so that the PEP can decrypt the TCP header and do performance optimizations. Use of ML-IPSEC requires that the security attributes be distributed correctly to all the relevant entities - this is done by defining a new type of security association called *Composite Security Association* (CSA). CSA is a collection of SAs that collectively afford a multilayer security protection for the traffic stream. The author contends that ML-IPSEC can be used in place of IPSEC without significant performance penalties, whereas it helps improve performance overall by allowing TCP PEP to function effectively. However, the design specification does not mention clearly how to establish the CSAs between the different entities. This would be a complex task, since here more entities than merely the endpoints are involved, and the security functions allowed to the different entities are different. Also, ML-IPSEC requires trust in third parties like the satellite gateways. Moreover, ML-IPSEC, as envisioned currently, is strictly for point-to-point communication and has no support for groups.

Another problem arises with application level optimizations that do not work in the presence of network level security. Although our focus is security at the network level, this problem is important enough to merit mention. Satellite networks employ application level proxies to further enhance performance. For example, if HTTP is used as the application layer protocol, then an HTTP proxy would pre-fetch and cache all the webpages whose links are embedded in the webpage

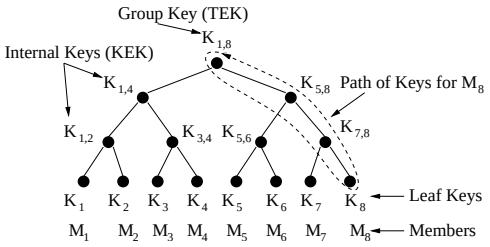


Fig. 3. Logical Key Hierarchy with 8 members

originally requested by the user. Use of IPSEC or layered IPSEC completely breaks the functionality of the HTTP proxy, since the the HTTP information is encrypted in the TCP payload and is therefore inaccessible to the HTTP proxy.

The previous paragraphs dealt with the application of standardized security protocols to hybrid networks. Some research has been done with individual algorithms that serve as tools in building the security protocols, for example, key management algorithms. Howarth et al. [14] have addressed the problem of key management for group communication in satellite networks. The paper proposes the use of Logical Key Hierarchy (LKH) [15], [16] for efficient key management for multicast groups in a satellite network. LKH makes use of a centralized key manager or group controller (GC), which constructs a logical key tree with the group members as the leaves of the tree (fig. 3). The internal nodes of the tree are the *key encrypting keys* (KEK) which are used to securely transport key updates to the group. The root of the tree is the session key or traffic encrypting key (TEK) which is used to encrypt the session traffic. The key corresponding to a leaf node is the long-term secret that the corresponding member shares with the GC. A leaf node knows all the keys on the path from its leaf to the root, and no other. The number of keys that need to be updated when a member node joins or leaves the group is $O(logN)$ (where N is the number of members in the group), which is less than the $O(N)$ keys required if the GC arranged the members in a flat topology.

To allow PEPs to function correctly when network layer security is used, [14] proposes use of ML-IPSEC. The paper proposes using a single LKH tree to manage the group key $K1$ used to encrypt the transport layer header (known to end users and trusted gateways), and the group key $K2$, known only to the end users and used for encrypting the transport layer data. As shown in fig. 4, users $M_1..M_8$ are leaf nodes in a subtree of degree 3, and gateways $G_1..G_4$ are leaf nodes in a subtree of degree 2. The root key of the member node subtree, $K_{1,8}$, is used to encrypt the transport payload. The root of the overall key tree, $K_{1,12}$, is used to encrypt the transport header. All member nodes know both $K_{1,8}$ and $K_{1,12}$, but the gateways know $K_{1,12}$ only (apart from the internal keys in the gateway subtree).

Ref. [14] does not say how the LKH tree would be managed. This is important since the users and the gateways might not be in the same administrative or security domain. The paper also considers all users and gateways as a "flat" network

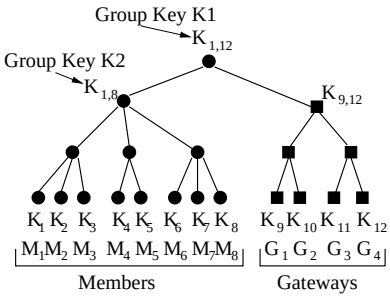


Fig. 4. ML-IPSEC Integrated LKH Tree with Users and Gateways.

for key distribution purposes, rather than take into account the hierarchical nature of the network topology, where the end users might be located in LANs or subnetworks, a level "below" the satellite *overlay* network comprising the gateways and the satellite, and therefore might be invisible to the key tree manager.

The use of LKH for key management in satellite links has also been proposed by [17], which suggests algorithms for dynamically managing the LKH tree in case of member joins and leaves.

Duquerroy et al. [18] has proposed a solution, called "SatIPSec", for key distribution and secure communication for both unicast and multicast in a satellite network. The paper describes a testbed implementation of the proposed solution (one of the very few in satellite network security that goes beyond simulation analysis). The solution is based on IPSEC, with additions to support key management for group communication. To support secure group communication, it proposes the Flat Multicast Key Exchange (FMKE) protocol. Management of SAs for both unicast and multicast communication is integrated into the FMKE protocol, though the proposed approach for unicast communication is not different from IPSEC. FMKE also incorporates reliability mechanisms to guarantee reliable key distribution in the lossy satellite setting. However, FMKE manages SAs between the satellite terminals or gateways only and does not extend to the end users. Therefore, end-to-end security is not provided when using SatIPSec. Also, FMKE treats all the satellite terminals it services (which are called SatIPSec clients) in a "flat" topology, and establishes separate secure channels to all SatIPSec clients. This will not scale when there are a large number of clients. Such scalability issues have not been considered in the paper, but they are very important in laying out a network solution. SatIPSec also does not consider dynamic joins and leaves of members in the group communication setting; a client needs to be pre-authorized for all the groups it wants to take part in. The protocol also requires complete trust in the group controller and key server (GCKS), which is a third party that is responsible for managing the SAs between the clients. All clients need to have pre-shared secrets with the GCKS.

In the following section, we describe the approach that we have taken to secure communication in hybrid networks, and highlight work we have done, and current research activity.

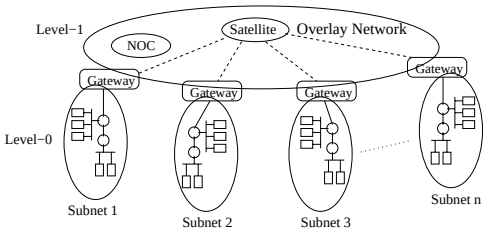


Fig. 5. Hierarchy in the Hybrid Topology

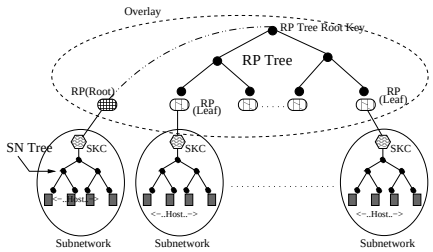


Fig. 6. Tiered Tree Key Management

V. A Hierarchical Approach to Security in Hybrid Networks

We have proposed a key management framework for secure group communication in hybrid satellite networks in [5]. The objective is to ensure data confidentiality, which requires that cryptographic keys be distributed securely and in a scalable manner to all members in a group. The key management framework is built on top of the routing architecture. We have considered the hybrid network topology of fig. 2(b), and designed a multicast routing architecture to allow users to communicate seamlessly between multiple terrestrial LANs (also referred to as subnetworks). Our design makes specific use of Asynchronous Transfer Mode (ATM) point-to-multipoint routing [19] over the satellite links, and Protocol Independent Multicast - Sparse Mode (PIM-SM) multicast routing [20] in the terrestrial LANs. However, the solution can be easily extended to a more generic framework where ATM is not used, which is a focus of ongoing research activity.

In our solution, we make use of the hierarchical nature of the network topology. We divide the network into two levels, the lower level of the terrestrial LANs where the users are located, and a higher level comprising the satellite gateways (called *Rendezvous Point* or RP in our architecture), the satellite and the NOC, which together form an overlay (fig. 5). Key management is done separately at the two levels. Each LAN has its own group controller (called the "subnetwork key controller" or SKC) to manage the keys for all groups active in the LAN. The overlay has its own key management, which is managed by the satellite gateway of the LAN that has been active for the longest continuous period in the group. The key management at each level is based on the LKH algorithm, therefore our solution creates a hierarchy of trees, the *SN Tree* at the subnetwork level, and the *RP Tree* at the satellite overlay level. We term the framework, Tiered Tree-based Key Management (fig. 6).

The detailed design and experimental results can be found in [5]. The solution is scalable and acknowledges the fact that the users might be located in different security domains, therefore a single network-wide security management might not be possible. This is a more realistic scenario, since the terrestrial LANs might be individual company domains, while the satellite overlay infrastructure is usually owned by a separate entity that provides network connectivity to the LANs, and is not responsible for generating the network traffic. The framework addresses the problem that all users might not be visible to a single, centralized security authority, and the dynamics of user joins or leaves in one LAN should not create an overhead to users in other LANs. Also, in the wide area satellite networks we consider, the satellite channel conditions at a given point in time might be different in different sections of the network. There might be loss in information due to bad channel conditions in some network segments; this will not disrupt communication in network segments where the channel conditions are better. Solutions which treat all users in a single tree will not be able to perform as robustly under such conditions. Our solution is also similar to the ML-IPSEC concept in that the satellite terminals are only partially trusted; they are allowed to do partial decryption/encryption of the IP packets for efficient routing. However, it is a generic solution aimed specifically at multicast key management and does not deal with an end-to-end security solution for secure communication or give any implementation specifics.

We are continuing our research on the security issues outlined in the previous sections, with a hierarchical view of the network. We are looking at efficient ways to integrate our solution with the SatIPSec protocol to provide a scalable and implementable security protocol for hybrid networks. This will also allow us to extend our key management to the unicast case. Since the work of Howarth et al. [14] has similarities to our approach, we are re-investigating their proposal to add support for layered encryption in a hierarchical framework. The results of our research efforts in the above areas is the subject of a future paper. It is to be noted that our solution does not address the question of user authentication or message integrity. Integration of our proposal with SatIPSec will automatically provide both due to the authentication features of IPSEC. However, this might not be an efficient solution since it requires public key cryptography. We are looking at other approaches to these problems, based on symmetric key cryptography.

VI. Conclusion

In this paper we have focussed attention on the issue of security in hybrid IP-based satellite networks. We have described the unique characteristics of hybrid satellite networks that makes the challenge of secure communication different from purely terrestrial networks. We have described the different topologies that are predominant in the scientific and commercial space, and detailed the important security issues in such networks. We have done a comprehensive survey of the various security solutions that have been proposed, and mentioned their advantages and disadvantages. Lastly, we have laid out our hierarchical approach to security in the hybrid networks, and highlighted some of the work we have done, and also our current research focus. We believe the security problems discussed here will receive more treatment from the research community, and this work will be a useful contribution to the field.

References

[1] “”Implementation Guide for the Use of the Internet Protocol Suite in Space Mission Communications”,” National Aeronautics and Space Administration - Goddard Space Flight Center, Greenbelt, MD, USA, Tech. Rep., September 2003.

[2] “”Operating Missions as Nodes on the Internet (OMNI)”,” http://ipinspace.gsfc.nasa.gov/documents/, February 2000.

[3] G. Akkor, M. Hadjitheodosiou, and J. S. Baras, “”Transport protocols in multicast via satellite”,” *International Journal of Satellite Communications and Networking*, 2004, to appear.

[4] E. Olechna, P. Feighery, and S. Hryckiewicz, “”Virtual Private Network Issues Using Satellite Based Networks”,” in *Military Communications Conference (MILCOM) 2001*, vol. 2, 2001, pp. 785–789.

[5] A. Roy-Chowdhury, “”IP Routing and Key Management for Secure Multicast in Satellite ATM Networks”,” Master’s thesis, University of Maryland College Park, http://techreports.isr.umd.edu/ARCHIVE/searchResults.php?searchString=A%yan\%20Roy-Chowdhury, 2003.

[6] R. Atkinson and S. Kent, *”Security Architecture for the Internet Protocol”*, IETF RFC 2401, November 1998.

[7] ——, *”IP Authentication Header”*, IETF RFC 2402, November 1998.

[8] ——, *”IP Encapsulating Security Payload (ESP)”*, IETF RFC 2406, November 1998.

[9] D. Harkins and D. Carrel, *”The Internet Key Exchange (IKE)”*, IETF RFC 2409, November 1998.

[10] “”Space Communications Protocol Specification (SCPS) - Security Protocol (SCPS-SP)”,” National Aeronautics and Space Administration - CCSDS Secretariat, Washington DC, USA, Tech. Rep. CCSDS 713.5-B-1, May 1999.

[11] “”Next Generation Space Internet (NGSI) - End-to-End Security for Space Mission Communications”,” National Aeronautics and Space Administration - CCSDS Secretariat - Office of Space Communication, Mantera, Italy, Tech. Rep. CCSDS 733.5-O-1, April 2003.

[12] Y. Zhang, “”A Multilayer IP Security Protocol for TCP Performance Enhancement in Wireless Networks”,” *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 4, pp. 767–776, May 2004.

[13] M. Karir and J. Baras, “”LES: Layered Encryption Security”,” in *Proceedings of the Third International Conference on Networking (ICN’04)*, Guadeloupe, French Caribbean, March 2004.

[14] 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, February 2004.

[15] C. Wong, M. Gouda, and S. S. Lam, “”Secure Group Communications using Key Graphs”,” *IEEE/ACM Transactions on Networking*, vol. 8, pp. 16–30, February 2000.

[16] D. Wallner, E. Harder, and R. Agee, *”Key Management for Multicast: Issues and Architectures”*, IETF RFC 2627, http://www.apps.ietf.org/rfc/rfc2627.html, June 1999.

[17] G. Noubir and L. von Allmen, “”Security Issues in Internet Protocols over Satellite Links”,” in *Proceedings of the IEEE Vehicular Technology Conference (VTC 99)*. Amsterdam, Netherlands: IEEE, 1999.

[18] L. Duquerroy, S. Josset, O. Alphand, P. Berthou, and T. Gayraud, “”SatIPSec: an optimized solution for securing multicast and unicast satellite transmissions”,” in *22nd AIAA International Communications Satellite Systems Conference and Exhibit 2004*, no. AIAA-2004-3177, Monterey, California, 9-12 May 2004.

[19] G. Armitage, *”Support for Multicast over UNI 3.0/3.1 based ATM Networks”*, Internet RFC 2022, November 1996.

[20] S. Deering, D. Estrin, D. Farinacci, V. Jacobson, C.-G. Liu, and L. Wei, “”The PIM Architecture for Wide-Area Multicast Routing”,” *IEEE/ACM Transactions on Networking*, vol. 4, no. 2, pp. 153–162, April 1996.