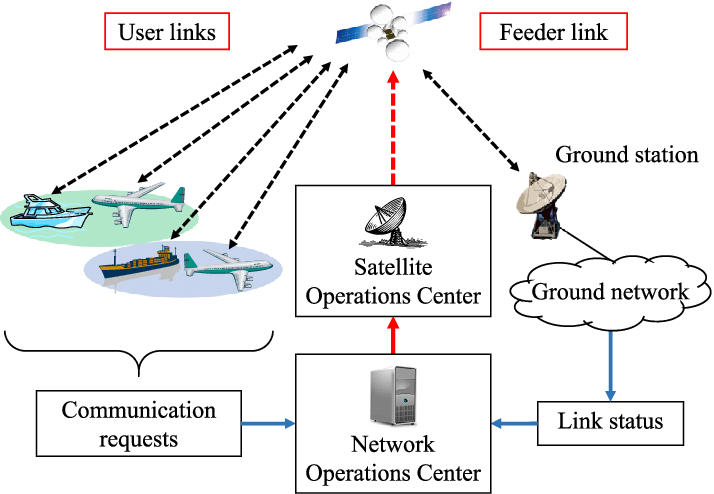
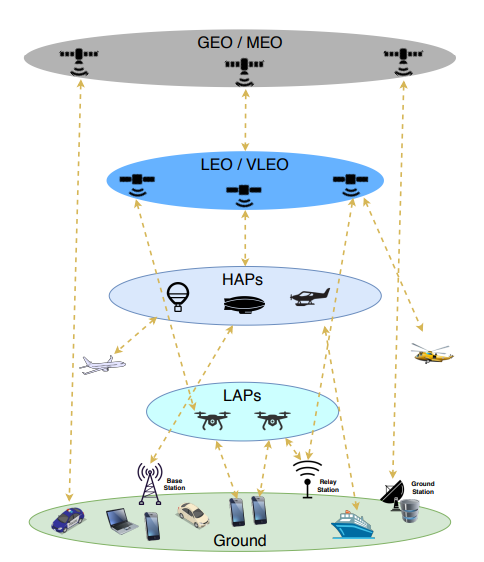
Satellite communication is a critical component of modern communication networks, with numerous advantages and disadvantages that must be considered. One of the key benefits of satellite communication is its global availability, as a large number of satellites are present all around the globe. Satellite communication provides high-speed internet access that is not possible with terrestrial providers, and supports all forms of communication, making it highly versatile and flexible for operation across large parts of the network. Additionally, the widespread use of satellite communication in various fields such as government, commercial, and military has proven to be useful for instant communication and urgent needs.

Another major advantage of satellite communication is its reliability. Satellite communications are independent of man-made and natural events that can impact other forms of communication. Furthermore, satellite communication systems are designed with redundancy and failover mechanisms to ensure uninterrupted service delivery.

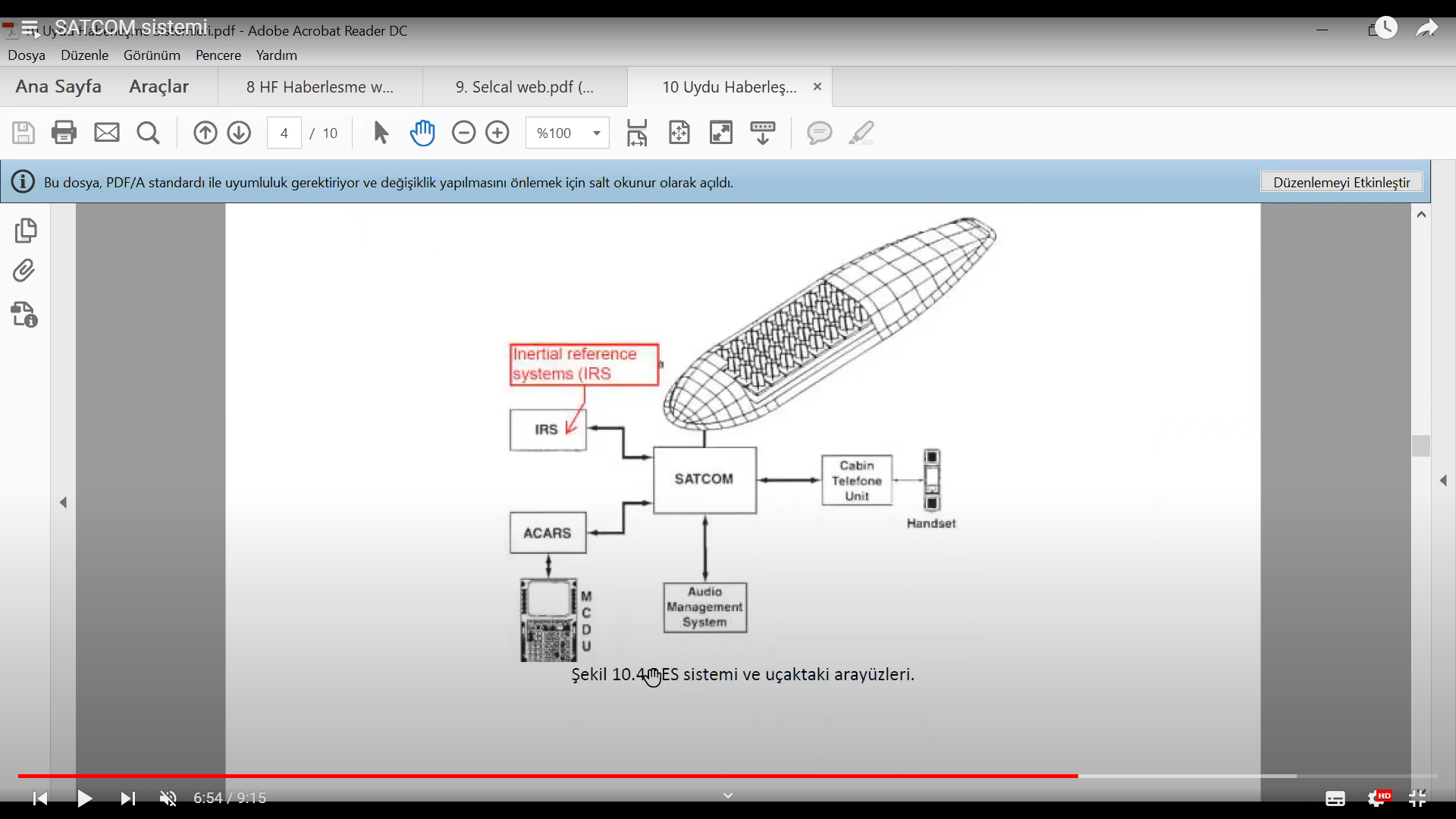
However, satellite communication also has several drawbacks. Firstly, the large number of satellites required to cover the whole radius of the earth, combined with the short duration of satellite visibility from earth, make the system complex. Secondly, satellite signals can easily get disrupted by man-made and natural interference, including weather conditions, which can make them unreliable. Lastly, the overall length of time taken by the satellite to communicate with the earth is called its delay time, which can cause echo over telephonic connections and vary on a large scale.



multi-layer communications architecture

**Satcom Hardware Components**

**AES**



**IRS Internal Reference systems**

**ACARS**

**MCDU keypad for writing text for reporting**

AES receives data from different sources and transports, analyzes and modulates this information in the most appropriate way.

**SDU**

It is responsible for control and monitoring. It makes protocol decisions for time functions, system sounds, data encoding and decoding functions. It digitizes and decodes audio and data signals, and sends the encoded signals to HPA. It sends navigation information to the BSU with azimuth and elevation information to ensure the position of the satellite antennas.

**HPA**

It elevates the signals in the L band to the required levels for transmission to the satellite. It can transmit multiple data without the need for intermodulation. It controls the output power and generates the power required for the AES system. The SDU unit performs HPA control via ARINC429. It ensures automatic control to adapt to variable conditions.

**BSU**

It is used in conjunction with electronically steerable antennas and has two main functions: control of the antenna power supply interface and control of the monitoring circuit interface. It receives antenna position data and SDU position change information as input. These data, which are received in standard digital format, are converted to enable the antenna to adopt the appropriate position, thus ensuring that the antenna remains in the correct position.

**RFU**

It can provide simultaneous reception of satellite signals and transmission of signals to the satellite. The transmitter side uses a power amplifier to amplify the signals from the SDU and sends the radio signals. The receiver side uses the signals from the LNA and performs conversions for the SDU.

**LNA**

It can perform two-way communication and has three important functions. It shapes the transmitted signals and prevents loss of sensitivity in the receiver channel during data transmission. The received signals are then filtered to reduce out-of-band signal interference. Additionally, an ultra-low noise preamplifier is present to improve the receiver system performance.

**SATCOM Management Units**

**Server Management Unit (SMU)**

The SMU is responsible for monitoring and controlling various subsystems and sensors on the aircraft, such as the engines, weapons systems, and navigation equipment. It collects and processes data from these systems, and can also provide diagnostic information to the pilot or maintenance crew if any issues arise. It also provides data exchange between the peripheral circuits in the cabin, as well as discrete status data such as wheel weight. In addition, it is capable of establishing 3G data links only on the ground.

To summarize, SMU is responsible for transmitting the data from the MDU to the ground or other aircraft via the SATCOM system. It receives the data from the MDU, modulates it for transmission over the SATCOM system, and sends it to the HPT for transmission.

**Modem Data Unit (MDU)**

MDU is used for communication purposes. It allows the aircraft to transmit and receive data over various communication channels, such as satellite, radio, and digital data links. This can include things like receiving mission updates from ground control or transmitting video feeds from onboard cameras. The MDU sends the data to the SMU for transmission.

**Antenna Control Unit (ACU):**

The ACU is a device that controls the orientation and positioning of an aircraft's antennas. It receives signals from the aircraft's communication systems, like MDU and SMU, and uses motors and other mechanisms to adjust the position and direction of the antennas in order to maintain the strongest possible signal. The ACU can be manually controlled by the crew, or it can operate automatically based on pre-programmed settings or inputs from other onboard systems. The ACU is critical for maintaining reliable communication links between the aircraft and ground stations or other aircraft.

**High Power Transceiver (HPT):**

The HPT is a device that amplifies and transmits signals from SMU to the aircraft's communication systems. It receives signals from the aircraft's avionics systems, processes them, and then sends them out at a much higher power level in order to reach distant targets. The HPT is typically used for long-range communication, such as transmitting data to other aircraft, satellites, or ground stations. It can also be used for jamming enemy communication systems or for other specialized applications.

**Modem Manager (ModMan)** The MODMAN hosts the modem, which modulates and demodulates signals to and from baseband but also implements core functionalities such as interfacing with the KANDU and KRFU (Ku/Ka-band) or receiving external signals from other aircraft sensors or units.

**Ku/Ka-band Data Unit (KANDU)** Provides power to the satellite antenna and uses external inputs, such as navigational data, to control its movement. Also provides data communication services over the Ku/Ka frequency bands. In addition to implement the positioning algorithms it also interfaces with the KRFU. It supports data rates up to several hundred megabits per second and can be used for high-bandwidth applications like video streaming and data transfer.

**Ku/Ka-band Radio Frequency Unit (KRFU)** The KRFU converts modem IF(Intermediate Frequency) to Ku- or Ka-band frequencies from the modem to prepare for transmission to the satellite. It also works as a high-power amplifier for transmitting the signal. The KRFU governs this process in reverse as well, converting the Ku- or Ka-band transmissions received from the satellite back to the IF.

**What is IF?**

The abbreviation "IF" stands for "Intermediate Frequency" and is a signal processing technology commonly used in electronic systems. In the context of SATCOM systems, the IF term is related to the frequency of the signal. Typically, the signal frequency in a receiver is high and difficult to process directly. Therefore, the signal must first be down-converted to a lower intermediate frequency (IF). IF refers to the signal in this down-converted state. This process makes the signal easier to process and modulate. In addition, IF can also refer to a filtering stage that the signal passes through before analog or digital processing. At this stage, unwanted components in the signal (such as noise) are filtered out to improve the quality of the signal.

**Outside Antenna Equipment (OAE)** This is the antenna unit that may be located in different positions, such as Tail Mounted Antennas (TMA) or Fuselage Mounted Antennas (FMA). OAE includes all the components required for the operation of the SATCOM antenna, including the antenna itself, its support structure, and the cabling and connectors that connect it to the other components of the SATCOM system.

MDU, HPT and ACU are equipment of ARINC791 wich defines ku and ka band satellite data airborne terminal. As a result, once the MDU is compromised, it is possible to reach both the ACU and HPT. The SMU remains accessible from the in-flight WiFi; although this does not intrinsically mean it can be easily compromised. If that situation ever happens the attacker will be in a position to gain control over the entire ARINC 791 deployment aboard the target aircraft.

The SMU serves as the system controller, providing core functionalities to both the KANDU, KRFU and MODMAN but also to passengers and crew as it is exposing the IFE Portal (Inflight Entertainment System).

**ARINC791**

ARINC 791 is a standard for aircraft satellite communication (SATCOM) systems. The standard defines the requirements for the installation and operation of SATCOM antennas on aircraft, with the goal of ensuring reliable and safe operation of the antenna system while minimizing interference with other aircraft systems. Some of the key requirements defined by ARINC 791 include:

Structural Requirements: The standard defines the structural requirements for the installation of the antenna on the aircraft. This includes the materials used for the antenna and its support structure, as well as the location and orientation of the antenna on the aircraft.

Electrical Grounding and Bonding Requirements: The standard defines the requirements for electrical grounding and bonding of the antenna and its support structure to the aircraft. This helps to ensure that the antenna is properly grounded and does not generate unwanted electrical interference that could affect other aircraft systems.

Environmental Requirements: The standard defines the environmental requirements for the antenna, including temperature, humidity, and vibration levels. This ensures that the antenna is capable of operating reliably in the harsh conditions of an aircraft environment.

Electrical Interface Requirements: The standard defines the electrical interface requirements for the antenna, including the RF and power connectors, cable lengths and types, and signal levels. This helps to ensure that the antenna is compatible with other aircraft systems and can be easily integrated into the overall aircraft design.

ARINC429

ARINC 429 is a digital data bus standard used in aircraft systems for the exchange of avionics data between different subsystems. It is widely used in commercial and military aircraft for flight control, navigation, and communication systems.

ARINC 429 uses a differential serial interface to transmit data at a speed of up to 100 kbps over two wires. The standard defines a data format that includes a 32-bit word consisting of a label, data, and parity bits. The label identifies the data and its source or destination, while the data itself contains information such as altitude, airspeed, or system status. ARINC 429 supports point-to-point, broadcast, and multi-point communication between avionics systems. It also provides error detection and correction through its parity bits. In summary, ARINC 429 is a digital data bus standard used in aircraft systems for the exchange of avionics data between different subsystems.

**How these systems Works together**

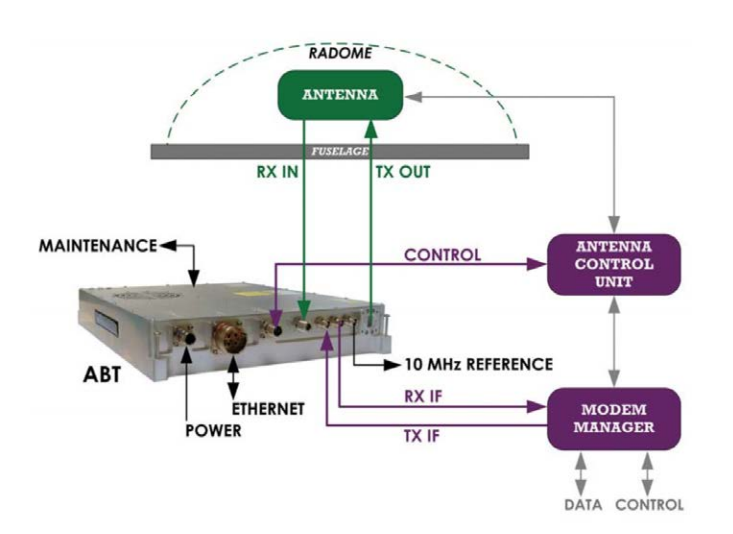
The HPA modulates and amplifies high-power signals and works with a KRFU or RFU unit to transmit these signals to other endpoints through the satellite system. The RFU unit receives digital signals from units such as KRFU or KANDU and processes them through appropriate modulation and filtering techniques before transmission to the HPA. The SDU, on the other hand, works with units such as MDU or SMU to convert signals to appropriate formats for transmission via satellite link. Together, these units, along with other units such as OAE and ACU, provide all the necessary components for a satellite-based communication system. This enables high-quality voice and data communication from aircraft to the ground or other aircraft.

BSU, RFU, HPA, HGA, and LNA are the necessary equipment for communicating with a satellite. BSU processes data from other units and prepares signals for transmission to the satellite, while RFU amplifies these signals and turns them into strong radio frequency signals. HPA further amplifies and sends these signals to the satellite. HGA is a high-gain antenna used to receive a stronger signal during satellite communication, while LNA is a low-noise amplifier that receives satellite signals and transfers them to BSU.

MODMAN manages the modem required for satellite communication, KANDU is the unit required for data transfer over the satellite, and SDU collects and processes satellite data. ModMan, KANDU, KRFU, and OAE together make up the outside antenna equipment (OAE) and antenna control unit (ACU). ACU controls the position of the satellite antenna to ensure the best signal reception. The OAE collects satellite signals and sends RF signals to the KRFU. The KRFU processes the RF signals through amplification and modulation and sends them to the MDU in an appropriate format. MDU manages data transmission and reception in satellite communication. It converts data from aircraft systems into a suitable format for transmission over the satellite system and vice versa. The MDU is used to transmit data to the SMU. The SMU modulates the data received from the MDU appropriately and sends it via the HPT over the satellite system to the ground station or other aircraft. The HPT amplifies and modulates the data received over the satellite system and sends it to the ground station or other aircraft over the satellite system.

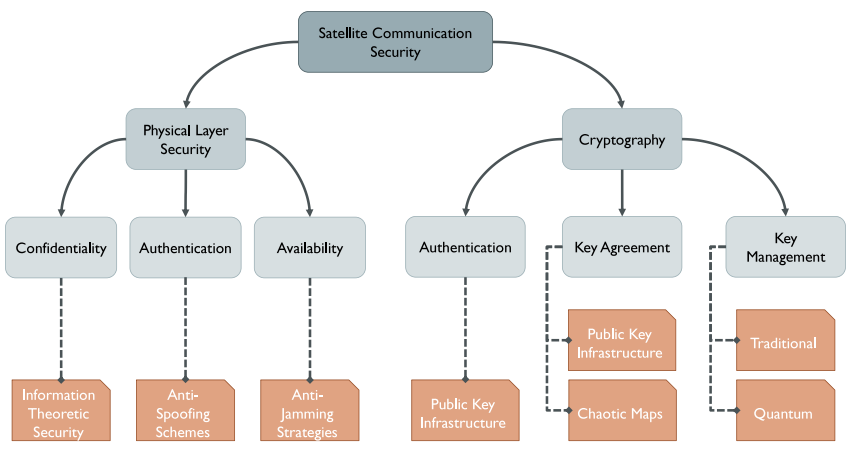
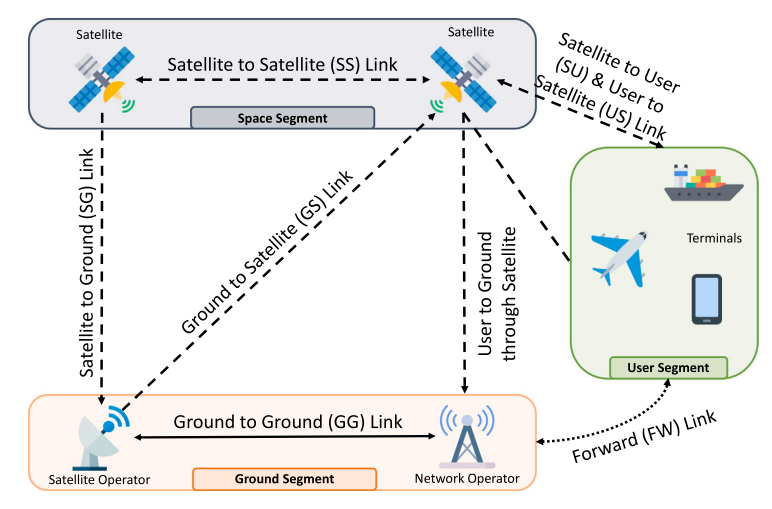
HPA, RFU, and SDU units process the radio frequency (RF) signals necessary for communication via satellite, while other units such as MDU, SMU, HPT, ACU, ModMan, KANDU, KRFU, and OAE work as part of a larger communication system. These units are used to process, manage, and control the voice and data signals transmitted via satellite connection.

In short, while HPA, RFU, and SDU units manage the components that make satellite communication possible, units such as MDU, SMU, HPT, ACU, ModMan, KANDU, KRFU, and OAE manage different components involved in controlling and operating these components.



**How the communication happens?**

The process of data transfer from on-board systems to satellite systems begins with the energization of the AES unit. The system login is started automatically by the SDU termination. The SDU receives position and orientation information from the aircraft navigation systems. The SDU sends routing commands to the antennas for the appropriate satellite connection and selects the appropriate channel for the satellite. During these operations, the AES unit informs the GES unit about issues such as the operation zone. The GES unit defines the address information of the AES unit and saves the working area and address information of the AES. All GES units in the satellite range note the information of the AES system. This feature helps to route all logged ground-to-air or air-to-ground calls in the satellite area. When an air-to-ground call is initiated by the AES unit, the AES unit sends a signal to the GES unit. When the GES unit receives a call request, it assigns a pair of C-type channels for a voice call or makes a T-type channel reservation for long-term data transfer. After that, the login process will start. The channels that are defined will be reserved during the initiated process.

When the GES unit receives information from ground systems to be sent to the AES unit of the aircraft, it makes verification of the AES units in the operation area. If the verification has been made, the GES unit informs the AES unit, the call starts and assigns the frequency, time and slot to the AES unit. Then the AES unit enters the assigned frequencies and informs the GES unit. The GES unit sends the information to the AES unit. If AES is not working in that area, the GES unit is informed. 

ACARS Aircraft Communications, Addressing and Reporting System

AES Advanced Encryption Standard

AES Aircraft Earth Station

AF Amplify and Forward

AGC Automatic Gain Control

AOC Altitude and Orbit Control

BOC Binary Offset Carrier

BPSK Binary Phase Shift Keying

BSU Beam Steering Unit

CDMA Code Division Multiple Access

CNR Carrier-to-Noise Ratio

CPS Cyber–Physical Systems

DF Decode and Forward

DoS Denial of Service

FDMA Frequency Division Multiple Access

GG Ground-to-Ground

GNSS Global Navigation Satellite System

GPS Global Positioning System

HGA High Gain Antenna

HPA High Power Amplifier

IF Intermediate Frequency

IMU Inertial Measurement Unit

IoST Internet of Space Things

IoT Internet of Things

KANDU Ku/Ka-band Data Unit

KRFU Ku/Ka-band Radio Frequency Unit

LNA/OIP Diplexer/Low Noise Amplifier

MAC Medium access control

MBOC Multiplexed Binary Offset Carrier

MDU Modem Data Unit

MIMO Multiple-Input Multiple-Output

MISO Multiple-Input Single-Output

MITM Man-In-The-Middle

MODMAN Modem Manager

NMA Navigation Message Authentication

PDR Packet Delivery Ratio

PS Power Splitting

QPSK Quadphase Shift Keying

QoS Quality of Service

RAIM Receiver Autonomous Integrity Monitoring Technology

RF Radio Frequency

RFU Radio Frequency Unit

RFID Radio Frequency IDentification

RPM Received Power Monitoring

RSMA Rate-Splitting Multiple Access

SATCOM Satellite-based Communication

SCER Secure Code Estimation and Replay

SDN Software Defined Networking

SDR Software Defined Radio

SDU Satellite Data Unit

SG Satellite-to-Ground

SMU Server Management Unit

SNR Signal-to-Noise Ratio

SOP Secrecy Outage Probability

SS Satellite-to-Satellite

SSSC Spread Spectrum Security Code

TDMA Time Division Multiple Access

TRANSEC Transmission Security

TS Time Splitting

TTCM Telemetry, Tracking, Commanding and Monitoring

UAV Unmanned Aerial Vehicles

USE Unmanned Systems and Equipment

VHF Very High Frequency

VSAT Very Small Aperture Terminal

**About the Satellites**

The main features that distinguish satellites orbits are the shape (circular or elliptical), the altitude (Low-Earth, Medium-Earth, or Geostationary), the travel direction (clockwise or counterclockwise), and the inclination to the plane of the Earth’s equator. The most popular of the previously cited features is the altitude: we distinguish Low Earth Orbit (LEO), Medium Earth Orbit (MEO) and Geostationary Equatorial Orbit (GEO). The respective altitude ranges from the Earth surface are 500 to 900 km for LEO, 5000 to 25,000 km for MEO, and 36,000 km for GEO. The altitude is directly related to the services offered to the end users. Without loss of generality, the farther is the satellite from the Earth surface, the greater is the Earth coverage area. For instance, Inmarsat is a provider of SATCOM services that adopt GEO satellites to provide telephone and data services to users worldwide. Companies like SpaceX and Iridium, are planning to launch in orbit thousands of LEO satellites to provide low latency, broadband internet systems, voice, and data services anywhere on Earth.

**The usage of types of satellites**

GEO satellites support business in navigation, data, mobile television, and radio broadcasting systems. At the same time, MEO satellites are deployed to deliver low-latency and high-bandwidth data connectivity to service providers, agencies and industries, and to support the network connectivity in the avionic/maritime domain. LEO satellite constellations are also adopted for several applications such as imaging, and low-bandwidth telecommunications and broadband internet. The space segment also includes military and defense communication systems, as well as commercial SATCOM transponders and payloads. The afore-mentioned communication links involving satellites all use frequencies in the L-band, in the range 1-2 GHz.

**The characteristics of types of satellites**

GEO satellites moves on the geostationary orbit, which is a synchronous fixedpoint orbit, i.e. a circular orbit on the equatorial plane. GEO satellites moves in a cycle that is equal to one round of earth rotation. When observed from earth, appear as static, and are therefore called synchronous fixed-point satellites. Satellites moving on this orbit have adopted mature technologies and are relatively inexpensive. They can communicate 24 hours a day and have a larger projected coverage area. Only 3 satellites on this orbit can cover the entire earth surface. MEO and LEO satellites are moving relative to ground, and their advantages include short time delay, small path loss, easy global coverage, and avoidance of congestion on a static orbit. But they only have a short communication duration and a small coverage area of satellite antenna, and they must be tracked by ground antenna. Typical LEO systems include Iridium, Globalstar and Teldest, while MEO systems include Odyssey, AMSC and INMARSMT-P.

**Satellite communication frequencies**

Different frequencies are used for the transmission of signals in a satellite network. Signals transmitted from the earth station to the satellite station use an uplink frequency, while signals transmitted from the satellite station to the base station use a downlink frequency. The uplink frequency typically ranges from 5.9 GHz to 6.4 GHz, while the downlink frequency ranges from 3.7 GHz to 4.2 GHz. The uplink frequency is always higher than the downlink frequency because the antennas at the ground stations are typically smaller and generate less power. Additionally, factors such as obstacles and atmospheric disturbances on the Earth's surface can cause attenuation of uplink signals, requiring a higher power level. Furthermore, the antennas on the satellite can be larger in size and provide higher gain, resulting in stronger downlink signals. Since the uplink frequency is always higher than the downlink frequency a mixer is required to convert it to a lower frequency. After this conversion, the communication satellite acts as a repeater, receiving and amplifying signals before transmitting them to the next frequency band to avoid interference. Two-way communication is established between the uplink and downlink frequencies with the help of transponders, which are considered the "brain" of the satellite. Transponders receive a radio signal and broadcast it as a different signal.

Satellites frequency bands and applications.

Satellite frequency

[GHz]

Band name Applications

1–2 L Positioning Systems, Mobile phones, Sea/Land/Air Communications, Radio

2–4 S NASA communications with Space Shuttle and International Space Station

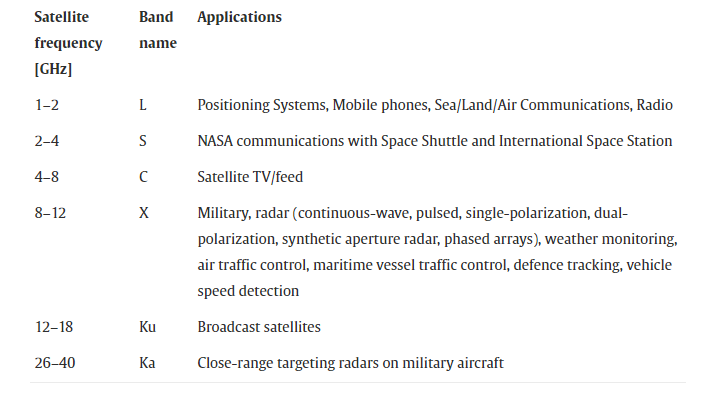
4–8 C Satellite TV/feed

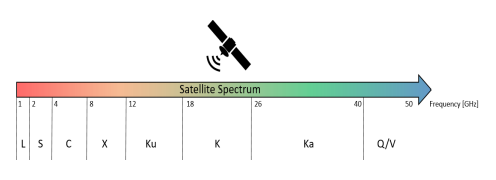
8–12 X Military, radar (continuous-wave, pulsed, single-polarization, dual-polarization, synthetic aperture radar, phased arrays), weather

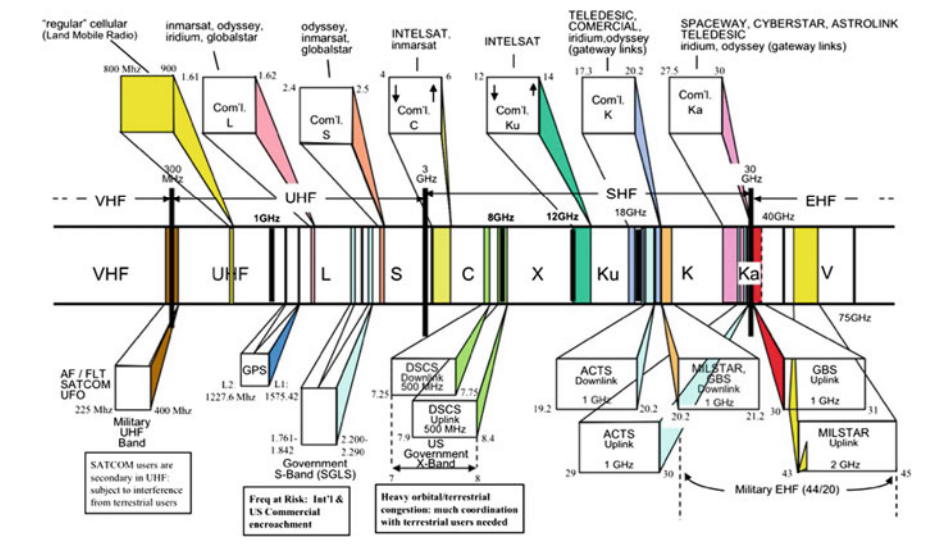
monitoring, air traffic control, maritime vessel traffic control, defence tracking, vehicle speed detection

12–18 Ku Broadcast satellites

26–40 Ka Close-range targeting radars on military aircraft







Satellite frequency band

The reference communication architecture of a SATCOM system is generally characterized by: (i) a space segment including the Satellite to Satellite (SS) and the Satellite to Ground (SG) links; (ii) a ground segment, defined by the satellite operators (or gateways) and network operators, enabling the Ground to Satellite (GS), Ground to Ground (GG), Satellite to Ground (SG), forwarding, and the Satellite to User (SU) links; and finally, (iii) a user segment, which includes the terminals, e.g., ships, airplanes, and satellite smartphones, enabling the additional User to Ground (UG) and the User to Satellite (US) links.

MULTIPLE ACCESS TECHNIQUES

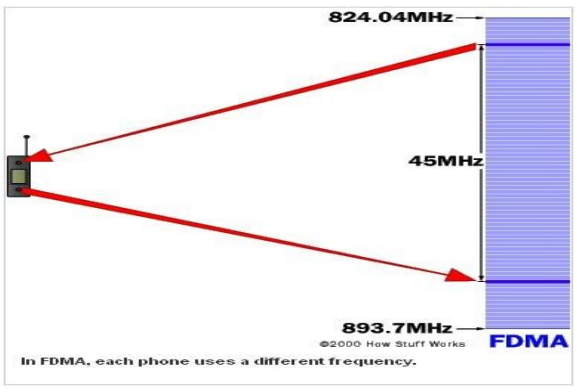
The need of multiple access technique can easily explain by the fact that users have limited bandwidth of radio spectrum in respect to that at times when user wants to access this radio spectrum then multiple access technique allow many mobile users to access finite amount of the radio spectrum. This helps in increment of number of channels in spectrum increases which in turn increases the capacity of spectrum or even the efficient of good users for that reason we go for this very technique in which multiple user can access the radio spectrum at the same instant or different of time. Depending on allocation of availability of bandwidth among the user they are classified in these two systems:

A. Narrowband Systems: Narrowband systems generally cover narrow range of frequencies. They used in slower communication for example voice and audio spectrum sounds which have lower range of frequencies. Narrowband systems have flat frequency responses. They have a greater range of receiving power than that of wideband and cancel out the unwanted wideband noises. It has lower transmission bandwidth of a channel than flat bandwidth of the channel.

B. Wideband Systems: Wideband systems generally cover wide range of frequencies. The transmission bandwidth of a channel is much larger than the flat bandwidth of the channel. The main advantage of wideband system is that it provides high data rates in comparison to narrowband systems. There are different ways to allow access to the channel Frequency division multiple-access (FDMA), time division multiple-access (TDMA), code division multiple- access (CDMA), space division multiple access (SDMA). Code division multiple access (CDMA) is used by all GNSS constellations except GLONASS in which frequency division multiple access (FDMA) is adopted. In order to transmit the satellite navigation messages through the radio frequency spectrum, GNSS coded signals are modulated using binary phase shift keying (BPSK) and variations of binary offset carrier (BOC). The modulated navigation message contains the location of the satellite (ephemeris data), transmission time, and other information that can be used to calculate the time and position of the user device.

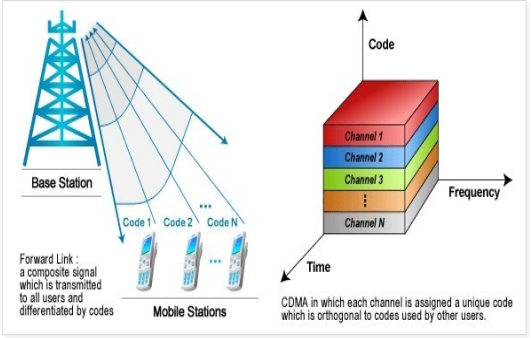
1) Frequency division multiple access (FDMA): In FDMA-based GNSS, each satellite transmits on a different frequency with the same PRN code used by all the satellites within the constellation. FDMA is the basic technology for advanced mobile phone services. Each user can use the frequency band at same instant of time. Let a user 1 to access some frequency at time t at the same instant of time user N can also access some other frequency or we can say that multiple frequency can access the base station at same instant of time.

The main drawback of this method is that whenever a user will have frequency slots adjacent to each other there will be the chance of interference called adjacent channel interface so for every slot a guard band is provided. This guard band will not participate in transmission of information as it is there just to support the channel and avoid the interface.



2) Time division multiple access (TDMA ): In TDMA all user uses same frequency of bands at different time of instants so for same base station different time slots are needed for each user. TDMA have a major drawback of interference due to lack of synchronization. In this each user user should ensure to have a proper synchronization with that to the transmitter no matter what receiver is used. For example, user 1 sends information at time slot T1 and if this is not known to the receiver then the receiver might issue the information of other time slot to the user 1, this may result in interference. To avoid this a good synchronization activity is always needed in TDMA.

3) Code Division Multiple Access (CDMA): Code division multiple access method provides several users to share a band of frequencies. In CDMA-based GNSS, the signals are modulated by a unique pseudorandom noise (PRN) code and each satellite uses a different PRN code. This enables the receiver to identify and track unique satellite signals which share the same frequency/channel. Whenever a user has n number of codes it needs to ensure that at receiver level there should be a control channel which take care of the coding point of information so whatever information is transmitted by the user it should have codes within it.



4) Space division multiple access (SDMA): Spot beam antennas are used in this type of access. No interference takes place in SDMA. In SDMA users access to the same channel at the same time. Spatial multiplexing is used here, it helps one satellite to communicate or connect with other satellite receiver having same frequency all over. This spatial multiplexing helps in better performance in radio multiple access.

**OPERATIONS IN SATELLITE COMMUNICATION**

In a satellite communication system, various operations take place. Among which, the main operations are orbit controlling, the altitude of a satellite, monitoring and controlling of other subsystems. The satellite consists of two segments those are the transmission of a signal to the satellite and reception of the signal from the satellite respectively named as earth segment and space segment.

A. Altitude and Orbit Control (AOC)

Altitude and orbit control consists of rocket motors that place the satellite into right orbit whenever it will deviate from the orbit. It is also helpful to make antennas. Altitude control helps the exact orientation of the satellite in orbit in which spinning, and 3 axis method is used for stability of satellite. During launching the spin system operates to make TTCM point toward each station and in 3 axis method orientation of the satellite in axis is controlled without moving the main body.

B. Telemetry, Tracking, Commanding and Monitoring (TTCM)

TTCM subsystem is very much necessary for any communication satellite to operate it successfully. In TTCM, Telemetry subsystem is a remote-controlled system. The telemetry system is present in both piles of the earth as well as a satellite station. At the ground station, it helps to provide information about the range and angles of the satellite. Satellite provides telemetry data and earth provide orbital data which is used to correct the position and attitude of the satellite. It is used during the launching time and when the satellite is present in LEO orbit. The tracking system used to determine the orbit of the satellite at the time of launching and then to track the satellite. It also determines the current orbit of the satellite. In the tracking system, the rate of change of range is determined by the Doppler effect. It mainly focuses on the range and looks angles of the satellite. Next is the Commanding subsystem, it is necessary to launch the satellite in an orbit and it's working in that orbit. This subsystem adjusts the altitude and orbit of the satellite, whenever there is a deviation in those values. It also controls the communication subsystem. This commanding subsystem is responsible for turning ON / OFF other subsystems present in the satellite based on the data getting from telemetry and tracking subsystems.

**Security of satcom**

SATCOMs are particularly prone to eavesdropping due to the broadcast nature of the wireless medium and the very large coverage area. Usually, the confidentiality of SATCOM communications is provided via traditional cryptographic protocols such as Advanced Encryption Standard (AES), working at the MAC-layer or above. However, legacy satellites deployments often use old and proprietary customized versions of AES, frequently found later to be insecure. As a result, motivated adversaries featuring powerful capabilities and tools can easily collect a consistent amount of encrypted data and possibly compromising communications confidentiality. Moreover, many satellites deployments were set up several years ago, when wireless security was not conceived as a requirement. Indeed, attacks on SATCOM channels was conceived by the operators as hard to achieve, and overall, security was thought as a slow-down factor rather than an enabler. Thus, many satellites do not implement any security protection, and updating them today would require high costs

POSSIBLE ATTACKS ON SATELLITES

Some of the Possible Attacks on Satellite networks are:

1) Side Channels Attacks: In this, the attacker observers the electromagnetic radiation from the device and based upon that attacker tries to guess the secret key. This is a passive attack and does not cause any physical damage.

2) Jamming: Jamming attack generally tries to stop the communication between transmitter and receiver by sending jamming (de-authentication) signals. Satellite signal Jamming is one of the least preferred attacks as it is easy to trace.

3) Eavesdropping: This attack is also known as spoofing. In this, the attacker intercepts the data packet and tries to find out the communication that is going between sender and receiver. The data interception is one of the most popular, effective and easy to conduct the attack. This attack also allows the attacker to Modify Data that is being transmitted through the channel.

4) DDoS Attack: DDoS (Distributed Denial of Service) is an attack in which a huge amount of data is sent to a server/ device, the server could not control this huge amount of traffic and crashes. The DDoS attack has been proved a severe threat to organizations in the past few years. The DDoS Trojan is spread on the Internet and the system having this Trojan acts as a ‘botnet' during the attack. It has only one purpose i.e. to send a large amount of traffic to a website so that the server gets overloaded which results in shutting down the network.

5) Hijacking: Hijacking a satellite refers to hacking into the cyberspace of satellite base station and taking full control over the satellite. Satellite hijacking is one of the deadliest attacks among all as thousands of systems can be hacked using a single satellite. Also, hijacked satellites can be used in the communication of terrorist organizations.

**SATCOM Vulnerabilities**

SATCOMs are particularly prone to eavesdropping due to the broadcast nature of the wireless medium and the very large coverage area. Usually, the confidentiality of SATCOM communications is provided via traditional cryptographic protocols such as Advanced Encryption Standard (AES), working at the MAC-layer or above. However, legacy satellites deployments often use old and proprietary customized versions of AES, frequently found later to be insecure. As a result, motivated adversaries featuring powerful capabilities and tools can easily collect a consistent amount of encrypted data and possibly compromising communications confidentiality. Moreover, many satellites deployments were set up several years ago, when wireless security was not conceived as a requirement. Indeed, attacks on SATCOM channels was conceived by the operators as hard to achieve, and overall, security was thought as a slow-down factor rather than an enabler. Thus, many satellites do not implement any security protection, and updating them today would require high costs.

**Hard-coded Credentials And/Or Backdoors**

Hard-coded credentials function as cybersecurity master keys, common back doors that allow service technicians to access multiple pieces of equipment with the same log-in credential andpassword.

Backdoor Trojan as the name says is used to give a reverse connection to the attacker on targets machine. In other words, the attackers get full control over the compromised system without the knowledge of a user. Backdoor Trojan is the main reason for satellite hijacking.

**Insecure Protocols**

Weak system protocols could allow malicious actors access to satcom channels. Insecure Protocols are vulnerable to cyber-attacks. Data sent through insecure protocol is generally prone to data modification and data theft. Although, inmost cases, care has been taken regarding the security of the protocol being used, there is invariable weakness that can be exploited.

**Encryption**

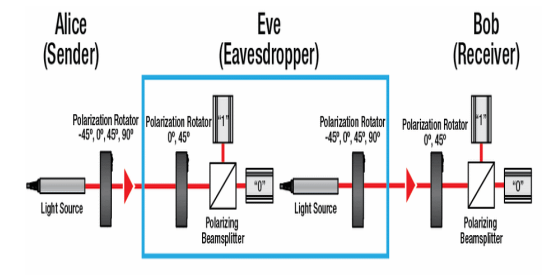
Encryption primarily ensures that the traffic through a satellite system cannot be overheard. For the most secure environments, the encryption is achieved outside of the actual satellite channels. Where encryption has been used on the satellite channels there are some examples where that encryption is so weak that it as been easily exploited. Using weak encryption techniques like DES can be a reason for satellite hacking. This vulnerability encourages data interception and easy decryption of data by attackers.

SATELLITE NETWORK ENCRYPTION

Out of all the attacks explained above, Data Spoofing is the most effective, easy to launch and undetectable attack on the satellite network. To solve this problem, we needed an encryption algorithm which is easy to compute but hard to reverse (One Way Function). The satellite network in 2010 used to Encrypt data using RSATriple DES where RSA encryption was used to Encrypt the actual message and Triple DES was used for Authentication purpose. Later satellite encryption was modified and RSAAES encryption came into the picture where RSA encryption was used to Encrypt the actual message and AES was used for authentication purpose. The encryption was hard to break but not impossible. RSA can be broken using Timing attack and Exhaustive search Attack if done by a very fast and Powerful hardware setup. To resolve this issue China successfully transmitted data using "Quantum Cryptography".

Use of Quantum Cryptography in Satellite Network Security:

The Traditional cryptosystems such as RSA, Megamall were based on a mathematical calculation of large co- prime numbers. But the problem with traditional cryptosystem is that with the increase in hardware power and efficiency, supercomputers can crack this encryption in very less time. So new cryptography has been introduced which store the information in photons known as Quantum Cryptography. As we know data travels in binary format (0 and 1), in Quantum cryptography the polarization of photon particles is used to denote binary data. Polarization of Photons can be horizontal (1), vertical (0), left diagonal (0) and right diagonal (1) as shown in above figure. So, the Alice generates a random key using ‘Random Key Generator'. The polarized photons are then transmitted in any random order and received by Bob. At the receiver end, we have two detectors which translate photons into bits.

fig: quantum cryptography

1) Rectilinear detector: This detector only detects the horizontal and vertically polarized photons. If the photon is vertically polarized, then it scans it as 0 and if it is horizontally polarized it scans it as 1.

2) Diagonal detector: This detector only detects the left and right diagonally polarized photons. If the photon in left diagonally polarized, then it scans it as 0 and if it is right diagonally polarized it scans it as 1. In this procedure of scanning the photons, there is only a 50% chance of measuring a 0 or 1.

Now the photon sequence sent by the Alice filter is compared with the sequence obtained by Bob's detector. Based on Alice's filter the number will be either right or wrong as shown in the above figure. After each result is checked publically, each incorrect match is thrown out and we get a sequence of polarized particles which on converting to bits gives us the secret key. If the malicious hacker tries to Intercept the signal, then the photon particles will change their polarization and if the polarization of any of the photon changes then the secret key can't be obtained. By use of this method, the receiver will come to know that someone is eavesdropping in between the network. If the photons are intercepted the old key will automatically get destroyed and a new session of data transmission must be started with a new key. This method completely removed the problem of data interception.

Quantum cryptography is less time consuming and more secure than traditional Public Key-Private key cryptosystems. Quantum cryptosystem resolves the major problem of satellite network security, specially spoofing.

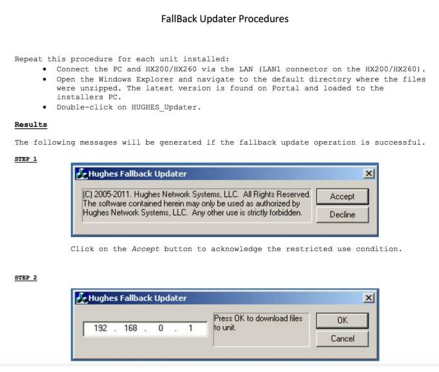
**Vulnerable Software**

While kinetic dangers (i.e., being hit and/or damaged by stray objects such as meteorites or othersatellites) remain rare, satellite systems are remarkably vulnerable to a range of cybersecurity issues and hostile attacks because they are hugely complex and expensive, take months todeploy, and the primary emphasis is on getting a working system that meets specification and thecontract deliverables. Most cyber exploit attacks take advantage of in complete code that does not boundary checkin coming data allowing for stack buffer overflow attacks. These are very prominent in embedded C and C++ systems and require an additional vulnerability assessment exercise, at great costand time, in order to fully secure a system. In these cases an internal buffer may be overrun byan intentionally ‘malformed’ packet and code execution achieved by overwriting the area of memory where the return address resides. Once basic code execution is achieved, new threadsand processes may be started and most, if not all, facilities within the system can be accessed.

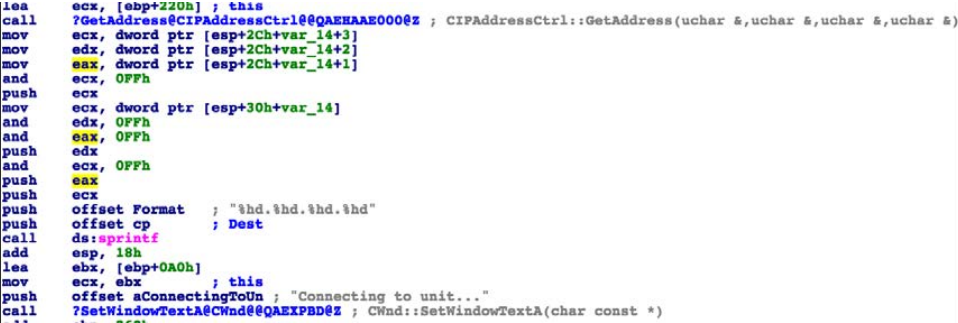
**The Fallback Updater**

One of the security vulnerabilities was detected in the program named Hughes Fallback Updater. The SATCOM Hughes infrastructure is a global satellite network used for communication and data transfer. It consists of a network of satellites, ground stations, and other equipment, providing services to government, military, and commercial customers. The infrastructure includes various components such as modems, antennas, and control units, which work together to enable communication between the satellites and ground stations. The infrastructure's architecture is designed to provide reliable and secure communication services even in remote and difficult-to-reach locations.

The Fallback Updater is designed to be a backup mechanism to re-flash the modem in case of a failed firmware update. However, this mechanism could be exploited by an attacker to gain unauthorized access to the modem and potentially even the underlying aircraft systems. This vulnerability allows an attacker to manipulate a series of commands and parameters used during the update process, resulting in processing errors. By reverse engineering the firmware update process and analyzing the code responsible for the Fallback Updater, it was possible to manipulate certain parameters and send custom firmware images to the modem without proper authentication. This could allow an attacker to take control of the modem and potentially gain access to other systems connected to it.

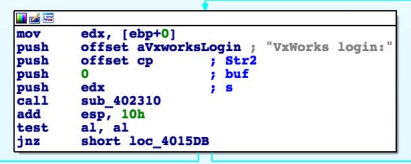


Software that is able to install new firmware to the unit without asking for a password is definitely a good candidate to host a backdoor. Using a simple google search it is possible to download the fallback updater software from the website of a satellite provider. This program contains both the recovery firmware ‘fallback.bin’ and the Windows program ‘HUGHES\_updater.exe’ to update the device. By reverse engineering this binary we can know more about how the updating mechanism has been implemented.

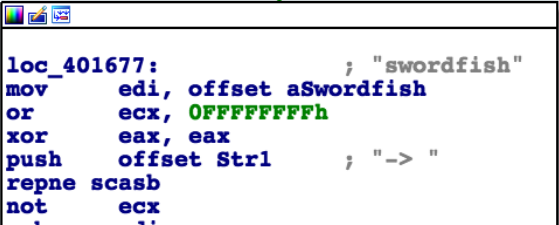
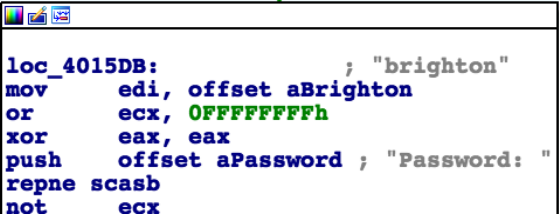


The binary code of the above interface

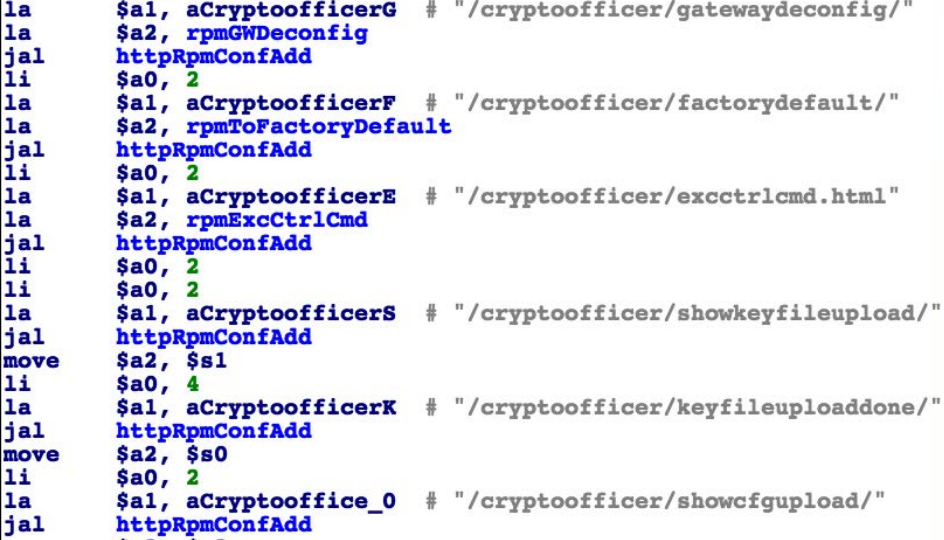
With the reverse engineering of the interface, we can obtain password and username and create a backdoor. In this way, unauthorized access to the modem is provided.



Once connected it looks for the following login prompt “VxWorks Login:” which corresponds to the default VxWorks’s shell service.

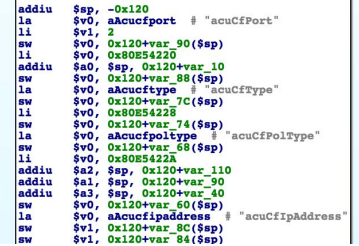


It is also possible to access the FTP server using the same credentials. In addition to these credentials we can find another pair: ‘crypto/officer’. These are apparently used for the Crypto-officer role that terminals need to support.



It has also been detected that the Gafgyt IoT botnet was attempting to access the system through telnet, to which the fallback updater is also connected.

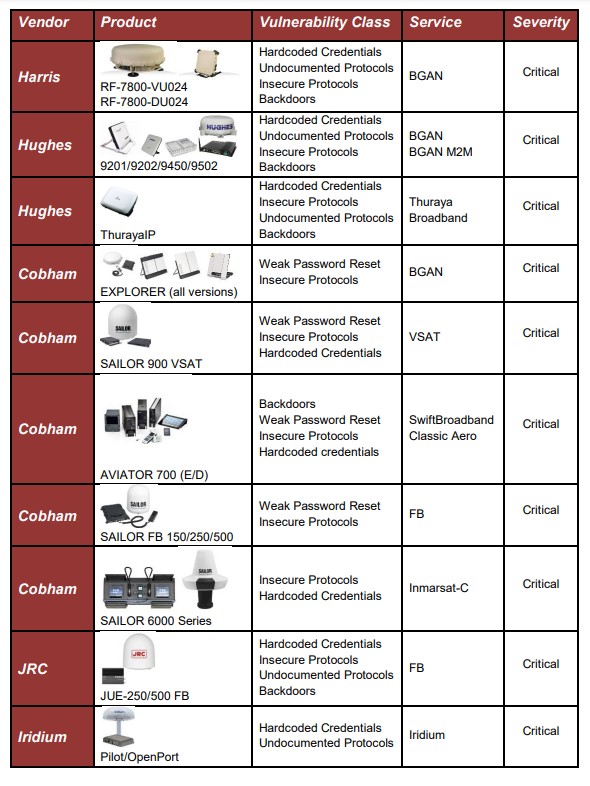
ABS (Automatic Beam Switching) technology is a technology designed to meet the mobility requirements in satellite communications, allowing an ACU to switch between different beams. However, one disadvantage of ABS is that it can provide access to ACUs that can be directly controlled by a modem. This can be risky from a security standpoint, so ABS has been disabled for this specific application. In this example we can clearly see that when we examine the binary codes we can observe the process of ABS and ACU. The firmware checks whether ABS has been enabled, and if so then proceeds to obtain the required parameters for the supported ACU, from the same configuration file, such as IP and port.



Then the MDU tries to connect to the ACU. Once connected, it uses the custom ACU’s protocol to initiate the handshake. When this handshake has been completed, and the modem has successfully established a connection to the ACU, there are different commands that can be sent to this ACU in order to mute/unmute the transmission.



Having control over whether an antenna is transmitting or not is a key capability when considering RF attacks in SATCOM environments. The issue at hand also brings up concerns regarding the security measures implemented in protocols used to communicate with various ACUs, including those used in the maritime industry. One example is OpenAMIP, an IP based protocol that facilitates the exchange of information between an ACU and a satellite router, which does not have a strict requirement for a particular authentication or authorization mechanism. Similar problems have been identified in other closed-source protocols.



Identified critical SATCOM security vulnerabilities which obtained by using reverse engineering in a security research conducted in 2014.

**Countermeasures**

TRANSEC

TRANSEC stands for Transmission Security, which is a term used to describe the measures taken to secure the transmission of information in satellite communications. It is not a product or protocol, but rather a set of techniques used to ensure secure satellite communications. TRANSEC enables the following protections:

Masks Channel Activity - This technique conceals traffic volumes and obfuscates acquisition activity to prevent unauthorized access and potential attacks.

Controls Channel Information - This technique disguises traffic volumes to secure the traffic source and destination, reducing the risk of interception and manipulation by unauthorized entities.

Authenticates and Validates Hub and Remotes - This technique ensures that remote terminals connected to the network are authorized users, preventing unauthorized access and ensuring the integrity of the network.

**Real Life Examples**

**Intelsat**

In April of 2007, there were reports of Tamil rebels in Sri Lanka being accused of hacking into the Intelsat satellite over the Indian Ocean for communication purposes. Intelsat responded by saying that this was not hacking but rather signal piracy, which they would not tolerate. The rebels denied accessing the satellite illegally and suggested a relationship with the service provider, but did not provide any further explanation.

**Landsat-7 and Terra AM-1**

The media reported in 2007 that the NASA Landsat-7 satellite was hacked for 12 minutes, followed by another NASA satellite, Terra AM-1, in 2008 for 2 minutes in June and 9 minutes in October. These attacks performed with theinterference and jamming of radio signals disrupting satellite communications.

**Predator and Reaper**

In October 2011, Creech Air Force Base was targeted by a malware attack on Predator and Reaper drones, with ground control stations infected by a keystroke logger. The malware, believed to have been created by a foreign nation-state, persisted after multiple system cleanings, potentially aimed at gathering information on the US's drone activities.

**S-100 Camcopter**

There has been only one publicly reported actual attack on sUAS (small Unmanned Aerial Vehicles), and it was a GPS Jamming attack. A suspected GPS Jamming attack was executed on S-100 Camcopter, a rotor based UAV by Schiebel, resulting in a crash into the ground control van killing a Schiebel engineer and injuring two remote pilots during testing. Schiebel said that an incorrect response by the operators after the Camcopter lost its GPS signal led to the crash, some minutes later. The UAV is equipped with multiple inertial measurement units (IMUs) for backup, the company noted. The recorders on board the UAV and in the ground station were burned during the crash, and could not provide any explanatory data. The attack was performed by an unknown actor on 10th May 2012 during the UAV test by the engineer, near the western port city of Incheon, South Korea. The attack was detected after the crash and is suspected that GPS Jamming started on April 28th, also disrupting passenger flights at Kimpo and Incheon.