Security

Security levels

- Infrastructure
- Communication
  - Physical link
  - Acquisition & Synchronization
- Transmission (equipment)
- Information protection
  - IP working
  - IP security

Intrinsic security

- Facilities and equipment well localized
  - Not spread over the territory
  - Extremely easy to be garrisoned
- Utilization of proprietary standards
- Extremely high level of reliability of equipment and devices

Satellite systems characteristics and security

- Type and extension of the coverage area,
  - Capability to reach even remote, isolated and even impervious locations where typically some secret office can be located.
- Broadcast nature of the signal from satellites
  - Capability to distribute keys to a large set of users with low cost
- Accurate pointing
  - To receive signals accurate pointing is needed
- Propagation delay
  - Impacts costs in distributing keys

Satellite Vulnerabilities

- Three classes of vulnerabilities have been identified
  - **"Satellite-specific"**: vulnerabilities completely relying on satellite characteristics and technologies (usually involve lower protocol layers)
    - Indirect Effect-Impact only on the interconnected networks
    - Remediation must be sought within satellite domain
  - **"Non Satellite-specific":** vulnerabilities common to all the IP-based networks
    - Attack→ Detection → Remediation are irrespective of the target communication segment
  - **"Satellite Intersection-based"**: vulnerabilities specific of the adopted satellite technology, while arising from (or impact to) interconnection of satellite segment with terrestrial networks

Satellite-specific vulnerabilities

	Satellite Jamming	Unauthorized access	Satellite Orbital Positioning	Eavesdropping	Scrambling /Descrambling corruption	Entitlement checking	Acquisition and synchronization procedure disruption	User Discrimination Infringement
Main effect	Denial of Service	access services (i.e. TV) without any subscription	Wrong orbit determination (TT&C)	Violation of the communication confidentiality (two way)	Denial of Service (DVB CA)	Denial of Service (DVB CA)	Denial of Service	Unauthorized access, denial of service, privacy violation
Likelihood of the vulnerability	Very low (limited to military and terroristic scenario)	High	Very low	Very high	Very low	Low	Low	Very low

Satellite jamming

- Jamming is flooding or overpowering a signal, transmitter or receiver
  - The attacker goal is to not allow legitimate transmission to reach its destination
  - Similar to a DoS attack on the Internet but using radio waves in the satellite uplink/downlink
- Requires advanced knowledge and tools
  - Directional antenna
  - Knowledge of frequency (and in some cases of access scheme)
  - Enough power to override source
- Jamming of satellite receiver is the easiest form of satellite hacking
  - Just throwing enough noise at the receiver so that total C/N is no longer guaranteed due to a very low C/I
  - Jamming the uplink requires more skill and power than a downlink, but its range of disruption tends to be greater (up to the outage of the entire system)

Timeline of Documented jamming Incidents (1/3)

- ***1995*** Kurdish satellite channel, MED-TV, was intentionally jammed because it was believed to be promoting terrorism and violence .
- ***1997*** Resulting from the use of a disputed orbital slot, Indonesia jammed the communication satellite APSTAR-1A by transmitting interference from their own satellite Palapa B1.
- ***1998*** Kurdish satellite channel, MED-TV, launches "a major campaign to combat what it alleges is the persistent interference of its transmissions by the Turkish Government, taking the issue to the European Court of Human Rights.
- ***2000*** During tank trials in Greece, the British Challenger and United States Abrams suffered from GPS navigational problems. An investigation later revealed that those signals were being jammed by a French security agency.
- ***2003*** The Cuban and Iranian governments collaborated to jam Telstar 12, a US commercial communications satellite in geostationary orbit used to transmit programming by Voice of America to Iran.
- ***2003*** Iraq acquired GPS jamming equipment during Operation Iraqi Freedom allegedly from Russian company Aviaconversiya Ltd. Six jamming sites were discovered and destroyed in the air campaign prior to ground operations. The equipment's effectiveness appeared to be negligible; however it does suggest "that jamming capabilities could proliferate through commercial means".
- ***2004*** The mobile, ground-based CounterCom system, designed to provide temporary and reversible disruption of a targeted satellite's communications signals, was declared operational.

Timeline of Documented jamming Incidents (2/3)

- ***2005*** The Libyan government jammed two telecommunications satellites, "knocking off air dozens of TV and radio stations serving Britain and Europe and disrupting American diplomatic, military and FBI communications".
- ***2005*** In response to several jamming incidents attributed to the Falun Gong, China launched its first anti-jamming satellite, the Apstar-4 communications satellite.
- ***2006*** Thuraya mobile satellite communications were jammed by Libyan nationals for nearly six months. The jamming was aimed at disrupting smugglers of contraband into Libya who utilize satellite phones dependant on Thuraya satellites.
- **2006** "During the 2006 Israel-Lebanon war, Israel attempted to jam the Al-Manar satellite channel which is transmitted by the Arab Satellite Communications Organization (ARABSAT), illustrating the potential for commercial satellites to become targets during conflict
- ***2007*** Reports emerged that China had deployed advanced GPS jamming systems on vans throughout the country.

Timeline of Documented jamming Incidents (3/3)

- ***2007*** "Landsat-7, a US earth observation satellite jointly managed by NASA and the US Geological Survey, experienced 12 or more minutes of interference. This interference was only discovered following a similar event in July 2008".
- ***2010*** Persian-language satellite broadcasts originating from European satellite signals, including broadcasts of the BBC, Deutsche Welle, and France's Eutelsat were intentionally jammed from Iran.
- ***2011*** LuaLua TV, a London-based Bahraini current affairs network founded by 15 members of the Bahraini opposition, was jammed four hours after its first broadcast.
- ***2011*** Libyan nationals jammed Thuraya satellites for more than six months in an effort to disrupt the activities of smugglers who use satellite.
- ***2011*** Ethiopian Satellite Television (ESAT), an Amsterdam-based satellite service, was repeatedly jammed by the Ethiopian government, with the assistance of the Chinese government.
- ***2012*** The Eritrean Ministry of Information accused the Ethiopian government of blocking transmissions from Eritrea's state-run satellite television

Satellite Eavesdropping

- *Eavesdropping* allows a hacker to see and hear what is being transmitted
  - View satellite television
  - Eavesdrop on satellite telephone conversation
  - Eavesdrop on Internet traffic
  - View satellite imagery
- Lack of reported incident since eavesdropping is usually considered as a simply illegal activity rather than "satellite hacking"

Satellite Hijacking

- Hijacking consists in illegally using a satellite to transmit the hacker's signal
  - Overriding or altering legitimate traffic
  - Unauthorized use of satellite
- Hijacking is predominantly connected to communication broadcast or Internet over satellite
  - The same technique and COTS software used for eavesdropping can be used for some types of hijacking
    - i.e. spoofing legitimate users web pages

Timeline of documented Hijacking incidents (1/3)

- ***1977*** The audio portion of an ITN news broadcast on Southern Television in the UK was replaced by an audio message claiming to be from outer space. The message warned that human kind's current path would lead to an undesirable future.
- ***1985*** Four astronomers at Poland's University of Torun used a home computer, a synchronizing circuit, and a transmitter to superimpose messages in support of the labor movement Solidarność (Solidarity) over state-run television broadcasts in Torun.
- ***1986*** A Florida man using the name Captain Midnight disrupted the uplink to a Galaxy I satellite. For 4 to 5 minutes viewers of HBO on the US East coast saw the following message, placed over SMPTE colour bars:

GOODEVENING HBO
FROM CAPTAIN MIDNIGHT
$12.95/MONTH ?
NO WAY !
[SHOWTIME/MOVIE CHANNEL BEWARE!]

Timeline of documented Hijacking incidents (2/3)

- ***1987*** The Playboy Channel, based on the popular adult magazine, had its signal hijacked by an employee of the Christian Broadcasting Network.
- ***1987*** A Max Headroom impersonator overtook the television signal of two Chicago based stations, commandeering a live news broadcast and an episode of Dr. Who for 25 seconds and 90 seconds respectively.
- ***2002*** The Falun Gong illegally used an AsiaSat satellite to broadcast into China disrupting broadcasts of China Central TV (CCTV) with anti-government messages
- ***2006*** "During the 2006 Lebanon War, Israel overloaded the satellite transmission of Hezbollah's Al Manar TV to broadcast anti-Hezbollah propaganda. One spot showed Hezbollah leader Hassan Nasrallah with crosshairs superimposed on his image followed by three gunshots and a voice saying 'Your day is coming' and shots of the Israeli Air Force destroying targets in Lebanon.
- ***2007*** An intrusion incident occurred on Czech Television's Sunday morning programme Panorama, which shows panoramic shots of Prague and various locations across the country, to promote tourism. One of the cameras, located in Černy Důl in Krkonoše, had been tampered with on-site and its video stream was replaced with the hackers' own, which contained CGI of a small nuclear explosion in the local landscape, ending in white noise

Timeline of documented Hijacking incidents (3/3)

- ***2007*** A grainy photo of a man and woman interrupted Washington, DC ABC affiliate WJLA's digital or HD signal for two hours. The incident was initially deemed a genuine signal intrusion by various websites but has been confirmed to be the result of an older HDTV encoder malfunctioning in the early morning hours and going undetected.
- ***2007*** The Tamil Tigers (LTTE) in Sri Lanka illegally broadcast their propaganda over Intelsat satellites.
- ***2009*** Brazilian authorities arrested 39 university professors, electricians, truckers, and farmers who had been using homemade equipment to hijack UHF frequencies dedicated to satellites in the US Navy's Fleet Satellite Communication system for their personal use.
- ***2013*** TV stations in Montana and Michigan had their Emergency Alert System systems commandeered and used to warn of a Zombie attack. In one case an audio recording announced that "dead bodies are rising from their graves" and in another the ticker, or message that scrolls across the bottom of the screen, was used for this same message

Telemetry, Tracking and Control (TT&C)

- TT&C links allows to control satellites
- Hacking TT&C means to control a satellite or to hamper control to the legitimate owner
- Possible actions:
  - Force the use of reserve propellant to enter a graveyard orbit
  - Rotate satellite so that solar panels and antennas are pointed in wrong directions
  - Cause satellite collisions with consequent debris
- It is the most difficult satellite hacking
  - TT&C has the greatest security
  - Military satellite networks locate TT&C links and satellite ground stations within military bases and they employ encryption at multiple levels

Timeline of documented TT&C incidents

- ***1998*** A US-German ROSAT satellite, used for peering into deep space, was rendered useless after it turned suddenly toward the sun damaging the High Resolution Imager by exposure. NASA investigators later determined that the accident was linked to a cyber-intrusion at the Goddard Space Flight Center.
- ***1998*** "Members of a hacking group called the Masters of Downloading claim to have broken into a Pentagon network and stolen software that allows them to control a military satellite system. They threaten to sell the software to terrorists. The Pentagon denies that the software is classified or that it would allow the hackers to control their satellites, but later admits that a less-secure network containing 'sensitive' information had been compromised".
- ***1999*** Media reports alleged that a Skynet, British military communications, satellite had been taken control of through hacking and was being held for ransom. These reports were later claimed to be false.
- ***2008*** "On June 20, 2008,Terra EOS [earth observation system] AM– 1, a National Aeronautics and Space Administration-managed program for earth observation, experienced two or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands".
- ***2008*** "On October 22, 2008, Terra EOS AM–1 experienced nine or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue Commands".

Non-satellite specific vulnerabilities

Satellite Intersection-based vulnerabilities

	Interception (i.e. at satGW)	Data corruption	Transport layer violation	IP or IPsec addressing infringement (with PEP)	TCP Spoofing (with PEP)	Abuse of Satellite shared requests	AAA infringement
Main effect	Denial of Service, loss of confidentiality	Denial of Service	Denial of Service	Denial of Service, Loss of confidentiality	Denial of Service, loss of reliability, performance impairments	Denial of Service	Denial of Service
Likelihood of the vulnerability	Very low	Very high	Medium	High	Very high	Medium	Medium

Vulnerabilities effects

- RF level: it is quite unlikely that an attack can take place because it would require:
  - Physical neighbouring to the station
  - Availability of proper infrastructure. This appears difficult (but possible) to replace a single user terminal but unreasonable for replacement of a master station.
- Access level: they are the same of any other IP system. The difference is in the effects.

DVB Threats & Security Requirements

- DVB Threats:
  - Passive Threats:
    - Monitoring data and the identity of the communication parties.
    - Easy in satellite network due to the broadcast nature and availability of inexpensive receivers.
  - Active Threats:
    - Data modification, masquerading, terminal cloning, or Local / Global hijacking of the service.
    - More difficult since it require direct access to the transmitter and expensive equipment.
- Security requirement (Passive Threats):
  - Data confidentiality,
  - Protection of the receiver identity.
- Security requirements (Active Threats):
  - Source authentication and data integrity.

Conditional access in DVB-S

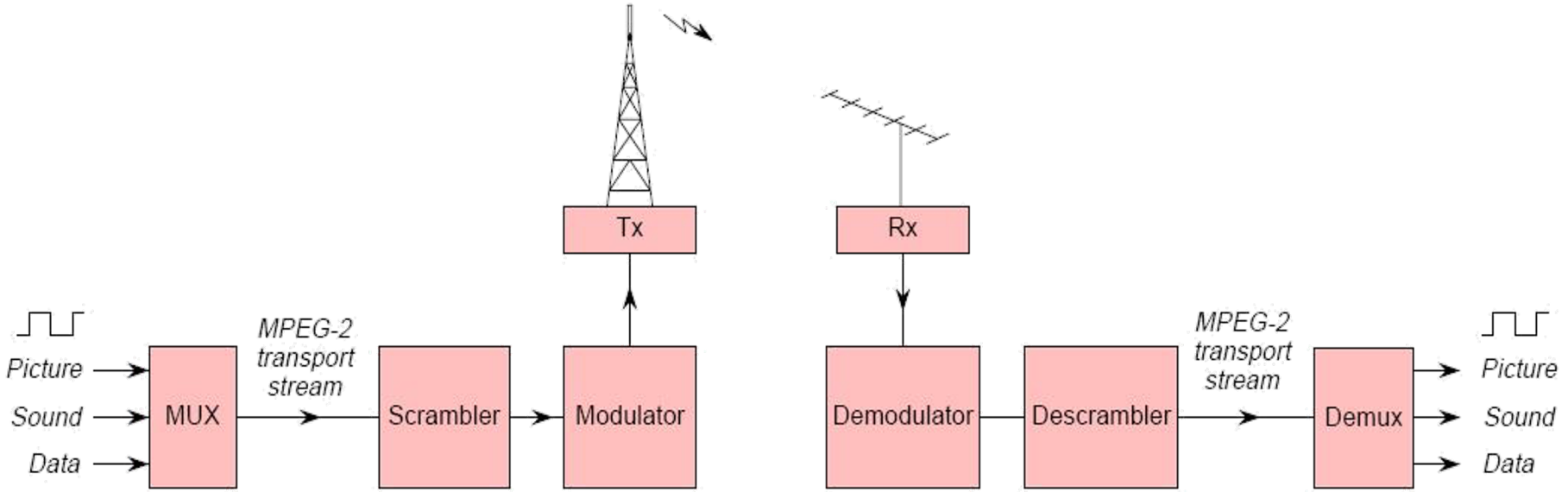
- Based on encrypting signals to allow only a restricted number of users to view certain programs.
  - First level of restriction: allows the view only to subscribers
  - Further levels: restricting only to particular subsets of users (adult movies, partial subscription, geographic restriction).
  - Pay-per-View and Video on Demand can be implemented.
- Performed through three functions:
  - **scrambling/descrambling**,
    - modifying the information sequence so that only who knows a secret Control Word can recognize the original information
  - **entitlement checking**,
    - in charge to broadcast the encrypted secret codes to enable proper descrambling utilizing a specific message (Entitlement Checking Message).
  - **entitlement management**.
    - in charge to manage this process.
- Weakness: broadcast (one way) nature of transmission
  - not having any return channel, it is not possible to be aware eventual cloning of smart cards.

DVB-Conditional Access (DVB-CA)

- A Conditional Access (CA) system is composed of a combination of ***common*** "scrambling" and "encryption" to prevent unauthorized reception. In particular:
  - Scrambling is the process to rendering sounds, pictures and data unintelligible.
  - Encryption is the process of protecting the secret keys that have to be transmitted with the scrambled signal to allow the descrambler to work.
  - A single key is shared by all users. The broadcasting station encrypts the channel using this shared key, and all the users who have this key use it for decrypting the broadcasted scrambled channel.
- CA system must be transparent: after descrambling any defects on the sound and pictures must be imperceptible (no additional errors introduced).

CA functional model

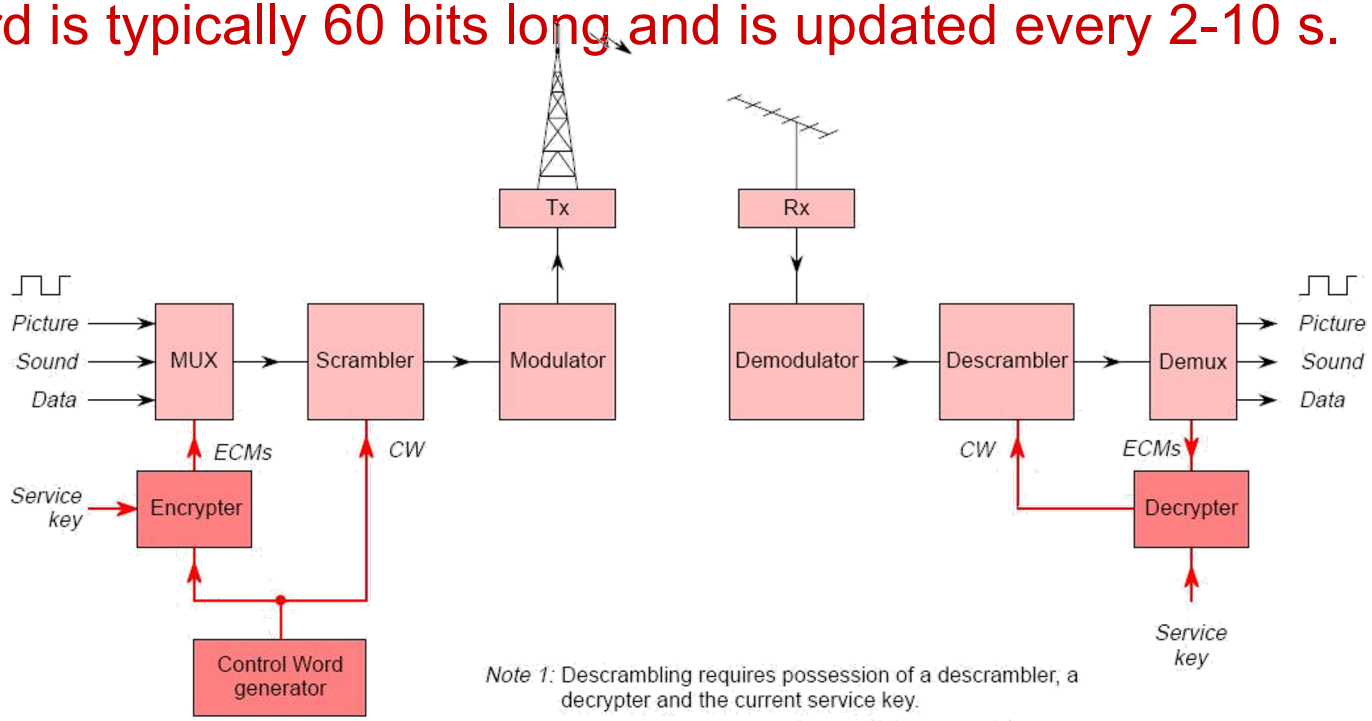
- A Conditional Access Sub-System (CASS) is a detachable security module which is used as part of the CA system in a receiver.



Note: In such a basic scrambling system, possession of a descrambler gives permanent entitlement to view.

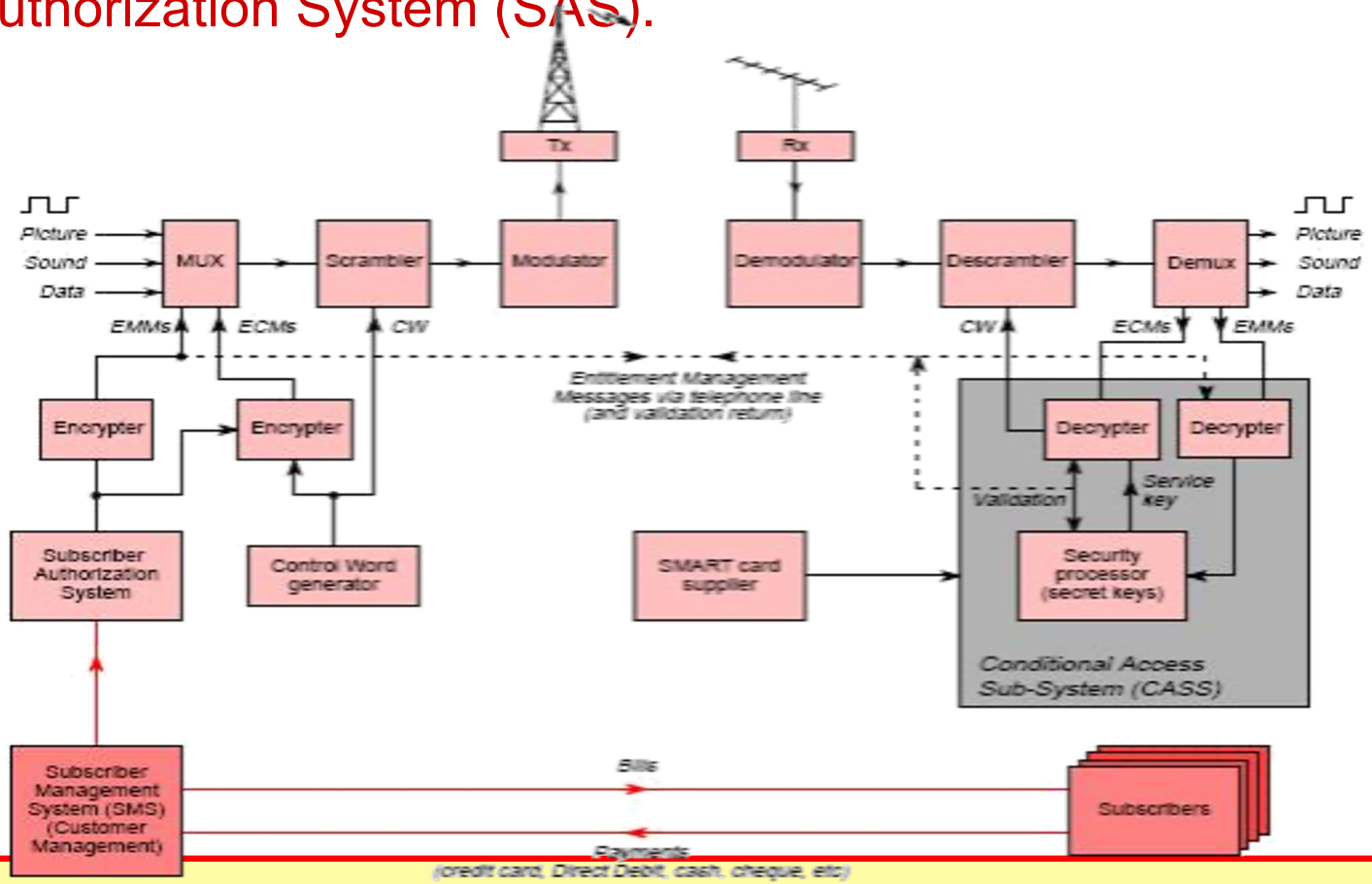
Entitlement Control Messages (ECMs)

- Entitlement Control Messages (ECMs) are generated and transmitted to recover the descrambling control word in the decoder.
- The ECMs are combined with a service key and the result is decrypted to produce a control word. At present, the control word is typically 60 bits long and is updated every 2-10 s.

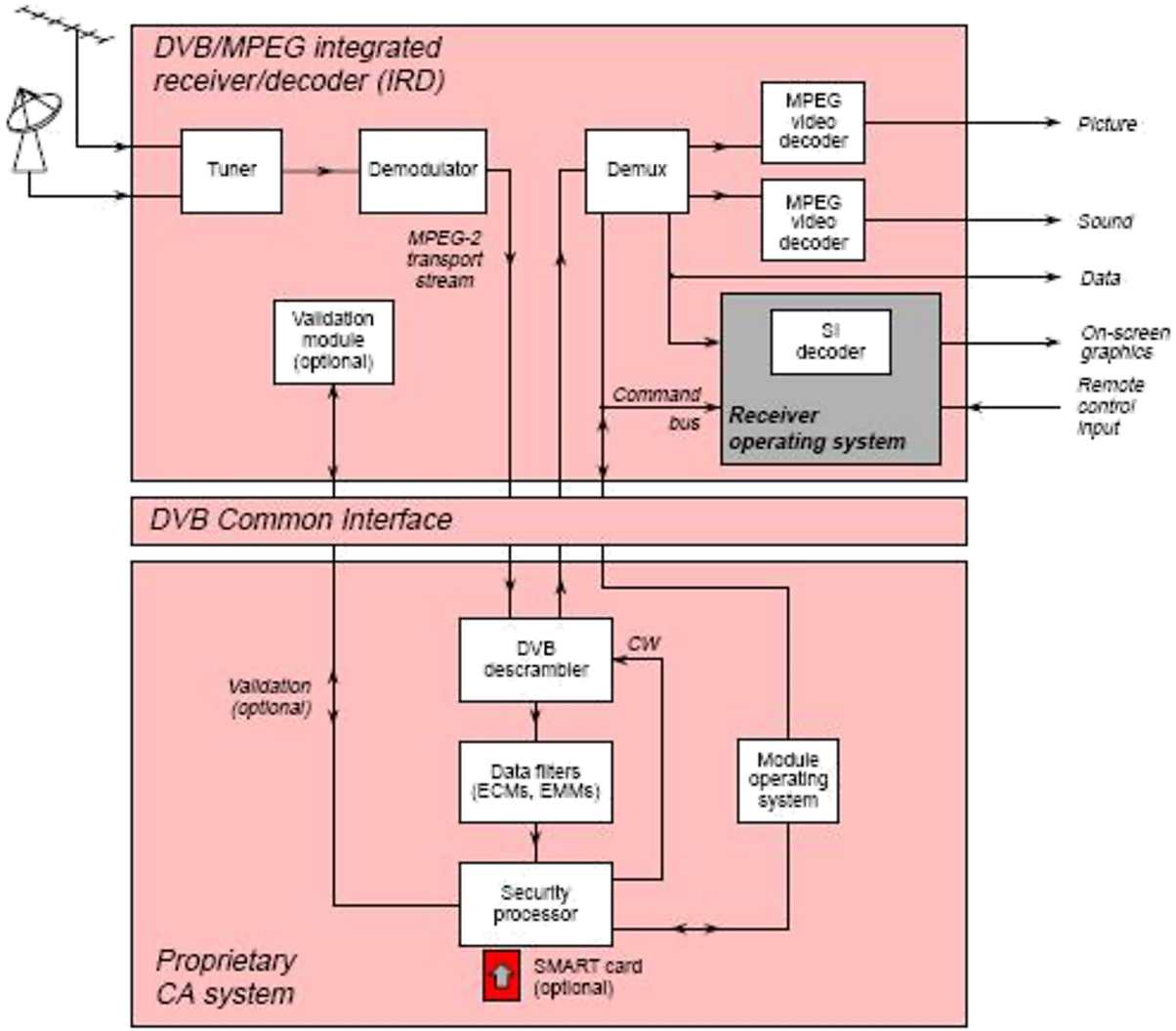


Entitlement Management Messages (EMMs)

- To change the access conditions at the programme boundary
- Addition of the Subscriber Management System (SMS).
- EMMs are generated and transmitted by the Subscriber Authorization System (SAS).



DVB Common Interface



Security in DVB RCS

- Forward link: based on the above mentioned DVB common scrambling/descrambling mechanism.
- Return link: similar mechanism as well as authentication algorithms implemented at MAC layer.
- IP interface: further degree of security provided through proper IP addressing.
- IP security mechanisms (such as IPSec) can be applied taking into account the constraints presented later or also application layer security.
- Satellite interactive network individual user scrambling for both forward and return link.

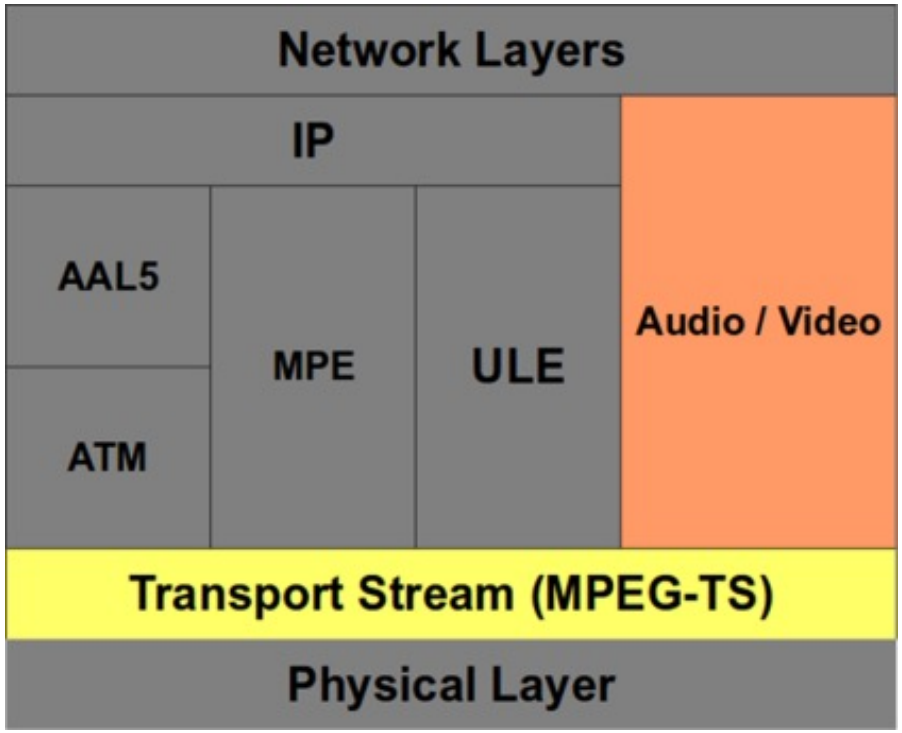
DVB Common Scrambling in the forward link

- Feasible for broadcasted TV channels
- It does not provide high security for IP traffic, becasue the encrypted IP traffic for one user can be decrypted by any other user.
- Applicable for IP over MPE but not for ULE
- Moreover this mechanism is only used in the forward link.

DVB-RCS Security Mechanisms

DVB Common Scrambling Algorithm (CSA)

- Encrypting the forward link traffic using a single key. Ideal for audio/video channels, not for data.



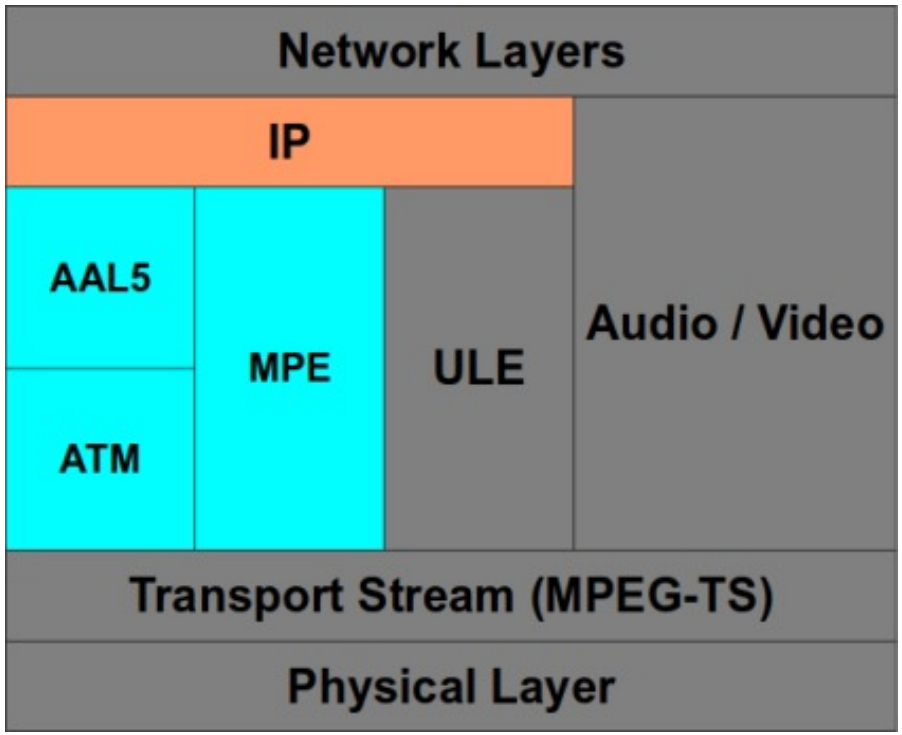
Interactive network individual user scrambling for both forward and return link

- It can be used for both forward and return link.
- The DVB RCS security specification currently supports the authentication of each DVB-RCS Terminal (RCST) and the encryption of both forward and return link traffic.
- The DVB MPE section is encrypted using a symmetric-key block cipher1 used in the Cipher Block Chaining (CBC) mode.
- Keying mechanisms have been defined for generating session keys for each user for encrypting the IP traffic.
- Data destined to different RCST's can be encrypted with different keys.
- It provides scrambling for individual users, but only applicable for IP over MPE and not for ULE.

DVB-RCS Security Mechanisms (3)

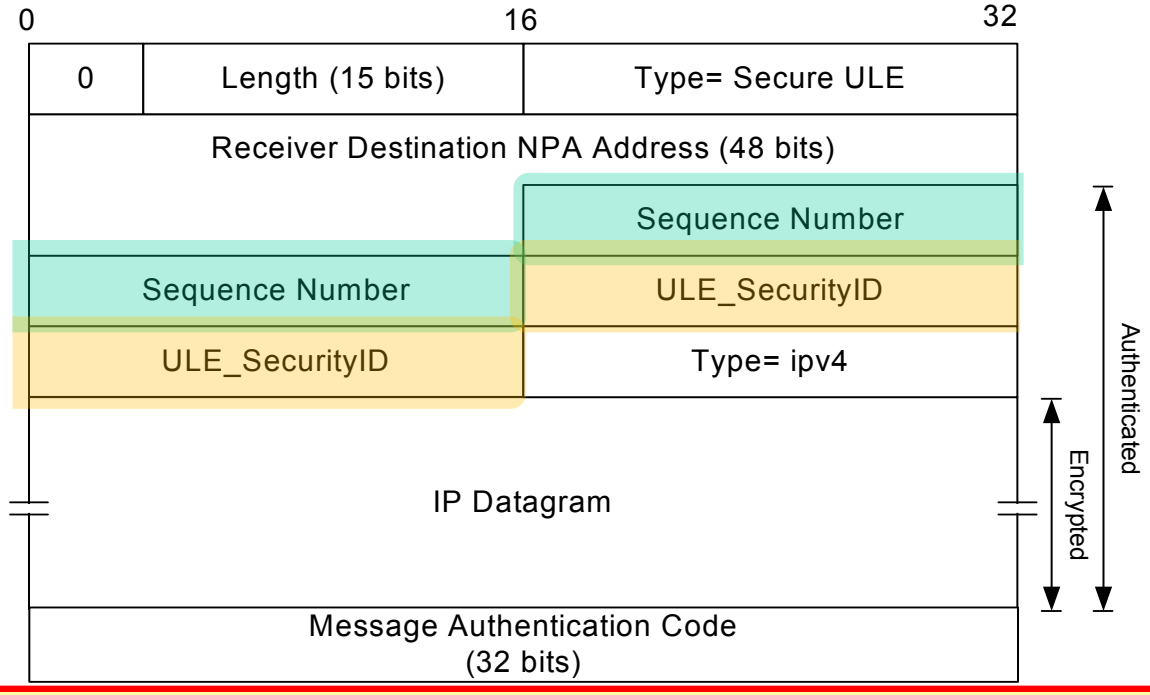
Satellite interactive individual user scrambling

- Provides individual terminal authentication, on the fly encryption for the uplink/ downlink with an individual key for each terminal.
- Supports Terminal log-off, Re-keying.
- Provides Inherent Secure System.
- **Not supporting lightweight encapsulation (ULE/ GSE).**
- **Not supporting Multicast (Special Key Exchange mechanism required).**
- **Destination address has to be clear.**

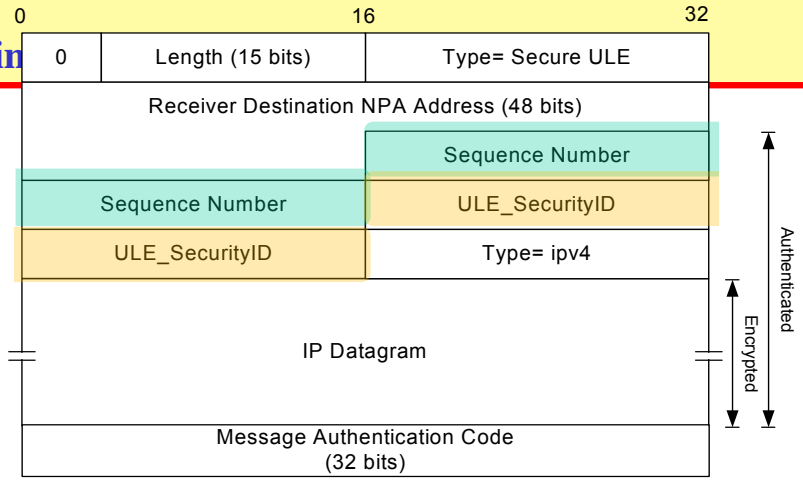


Secure ULE

- Secure the transmission of user traffic over MPEG-2 Transport Streams
- The security extension: 32-bit security identifier (similar to IPSEC) can be used for filtering the traffic for a given user.
- Encrypting the data payload to provide data confidentiality.
- No mechanisms have been defined for providing data integrity, data authentication and methods to prevent replay attacks.



Secure ULE (2)



- The Secure ULE Header extension follows the base ULE header
- The extension header for S-ULE consists of a 32-bit security identifier (ULE_Security_ID) and a 32- bit sequence number. This is then followed by the type field (type of payload carried).
- To achieve confidentiality, the traffic between the DVB gateway and the DVB receiver needs to be encrypted.
- The IP datagram is encrypted and then encapsulated in the S-ULE SNDU.
- A 32-bit security identifier (ULE_Security_ID), similar to the Security Parameter Index used in IPSEC, added to uniquely identify the secure session.
- This ULE_Security_ID would correspond to the security configuration between the DVB gateway and receiver for a particular session thereby indicating the key and algorithm used for encrypting the data payload (DES, 3DES).

Secure ULE (3)

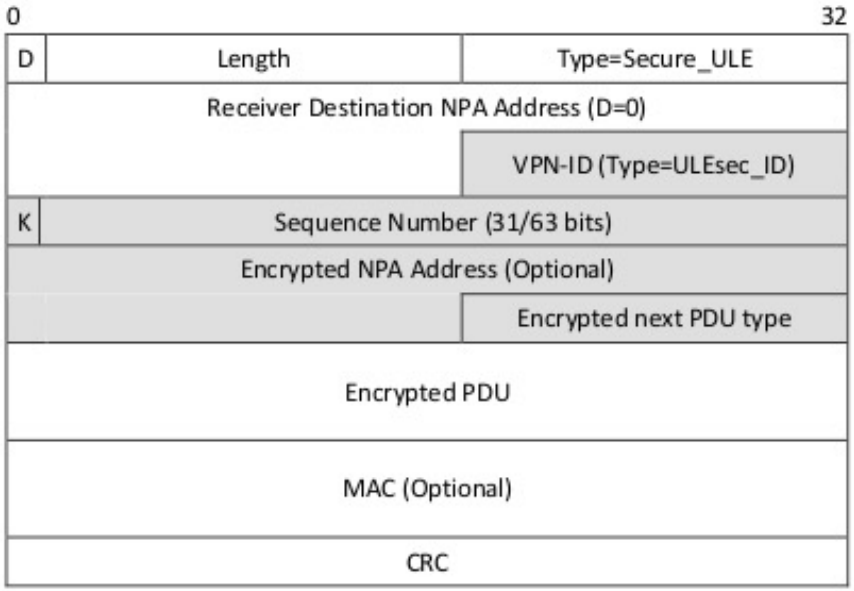
- To provide both data authenticity and data integrity, a **Message Authentication Code** (MAC) is used instead of the 32-bit CRC proposed by the original ULE protocol.
- The MAC is calculated over the extension header and the data payload, thereby protecting the extension header and payload. The receiver would calculate the MAC for the received packet and compare it with the transmitted value.
- The two codes would not match in only 2 cases:
  - there was an error during processing or transmission over the satellite,
  - the packet has not been sent from an authenticated entity.
- In either case, the packet should be discarded.
- As Secure ULE can be used in conjunction with common scrambling and/or DVB-RCS individual scrambling mechanisms, a 32-bit MAC is sufficient.
- A 32-bit sequence number has been added to the ULE SNDU to prevent replay attacks. The value of this sequence number would be set to 0 at the beginning of the session. The gateway would monotonically increment this number when it sends a packet to the receiver and the receiver would verify the correct sequence number. If an adversary tries to inject or replay old packets the sequence number would not match. This would result in discarding the packet.

DVB-RCS Security Mechanisms (4)

Secure ULE

- Different security extension headers for ULE have been presented.
- Lightweight security extension header using a security identifier (SID), similar to (SPI) in IPSec, key to encrypt the data payload and receiver address, Message Authentication Code (MAC) to provide authentication and integrity.

➢ **MAC as a symmetric function may not be reliable for source authentication, anyone holding the key can pretend to be the real author of the message.**



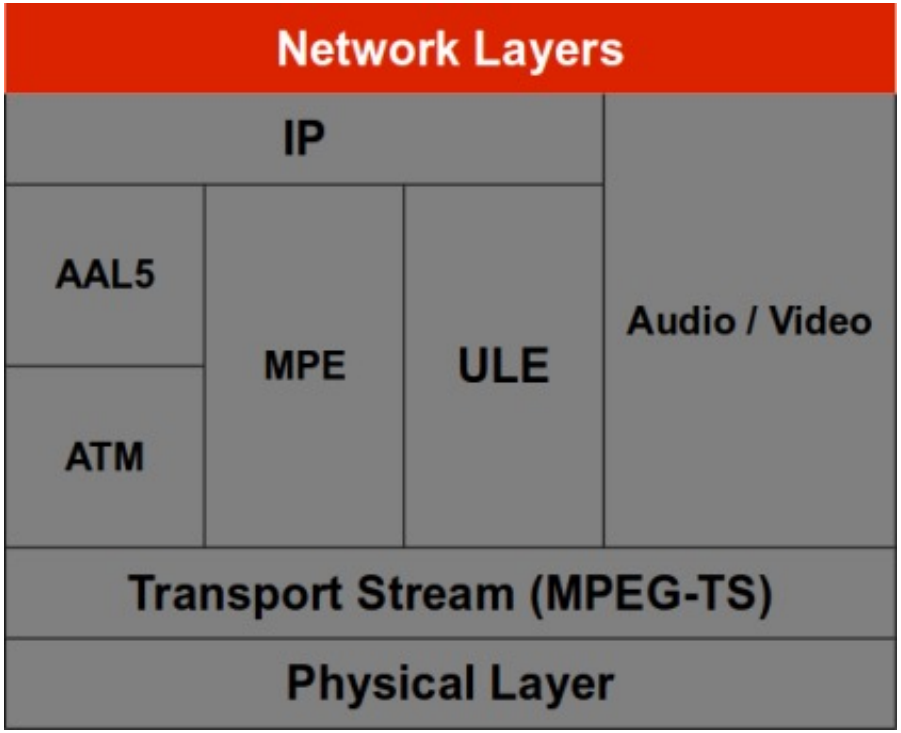
Higher layer security mechanism

- IPSEC in tunnel mode may also be used to secure the IP traffic over DVB.
- IPSEC has large overheads especially due to the two IP headers.
- IPSEC can be used only for IP traffic, and would not provide any security for other protocols that can be carried by ULE.

DVB-RCS Security Mechanisms (2)

IP or higher layer security mechanisms

- Such as IPSec, TLS, other application layer security Protocols.
- IPSec provides end to end security but as drawback (symmetric security mechanism in both communication sides, large overhead, applicable only to IP, incompatibility with some network layer techniques used in the satellite networks to enhance the bandwidth (PEPs).
- TLS can only directly support TCP transport protocols.



Authentication in TDMA networks: The Viasat Linkway case

- Network architecture
  - NCC Network Control Centre
  - MRT Master Reference Terminal
  - TT Traffic Terminal

NCC Acquisition

Startup & reference station synchronization

- NCC establishes contact with MRT (and/or Secondary Reference Terminal SRT) and initiates acquisition & synchronization process
- MRT transmits reference burst
- After MRT synchronization, NCC initiates procedure for TTs, using MRT/SRT as relay

Acquisition & Synchronization

- After initial acquisition & synchronization:
  - TTs: periodically transmit control burst
  - MRT: measures timing & frequency
  - NCC: sends further corrections to TTs
- Corrections keep TTs synchronized with satellite drift

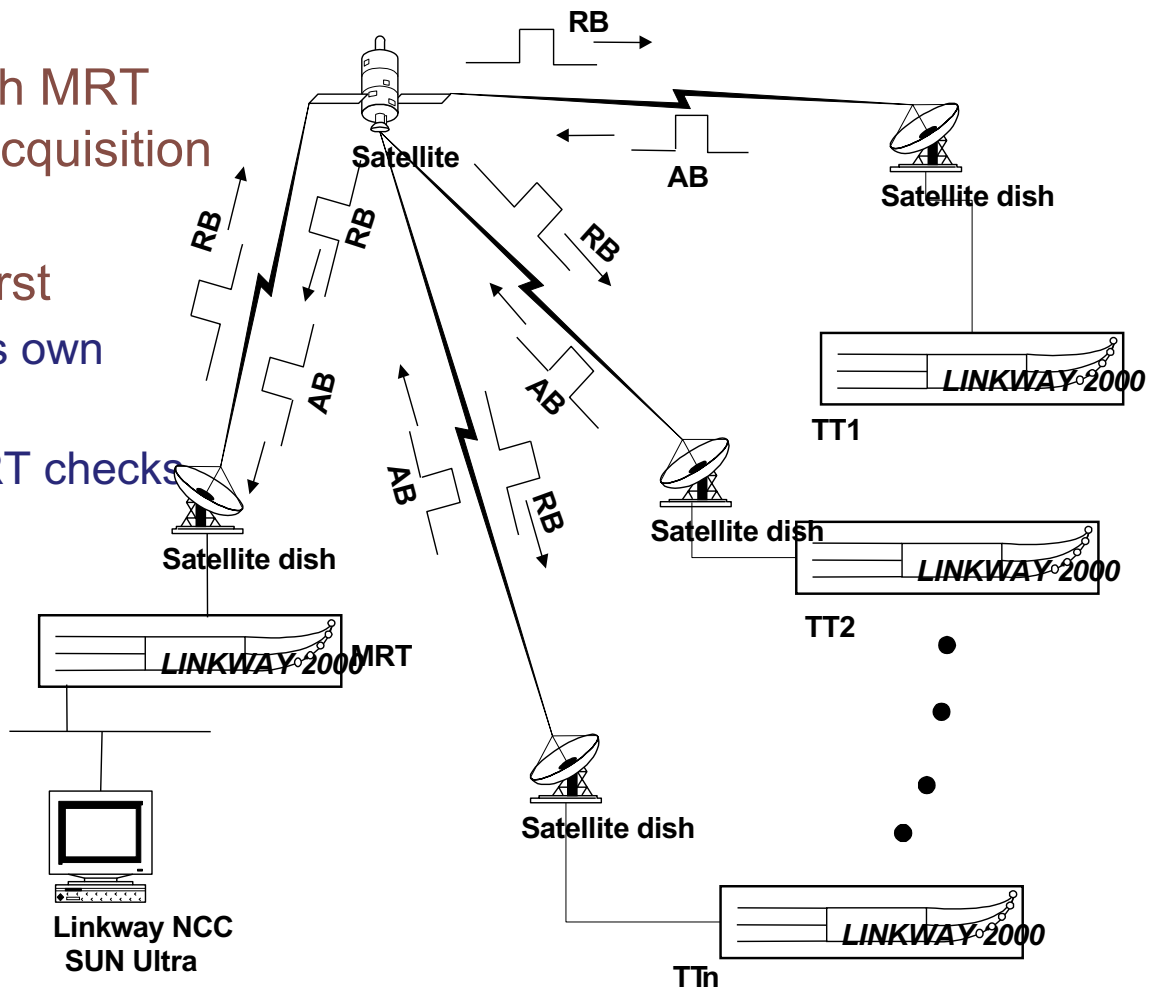
NCC Security Management

- Network Management Station NMS User log-in & password information part of configuration data
  - Used for authentication when User logs into system
- Several Levels of User Access
  - Full-SuperUser
  - Read-Only
  - Restricted

NCC Acquisition & Synchronization

Startup & reference station synchronization

- NCC establishes contact with MRT (and/or SRT) to initiate RT acquisition & synchronization
- MRT transmits reference burst
  - Single-beam: MRT checks own transmission
  - Multiple-beam: MRT & SRT checks each other's burst



Network Acquisition & Synchronization (2)

After MRT synchronization, NCC initiates procedure for TTs, using MRT/SRT as relay

- TTs: commanded to transmit acquisition bursts
- MRT: measures arrival time & frequency
- NCC: sends frequency/timing corrections to TTs
- TTs: ready to carry User data traffic

- After initial acquisition & synchronization
  - TTs: periodically transmit control burst (CB)
  - MRT: receives CB and measures timing & frequency
  - NCC: sends further corrections to TTs
- Corrections keep TTs synchronized with satellite drift during a single day

Network Acquisition & Synchronization (3)

- RT & TT procedures
  - Establish & maintain burst synchronization
- Separate local frame counters
  - Transmit frame identifier (TFID) values
  - Receive frame identifier (RFID) values
- TT "receive synchronized" when
  - TT receives RB continuously
  - Received FID matches TT's local receive FID count
- TT "transmit synchronized" when
  - Its controlling CB is received within its MRT's prediction aperture
  - Transmitted TFID value matches MRT's local receive RFID count

Bootfiles

Bootfiles contain the information required for a Linkway terminal to acquire transmit and receive synchronization on the network.
Important parameters:

- Tx and Rx center frequencies of the site
- Carrier frequency of reference carrier
- Where to find the RB from the MRT (in TDMA frame structure)
- Tx Power
- Identity -- site Id, QB Id

- Bootfiles are created by the NCC when directed by a **makeboot** command.
- Bootfiles can be transported by
  - Copying onto floppy disk
  - FTP file transfer to laptop or PC
  - Attachment to an e-mail

Security in CDMA networks

- Code discrimination
  - To decode information from the signal the proper code must be known.
- Proper authentication mechanism.
- Globalstar:
  - Security is provided as authentication mechanism and as voice/data encryption applicability.
    - The former is exploited by the SIM Card similarly to the terrestrial cellular systems,
    - The latter can be implemented using end-to-end devices such as DCS-1800.
  - The IS-41 User Terminal (UT) utilizes a Security Module (SM) in charge to store long term cryptographic keys as well as to store and execute cryptographic algorithms. The SM is associated to an UT HW identity through a unique Electronic Serial Number (ESN). This association is stored in the HLR (Home Location Register) in order to hamper working of any SM into any other UT.

Security for IP satellite networks

- A number of services to be provided
  - Confidentiality
    - protection from passive attacks, unauthorized release of message content and traffic flow analysis
  - Authentication
    - the message sender is really who he claims to be
  - Integrity
    - the message content is not modified
  - Non repudiation
    - sender or receiver don't deny a transmitted message
  - Access control
    - limit access
  - Key management
    - negotiate security keys between communication entities

Confidentiality

- Data protection from passive attack, against unauthorized release of message content
- Protection against traffic flow analysis (source, destination, frequency, length, etc.)
- Mandatory unless the user doesn't require any privacy (free broadcasting)

Authentication

- Guarantee that the communication is authentic
- The recipient is sure that the message is from the source that it claims to be
- The process must be sophisticated because in wireless systems it may be quite easy to impersonate a user

Integrity

- The received message (or at least the protected part of it) is the same that was sent
- Cryptography to ensure packet integrity
- Mandatory

Non-repudiation

- Prevents either sender or receiver from denying a transmitted message
- Necessary for some applications

Access control

- Limits access to host systems and applications via communication links
- Authentication required

Key management and exchange

- Allows to negotiate security keys between communication entities
- Complex applicability to multicast (peculiar characteristic of satellite systems)

IPSec over satellite links

- IPSec is designed to provide:
  - Confidentiality
  - Integrity
  - Authentication
  - Non repudiation
- Security independent on upper layer protocols,
- Traffic re-routing and network configuration modifications are preserved,
- Both real time and non real time applications are protected.

IPSec protocols

- Authentication Header (AH)
  - Authentication, integrity, no confidentiality
- Encapsulating Security Payload (ESP)
  - Confidentiality, optional authentication and integrity

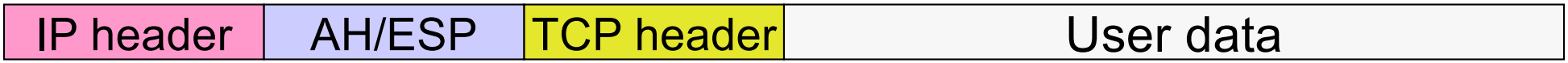
Operational modes

- Transport mode
  - To protect upper layer protocols
  - Applies to host-to-host authentication
- Tunnel mode
  - To protect the whole datagram
  - Applies to gateway-to-gateway and host-to-gateway
    - Useful in case the same entity owns two or more private networks connected through the public Internet.

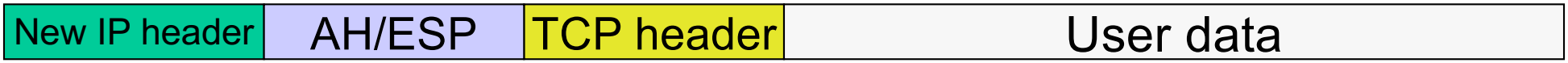
IP datagram

- IP header
- TCP header
- User data

Transport mode



Tunnel mode



In both cases, the IP payload, composed of TCP header and user data, results **one indivisible protected unit**.
The keys used to encrypt and authenticate must be known **only at the two end users**. The intermediate nodes (routers) are only allowed to forward packets based on routing tables.

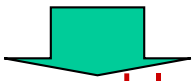
IPSec compatibility

- End to end semantic required.
- If upper layer protocol doesn't introduce violation to this concept, no particular problem (excluding the delay in key distribution).

- To speed up TCP process, modification to the standard mechanism must be introduced.

TCP modification

- Flow control
  - Only the two end host involved (in some case just one)
  - The intermediate routers involved, but not requiring access to TCP data encapsulated in the IP packet



No problem

- PEP (splitting) or Network Address Translator (NAT)
  - Requiring to access
    - flow identification number (identifying source and destination port numbers)
    - sequence numbers (used to match acknowledgements with the data segments)

Not compatible

Possible solutions

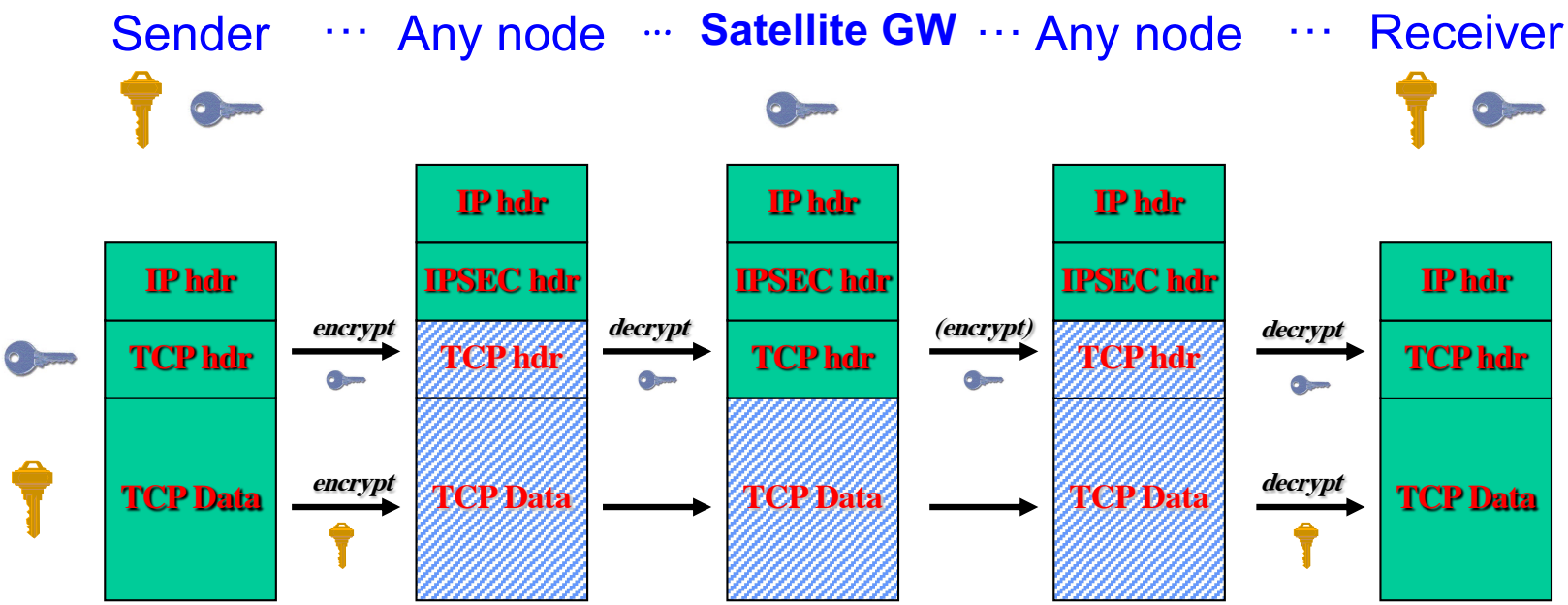
- Replacing IPSec with a transport layer security mechanism,
- Tunneling one security protocol within another,
- Using transport friendly ESP format,
- Splitting IPSec into as many segments as the whole path is splinted

Each has its own limitations.

Multi layer IPSec

- Partitioning the IP packet into different parts (TCP header and TCP data)
- Applying to each different kind of protection
  - The former can use a protection scheme with key shared among the source, the destination and a certain number of intermediate nodes, where PEP is implemented.
  - The latter can use classical end-to-end protection with keys shared only between the source and destination hosts.
- Fully compatible with standard IPSec
- Not too much complexity added
- Promising performance

ML IPsec concept

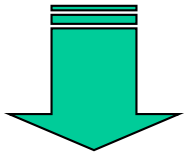


Security at transport layer

- The IP header (addresses) is not protected and therefore traffic analysis is possible but key management is simplified.
- Two solutions are applicable:
  - TLS (Transport Layer Security)
    - designed to provide privacy, composed of two layers
    - TLS Record Protocol
      - works on top of TCP (therefore not useful for UDP connections, largely used for multicast and real time traffic) ensuring privacy and reliability. Symmetric cryptography is used (DES or AES).
    - TLS Handshake Protocol
      - provides connection security working at authentication level before starting transmission of application data
  - SRTP (Secure Real Time Transport Protocol).
    - profile of Real Time Transport Protocol (RTP).
      - provides confidentiality, message authentication and replay protection.

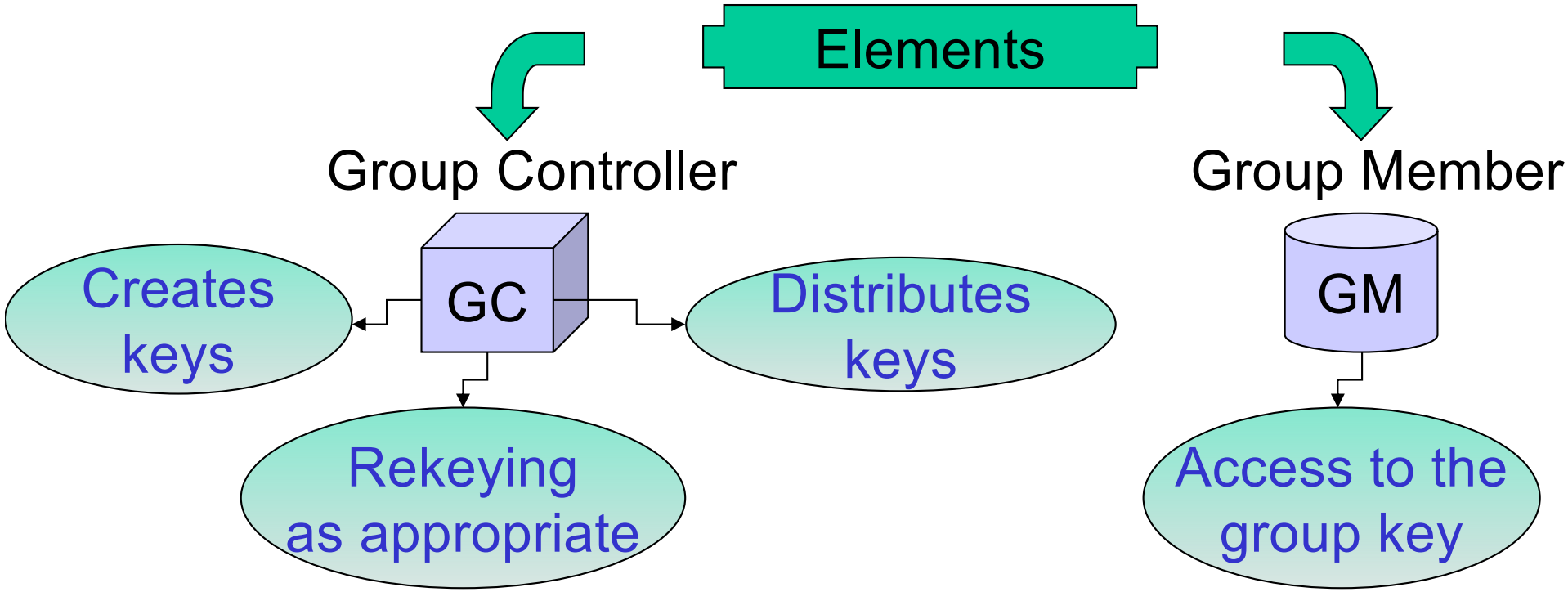
Key management in multicast

- From security point of view multicast connection can be approached as a set of unicast



- Not scale well for large groups
- Protocols to manage multicast under development

Multicast key management protocols



Not need to be colocated with multicast data source

Each GM initial 1-to-1 secure association with the GC. Then used to create and share information

A single key GROUP TRAFFIC ENCRYPTION KEY (GTEK) known to the GC and all GM and no outside the group

Rekeying in multicast

- The rekeying procedure must be performed
  1. Regularly (every few seconds or minutes) to avoid cryptanalysis of traffic,
  2. On demand if the key may be compromised,
  3. When a new user joins the group to avoid that previous traffic may be decrypted,
  4. When a member leaves the group to avoid to decrypt future traffic.
- The cost of the operation can be high especially if the multicast group membership updates frequently
  - the bandwidth is expensive
  - the delay is meaningful,

Rekeying approach

- In case of rekeying for 1. and 3.
  a. Old group key
  b. Separate "control" key negotiated during session establishment
- In case of rekeying for 2. and 4.
  – Different rekeying approach is required since the old key is known by at least one user who is no longer in the multicast group

Cost parameters

- GC encryption effort
- GC memory requirements
- Network traffic
- GM decryption effort
- GM memory requirements

Key management techniques

A. Flat
   - GC shares a unique key with each GM
   - GTEK sent to the members by encrypting it N times with each unique key
   - Encryption load and rekey traffic increase linearly with N
   - Broadcast nature doesn't help since all messages are different

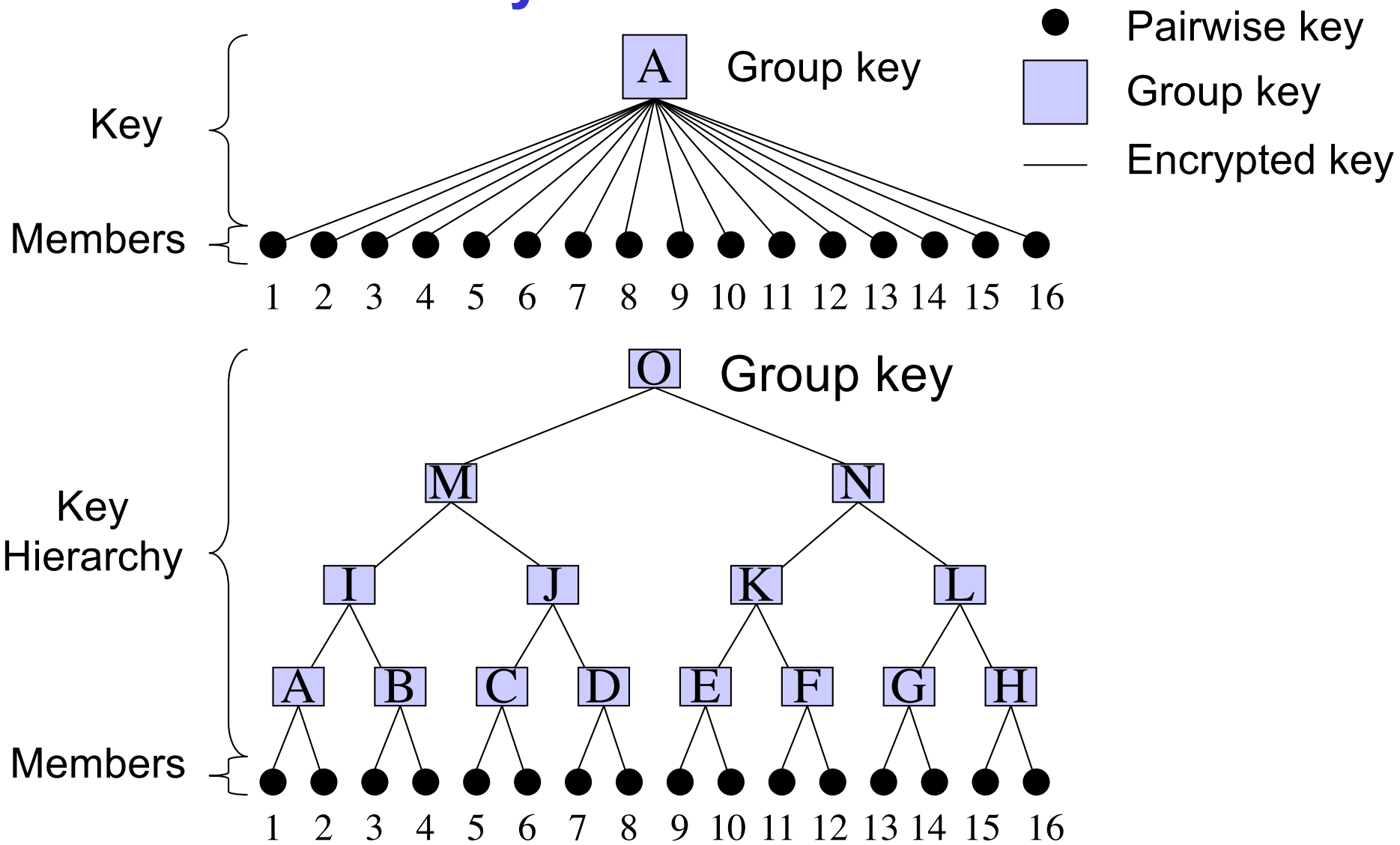
B. Iolus
   - Multicast group partitioned in several sub groups
   - GC manages a tree of group subcontrollers (GSC)
   - Each GSC manages a subset of the group membership
   - Advantage
     - The rekey effort is shared among GSC
   - Disadvantages
     - Large number of GSC in large groups
     - To trust subcontrollers
     - Additional delay

Key management techniques (2)

C. Logical Key Hierarchy (LKH)
   - Uses a set of keys arranged in a tree structure to reduce cost of rekeying
   - For fully populated tree (rekey 2. and 4.) outdegree k and depth d ➔ number of rekeys $k\log_k N-1$ instead of $N=k^d$
   - For binary trees (k=2) further optimization leads to $2*\log_2 2^d-1$

D. Kronos
   - If two users depart (case 4.) two rekey events occur
   - Some of the keys that change will be common to the two rekey events
   - Rekey traffic can be optimized rekeying every few seconds

Key hierarchies



Flat key management system

- N pairwise keys
- Each key shared between the GC and one of the N GM
- If the group key changes, the new group key is encrypted with each member's unique pairwise key and then sent to that member
- N encrypted keys are generated and transmitted across the network
- Key management network traffic volume independent of whether the keys are unicast, multicast or broadcast

LKH management system

- Tree (logical) of keys is used, characterized by outdegree k and depth d
- Each member holds the keys on the tree path from the member's pairwise key (at a tree leaf) back to the root
- Example: member 11 leaves the multicast group
  - All of the keys held by member 11 (F, K, N, O) must be changed and distributed to the members who need them
  - Bottom up procedure
  - GC chooses a new key for the lowest node (not the leaf for which a unicast secure association exists between GC and GM) and then sends it encrypted with the appropriate child key.
  - Key F replaced and the new key sent encrypted with member 12 unique pairwise key.
  - Key K replaced and sent encrypted with the new key F (GM 12) and sent encrypted with key E (GM 9 and 10).
  - Key N replaced and sent encrypted with the new key K (GM 9, 10, 12) and also encrypted with key L (GM 13-16)
  - Key O replaced and sent encrypted with the new key K (GM 9, 10, 12-16) and also encrypted with key M (GM 1-8)

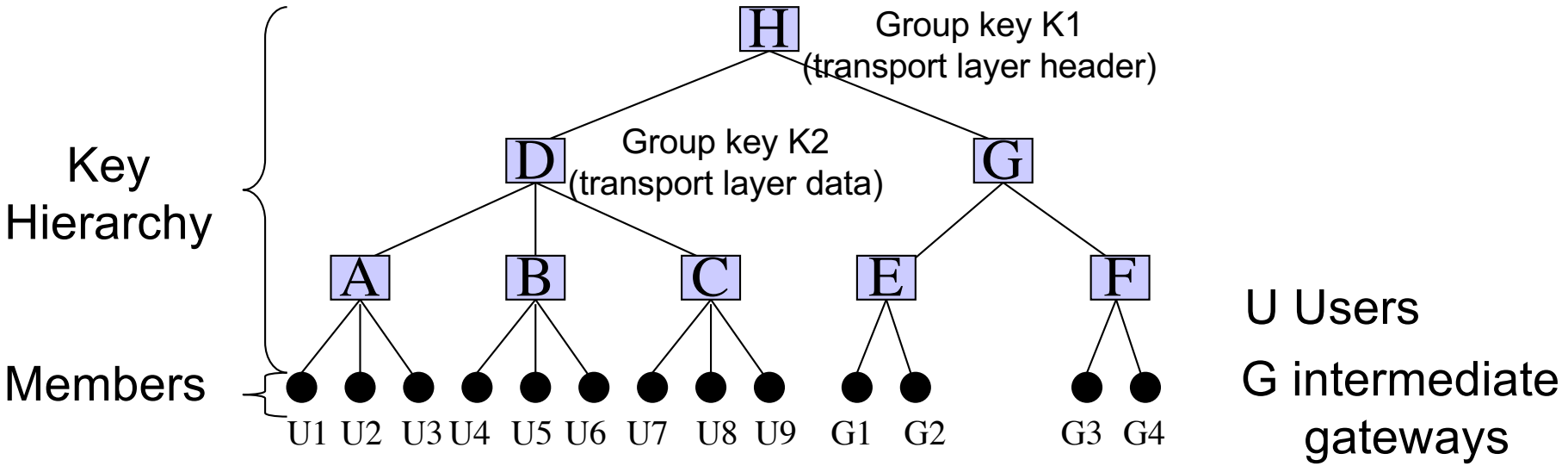
LKH management system (2)

- Each of the replacement keys replaced before used to encrypt another key
- The encrypted keys are multicast
- Result: 7 keys sent instead of 16 of the FLAT system
- The GTEK may either be key O or it may be encrypted using key O and transmitted to all GM.

Life cycle cost

- Cost factors= Initialization + updating group
- Assumption: updating the group is the main cost (?)
- Exception
  - FTP (population with low volatility)
  - Pay per view (subscribers join the group almost simultaneously, high demand on the establishment of the group secure association)

ML-IPSEC and LKH interworking



- Two separate LKH trees integrated into a single hierarchy
- All users and intermediate gateways are members of the multicast group
- User subtree k_U=3, gateway subtree k_G=2, root H two children, regardless k_U and k_G
- In LKH each member only knows the keys that lie on the path from the member leaf node to the root ➔ **users have access to both K1 and K2 while gateways access only K1**