Satellite Communications: Cyber security vulnerabilities and strategies

Fabio Patrone

Polytechnic School, University of Genoa

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

EUSPACE
European Union in Space
JEAN MONNET MODULE

Overview

UNIVERSITÀ DEGLI STUDI DI GENOVA

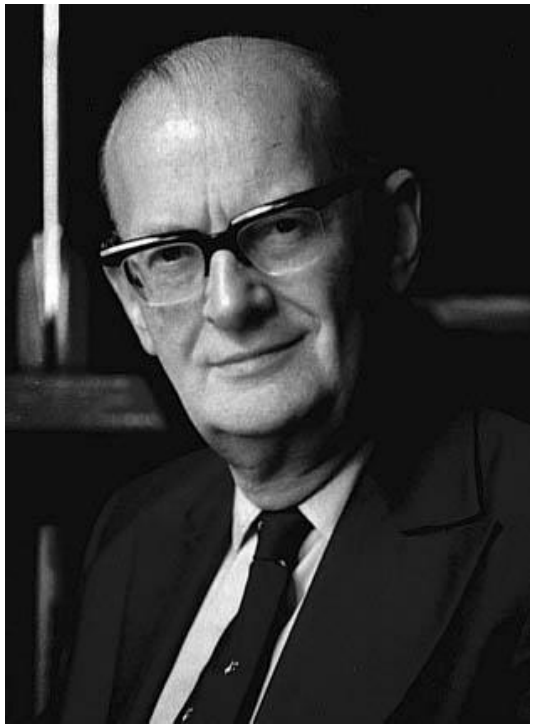
- Satellite mission goals, categories, structural subsytems, network architectures, and communication systems
- Cybersecurity vulnerabilities and threats
- Possible solutions and employable strategies

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

First person to talk about satellite

Arthur C. Clarke



Sir Arthur Charles Clarke was a British science fiction writer mainly known for the science fiction novel "2001: A Space Odyssey".

When he was a 27-year-old Royal Air Force officer published the paper "Extra-Terrestrial Relays: Can rocket stations give world-wide Radio Coverage?", in October 1945.

He was the first one to understand the importance of a satellite with a fixed position relative to a point on the Earth from a communication viewpoint.

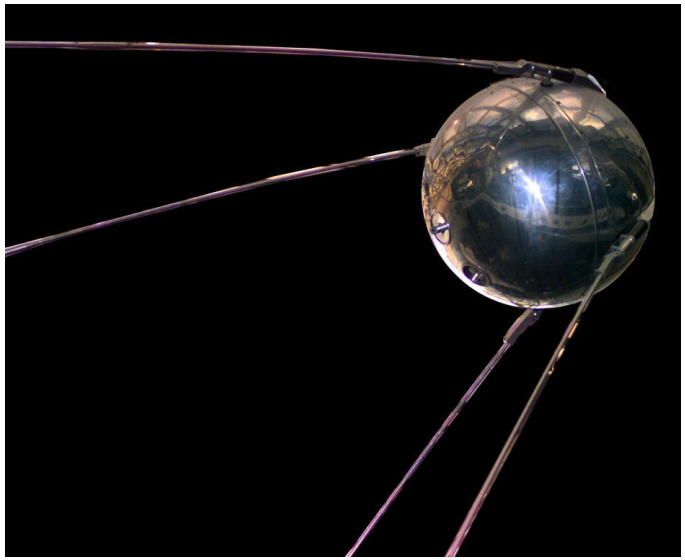
He wrote: "A true broadcast service, giving constant field strength at all times over the whole globe would be invaluable, not to say indispensable, in a world society".

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

First artificial satellite

Sputnik 1



Sputnik 1 was launched by the Soviet Union on 4 October 1957.

It was a 58 cm diameter metal sphere, 83.6 kg weight, with four external antenna.

It was active in an eliptical low Earth orbit (perigee 215 km, apogee 939 km) for 3 weeks and laid in the space for 3 months before its fall into the atmosphere.

It travelled at about 29000 km/h, 1440 orbits completed (96.2 minutes each), 1 Watt power, 20.005 and 40.002 MHz transmission frequency (radio amateur bands)

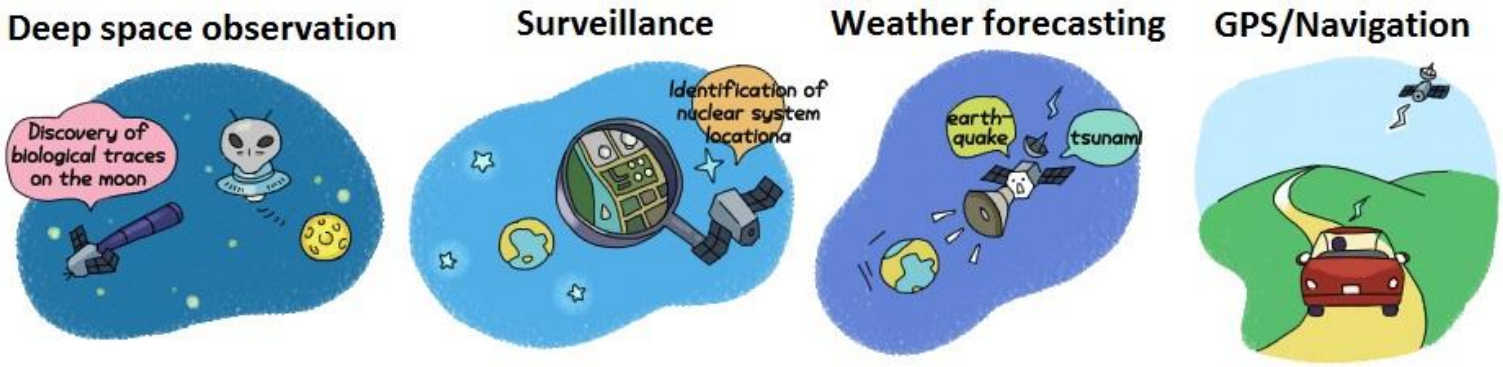
EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite classification

by mission goals

- Telecommunication (satellite phones, Internet, ...)
- Deep space observation
- Surveillance
- Earth observation and monitoring (disaster recovery, weather forecasting, ...)
- Remote Sensing
- GPS/Navigation
- Entertainment and content delivery



EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite classification

by weight

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite classification

by altitude

	Altitude [km]	Orbit time [min]	Speed [km/h]	Radius coverage area [km]	Example
Low Earth Orbit (LEO)	200÷2000	90÷120	28000÷25000	500÷2700	Iridium
Medium Earth Orbit (MEO)	6000÷35786	230÷1400	20000÷11000	5000÷7800	GPS
Geo-Stationary or Geo-Synchronous Earth Orbit (GEO)	35786	1436 (23 h, 56 min, 4 s - one sidereal day)	~11000	~8000	Inmarsat
Highly Elliptical or High Eccentricity Orbit (HEO)	not constant	not constant	not constant	not constant	Molnya

Most orbits are circular (altitude, orbit time and speed are constant)

Lower the altitude, smaller the coverage area and faster the satellite

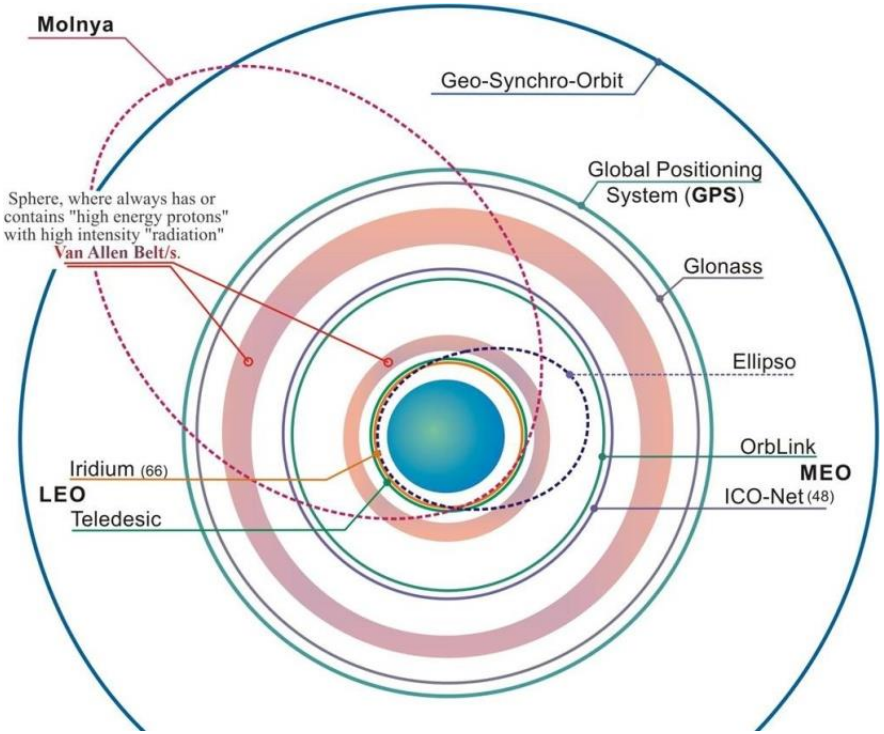
GEO satellites lay in an equatorial plane and are fixed points in the sky, while others move faster than the Earth's rotation speed

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite classification

Satellite orbits



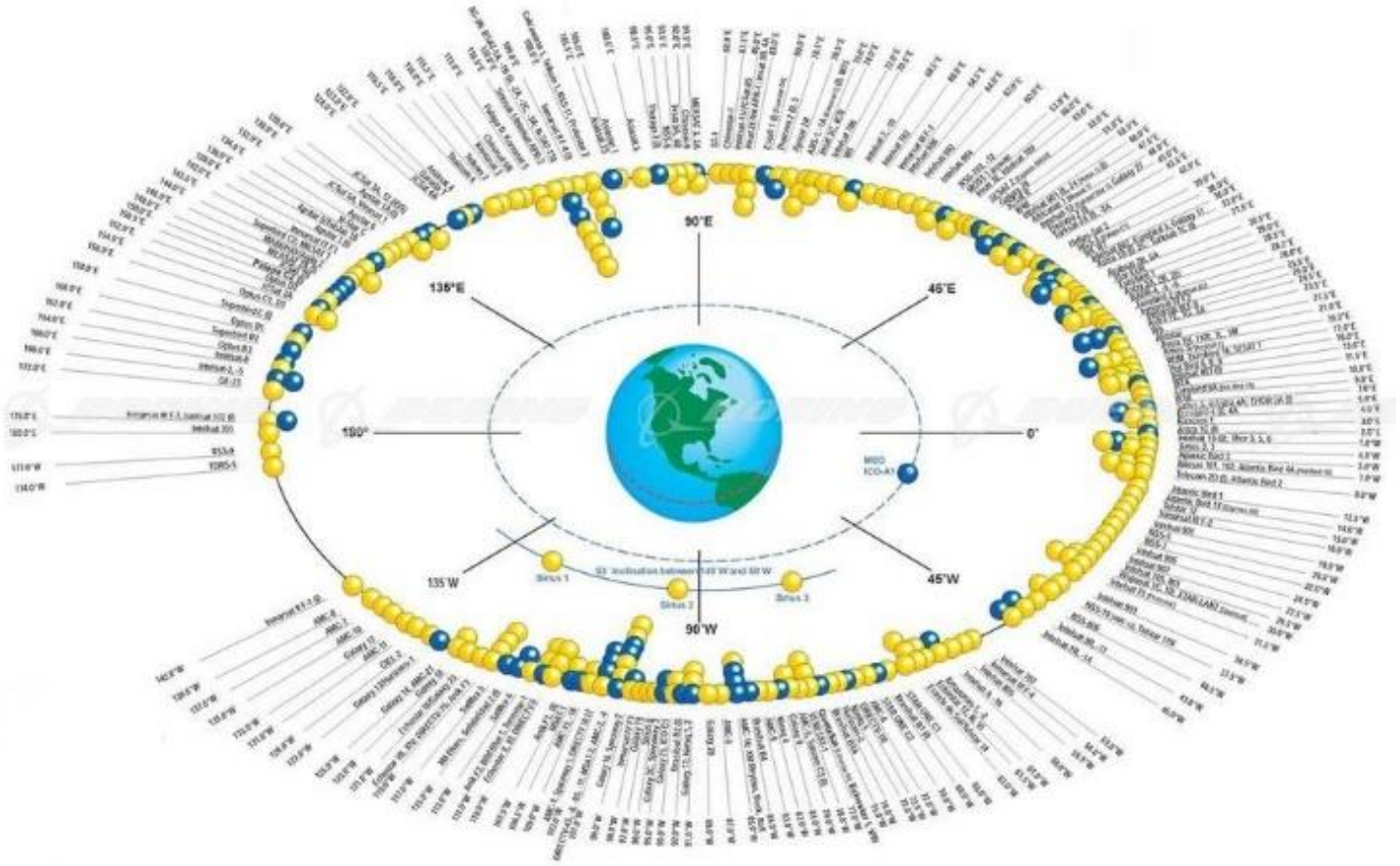
Van Allen radiation belts are zones full of energetic charged particles: Inner belt (1000÷6000 km), Outer belt (14500÷19000 km)

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite classification

GEO satellites



EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite classification

Space debris

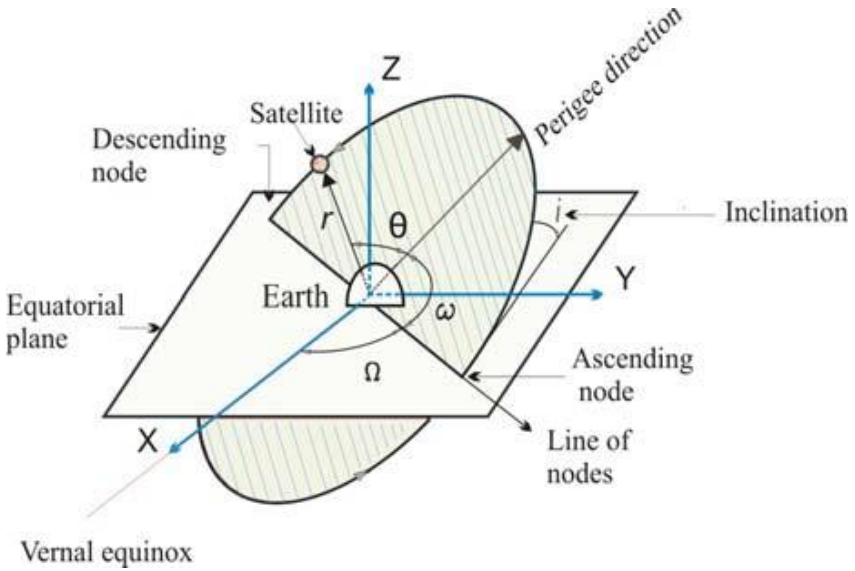
EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite classification

Orbital parameters

- ***eccentricity e***: it defines the shape of the orbit (e=0: circular, 0<e<1: elliptic);
- ***semi-major axis a***: it defines the size of the orbit (in a circular orbit, a is the radius of the orbit r);
- ***inclination i***: the angle of the orbital plane with respect to the Earth's equator;



- ***right ascension of the ascending node (RAAN) Ω***: angle which defines the location of the ascending and descending orbital crossing points with respect to the fixed direction in space called Vernal Equinox, which is the direction of the line joining the Earth's centre and the Sun on the first day of spring;
- ***argument of perigee ω***: angle, measured positively in the direction of the satellite's movement from 0° to 360°, between the direction of the ascending node and the direction of the perigee of the orbit. It indicates the orientation of the orbit in its plane;
- ***true anomaly θ***: angle, measured positively in the direction of the satellite's movement from 0° to 360°, between the direction of the perigee and the position of the satellite. It indicates the actual position of the satellite.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite classification

Kepler's laws

1. The orbit of every planet is an ellipse with the Sun at one of the two foci.

$$r = \frac{p}{1+e\cos\theta} \qquad r_{max} = \frac{p}{1-e} \qquad r_{min} = \frac{p}{1+e} \qquad a = \frac{p}{1-e^2} \qquad b = \frac{p}{\sqrt{1-e^2}} \qquad A = \pi ab$$

r: distance between planet (or satellite) and the Sun (or the Earth), p: semi-latus rectum, e: eccentricity, θ: true anomaly, a: semi-major axis, b: semi-minor axis, A: area ellipse

2. A line joining a planet and the Sun sweeps out equal areas during equal intervals of time.

3. The square of the orbital period of a planet is directly proportional to the cube of the semi-major axis of its orbit.

$$mr\omega^2 = mr\left(\frac{2\pi}{T}\right)G\frac{mM}{r^2}$$

m: mass of the planet (or the satellite), ω: angular velocity, T: orbit time, G: gravitational constant, M: mass of the Sun (or the Earth)

EUSPACE
European Union in Space
JEAN MONNET MODULE

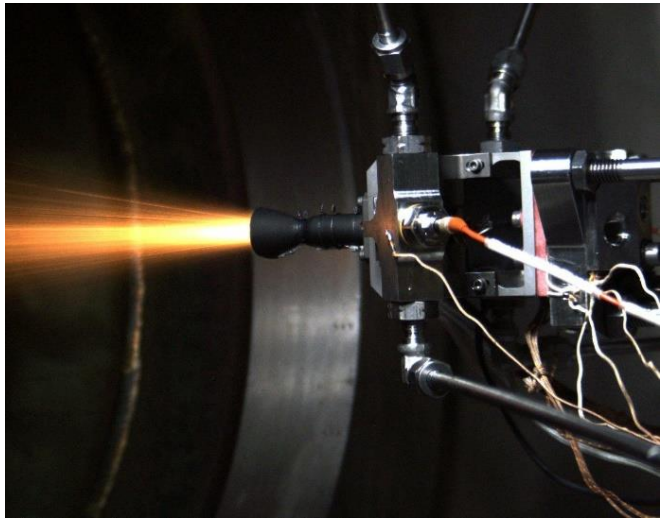
UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite hardware system

Satellite subsystems

External structure: the hardware skeleton which defines the shape of the satellite and allows all other hardware components to be merged together.

Propulsion: thrusters aimed at satellite position keeping, attitude control, reaction control and satellite de-orbiting at mission end. Different kinds of thrusters depending on the satellite weight, such as vacuum arc, colloid, electrospray, pulsed-plasma, which operate with different propellant, such as hydrogen perexodi or hydrazinium nitroformate (HNF) or ammonium dinitramide (ADN).

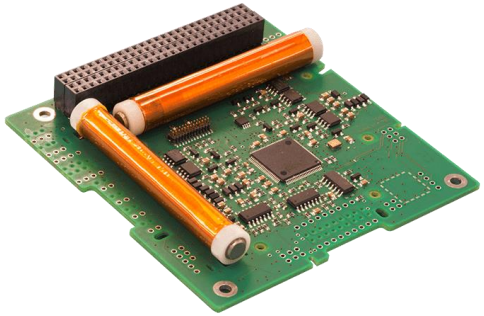


EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite hardware system

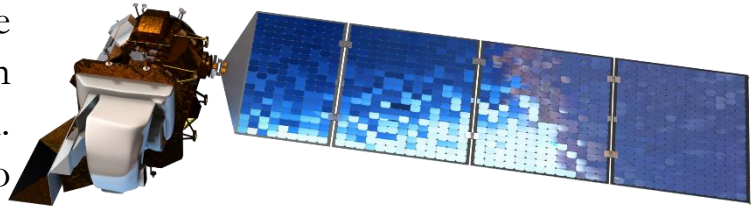
Satellite subsystems



Attitude Determination and Control (ADC): sensors aimed at measuring, maintaining and adjusting the orientation of the satellite as appropriate for mission requirements but also for power generation and communications.

Electrical Power System (EPS): manages all aspects related to power generation, storage, conditioning distribution and conversion. It includes:

- **Solar Panels**: can be fixed or deployable and generate power in all time periods when the satellite is in visibility with the Sun. They can produce from few Watts to hundreds of Watts. Most used are made of Gallium Arsenide or Silicon.
- **EPS card**: distributes all generated energy to all satellite subsystems
- **Batteries**: store the gathered energy keep all subsystem active during shadow periods. Most batteries are rechargeable and made of Lithium-Ion or Lithium-Polymer



EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite hardware system

Satellite subsystems

Command and Data Handling (CDH): It is the brain of the overall system. It collects mission and science data for transmission, provides the ability to execute received commands, controls the deployment of the antennas and solar panels and provides some measure of robustness in order to cope with failing subsystems.

Data reception/transmission: allows command & control messages reception and data transmission and reception in the scheduled frequency band. It includes:

- **Transceivers**: include transmitter and receiver combining and sharing common circuitry
- **Antennas**: generate and capture radio waves. They can have different shapes, such as dish or dipole, and size depending on the exploited frequency band

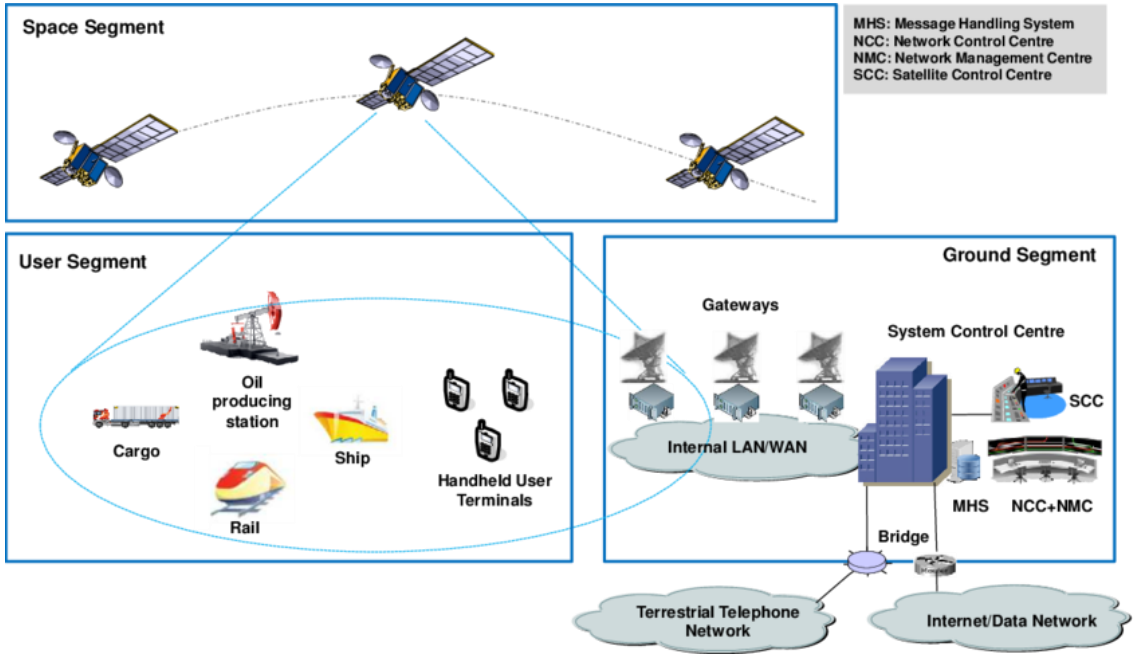
All these subsystems constitute the **primary system**. All other hardware components related to each specific mission goal, such as sensors, camera, high memory storage, ….. constitute the so called **payload**

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite communications

Network architecture



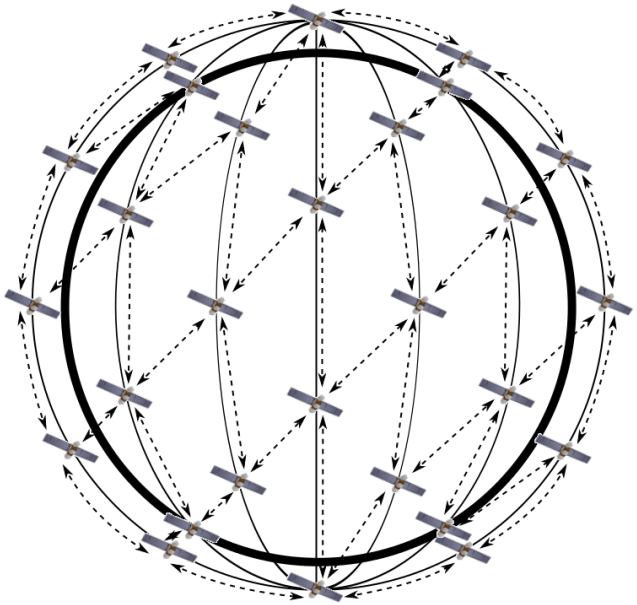
- **Space segment**: satellite or satellite constellation
- **Ground segment**:
  - **Satellite gateways**: guarantee access to satellites acting as interfaces between satellites and ground infrastructure
  - **System Control Centre**: control and manage satellite network resources and supervise the service provision
- **User segment**: user terminals, both stationary and mobile

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

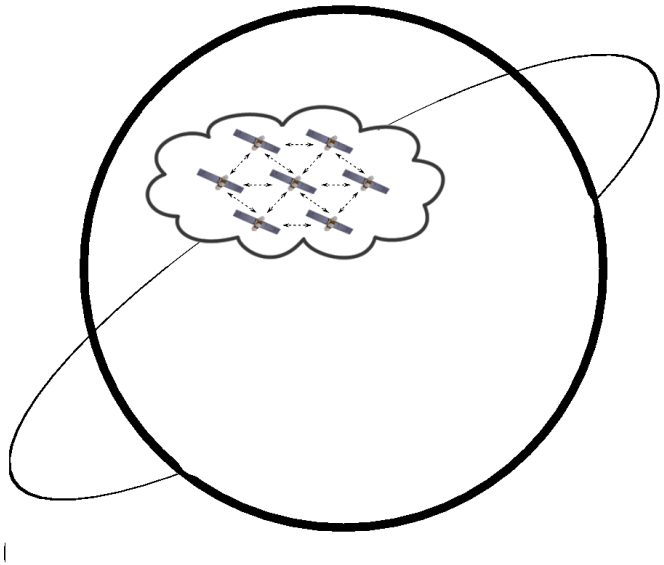
Satellite communications

Network topologies



Constellation

All satellites are equally spaced in the chosen orbital plane (or planes) owing to their sequential deployment. They can cover a greater area, even the entire Earth's surface



Swarm

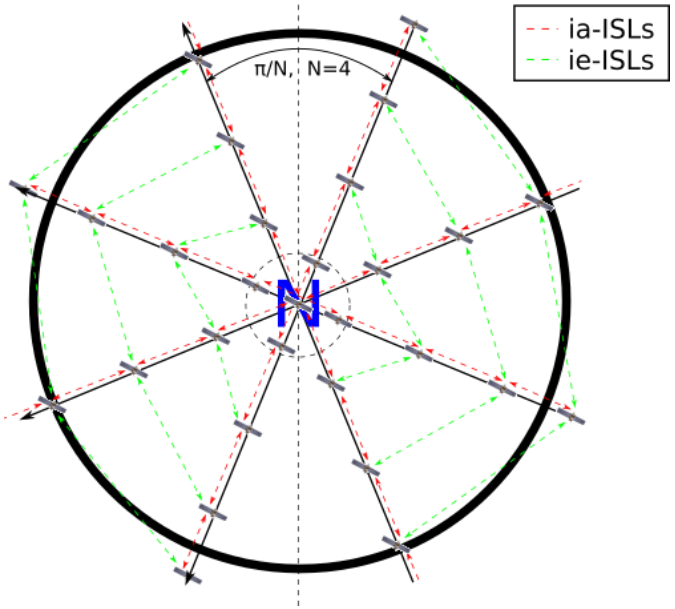
All satellite are very close to each other owing to their rapid deployment one after the other. They can share the available resources (energy, processing power, storage capacity, …)

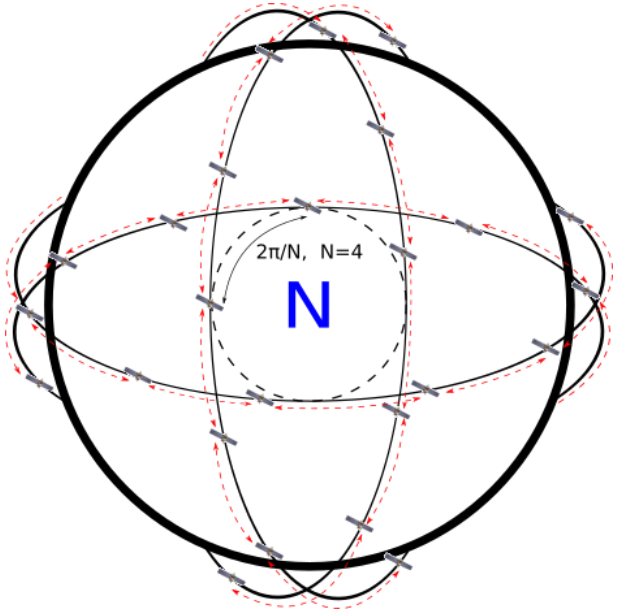
EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite communications

Constellation kinds





π- or star or polar

All orbital planes N have the same inclination (near 90°) and are equally spaced with an angle of π/N. It offers high coverage especially in polar zones. Data exchange through Inter-Satellite links (ISL) among satellites of the same orbit (Intra-orbit ISL "ia-ISL") or of different and adjacent orbits (Inter-orbit ISL "ie-ISL")

2π- or delta or rosette

All orbital planes N have the same inclination (lower than 90°) and are equally spaced with an angle of $2\pi/N$. It allows obtaining a better coverage at mid-latitudes. Data exchange through Inter-Satellite links (ISL) only among satellites of the same orbit (Intra-orbit ISL "ia-ISL")

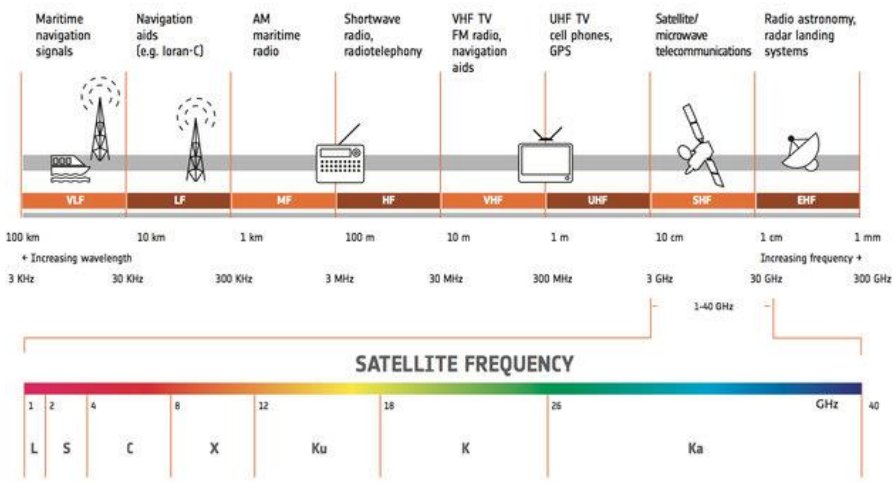
EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite communications

Link parameters

- **Transmission rate**: from few kbps to hundreds on Gbps (few Tbps in the near future) depending on the frequency band
- **Attenuation factors**: different kinds of attenuations depending on the transmission frequency, such as gases absorption, antenna misalignment, fading, scattering, ionospheric scintillation, rain



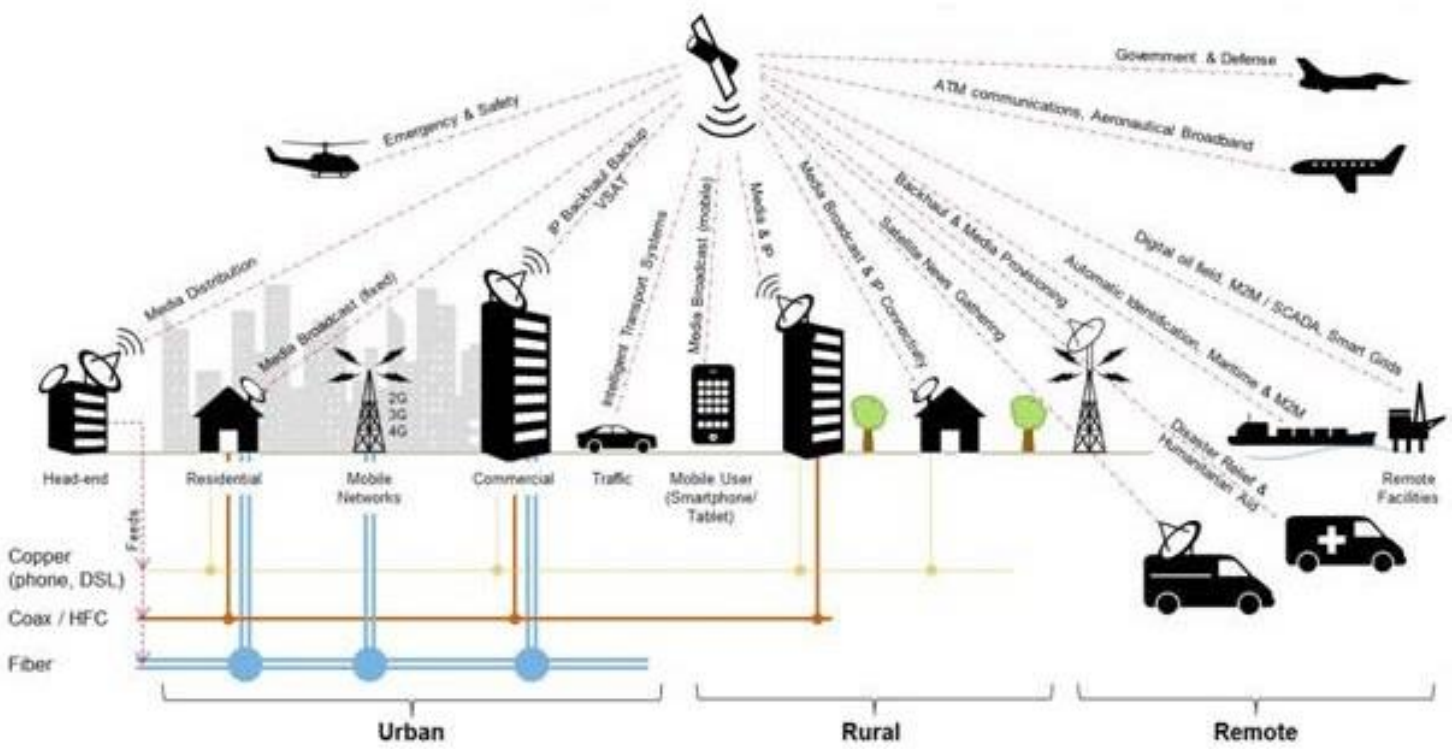
- **Propagation delay** (one-way): from 1 to 140 ms depending on the satellite altitude and elevation angle
- **Loss rate**: high loss rates highly variable depending on a lot of different parameters such as the frequency band

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite communications

Possible applications



EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite communications

Positive aspects

- **Coverage**: satellites can cover the entire Earth's surface
- **Availability**: satellites can always be available providing a persistent service without any disruptions
- **Reliability**: most satellites keep functioning for the entire planned lifetime without irrecoverable damages which make satellites inoperable
- **Group communications**: satellite can forward data to different users located in different geographical areas at the same time owing to their broadcast capability
- **Energy consumption**: satellites are self-sustainable for the energy viewpoint and do not require terrestrial energy sources

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite in the near future

Role of satellites in 5G

- **Extend the Internet access** to people who live in areas without a terrestrial infrastructure, such as rural and remote areas
- **Increase resilience and reliability** of the entire 5G network acting as a backup solution, for example in case of emergency and disaster situations where the terrestrial infrastructure has been damaged
- **Offload the terrestrial network** of data belonging to delay-tolerant applications, such as Internet of Things (IoT) and Machine-to-Machine (M2M) communications, in case of congestion
- **Move data at the edge** of the terrestrial network (nearest to the final users) to decrease the latency and increase the end users' Quality of Experience (QoE)

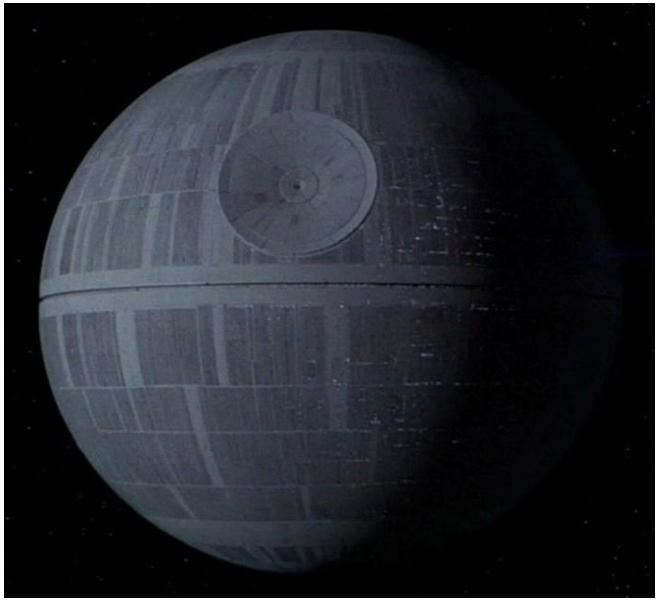
EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite cyber security

System design

A **system** should be designed having in mind all possible security vulnerabilities in order to minimize them, define proper system requirements and control procedures, employ proper mechanisms to increase the security, and consider proper strategies to be carried out when needed



<u>Bad example to avoid</u>

Do not design a big and powerfull space station which can be destroyed by a single small starfighter!!!

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite cyber security

General view

Security can be defined as the process of minimizing the vulnerabilities of assets or resources

The first task is to assess the security threats to the system.

A **threat** is "a potential violation of security which may result in harm of systems and organizations"

A **threat agent** (or **threat source**) can be human or non-human, intentional or unintentional, and attempts to do harm against a physical or logical resource/asset

The **threat assessment** process should assess the vulnerabilities of the system and then establish the likelihood, consequences and cost of realization of each threat. A threat is a problem only if the system is vulnerable

Specific security services should be identified to counter each threat/vulnerability. The selection of countermeasures requires a cost-benefit analysis to justify the implementation cost of security services

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite cyber security

General view

Any remaining vulnerabilities are deemed residual risk and must be accepted by system management before putting the system into production

A **risk** is "a possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability" and is a function of the impact of an occurrence and the likelihood of that impact's occurrence

The **risk assessment** exploits the output of the threat assessment to assess the likelihood of any potential impact occurring, and should also identify, for each risk found, a security control to reduce that risk or a recommendation to accept it

Each designer should develop a **System Security Plan (SSP)** that references and provides a summary of the system security requirements, describes the security controls in place or planned for meeting those requirements, and describe the threat and risk assessment of the system for each phase of the planned mission

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite cyber security

Threat assessment

Construct Representative Mission Scenarios

- Human space flight
- Meteorological satellite
- Communications satellite
- Science mission
- Navigation satellite

→ **Identify Threats to Space Missions**

↓ **Assess Impact of Threats on Scenarios**

↙ **Identify Candidate Security Mechanisms to Counter Each Threat**

→

- If the *threat* is viable and cannot be countered, it becomes a *risk*.
- If the *threat* is exploitable, the system becomes *vulnerable*.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite cyber security

Security controls

The aim of a security control framework is to test the designed system. Most **security controls** can be classified as belonging to one of three basic types*:

1. **Proactive**: designed to prevent a negative event from occurring
2. **Detective**: aim to detect and inform about the occurrence of a negative event
3. **Reactive**: restore the system to nominal operation and/or collect information about the nature and consequences of a negative event

In the past, space civil and scientific missions were not likely targets of malicious attackers, but in today's global environment of ubiquitous cyber threats this view is no longer true

To date, as space systems become increasingly more interconnected with ground-based networks, including the Internet, it becomes more important to provide an integrated approach to address all security concerns

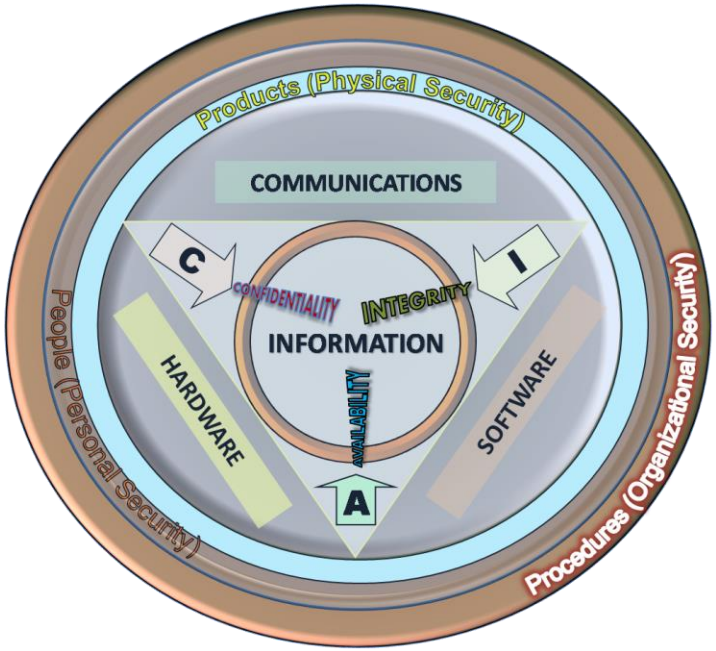
* a complete list is reported in «Security guide for mission planners», CCSDS's Informational Report 350.7-G-1

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite cyber security

Security properties



CIA interactions scheme

- **Confidentiality**: assurance that information is not intentionally or accidentally disclosed to unauthorized individuals
- **Integrity**: assurance that information in not intentionally or accidentally modified in such a way as to call into question its reliability
- **Availability**: assurance that users have both timely and reliable access to information when needed

In space missions: confidentiality prevents the disclosure of sensitive information contained within any part of the space mission data system; integrity ensures that mission data has not been manipulated in any way during transmission across ground segments or over satellite links; availability ensure satellite access to the control station every time a contact with a satellite gateway is ongoing

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite cyber security

Security properties

- **Access control**: process of granting access to the system's resources only to authorized entities inhibiting unauthorized use of a resource
- **Authentication**: ability to verify the identity of a user, device, or other entity as a prerequisite to allow access to a resource
- **Accountability**: all system actions are logged along with the identity of the entity performing the action and the date and time the action occurred

In space missions: access control includes mechanisms and procedures to enable only approved operators to access the mission control system; authentication assures that the received data has been sent by an authorized space mission control centre; accountability records all satellite network actions in a log for later use (for example in case of forensics analysis)

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite cyber security

Potential attack consequences

If satellite commands were disclosed to unauthorized entities, unauthorized commands could be sent to the satellite, resulting in possible harm or total mission loss

The corruption of satellite telemetry data may lead to unnecessary and potentially dangerous commands from the control station

Unauthorized access may result in the distribution of private information to unauthorized entities

Due to the unbounded nature of satellite links, access to satellites can be prevented at all jamming the transmission/reception frequencies or overloading the network with unauthorized traffic flows

If unauthorized entities gain access to satellite resources, they can hack satellites with different possible consequences, from satellite deviation to prolonged data theft

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security threats

Passive attacks

Passive attacks do not involve any modifications of the normal system's operations. They are typically accomplish by **eavesdropping / interception** and mainly compromise data confidentiality

In space systems, there are mainly two types of passive attacks:

1. **Tapping on communications links** (wireless or wired)
2. **Traffic analysis** to know information about data travelling through the system, such as source and destination entity and traffic volumes

Passive attacks entail loss of confidentiality

Possible solutions: data encryption, Spread Spectrum techniques

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security threats

Active attacks

Active attacks modify the normal system's operations with different aims and can lead to several different consequences.

Most common active attacks are:

- Data and commands corruption/modification
- Jamming
- Denial-of-Service
- Masquerade
- Replay
- Software threats

EUSPACE
European Union in Space
JEAN MONNET MODULE

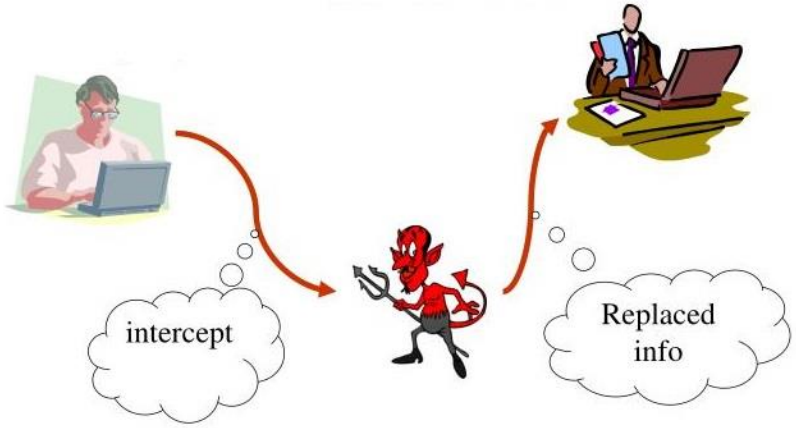
UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security threats

Data corruption/modification

Applicable to: space segment, ground segment, space-link communications

Possible mission impact: loss of data integrity



Description: Data corruption/modification refers to the intentional or non-intentional alteration of data, whether being communicated or stored. The corruption can take place at the sources or in transit within the system: within the ground segment, in transmission to/from or on-board satellites.

Possible solutions: data integrity schemes (Hashing, Digital Signature), data encryption

EUSPACE
European Union in Space
JEAN MONNET MODULE

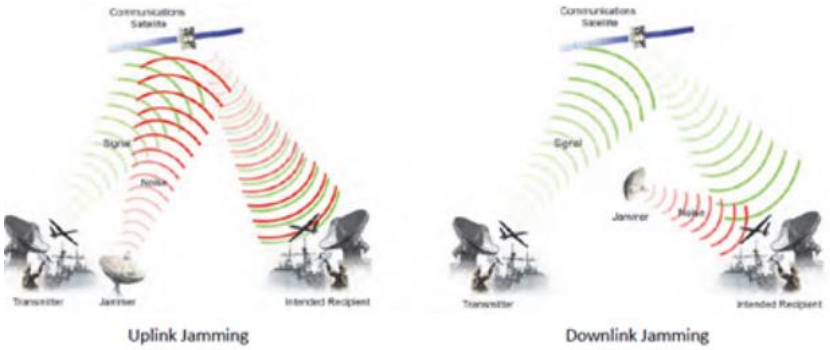
UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security threats

Jamming

Applicable to: space segment, ground segment, space-link communications

Possible mission impact: authorized access blocked, delay in operations, data losses, mission control loss



Description: the attacker interferes with the radio signal in satellite links by injecting noise, by transmitting on the same frequency of authorized transmissions, or by overpowering the original source signal. The ability to send/receive any kind or data and to have access to the satellites is blocked

Possible solutions: multiple uplink/downlink paths, multiple access points, Spread Spectrum techniques

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security threats

Denial-of-Service (DoS)

Applicable to: space segment, ground segment

Possible mission impact: loss of system availability, mission control loss, inability to obtain data

Description: DoS attacks seek to make the attacked system unable to perform their proper functions and provide its service to the authorized entities. They can performed saturating the available resources (computational power, memory capacity, channel bandwidth) or disrupting network configurations and components

Possible solutions: Firewall, Intrusion Prevention System, Encryption and Authentication

EUSPACE
European Union in Space
JEAN MONNET MODULE

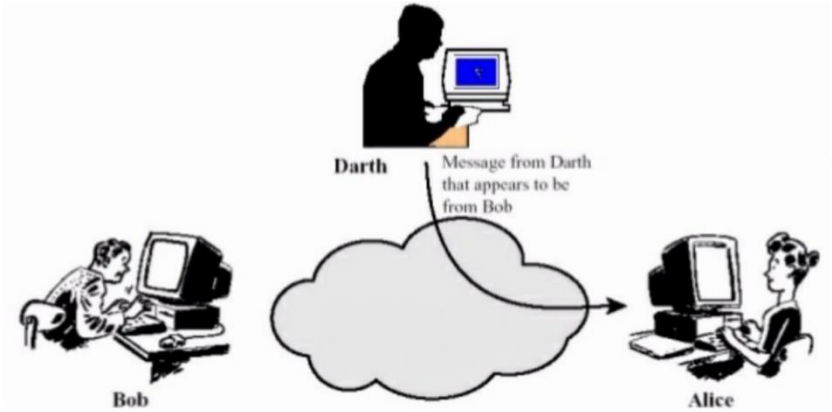
UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security threats

Masquerade

Applicable to: space segment, ground segment

Possible mission impact: sent of unauthorized commands, data loss, mission loss



Description: the attacker lies about their true identity or pretends to be an authorized entity in order to gain access to the system or to gain greater privileges

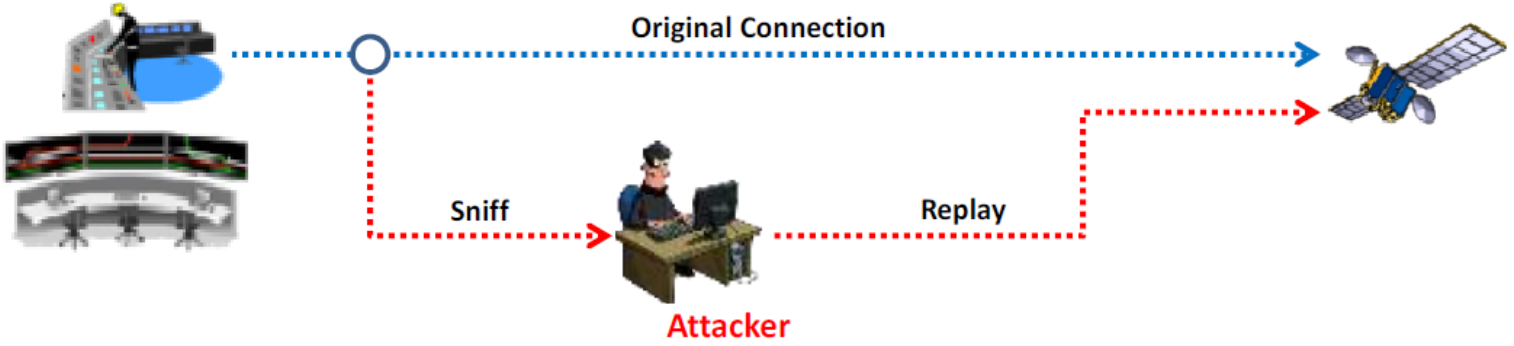
Possible solutions: Authentication, Intrusion Prevention System, Intrusion Detection System

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security threats

Replay



Applicable to: space segment, ground segment, space-link communications

Possible mission impact: damages due to multiple executions of the same commands or multiple reception of the same telemetry data

Description: transmissions to or from satellites or among ground segment nodes are intercepted, recorder, and played back at a later time

Possible solutions: data integrity schemes (Hashing, Digital Signature), Intrusion Prevention System, Intrusion Detection System

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security threats

Software threats

Applicable to: space segment, ground segment

Possible mission impact: data loss, mission control loss, unauthorized satellite control

Description: software threats include but are not limited to **Viruses** (infect and disrupt computers of the network), **Worms** (infect and try to replicate themselves throughout the network), **Trojan horses** (infect the system by masquerading themselves inside other data apparently normal), **Spyware** (cause systems slow down or unauthorized information leakage)

Possible solutions: Anti-virus

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security threats

Unauthorized access

Applicable to: space segment, ground segment

Possible mission impact: loss of both satellite gateways access and satellite control, sent of unauthorized data and commands, mission shut down, data contamination

Description: attacker can exploit intercepted sensitive data such as passwords to take control of the system

Possible solutions: Command encryption, Authentication, Intrusion Prevention System, Intrusion Detection System

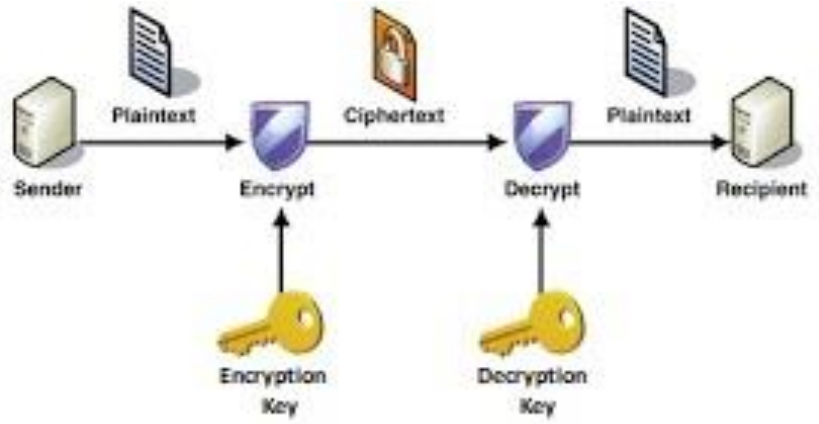
EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Cryptography

Encryption and **decryption** transform sensitive data (*plaintext*) in less sensitive data (*ciphertext*) and vice versa by using appropriate keys in order to unable unauthorized entities to have access to them.



Encryption algorithms may be:

- **Symmetric**: encryption and decryption keys are the same (Data Encryption System – DES, Advanced Encryption System – AES)
- **Asymmetric**: encryption key (*public key*) and the decryption key (*private key*) are different (Rivest-Shamir-Adleman – RSA, Elliptic Curve Cryptography – ECC)

Combinations of symmetric and asymmetric algorithms (hybrid encryption) are widely employed

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Symmetric Key Infrastructure (SKI)

Symmetric (or secret) Key Infrastructure makes use solely of secret (or symmetric) keys originated starting from a shared secret among involved entities and thanks to proper negotiation protocols.
The decryption function is the exact reverse of the encryption function.

ADVANTAGES

- **Simplicity**: SKI architecture is simple and straight forward, it can be easily deployed
- **Performance**: SKI outperforms asymmetric encryption in processing speed and required memory to store shared secret and keys

DRAWBACKS

- **Require an additional secure channel**: to provide the distribution of the initial shared secret (it can also be stored in the satellite read-only memory before the launch)
- **Limited scalability**: all entities must share the same secret key
- **Missing identity binding**: there is no way to be sure of the owner's identity of a key

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) uses pairs of keys (private and public) to establish secure communication channels. Public keys are known while private keys are kept secret.
Texts are encrypted with public keys and can be decrypted only by using the related private key, which is stored in the destination entity memory and has never been sent through the insecure communication mean.
Public **certificates** bind the public keys to their respective owner entities. They are generated by trusted authorities called Certification Authorities (CAs).

ADVANTAGES

- **Identity binding**: the identity of each entity is binded to a public key through a certificate
- **Scalability**: it is better for a large number of entities than that of a SKI
- **Better control**: certificates have an expiration date and can be revocated for several reasons, such as the owner's private key is compromised
- **Initialization**: key establishment is easier since no initial shared secret is required to be exchanged

DRAWBACKS

- **High complexity**: a greater number of entities is required to properly configure and deploy the system
- **Performance**: PKI has worse performance than SKI in terms of processing speed and requires higher memory to store key pairs and certificated

EUSPACE
European Union in Space
JEAN MONNET MODULE

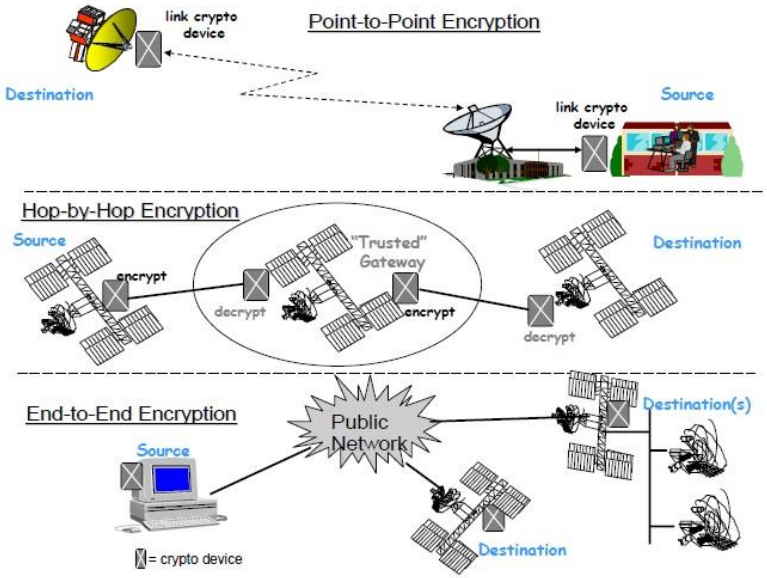
UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Cryptography

Cryptography may be:

- **Point-to-point**: only between two entities
- **Hop-by-hop**: data are decrypted and re-encrypted by each intermediate node
- **End-to-end**: encryption and decryption are applied only at the source and destination, respectively



Cryptography can contribute in assuring confidentiality, integrity, and authentication and in increasing protection against Eavesdropping, Data corruption/modification, and Unauthorized access attacks

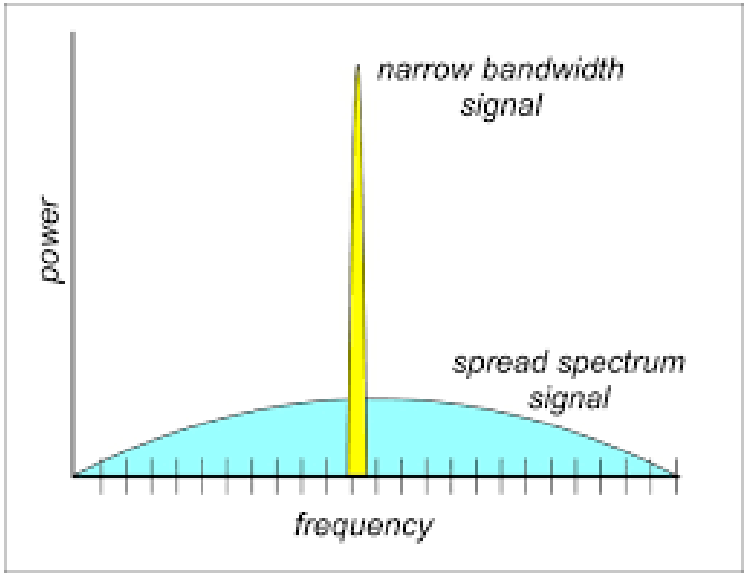
EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Spread Spectrum (SS)

Spread Spectrum (SS) techniques spread in the frequency domains the signal generated with a certain bandwidth in order to prevent their detection to increase their resistance to natural interferences, noise, and jamming



Most common SS methods are:

- **Direct Sequence (DS)**: data is divided into small pieces each of which is allocated to a different small frequency sub-band across the wide allocated frequency band
- **Frequency Hopping (FH)**: data is transmitted over a single small frequency band which frequently changes over time during the transmission

SS techniques contribute in increasing availability and protection against Eavesdropping and Jamming attacks

EUSPACE
European Union in Space
JEAN MONNET MODULE

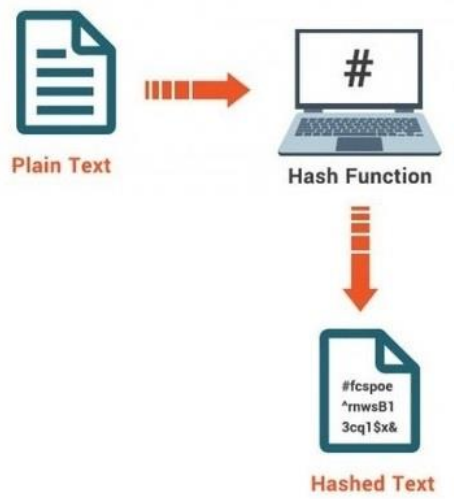
UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Data integrity schemes

Data integrity schemes enable receiver users to verify if the received data have not been modified during transmission.

They also allow to authenticate the received data in order to verify the sender identity



Most common data integrity schemes are:

- **Hash functions** (Message Digest 5 – MD5, Secure Hash Algorithms – SHA): one-way functions which univocally generate a block of data of fixed size for each message which are attached to the original message
- **Digital Signature**: messages are encrypted by using the sender private key. In this way, they can only be decoded by using the sender public key, confirming that they have not been modified and they have been send by the correct entity

Data integrity schemes contribute in assuring data integrity and authentication and in increasing protection against Data corruption/modification and Replay attacks

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Firewall and anti-virus

Both **firewalls** and **anti-virus** are solutions aim at increasing system's robustness against malicious software

- **Firewall**: its aim is to filter the incoming traffics in order to block the unauthorized and possibly malicious new traffic connections acting as a barrier between the trusted network to protect and the untrusted external networks
- **Anti-virus**: software used to prevent, detect, and remove malicious software installed inside the nodes of the protected network

Firewall and anti-virus contribute in increasing protection against Software threats and Denial-of-Service attacks

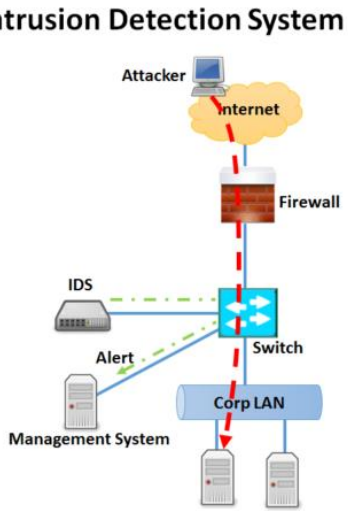
EUSPACE
European Union in Space
JEAN MONNET MODULE

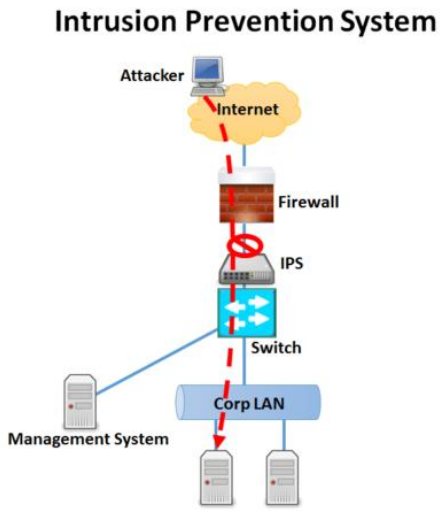
UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Intrusion Detection System (IDS)
Intrusion Prevention System (IPS)

- **Intrusion Detection System (IDS)**: passive solution which analyses the traffic flows travelling across the protected network in order to identify and report unusual behaviours





- **Intrusion Prevention System (IPS)**: active solution which inspects traffic flows through the protected network and blocks the ones with malicious data

IDS and IPS contribute in increasing protection against Denial-of-Service, Masquerade, Replay, and Unauthorized access attacks

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Terrestrial security protocols

- **Transport Layer Security (TLS)**: TLS offers end-to-end data encryption aims primarily to provide privacy, data integrity and confidentiality. It includes symmetric cryptography to encrypt transmitted data and asymmetric cryptography to guarantee entities authentication
- **Internet Protocol Security (IPSec)**: IPSec is a secure network protocol suite which provides network-level authentication, data integrity and confidentiality, and protection against replay attack
- **Secure Shell (SSH)**: SSH allows connecting two nodes providing a secure channel over an unsecure network.. It contributes in increasing authentication robustness and protection against unauthorized access

Another possible solution to increase authentication robustness and protection against unauthorized access is called **Virtual Private Network (VPN)** aims to extend a private network across a public network

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Satellite security protocols

- **Satellite data bulk encryption**: point-to-point encryption of the full physical layer data structure. It provides the highest possible available level of data confidentiality

- **Space Data Link Security**: protocol suit which includes data link security protocols such as **Telecommand (TC) Data Link security** and **Telemetry (TM) Data Link security protocols**. It offers confidentiality, integrity, and authentication applying hop-by-hop cryptography

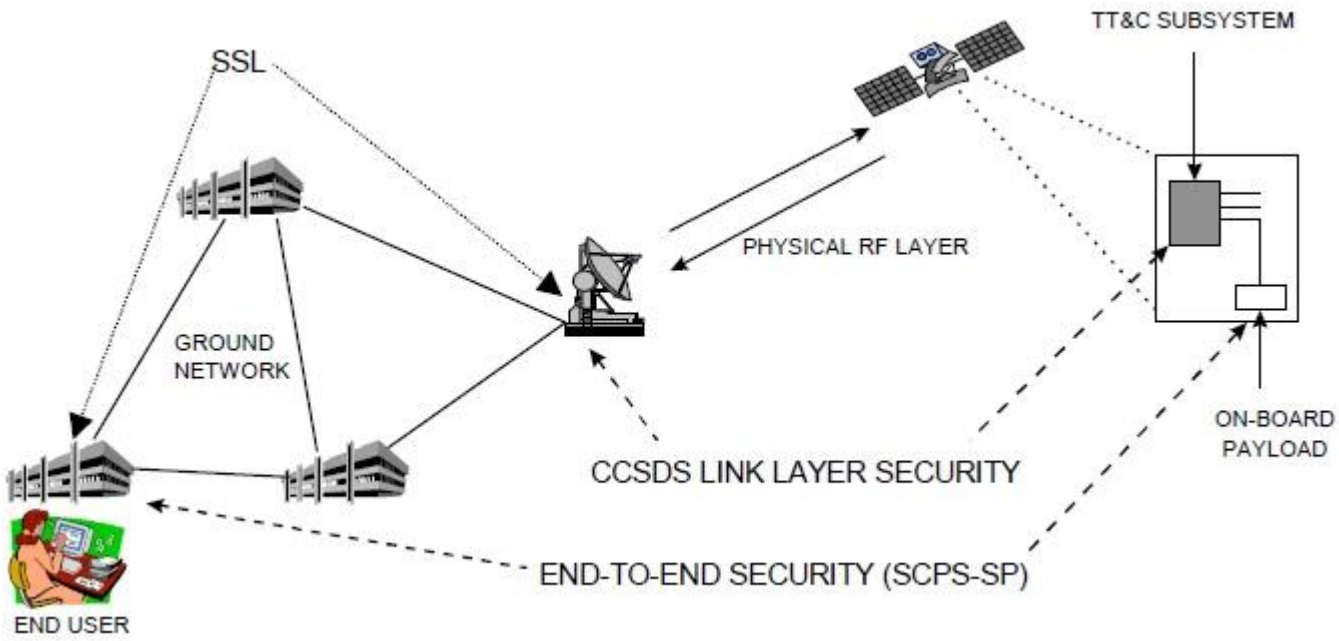
- **Space Communication Protocol Specification – Security Protocol (SCPS-SP)**: SCPS-SP has been designed to offer end-to-end security services ensuring minimal overhead size.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Satellite and terrestrial protocols combination



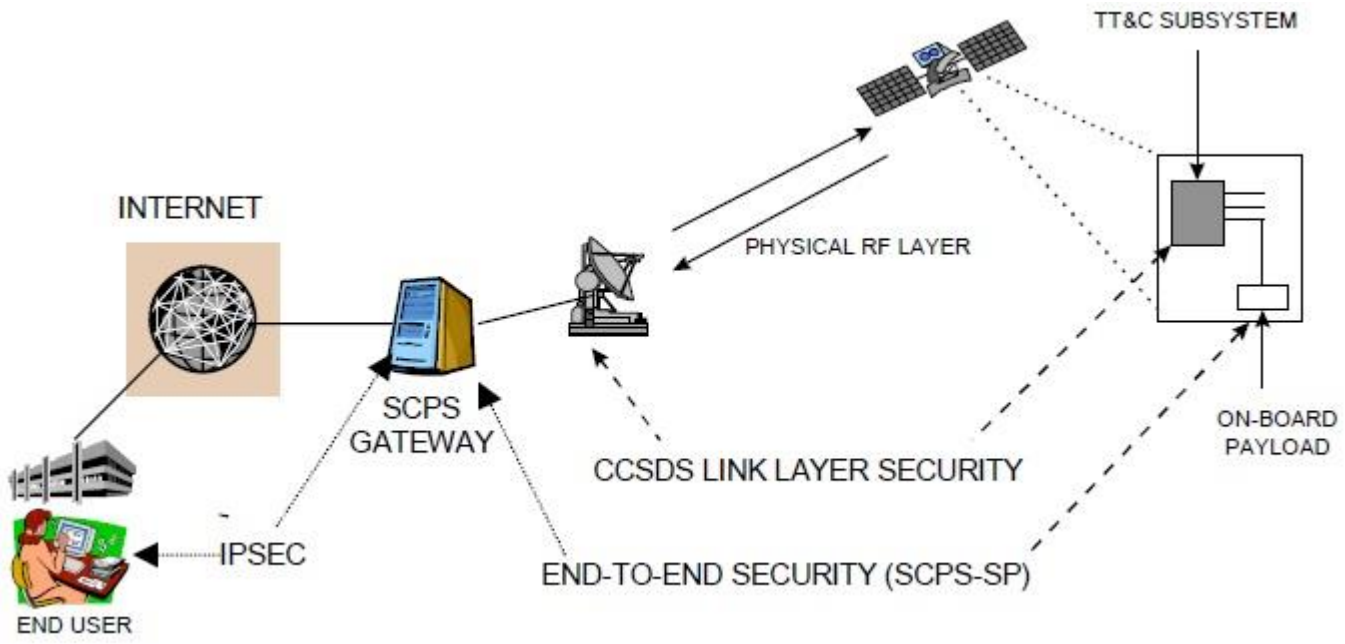
Some systems may require security mechanisms to guarantee end-to-end data protection and lower layer security solutions operating only on satellite links to prevent traffic analysis.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Satellite security solutions

Satellite and terrestrial protocols combination



In case both authorized users and satellite gateways are connected through the Internet, Internet security protocols, such as IPSec, and space security protocols can be jointly employed to guarantee security inside the ground segment (from users to satellite gateways) and the space segment, respectively

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Reference documents

[1] "Security threats against space missions", CCSDS's Informational Report 350.1-G-2

[2] "Security guide for mission planners", CCSDS's Informational Report 350.7-G-1

[3] "CCSDS guide for secure system interconnection», CCSDS's Informational Report 350.4-G-1

[4] "The application of CCSDS protocols to secure systems", CCSDS's Informational Report 350.0-G-2

[5] "Space missions key management concept", CCSDS's Informational Report 350.6-G-1

[6] "Security architecture for space data systems", CCSDS's Recommended Practice 351.0-M-1

[7] "Space data link security protocol", CCSDS's Recommended Standard 355.0-B-1

[8] "Space data link security protocol – Summary of concept and rationale", CCSDS's Informational Report 350.5-G-1

[9] "Network layer security adaptation profile", CCSDS's Recommended Standard 356.0-B-1

[10] "CCSDS cryptographic algorithms", CCSDS's Recommended Standard 352.0-B-1

[11] D. Housen-Couriel, "Cybersecurity threats to satellite communications: Towards a topology of state actor responses", Acta Astronautica, vol. 126, pp. 409-415, 2016.

[12] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou, S. Papademetriou, "Security issues in hybrid networks with a satellite component", IEEE Wireless Communications, vol. 12, no. 6, pp. 50-61, 2005.

[13] X. Wang, J. Du, J. Wang, Z. Zhang, C. Jiang, Y. Ren, "Key issues of security in space-based information network review", International Conference on Cyberspace Technology (CCT), pp. 1-6, 2014.

EUSPACE
European Union in Space
JEAN MONNET MODULE

THANK YOU!
ANY QUESTIONS?

UNIVERSITÀ DEGLI STUDI DI GENOVA