Protection of the European Space Infrastructure

IST Project SatNEx JA2350 Network Security and Management

Frank Hermanns
Institute of Communications and Navigation,
German Aerospace Center (DLR), 82230 Wessling, D
Email: frank.hermanns@dlr.de

Dr. Haitham S. Cruickshank and Sunil Iyengar
Centre for Communication Systems Research (CCSR),
University of Surrey, Guildford, Surrey GU2 7XH, UK
Email: H.Cruickshank@surrey.ac.uk, S.Iyengar@surrey.ac.uk

***Abstract*— This paper comes from the joint activity JA2350 "Network Management and Security" of the SatNEx IST project. A major aim of the Satellite Network of Excellence (SatNEx) is to rectify the fragmentation in satellite communications research by bringing together leading European academic research organisations in a durable way. Especially the security research suffers from a great fragmentation within Europe, with strong national focus of individual member states. For a European Homeland Security program similar to the US counterpart, cooperation and coordination in research and industry is essential. The protection of the space infrastructure is a big challenge that can only be done in a large European effort. Major problems and possible future research directions are shown in the paper.**

I. Introduction

The European Union becomes more and more dependent on Satellite Communications. Similar to the ideas of the American Homeland Security, Europe also needs to protect its critical infrastructure, of which Space is a valuable part. Not only Communication satellites but also human spaceflight, rocket telecommanding and other missions are very critical. For Pay-TV broadcasting, security problems cause massive financial losses to the providers. Private and business users expect secure transmission of their data.

II. Critical Space Infrastructures - Threats and Countermeasures

Spacecrafts are in an exposed and vulnerable position. They are easy to kill, easy to jam and easy to eavesdrop. No simple armouring can protect them; they are not hidden in ground like terrestrial networks. Signals are transmitted over wide areas up to continental size. Dedicated security techniques are therefore necessary. With the evolution of personal satellite communications, attacks could increase drastically like in the Internet today. Security considerations, computer viruses, hacker attacks, theft of passwords, financial fraud became part of our civil life. Satellite communication protocols should avoid many problems by taking security considerations seriously during the whole research and development process.

As the European economy relies more and more on a functional space segment, satellite TV, satellite navigation and communications, the protection of the space infrastructure should play an important role in European research. Generally, attacks on the space infrastructure can be divided into two main categories:

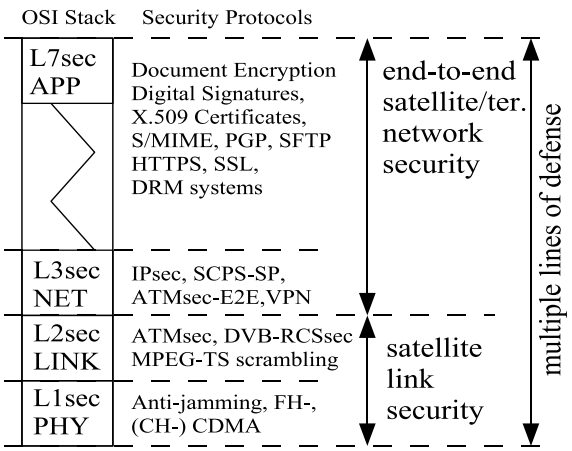

Fig. 1. Satcom Security vs. OSI layers

Physical threats with ASAT (anti-satellite weapons):

- *Kinetic kill vehicles*: Simply rockets that destroy a specific satellite by collision and explosion. Developed during the cold war time by the US and USSR. No reasonable defence against this brute force is possible.
- *Nuclear warheads in Space*: Satellites are killed by the strong electromagnetic pulse (EMP). The "Outer Space Treaty" of 1967 banned the use of nuclear weapons in space.
- *High energy Lasers*: In GEO orbit, the thermal effect of ground-based lasers is not strong any more. But in 400km LEO orbits, military Megawatt lasers could possibly damage a satellite.
- *Microwave guns*: High-power microwave (HPM) weapons currently reach Gigawatt pulses [1]. While there is sufficient free-space loss to protect GEO-satellites, LEO and MEO satellites might be in danger. Microwaves cause electromagnetic interference with the inner electronic circuits.

Satellite Hacking

- *Denial of Service (DoS) attacks*: Misusing protocols and service processing in a way that prevents a system from performing normal operations. Flooding communication systems with control messages that cause an overload (e.g. TCP SYN flood). Or in a Distributed-DoS (DDoS) fashion to infect millions of computers with viruses that simultaneously attack a victim system by command.
- *Stealing bandwidth from other users*: A user or hacker is taking over bandwidth that belongs to other users. I.e. in Wireless LAN by cheating the WLAN MAC protocol, one user can take over the full bandwidth in the radio cell, kicking out all other users. Satcom systems should be designed to protect against this threat.
- *Misusing satellite capacity for propaganda*: TV and Radio broadcasting satellites might in future be a prime target for rebel groups to be misused as a propaganda platform. By using the same channels as popular national broadcasting programmes, a huge population can be reached this way. [2]
- *Signal jamming*: Jamming of satellite signals is a traditional threat in a military scenario. But nowadays when satellites are used for personal communications, also hackers could use jamming techniques. No huge ground station antennas are needed any more. Attackers can use the same small antenna as regular mobile satcom users. Uncorrelated noisy signals (broadband jammer) or coded signals for maximum efficiency can be used. In the evolution of jamming, more intelligent methods appear, such as DoS-Attacks.
- *Breaking security codes*: No code except the one-time-pad is provable secure. Although modern symmetric and asymmetric codes are very strong, the race between cryptographers and cryptanalysts is going on. Continuously we hear reports about broken codes. It is not always published. Even worse, to trust a code that the enemy is able to read (e.g. the Enigma in WW-II). Often it is not necessary to break the code itself, when there are vulnerabilities in the usage and in the protocols.

- *Modification of signals (manipulation)*: To modify the downlink signal, the attacker needs to be in a relatively close radius of the receiver. The uplink signal can be disturbed in the whole spot beam area. A hacker can choose very remote or crowded places for his attack, very hard to localize. Manipulation is the problem of data integrity and sender authenticity. Dedicated manipulation-resistant communication protocols are needed for the various services of satellite communication.
- *Interception and eavesdropping of communications*: This is an important topic for satellite communications, because they use spot-beams of up to continental size. The hurdle to set up a dish somewhere in Europe is much lower than to dig for glass fibre cables and intercept terrestrial communication lines. It is known that national intelligence agencies are continuously listening into foreign satellite communications. Placing interception devices in terrestrial networks of foreign countries is not so easy. Next to espionage from big organization, also single hackers or groups are listening into other people's communications. Passwords and credit card details have a high value. Also industrial secrets are sold. [3] has shown that eavesdropping is a hot topic in current DVB-S Internet services.
- *Traffic analysis*: The process of intercepting and examining messages in order to deduce information from patterns in communication. The message content itself is not affected, so even encrypted communications can be vulnerable to traffic analysis. Interesting parameters are size, timing, origin and destination address of a data packet. Especially the information about who is communicating with whom has to be protected. End-to-end security schemes cannot hide these addresses as they are required for routing. Additional link-layer security helps to avoid these attacks. For terrestrial cables, traffic analysis is less important, but personal satellite communications due to its broadcasting nature needs this protection.
- *Masquerade (Impersonation)*: This is in principle the problem of authentication. By breaking into the communication protocol or stealing passwords and credentials, someone could imitate legitimate users. He could use paid services on foreign accounts, bank accounts, foreign email addresses, sign contracts under foreign name ... To minimize fraud, the security model should include the human user and not only the communication system. Biometric features or smartcards with PIN could serve as prove that the legitimate user was interacting with the communication system.
- *Repudiation by a party*: Repudiation of origin occurs when a party denies being the originator of a message. Repudiation of destination occurs when a party denies the reception of a message. Both are very critical for voting, digital signing, paid services and electronic trade. Next to authenticity and integrity, also secure acknowledgements have to be implemented.
- *Placing backdoors in communication systems*: A tricky method to get control over systems is to place a backdoor, either in the system design or later by a virus or network intrusion. For third-party software, there can be no guarantee that nobody placed a backdoor, especially when there is no source-code to verify. History had shown that companies intentionally introduced a so-called "work factor reduction" that reduced the effective cryptographic key size to a vulnerable minimum. This backdoor is not immediately visible, but has a great influence on the statistics for cryptanalytic attacks. Even open-source programmers might introduce backdoors. The code is public and can theoretically be verified by anybody. But quite often, only a few programmers really do it. A total provable security usually does not exist. Furthermore, not many people are able to verify cryptographic algorithms and even experts do not necessarily find all bugs. So, there will always be an uncertainty about this. Multiple layers with security protocols from independent vendors reduce the risk of such compromises.
- *Operating system and other software bugs*: The most prominent bug is a "buffer overflow". If the software does not check the size of certain parameters, data fields can overflow and overwrite memory segments for executable code. This can happen in communication protocols or in document handling. Both can be used for gaining remote control over systems. Only by opening "infected" documents like Word, PDF, Video or Music files the machine gets compromised. Also server processes often have those vulnerabilities.

The security of satellite communications has one more important aspect, the operator-to-satellite link. Losing control over a satellite is disastrous. In terrestrial installations it is possible to repair, to exchange modules, to clean up software after hacking. But for a satellite, the link for telemetry, telecommand and control is unique. Repair missions can only be economic for very special installations like the Hubble space telescope. All other satellites are simply lost when there can be no communication any more. So, this link is the most valuable and needs the best possible security architecture. Only one trade-off with availability is needed: security protocols should not block the legitimate operator from accessing the system. This can reduce security strength in parts that have a potential to cause failure of communication. The Consultative Committee for Space Data Systems (CCSDS) defined a set of protocols for space communications. While the Transport Protocol SCPS-TP has a high reputation for broadband Internet connection over stressed space links, it is often recommended to use IPSec instead of the CCSDS Security Protocol SCPS-SP [4].

A. Broadcast Satellites

In July 2002, the SpaceDaily service [2] had a shocking headline "Beijing Alleges Falun Gong Hijacked Chinese TV Sat During World Cup". The satellite was called an "orbiting propaganda machine". Television signals illegally broadcast by the Falun Gong cult cut into transmissions using the Sino Satellite (SINOSAT) from June 23 to 30, blocking the World Cup finals for viewers in some rural and remote areas in China ... But that was not the first event of that type. The satellite broadcast in China was manipulated several times [5]. Other hacker successes were not published by the satellite owners, especially not the attacks on the telecommand and control link.

One important lesson learnt here is that in future, broadcast satellites should be able to verify the integrity of the programme and authenticity of the ground stations before transmitting unwanted propaganda over a whole continent to millions of spectators. Even if the content is public, security considerations are necessary. As most broadcast satellites are only bent-pipe systems today, the verification procedures are very difficult. With future on-board processing, the data is decoded anyway with an option to check digital cryptographic signatures. Ground stations and other media uplink facilities would need cryptographic certificates (like X.509) that are issued by a trust centre. The satellite would reject all media streams from stations that are not in the trust path. This is not yet standardized, but technically possible as an upgrade to the DVB-S/S2 system.

Broadcast for closed user groups (Pay-TV) is another topic. Up to now, all analogous and digital scrambling systems are compromised. A great share of Pay-TV spectators was watching streams illegally. Recent scrambling system upgrades reduced their number, but Pay-TV can still not be called secure. A main disadvantage here is the lack of a return channel. With a possibility to interact with spectators, Pay-TV security could be greatly increased. Subscriptions would be more dynamic and key-exchange procedures would be more individual and thus more secure. With tamper-resistant public/private key cryptographic smartcards and bi-directional communications, modern multicast security schemes are possible.

B. Communication Satellites

Satellites for personal and corporate communications have to protect the privacy of its users. That is not always guaranteed. The German Ruhr-University Bochum discovered private EC card details from customers of T-DSL via Satellite. [3] They were broadcasted

in DVB-S clear text IP packets over Europe. The Problem was a systematic difficulty between Proxies, PEP/TCP-Split and partial secured IPSec-VPN traffic.

The application layer would ideally protect sensitive confidential and financial data. With strong cryptography, this gives most security for the end-users. Especially on multi-user machines, user-specific smartcards and keys are needed to provide a good security. However, quite often applications do not offer security. Ideally, passwords have to be entered in HTTPS-protected forms, but sometimes they are just transmitted in the HTTP plaintext. Like credit card details, account numbers, social security numbers and personal messages ... And more than 99% of the Email today is not encrypted in the application layer. Email between the mail transfer agents is still forwarded by the old SMTP ASCII format. To close all those leaks, other security layers are necessary. Transport layer encryption (TLS) and network layer encryption (IPSec) are rarely used. HTTPS has a problem when the user does not check the server fingerprint. It was demonstrated, that with DNS spoofing, people delivered their banking secrets to a hacker server that had the same name as the bank website.

C. Military Satellites and Aircraft

Military satellites and aircraft communication have even higher demands in security. Up to now, they are still vulnerable in many aspects. This is a critical situation as human lives are involved in case of failures and manipulations.

The strong division between military and civil satellite communications is obsolete. Most of the security issues are common to these two worlds. Civil Hackers may have the same capabilities as military enemies. Civil targets become more and more interesting for military and terrorist adversaries. As a consequence, dual-use should be more enforced in European research and development

Another aspect is the long tradition and leadership of military security technologies. CDMA and spread spectrum was a military technology before it became attractive for civil use. Public key cryptography was used in intelligence, military and diplomatic communications before it came to our everyday life in secure financial applications and digital signatures. So, it remains attractive for the civil world to learn from military in the design of secure systems. The most economic way is to design dual-use systems that are suitable for both military and civil applications.

Hot topics for military and civil communications are unmanned vehicles (UAV). They are very demanding for security, availability and reliability of the data link. Jamming attacks could be catastrophic.

D. Human Spaceflight, the ISS

Human spaceflight is a very demanding task for communication networks. Up to now, the Tracking and Data Relay Satellite System (TDRSS) relay network provides only narrow-band uplink channels to the International Space Station ISS. Aim of the German MEDIS project [6] was to provide a bi-directional 155 MBit/s ATM broadband link for the European Columbus ISS module. Two MEO satellites with optical intersatellite links (ISL) should serve as orbiting ATM switches between the ISS and several ground stations. Security was a major concern in this space based multimedia network. A hybrid ATMsec/IPSec solution was developed at DLR for the MEDIS network. Some applications need ATM and ATMsec, because IP could not guarantee sufficient performance and timing requirements (e.g. CBR, packet jitter). The International Space Station would be a prominent target for hackers and terrorists. So, multiple lines of defence are needed for security on all communication layers and minimal risk of intrusion.

Spaceflight with the Russian Sojus or the American Space Shuttle need perfect safe and secure communications. Already failures of small elements can result in a big disaster. Up to now, no hacker attacks on manned space missions are known, but they might occur in future. Preventive security measures for the communication links have to be designed now. Such missions deploy very special hardware and network technologies. Standard security protocols and procedures have to be adapted.

E. Aircraft and Spacecraft Navigation

Satellite navigation becomes more important for aircrafts and spacecrafts. Aircrafts still rely on Radar and terrestrial radio navigation. But in future, satellite navigation systems like Galileo, Glonass and GPS may become the primary system. To increase integrity, accuracy and availability, additional augmentation systems like the European EGNOS are essential for aircraft navigation. Even spacecraft can use satellite navigation.

Security in the context of satellite navigation is rarely mentioned. In military conflicts, GPS jammers have proven to be effective in a wide radius. Even though military spreading codes are kept secret, security issues remain. Knowing the satellite spreading code, the jamming efficiency can be much higher than just disturbing the GPS frequency band with noise. In a worst case, the attacker would imitate a navigation satellite and introduce false positioning information into victim receivers. That can be fatal for aircraft and spacecraft. Hackers and terrorists would have an easy target. New security schemes have to be developed to secure navigation systems.

Integrated navigation and communication systems will have a great future. Satellite navigation information can be verified with securely transmitted radar data from ground. Digital signatures from satellites can be checked on a public key infrastructure (PKI) with certificates (like X.509). Satellite operators may serve as PKI trust centres.

III. Multiple Lines of Defence - Security in Multiple OSI Layers

Designing secure codes and breaking them is a continuous game. Almost all codes and protocols have been broken in history. Only the one-time-pad has a mathematical prove of perfectness, but is not practicable for a wide usage. With the grow of complexity in protocols and systems, no complete verification is possible any more. Many vulnerabilities are found later. Prominent security failures are: Pay-TV scrambling systems, WirelessLAN WEP, GSM encryption codes, DES, Office document encryption, smart cards, OpenPGP keyring, ...

Relying on one "secure" encryption system alone is not sufficient. Similar to aircraft control systems, multiple redundancies are essential against failures. To defend against the whole spectrum of attacks, security measures should be taken in multiple OSI layers. With these multiple lines of defence (Fig. 2), the risk of a successful attack on the user data can be minimized.

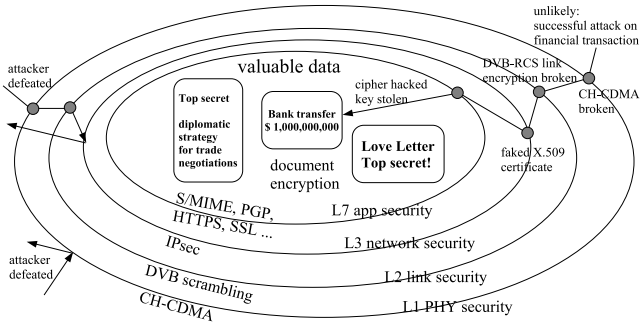

Fig. 2. Multiple lines of defence to protect satellite communications

A. Security Layers

Fig. 1 shows an overview of several security layers vs. the OSI stack. While the end-to-end security is very similar to the terrestrial architecture, the satellite link security uses satellite-specific protocols. Nevertheless, all the multiple lines of defence have to be seen as a whole. Major advantages and disadvantages are listed in Table I.

B. Physical Layer Security

Today, no special effort is done in civil satellite communications to secure the transmission on the physical layer. Even "secure" CDMA systems in military communications are using vulnerable linear feedback shift register (LFSR) generators to create the spreading

	Physical layer	Link layer	Network Layer	Transport Layer	Application Layer
Major advantages	Protects against jamming and interception, additional line of defence	Complete control of satellite link security, protects the most vulnerable wireless part	IPSec is the best solution for Internet security. End-to-end (host-to-host) security	Widely used for securing TCP connections, no need to modify the unsecured IP-networks	Can satisfy applications requirement very well. User-specific keys for documents
Major disadvantages	Not real crypto, complexity, synchronization issues	Only the satellite hop is secure, not end-to-end	IPSec works only for IP networks, not user-to-user, PEP / IPSec incompatibility	No security for UDP and multicast, applications have to be modified for TLS	No transparency, where applications need modification to fit security

TABLE I
SECURITY LAYERS COMPARISON

sequences. According to [7], the hidden 42-bit LFSR mask value of IS-95 mobile phone communications can be revealed in about 1 second of interception. The argument of CDMA-based "voice privacy" in IS-95 is weakened by this. Once knowing the PRNG seed values, also jamming becomes much easier and all the antijamming gain of CDMA is lost when the jammer is using the coded signal. When talking about SS/CDMA based security, the basic assumption usually is (from [8], p.139):

> "The jammer has complete knowledge of the spread-spectrum system design except he does not have the key to the pseudorandom sequence generators."

This static key, however, can be acquired by cryptanalysis or by theft of satcom devices. Nobody can really rely on this assumption. To exploit the power of CDMA for antijamming and low probability of intercept, flexible waveforms with dynamic spreading codes have to be developed [9]. A system architecture is shown in Fig. 3.

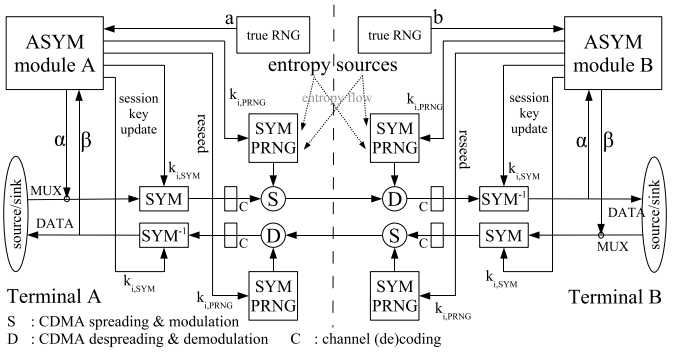

Fig. 3. System Architecture for secure flexible-waveform Code-Hopping-CDMA (DLR IKN, [9])

The main difference to traditional CDMA systems is the dynamization of secure pseudonoise spreading code generators by true random sources of entropy. That makes the actual spreading sequence unpredictable, but can still be synchronized by cryptographic means (asymmetric public key blocks). The spreading code can be realized in hardware by AES blocks in OFB mode [10]. Simple variants with basic LFSR generators are possible to reuse existing CDMA hardware. By dynamically re-seeding the LFSR, attacks become much harder. Cross correlation and BER performance of long AES codes are comparable to optimized LFSR Gold codes.

In military satcom systems, antenna nulling is used as an antijamming technique. With an interferometric circuit, the signal of a small narrow-beam antenna is subtracted from the signal of the usual wide-beam antenna. So, signals from a region around the jammer are simply blocked. With phased array SDMA antenna techniques, multiple regions can be blocked. The cost of antenna nulling is too high for a wide usage in civil satcom systems.

Code-Hopping CDMA seems to be the only reasonable antijamming technology for civil satcom systems. Interception and eavesdropping renders impossible for unpredictable spreading codes. At negative SNR, the signal disappears in noise and the attacker cannot even detect a signal. The advantages of CH-CDMA grow with the signal bandwidth. Best are modern Ultrawideband (UWB) transmission systems.

C. Link Layer Security

Wireless satellite links are the most vulnerable segments in global communication networks. They are used for state and industrial espionage, attacks on TV broadcast channels and hacker attacks. Even when using end-to-end encryption, additional link-layer encryption will balance the increased risk of the wireless segment against the cable segment. The risk of breaking the end-to-end encryption is greatly reduced. Capacity misuse, traffic analysis and DoS attacks are best defended in the link layer.

Today, link layer security is rarely used in communication satellites. DVB-S content scrambling is applied for Pay-TV but not for DVB-S Internet data communications. DVB-RCS-Security is defined as optional, but usually not implemented. So, no security is available today in the OSI layers 1-2. Even worse, due to problems with the TCP-Split PEP, part of the upper layer traffic is also not encrypted [3]. This way, private data is being broadcasted over whole Europe.

Security services can be provided at the Asynchronous Transfer Mode (ATM) cell level and MPEG-TS for DVB-S and DVB-RCS systems. This only protects the link and does not provide end-to-end security. ATM Forum specifications address the security issues in terrestrial fixed networks only. There is very limited work on done on securing satellite ATM. There are several technical challenges need to be evaluated carefully for securing ATM satellites such as the encryption synchronization in high bit error rates environment, where errors are of bursty nature. 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 programs. Consequently, the programs must be decrypted at the receiving end before they can be decoded for viewing. CA offers capabilities such as Pay-Per-View (PPV), interactive features such as Video-on-Demand (VoD) and games, the ability to restrict access to certain material (adult movies, for example) and the ability to direct messages to specific set-top boxes (perhaps based on geographic region).

The main weakness of DVB-S CA is the one-way (broadcast) transmissions. Therefore it is very difficult to stop fraud and cloning pay TV smart cards without an efficient return channel and an efficient way to update smart card keys. Security is intended to protect the user identity including its exact location, the signalling traffic to and from the user, the data traffic to and from the user and the operator/user against use of the network without appropriate authority and subscription. 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 system is inherently secure on the satellite section without recourse to additional measures. Also, since the satellite interactive network forward link is based on the DVB/MPEG-TS Standard, the DVB common scrambling mechanism could be applied, but is not necessary (it would just add an additional protection to the entire control stream for non-subscribers). The main weakness of DVB-RCS security is that it is optional and never used and it's still in infancy stage and had limited support for multicast.

A promising approach to reduce the massive overhead of IP-over-DVB/MPE is the alternative solution called Ultra Lightweight

Encapsulation (ULE) [11]. A security layer for ULE has not yet been defined. With respect to security, ULE is the same as MPE and encryption of the PDU may be supported in the future by using mandatory header extension fields as mentioned in the draft.

D. End-To-End Security in Layers 3-7

Security services can also be provided at the network layer. IPSec (RFCs 2401, 2402 and 2406) [12] is a protocol that operates ”above” IP and below layer 4 protocols such as TCP and UDP. In the case of IPSec, applying security services at the IP layer can cause interworking problems with related protocols. Two examples are: Network Address Translators (NAT) can not be used (since IP addresses cannot be changed en route); and PEPs (RFC 3135) used to enhance performance on links such as mobile and satellite will fail, since the datagram contents (e.g. a TCP segment header) are encrypted. Major problems with IPSec are also expected with QoS. To prevent traffic analysis, all streams between two hosts, between two corporate subnets or between a host and a ground station is concentrated in one IPSec tunnel. This way, no QoS service differentiation is possible any more. Satellite networks with QoS don’t offer appropriate solutions. To handle different QoS classes in different IPSec tunnels, a management system and special signalling has to be developed.

The CCSDS Security Protocol SCPS-SP [4] offers similar functionality than IPSec. That’s why it is usually recommended to use the IPSec standard instead. SCPS-SP needs to be evaluated against other security protocol combinations (incl. L2). The feature of ”header protection” might be better realized in layer 2. No distinct cryptographic advantage is seen in SCPS-SP. However, when IP in certain deep space missions is not available, SCPS-SP has the ability to run over different CCSDS data formats.

Also security at the transport layer like Transport Layer Security (TLS) and at application layer like SSH provide end-to-end security. A mix of all these security services at various levels of the protocol stack should be considered when designing security systems. Table I summarizes the pros and cons of the security services at several of the protocol stack. Many end-to-end security protocols are not satellite-specific, but not all terrestrial security architectures are suitable for space applications.

E. Multicast Security

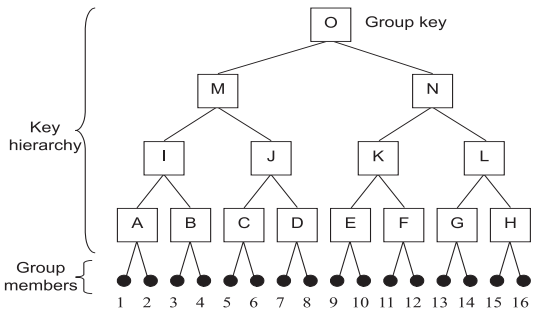

Fig. 4. Logical Key Hierarchy (LKH)

Satellites are ideally suited for delivery of multicast applications. 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. Protocols that manage the process of distributing keys in a multicast environment are few and under development such as Group Domain of Interpretation [12] and Group Secure Association Key Management Protocol (GSAKMP) [13].

LKH is a mechanism for security key management within a group of entities, providing the ability to initialise the group with a common key and then to rekey the group as required [14] (Fig. 4). It is, thus of particular application in secure multicast communications. In general, the number of transmissions required in LKH is the sum of the degrees of the replaced nodes. In a k-ary LKH tree of depth d, $kd-1 = k\log_k N - 1$ is a total of transmissions, where N is the number of users.

Using IPSec or other IETF conformant system allows such movie and sports TV service to be widely accessible through the Internet or any medium such as future 3G systems that support IP multicast, as well as the satellite network. Furthermore by converting to IP based systems, future revenue streams such as broadband Internet access, Interactive TV and email can be run alongside the existing offerings over the satellite, giving subscribers a tightly coupled one stop shop for all their multimedia needs. Standardising on IP allows a simplification of the transmission and receiving equipment producing potential cost savings and also allows new ideas to be brought to market quickly and inexpensively.

Video-conferencing in closed user groups could be a key application for satellite communication. Parallel to video, presentations can be transmitted to remote video beamers. Electronic blackboards can be synchronized globally for team-working. In corporate environments, those electronic meetings can save travelling costs and working hours. It allows very quick ad-hoc meetings and can be organized more often than real meetings. In terrestrial unicast networks, the bandwidth grows extremely nonlinear with the number n of participants. Satellite multicast is a good solution for those applications; the bandwidth grows only linear by n. One of the most important aspects of corporate multimedia conferencing is security.

IV. Conclusion

The European Space Infrastructure is still in danger. Security vulnerabilities, important threads and countermeasures are shown. While terrestrial communication protocols brought very good security designs like IPSec, satellites still broadcast private data without any security measures. Partly, Satcom protocol stacks can use existing technology like ATMsec and IPSec, but these solve not all security issues. Dedicated solutions are needed for the physical layer, satellite-specific MAC layers and special applications like multimedia-conferencing. Standardization of protocols and architectures in an overall security concept is not yet completed.

References

[1] M. Abrams, “Dawn of the E-Bomb,” *IEEE Spectrum*, Nov. 2003.

[2] Xinhua News Agency, “Bejing alleges Falun Gong hijacked Chinese TV Sat during World Cup,” *www.spacedaily.com*, July 2002.

[3] A. Adelsbach and U. Greveler, “Security of satellite-based internet service providers,” Ruhr-Universität Bochum, Tech. Rep., Nov. 2004. [Online]. Available: http://www.nds.rub.de/forschung/gebiete/sat_isp/

[4] Consultative Committee for Space Data Systems (CCSDS), “Space Communications Protocol Specification - Security Protocol (SCPS-SP).” [Online]. Available: http://www.scps.org/

[5] P. B. D. Selding, “AsiaSat assessing safeguards after four hours of pirated broadcast,” *Space News*, vol. 15, no. 47, p. 1, Nov. 2004.

[6] D. Giggenbach, F. Hermanns, E. Lutz, and C. Matarasso, “Multimedia satellite communications experiments with the International Space Station ISS,” *International Journal of Satellite Communications*, Nov. 2002, special Issue 2002 : Satellite Broadband Networking.

[7] M. Zhang, C. Carroll, and A. Chan, “Analysis of IS-95 CDMA voice privacy,” in *Seventh Annual Workshop on Selected Areas in Cryptography, Ontario/Canada*. Springer, Aug. 2000.

[8] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. McGraw-Hill, 1994.

[9] F. Hermanns, “Wireless security on the physical layer with code-hopping CDMA (CH-CDMA),” in *International Conference on Advances in Intelligent Systems (AISTA 2004)*. IEEE Computer Society, Nov. 2004.

[10] CAST Inc., “AES hardware designs in VHDL, verilog RTL & EDIF, up to 4.64 Gbit/s AES-128 bandwidth.” [Online]. Available: http://www.cast-inc.com/cores/aes/

[11] G. Fairhurst and B. Collini-Nocker, “Ultra Lightweight Encapsulation (ULE) for transmission of IP datagrams over MPEG-2/DVB networks,” 2005. [Online]. Available: http://www.ietf.org/html.charters/ipdvb-charter.html

[12] M. Baugher et al., “The group domain of interpretation,” IETF RFC 3547, July 2003.

[13] H. Harney, A. Schuett, and A. Colegrove, “GSAKMP,” draft-ietf-msec-gsakmp-light-sec-07.txt, Jan. 2005.

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