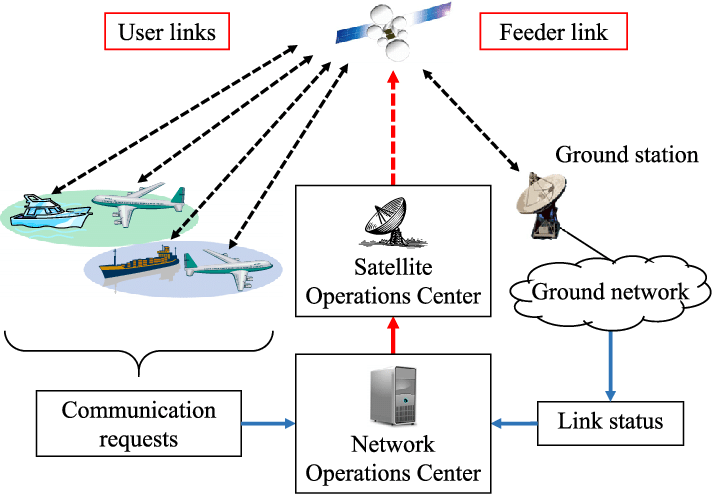
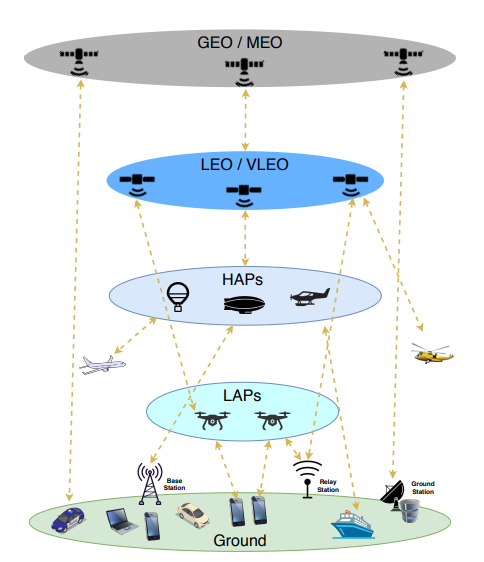
Satellite communication is a critical component of modern communication networks, with numerous advantages and disadvantages that must be considered. One of the key benefits of satellite communication is its global availability, as a large number of satellites are present all around the globe. Satellite 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.

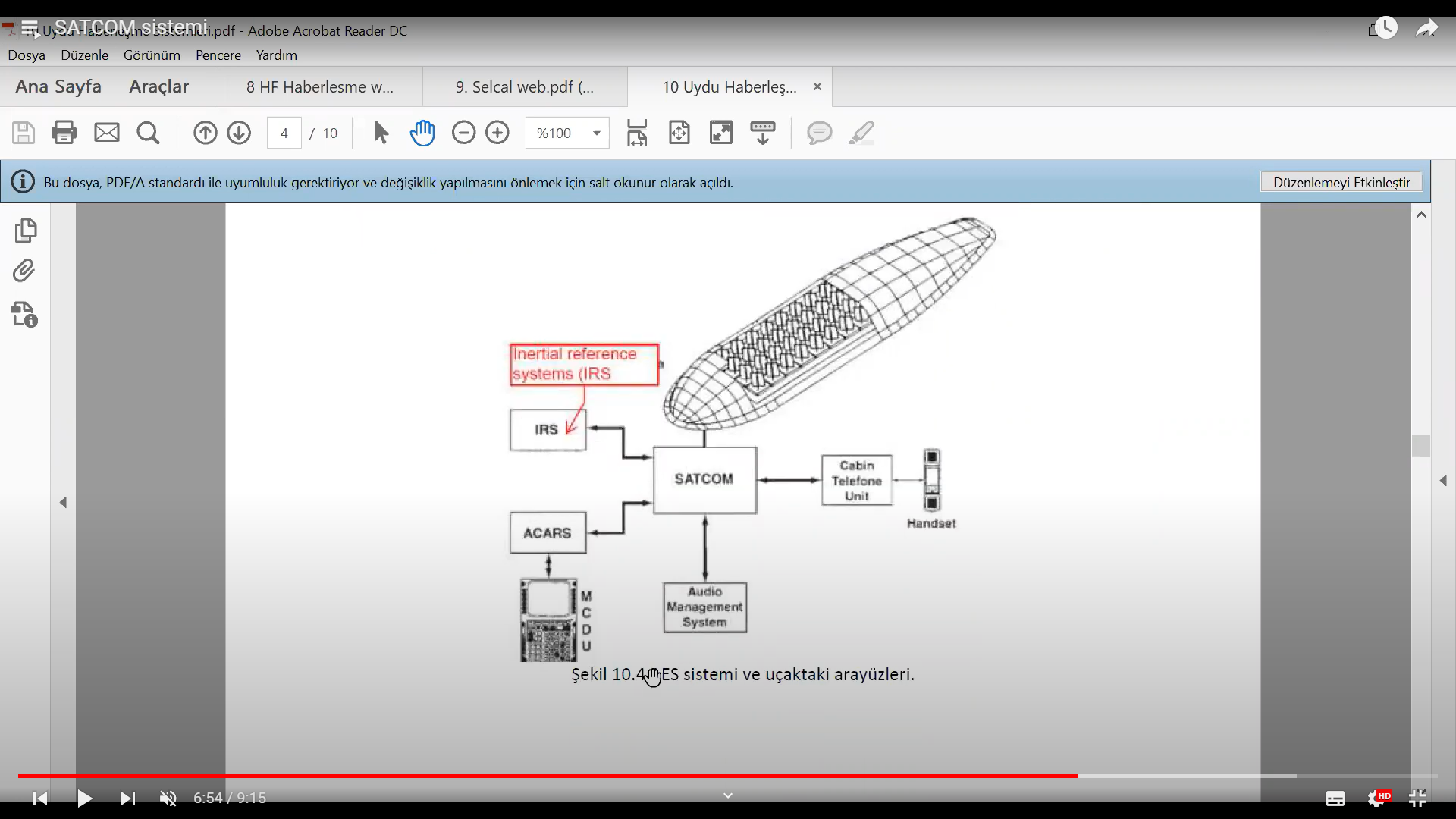
However, satellite communication also has several drawbacks. Firstly, the large number of satellites required to cover the whole radius of the earth, combined with the short duration of satellite visibility from earth, make the system complex. Secondly, satellite signals can easily get disrupted by man-made 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**

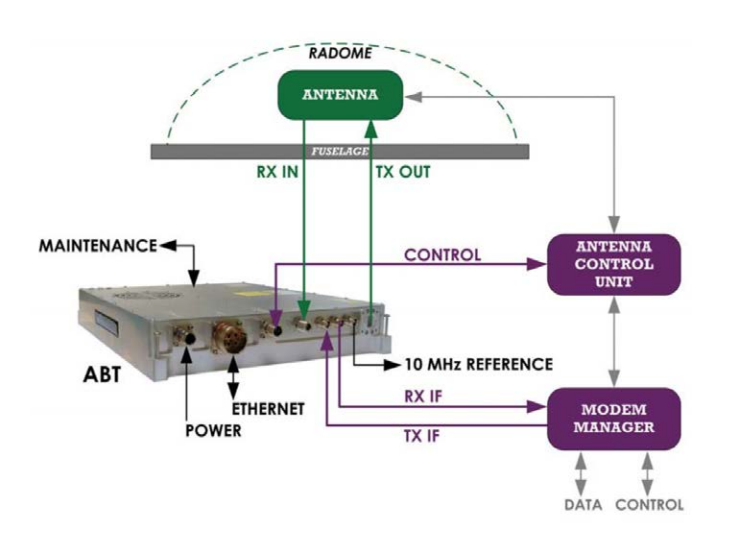
The HPA modulates and amplifies high-power signals and works with a KRFU or RFU unit to transmit these signals to other endpoints through the satellite system. The RFU unit receives digital signals from units such as KRFU or KANDU and processes them through appropriate modulation and filtering techniques 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.

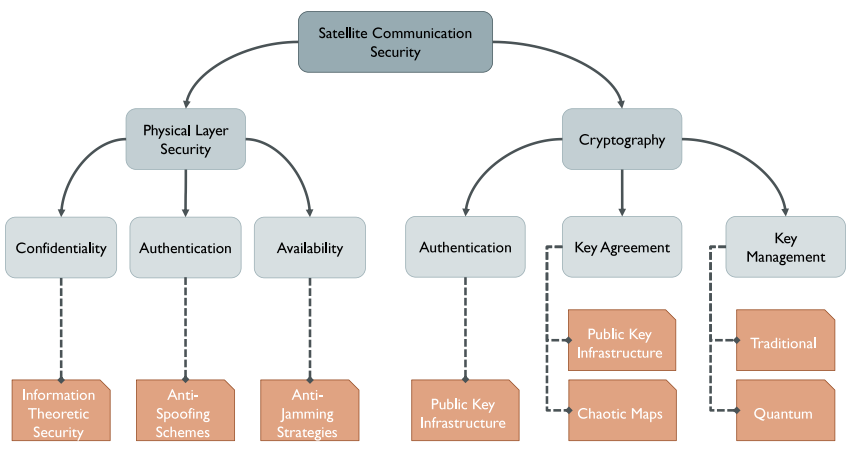
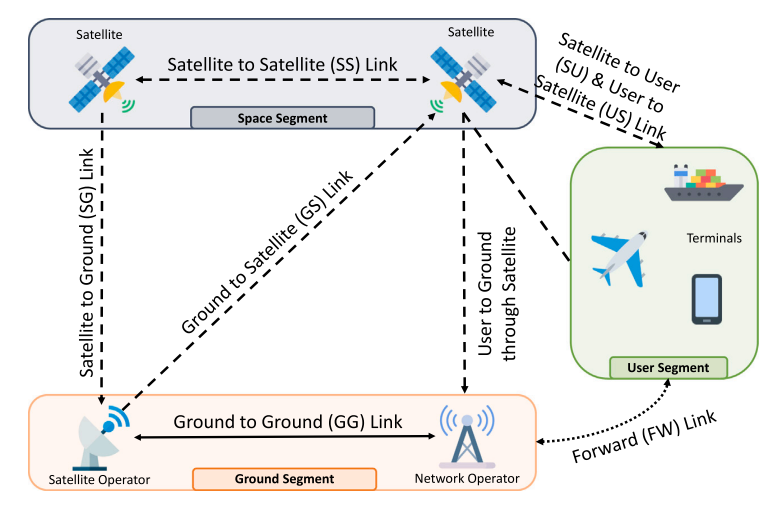
HPA, RFU, and SDU units process the radio frequency (RF) signals necessary for communication via satellite, while other units such as MDU, SMU, HPT, ACU, ModMan, KANDU, KRFU, and OAE work as part of a larger communication system. These units are used to process, manage, and control the voice and data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

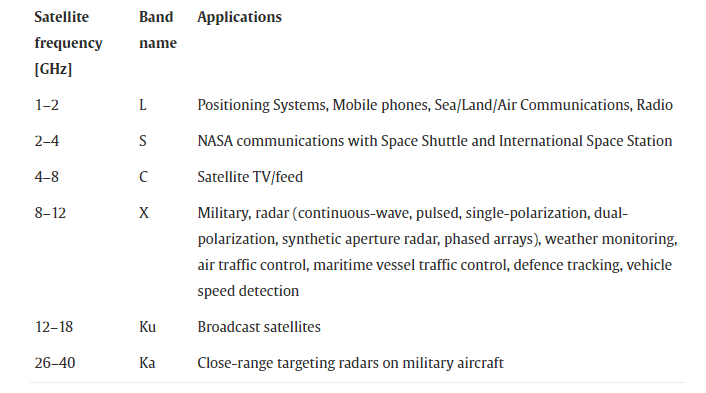
4–8 C Satellite TV/feed

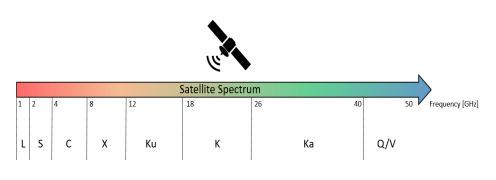
8–12 X Military, radar (continuous-wave, pulsed, single-polarization, dual-polarization, synthetic aperture radar, phased arrays), weather

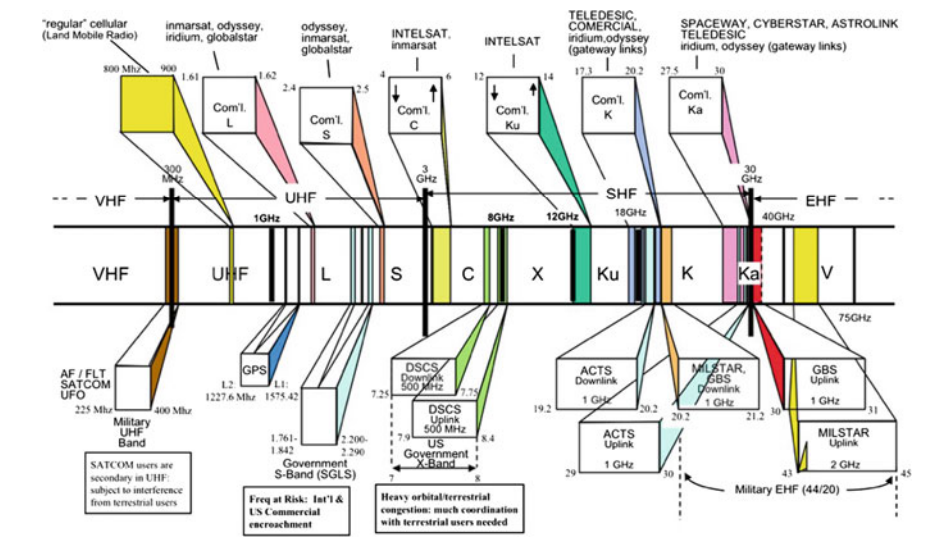
monitoring, air traffic control, maritime vessel traffic control, defence tracking, vehicle speed detection

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

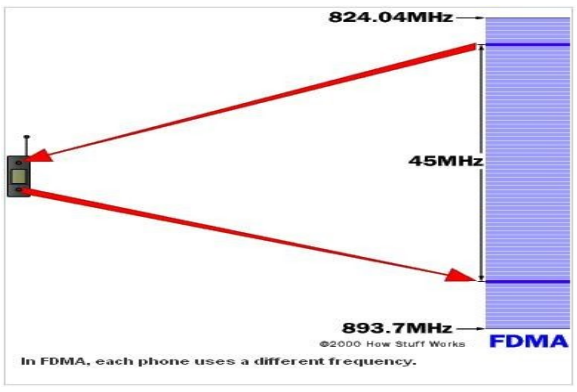
The need of multiple access technique can easily explain by the fact that users have limited bandwidth of radio spectrum in respect to that at times when user wants to access this radio spectrum then multiple access technique allow many mobile users to access finite amount of the radio spectrum. This 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.

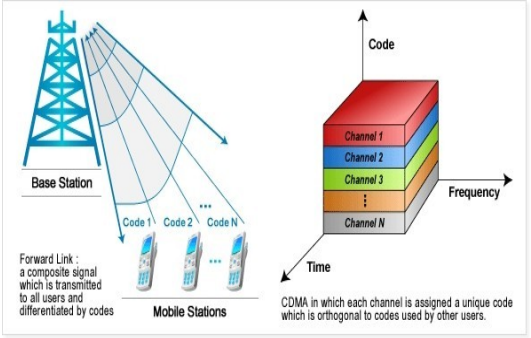
1) Frequency division multiple access (FDMA): In FDMA-based GNSS, each satellite transmits on a different frequency with the same PRN code used by all the satellites within the constellation. FDMA is the basic technology for advanced mobile phone services. Each user can use the frequency band at same 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**

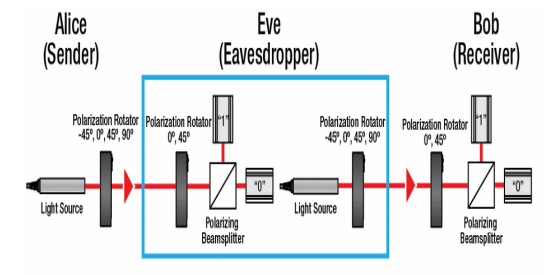
Encryption primarily ensures that the traffic through a satellite system cannot be overheard. For the most secure environments, the encryption is achieved outside of the actual satellite channels. Where encryption has been used on the satellite channels there are some examples where that encryption is 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.

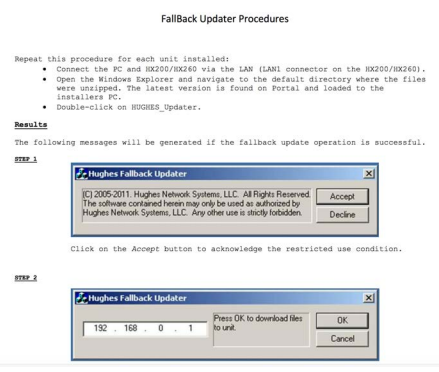
**Vulnerable Software**

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.

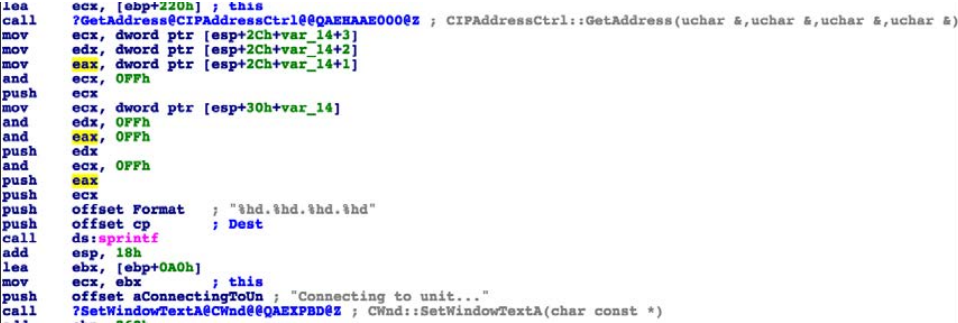
**The Fallback Updater**

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.

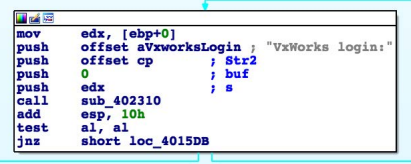


Software that is able to install new firmware to the unit without asking for a password is definitely a good candidate to host a backdoor. Using a simple google search it is possible to download the fallback updater software from the website of a satellite provider. This program contains both the recovery 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.

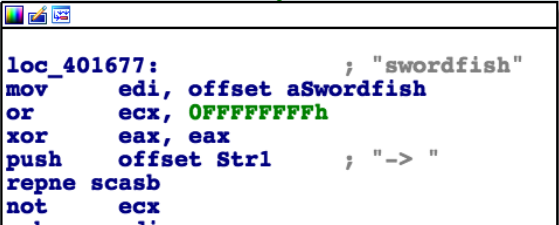
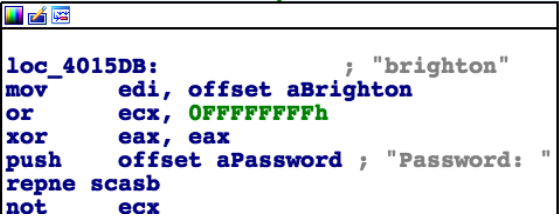


The binary code of the above interface

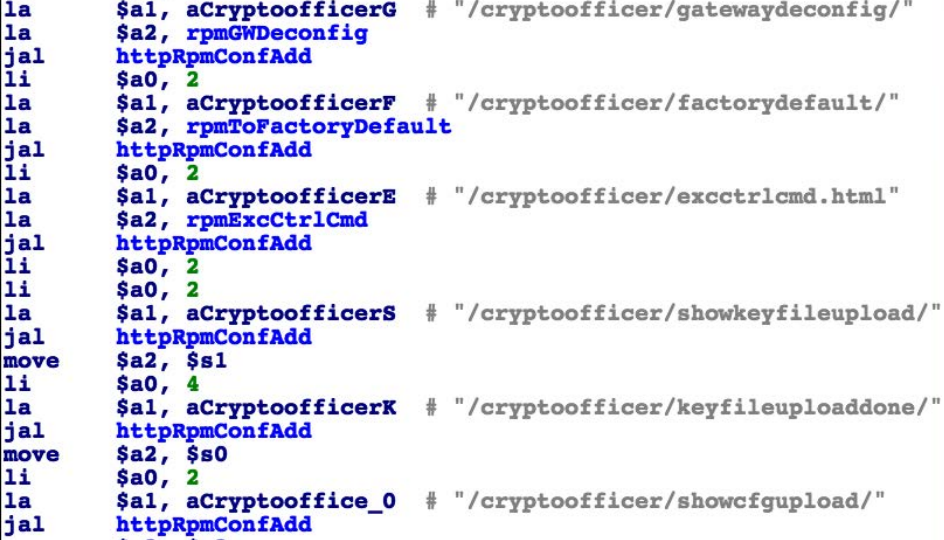
With the reverse engineering of the interface, we can obtain password and username and create a backdoor. In this way, unauthorized access to the modem is provided.



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

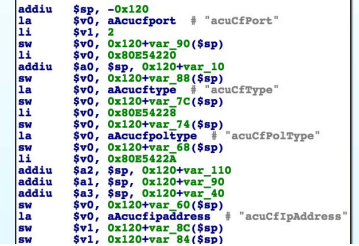


It is also possible to access the FTP server using the same credentials. In addition to these credentials we can find another pair: ‘crypto/officer’. These are apparently used for the Crypto-officer role that terminals need to support.



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.

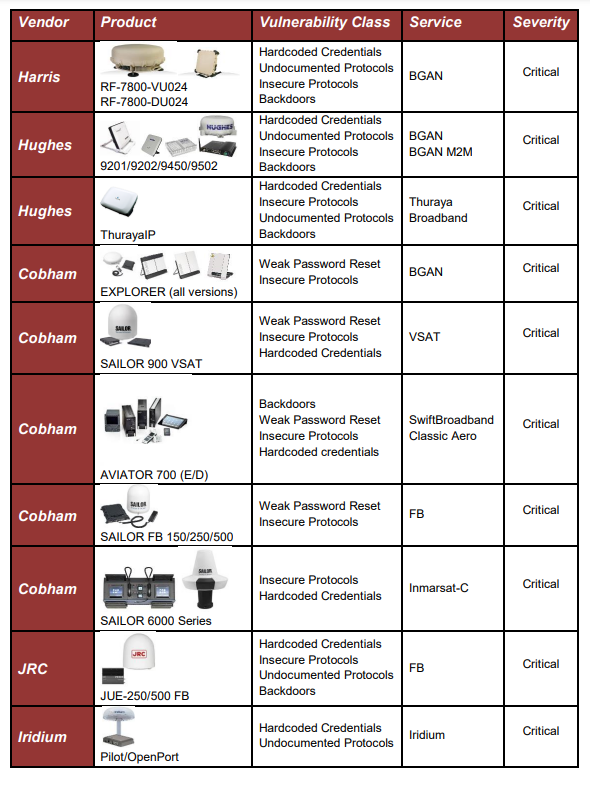
ABS (Automatic Beam Switching) technology is a technology designed to meet the mobility requirements in satellite communications, allowing an ACU to switch between different beams. However, one disadvantage of ABS is that it can provide access to ACUs that can be directly controlled by a modem. This 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**

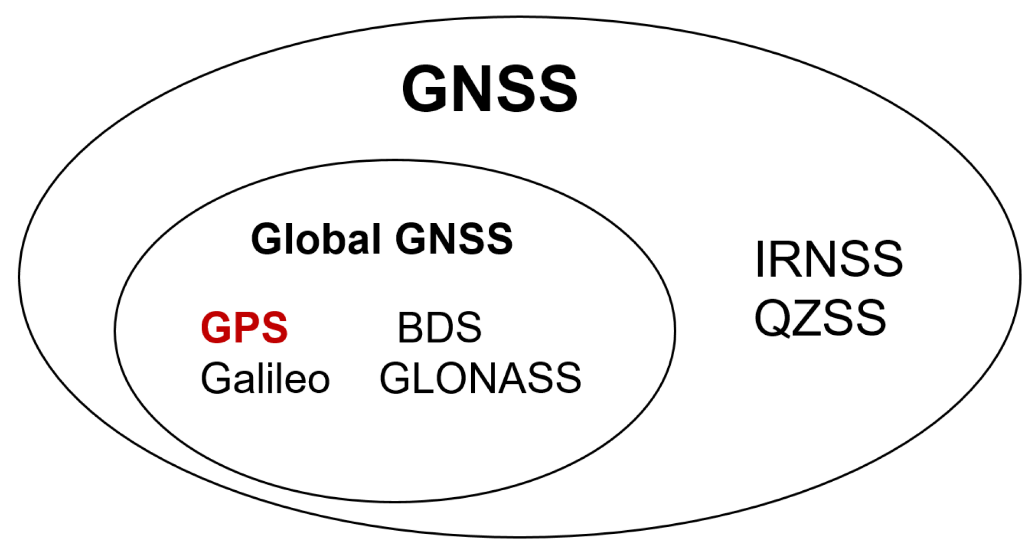
In October 2011, Creech Air Force Base was targeted by a malware attack on Predator and Reaper drones, with ground control stations infected by a keystroke logger. The malware, believed to have been created by a foreign nation-state, persisted after multiple system cleanings, potentially aimed at gathering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

**S-100 Camcopter**

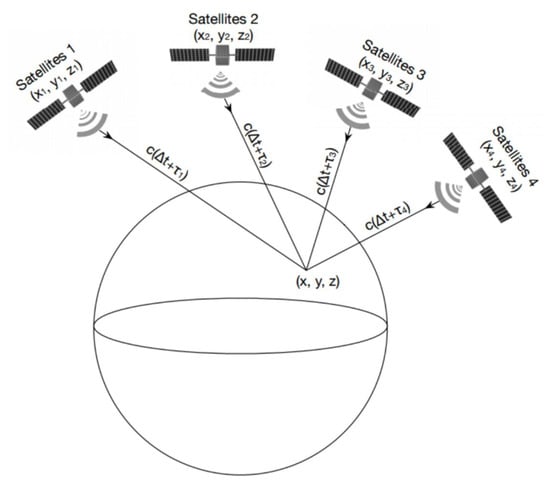
There has been only one publicly reported actual attack on sUAS (small Unmanned Aerial Vehicles), and it was a GPS Jamming attack. A suspected GPS Jamming attack was executed on S-100 Camcopter, a rotor based UAV by Schiebel, resulting in a crash into the ground control van killing a Schiebel engineer 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.

**GPS GNSS**

GPS (Global Positioning System) is a specific type of GNSS (Global Navigation Satellite System). GNSS is a generic term used to describe any system that uses satellites to provide positioning, navigation, and timing information to users worldwide. Examples of other GNSS include GLONASS (Russia), Galileo (Europe), and BeiDou (China). GPS (USA) consists of the space segment, control segment and user segment. The control segment consists of 1 master control station, injection stations and monitoring stations and is mainly used to detect and control the satellite’s movement, compose satellite ephemeris and monitor system time. The user segment is mainly composed of the GPS receiver system used to receive and process satellite signals and provide navigational positioning information. There are two types of receivers: navigational receiver (handheld, vehicular and airborne) and geodetic receiver (single-frequency and dual-frequency).



GPS satellites continuously transmit broadcast signals, that is, navigation messages, which mainly carry the current timestamp and orbital coordinates of the satellite. The time when the ground receiver receives the signal is subtracted from the time stamp carried by the message and then multiplied by the speed of light, *c*, to obtain the relative distance between the receiver and a single satellite. Therefore, when the ground receiver can receive more than three groups of GPS signals, the absolute position of the receiver on the earth can be solved directly according to the topological relationship of the satellites. It is worth mentioning that the timestamp carried by the satellite is verified by the atomic clock, and the accuracy is much higher than that of the clock of the ground receiver. In order to eliminate this error, a fourth satellite is generally introduced, and the current time is also used as a variable. This is the typical four-star positioning. The specific calculation process is as follows:



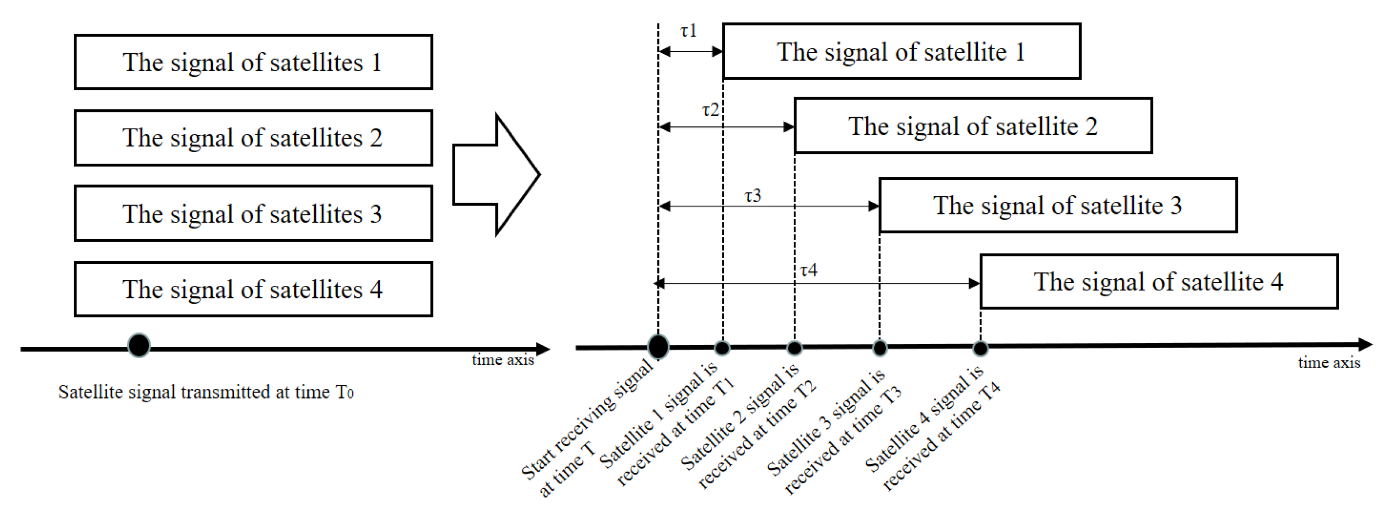
**Figure** Topological relationship between GPS signal receiver and satellites: typical four-star positioning.

According to the timing characteristics of the satellite signal received by GPS, the formula can be obtained for the signal of satellite **i** in the spatial coordinate system:

*(∆t+τi)∗c=P(xi,yi,zi)−P(x,y,z)*

where *∆t=T−T0, T0* is the transmission time of the satellite signal, *T* is the reference receiving time, τi is the time delay of the received satellite *i* signal relative to the reference time, *c* represents the speed of light, *P(xi,yi,zi)* are the space coordinates of satellite *i*, and *P(x,y,z)* are the space coordinates of the GPS receiver. The two vectors are subtracted into distance.

**Figure.** Example timing diagram of signal received by GPS receiver in four-star positioning.

**[](https://www.mdpi.com/remotesensing/remotesensing-14-04826/article_deploy/html/images/remotesensing-14-04826-g004.png)**

For four satellites, there are equations as follows:

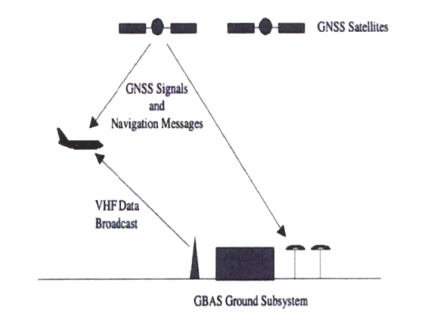
*(∆t+τ1)∗c=P(x1,y1,z1)−P(x,y,z)*

*(∆t+τ2)∗c=P(x2,y2,z2)−P(x,y,z)*

*(∆t+τ3)∗c=P(x3,y3,z3)−P(x,y,z)*

*(∆t+τ4)∗c=P(x4,y4,z4)−P(x,y,z)*

Thus, the quaternion equation can be solved and the receiver coordinates, P(x,y,z), can be obtained as long as the coordinate position of each satellite is known and the relative propagation delay of each satellite signal is measured. This achieves accurate positioning of the receiver.



**Typical gnss signal**

The overall designs of all forms of GNSS are remarkably similar. All transmit three basic messages:

a) A ranging signal for position, velocity and timing (PVT),

b) Precise ephemeris data, which speciﬁes the exact location of the individual satellite,

and

c) An almanac, which speciﬁes the locations and orbits of all satellites in the constellation, along with status information, used to select satellites for tracking.

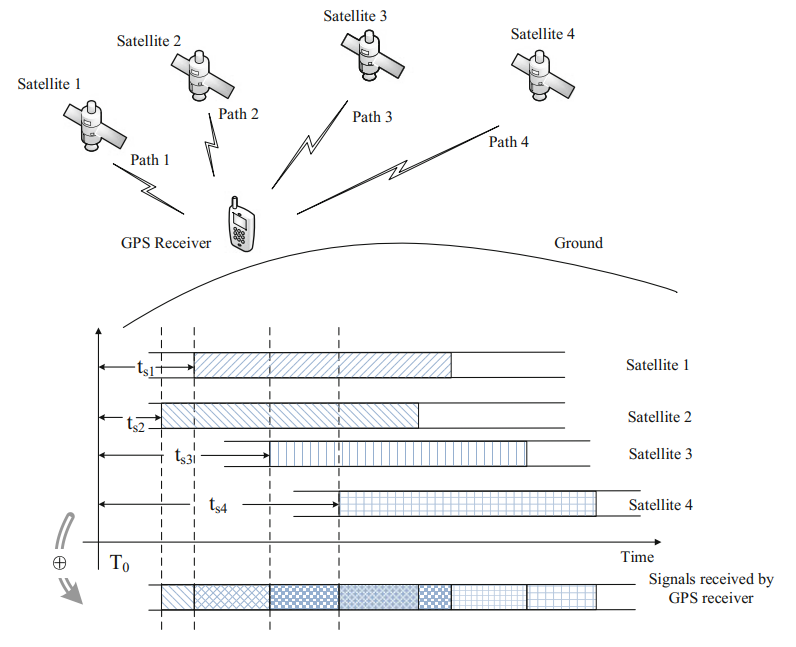
All types of GNSS satellites transmit on at least two bands: using the predominant GPS terminology, on frequency L1 an encrypted military code, called P(Y), and an unencrypted civilian code, called C/A, while on the L2 band the P(Y) code is repeated.

At the lowest level a GNSS navigation signal can be seen as an analog sinusoidal wave at a frequency that varies roughly between 1.2 and 1.6 GHz. In order to carry digital information, segments of this basic signal are phase-shifted, in the case of GPS or GLONASS L1 by π radians. The usual method is BPSK (binary phase shift keying), which encodes 1 bit per phase-shift. Other variations are QPSK (quadphase), which uses four phase shifts to encode 2 bits per shift, as used in Beidou-2, and MBOC (multiplexed binary offset carrier), as used in GalileoE1, which is designed to interoperate with the existing GPS L1 signal. The information transmitted on a given frequency is composed of two separate signals: the in-phase (I) and quadrature (Q) components. These are phase-shifted by 90◦ with respect to each other. In the case of GPS L1 (1575.42 MHz) the in-phase signal carries the civilian C/A code and the Q component the military P(Y) code. In all cases what is encoded onto the analog carrier wave is a PRN (pseudo randomnumber) sequence. The PRN is transmitted at an order of magnitude slower than the carrier, in the case of GPS L1, at 1 megabits per second. The length of the civilian PRN sequence is 1023 bits, which lasts for 1 millisecond, then it repeats. The W-code used in GPS L2, on the other hand, is 6.1871 ×1012 bits long and takes a week to transmit.

The encrypted military signal can be used to compensate for this delay by correlating the two versions of the P(Y) code, which are delayed by differing amounts due to their different frequencies. However, it is possible even for civilian receivers to align the two P(Y) signals, using codeless techniques, and so derive the same ionospheric delay to correct the C/A code.

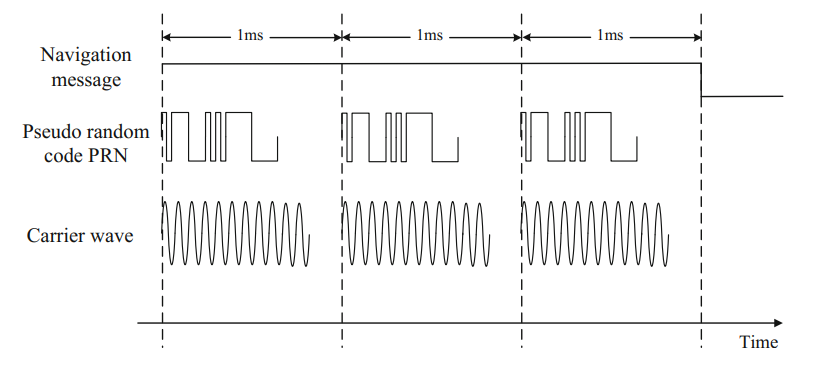
**Principle of gps signal system**

The distribution of satellites has been ingeniously designed to guarantee at least 4–8 satellites can be observed at any place and moment on earth surface and in territorial space. Why need at least 4 of satellites? The principle of GPS positioning is shown in the below figure. GPS positioning is implemented by distance measurement. The GPS receiver needs to measure the distance of every satellite to itself, and the distance is equal to light speed c multiplied by time, so we have: . Therefore, distance measurement is essentially time measurement. As shown in figure, the GPS receiver on the ground can receive the signals of 4 satellites. Suppose all satellites send their respective messages at the same moment *T0*, and the messages reach the receiver via different paths. Since time delay applies to all messages, their arrival times should be different. In the figure, represent the times it takes for the 4 satellites to reach the receiver, respectively.



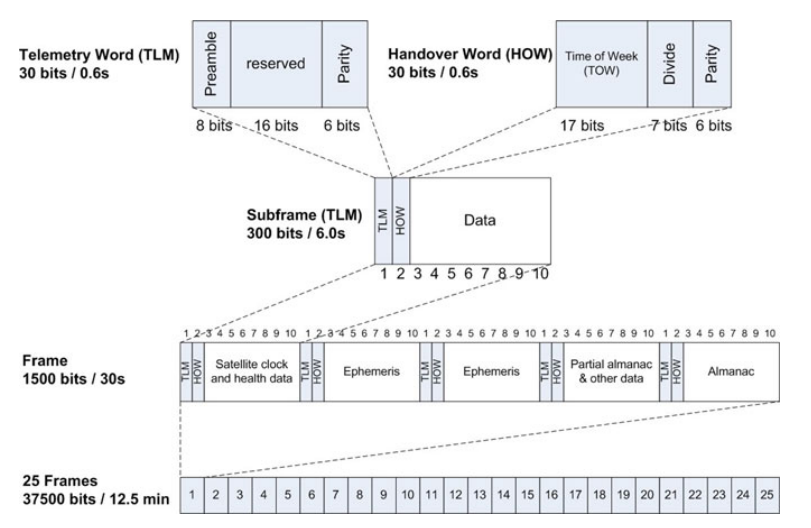
Principal of gps positioning

GPS signal is the product of carrier wave, PRN code and navigation messag. PRN, or pseudo random noise code, guarantees the ground user can detect and process weak signals with its spread spectrum characteristic. Meanwhile, the selfcorrelation and cross-correlation characteristics of these PRN code ensure the signals of multiple satellites which share the same carrier frequency can be differentiated. Navigation message is the modulated data in a GPS signal and plays a significant role in the signal’s composition. Every satellite is continuously transmitting its unique navigation message, which provides the signal’s accurate time of transmission and the satellite’s ephemeris data. And the satellite’s accurate position can be obtained by the receiver based on the above two parameters. The navigation message also provides information about the satellite’s health status, configuration, anti-spoofing technology, correction parameters of ionosphere and troposphere and almanac data. The above orbital parameters improves accuracy of positioning on one hand, and accelerates signal capturing on the other.



Basic components of a gps signal

The navigation message can be divided into 5 different layers. The most fundamental structure is bytes. The data rate of navigation message is 50 bps, which means one effective byte outputs every 20 ms. So, the data rate of GPS modulation is really slow. It was designed in this way in order to ensure minimum bit error rate with a sufficient spreading gain. The second layer is word, which consists of 30 bytes. And the 3rd layer is subframe, consisting of 10 words. Therefore one subframe contains 300 bytes. The fourth layer is page or frame. 5 subframes comprise a page. Lastly, 25 pages comprise a full-cycle navigation message. Every satellite is continuously transmitting cycled navigation messages consisting of 25 pages each.



layered structure of the navigation message

The receiver receives every satellite’s ephemeris data to determine the satellite’s position. It also needs the time of transmission and clock correction data to work out the pseudo distance (ρ in the formula) and thereby the receiver’s position. The above information is transmitted in the first three subframes, therefore the receiver needs at least 16 s (in the worst case 30 s) to obtain it. However, the satellite is moving at 3–4 km/s at high altitudes during spatial transmission, and the user might also be moving, therefore the satellite signal received by the user must have a Doppler frequency shift phenomenon. Besides, the relative movement between the satellite and the user’s receiver must be considered because of Doppler effect. As a result, The GPS simulator must simulate Doppler effect.

**GPS Vulnerabilities Analysis**

The vulnerability of GNSS itself is the basis of GNSS spoofing. The vulnerability of GPS mainly includes:

**Navigation signal format disclosure:** GNSS currently uses three public frequencies *L1, L2* and *L5* to broadcast navigation signals. The spectrum characteristics, signal modulation format and pseudo-random code sequence of each frequency point have been disclosed. Because the main signal parameters have been disclosed, this means that there is no “secret” for the spoofer. Spoofers can often take targeted spoofing actions according to relevant signal parameters and characteristics.

**Navigation data format disclosure:** GNSS navigation message data usually include ephemeris, almanac, satellite clock parameters, ionosphere/troposphere and other important parameters. These parameters play a very important role in accurate user positioning. However, in order to facilitate the use of relevant users, GNSS disclosed the arrangement mode, data definition and application method of its navigation message from the beginning. This also means that a spoofer can easily and pertinently intercept and tamper with relevant navigation data, which means relevant users can receive wrong navigation data for the location solution without being aware, so as to achieve the purpose of spoofing.

**Unprotected broadcast channel:** in order to ensure the convenience of users, GNSS adopts a broadcast communication mode, that is, directly broadcast navigation signals to the majority of users. This mode actually makes its communication channel directly exposed in the social space and vulnerable to interference, monitoring and tampering. In addition, because the GPS signal is extremely weak when it reaches the ground (the average signal power is often −150 dbw∼−160 dbw) , only low directional power is needed in order to interfere with and suppress the legal GNSS signal, which objectively leads to a more fragile GNSS signal in practice.

**3.Spoofing**

Because the position and clock difference of the receiver depend on the satellite position and observation pseudo-range, the receiver can get wrong results by changing the satellite position or observation pseudo-range through spoofing. There are two main spoofing modes: generating false message information and increasing signal propagation delay, which correspond to two spoofing modes: generating mode and forwarding mode. Generative spoofing is a kind of spoofing device that produced false navigation signals independently. By giving false satellite position information, the receiver's solution results deviate from the real position and time. Forwarding spoofing was to receive real satellite navigation signals and delay and forward them. By changing the observation pseudorange of the receiver, the result of the receiver's calculation will be wrong. Regardless of the spoofing mode, in order to achieve spoofing to the user receiver, the spoofing equipment need to modify the parameters such as signal power, navigation message and signal propagation delay when the spoofing signal enters the receiver. It is very difficult to control the power and direction of the spoofing signal when it entered the receiver, which was different from the real signal. The detection of spoofing signal was to detect and identify spoofing signal by comparing the difference of signal power, carrier-to-noise ratio, relative power of different frequency points, Doppler consistency, message information and other parameters between deception signal parameters and real signal parameters.

3.2 Meaconing.

The simplest form of spooﬁng is meaconing, which is the capture and retransmission of legitimate GNSS signals after a delay. Meaconing, however, is difﬁcult in the case of the encrypted military signal, such as the GPS P(Y), because it is modulated onto a far longer PRN sequence. Since receivers have their own clock they could easily detect the out of phase alignment of the W code. Also, because the P(Y) GPS signal is transmitted well below the background noise level, re-transmitting it would require an accurate estimation of the secret W code, which can be achieved via “semi-codeless” techniques. For the civilian signals, however, no such difﬁculty of spooﬁng arises. Since the relative arrival times of the four signals are unchanged by the meaconing process, the navigation solution will be that of the meaconer. The timing solution will likewise be that of the meaconer, plus the time taken to retransmit the signals to the victim. However, meaconing does not seem suitable for attacks against timers. The ﬁrst stage of an attack is to substitute the spoofed signal for the real one. Since a timer already knows its own location, it would read the delayed time being transmitted by the meaconer, resulting in a sudden shift in the timing solution equal to the time required to retransmit the signal. This would clash with the known local time maintained by the clock, and could be used to raise an alarm. However, meaconing could also be performed initially with a zero-delay, by predicting the signal values in advance and synchronising with the true signals.

3.2.1. SCER. A variation of meaconing called SCER (security code estimation and re-play) or “selective delay” involves the rebroadcast of individual satellite signals after a delay. This can modify both the position and/ortiming solutions. An attacker could then manipulate the position solution only and soavoid a time jump when starting an attack.

3.2.2. Other forms of spooﬁng. Other forms of spooﬁng are categorized by the level of so-phistication. Humphreys and Motella divide these into “simplistic” (broadcast of arbitrary GNSS signals without synchronization with legitimate signals), “intermediate”(spooﬁng synchronized with legitimate signals) and “sophisticated” (using multiple phase-locked intermediate spoofers). A spooﬁng device, called as “limpet spoofers”, can be attached to the vehicle or timer it is intended to spoof. These devices overcome many of the practical limitations on spooﬁng described in Section 5 below, but require both compromise of the physical security of the receiver, and in practice also a level of miniaturization that has not yet been achieved

In addition to the general definition mentioned above, there are also different classifications of spoofing. To properly understand the attacks that are carried out, it is necessary to take a look at these different approaches as well.

**4. Classification and Research Progress of Spoofing Technology**

*4.1. Traditional Classification of Spoofing Types Based on Signal-Generation Mode*

It is a typical classification method to classify the types of spoofing according to the generation mode of the spoofing signal. This is generally divided into two categories: production spoofing and forwarding spoofing.

* Production spoofing

Production spoofing usually refers to transmitting the signal generated by the signal generation equipment itself directly to the USE receiver so that the target USE produces the wrong position solution to achieve the purpose of cheating the USE by the attacker. Its advantage is that the navigation signal and transmission time have their own flexible decision, which can lag or advance the transmission time of the signal and can also give wrong location information in the navigation message.

* Forwarding spoofing

As its name implies, forwarding spoofing collects the real satellite signals then enhances them and delays forwarding so that the target receiver tracks the deception signal and gets the wrong navigation and positioning result. Compared with production spoofing, this type does not need to master the structure and setup of the signal in advance. Further, the essence of forwarding spoofing is to forward the real signal, which has strong consistency with the real signal, so it has good spoofing effect on GNSS civil code and military code receivers. However, at the same time, because its implementation is based on forwarding of the real phase signal, the delay processing of the signal can only be greater than the delay of the real signal. So the generation of the deception signal is less flexible and more restrictive. This also determines that it is not easy to achieve more complex deception purposes in the deception mode, and the enhancement processing before transmitting the deception signal also amplifies the noise.

* Gradual self-synchronization spoofing

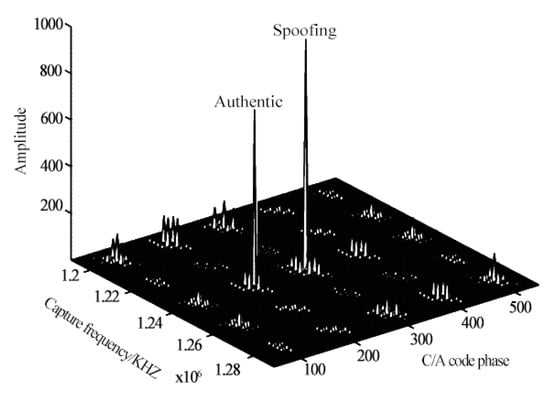
Under this classification standard, in addition to the above two traditional types, there has been a gradual self-synchronization spoofing developed in recent years that deceives the receiver tracking loop and is classified as an advanced type of spoofing in the relevant literature. After receiving the real signal, the spoofer carries out range delay and Doppler modulation according to the dynamic performance of the target receiver so as to control the satellite delay when the target is not aware. This method can realize the gradual guidance deception of booking location or path. It is a new concealed and efficient deception method. The key to the realization of gradual self-synchronization spoofing technology is how to effectively invade the target receiver to realize covert synchronization spoofing. For civil and military receivers, the technical implementation difficulty is different. For the civil receiver, due to disclosure of the civil pseudo-random code system, the pseudo-random code periodic signal can be repeatedly generated locally. When the spoofing signal has Doppler offset, it can move to the same code phase of the real signal within a period of time, so as to realize spoofing. For the military receiver, because the military pseudo-random code is unknown, it is necessary to use an antenna with strong directionality to isolate different satellite signals and spoof by forwarding indirect control. Moreover, it is difficult to predict the general position and motion trend of the target in advance to obtain the spoofing phase conditions. Gradual self-synchronization spoofing technology will be the research focus of GNSS spoofing in the future.

*4.2. Classification of Spoofing Types Based on Spoofing Implementation Stage*

Another attack classification method is based on the receiving state of the GNSS signal by the receiver. The receiving of GNSS signals by the receiver is mainly divided into two stages: capture signal and tracking signal. The attacker’s spoofing attack behavior can be expanded according to the characteristics of the receiver in different phases of receiving signals.

* Capture-phase spoofing

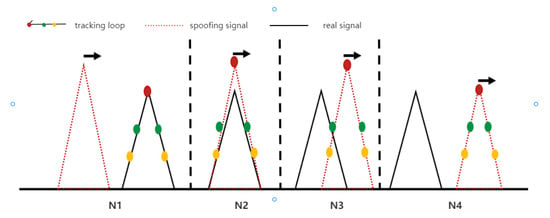
In the capture phase, as the receiver has not locked the signal, it needs to implement three-bit searches in a large range. The receiver needs to traverse 1023 code phases for each satellite signal (taking GPS C/A code as an example) to search for a wide range and carrier frequency. At this time, the deception signal power only needs to be slightly stronger than that of the real signal to successfully realize the deception attack, that is, to let the target receiver lock the deception signal. Because it does not need strong power and does not need to consider the synchronization of the phase and carrier frequency between the deception signal and the real signal number at the beginning, the implementation of a deception attack is easier. For a target receiver that has normally tracked the real signal, the target receiver can lose lock and recapture by suppressing interference to realize a deception attack.



**Figure.** Spoofing attack in capture stage.

* Tracking-phase spoofing

When the receiver finishes locking the signal and enters the tracking stage, the receiver will no longer carry out fuzzy search over a large range as in the capture stage. If the carrier frequency and code phase of the spoofing signal are not aligned with the real signal, even a strong spoofing signal cannot easily affect the normal tracking of the receiver, so it is difficult to achieve the goal of spoofing. At this time, the synchronization of code phase and carrier frequency must be considered. The feasible method is to realize the traction of the tracking loop of the target receiver by sliding-step self-synchronization. It is worth mentioning that this can also be called the gradual self-synchronization spoofing method.



**Figure.** Schematic diagram of sliding self-synchronization mode of spoofing attack in tracking stage. N1: Align the phase of the spoofing signal number with the real signal; N2: Carrier ring of control receiver; N3: Introduce code phase change to spoofing signal; N4: Properly reduce the power of spoofing signal and complete the tracking loop control of receiver.

*4.3. Traditional Classification of Spoofing Types Based on Priori Knowledge*

* CS Spoofing starts before acquisition and the receiver has no a priori knowledge: This situation occurs after a receiver is switched on (cold start). It provides a maximum of options to the spoofer who wants the receiver to capture his signal first. The receiver cannot distinguish the spoofer’s signal from an authentic GNSS signal unless the signal is somehow authenticated. The receiver’s clock might have drifted substantially and the position might be completely different at power-up than it was at power-down.
* Ra Spoofing starts before acquisition but the receiver has a priori knowledge: This occurs if the receiver has lost one or all satellites for a short while, or acquires satellites that have newly raised above the horizon. Snap-shot receivers are in this situation for every estimate that they perform once they have prior knowledge. In all these cases, the spoofer has to be aware that the receiver combines knowledge about its state, the environment, and their evolution to detect spoofer activity. Changes that a receiver might analyze against models include position, clockoffsets, and atmospheric delays.
* Tr Spoofing during tracking: This is the most demanding situation for the spoofer, since the signals now have to change in a manner compatible with the detailed physical movement of the receiver, as well as with the changes in its environment. Vector tracking can be used to further harden the receiver in this state. The above description provides a characterization with respect to the relative timing of spoofing and acquisition.

The naming of these states is CS for “Cold Start,” Ra for “Reacquisition,” and Tr for “Tracking.” The first situation, i.e., “Cold Start,” gives the largest freedom to the spoofer. The last situation, “Tracking” (Tr), is easiest to defend by the receiver. The spoofer might thus aim at provoking a “Reacquisition” by jamming the receiver before initiating the spoofing procedure. Although such jamming creates a signature, the latter signature could also have a natural cause. If the target receiver uses this signature as a sole trigger for detecting the spoofer, this might reduce service availability to an unacceptably low level. The spoofer has the final option to willingly cause a denial of service if he feels that he cannot deceive the receiver otherwise.

*4.4. New Classification of Spoofing Types Based on Spoofing Strategies*

With the development of anti-spoofing technology, spoofing attacks are no longer carried out in a single way; rather, they have become gradually diversified and complex. In some papers there are some proposes that a new classification method by analyzing the spoofing strategies taken by attackers to achieve their goals. The new classification method puts forward three new classification indexes.

* Self-consistent spoofing

Self-consistent spoofing is generally used to cheat the traditional RAIM strategy of considering pseudo range residuals. This method provides the desired position/timing for the potentially deceived receiver by synthesizing the false code phase and maintaining a small pseudo-range residual. In this method, the calculation required in the phase stage of synthesizing error code is very simple. The change of the false beat carrier phase is usually designed to be consistent with the phase of the false deception code. Otherwise, the potentially deceived receiver may issue a warning due to unusual C/A differences or may lose the lock on the spoofing signal.

The main difficulty of self-consistent spoofing is how to induce the potentially deceived receiver to lock the false signal it provides. There are two main ways to achieve this goal.

The first is to interfere with the victims, destroy their original normal signal acquisition and induce them to try to obtain a new signal. If the deception signal power is significantly stronger than the real signal power, the receiver will most likely lock onto the deception signal during signal re-acquisition. Another method is to send false signals from low power to make them code match and Doppler match with the real signal at the position of the victim receiver antenna. The power of deception starts low and then increases until it is sufficient to capture the tracking loop. Finally, the deceiver completes the deception of the coding phase and carrier phase to the deceived receiver in a self-consistent way.

* Signal estimation and replay spoofing

The deception method described in self-consistent spoofing must recreate the spread spectrum code  to be transmitted and the data bit stream  to be transmitted. If they are completely predictable, they are easy to synthesize. However, the enhanced civil GNSS signal will adopt orthogonal modulation and protect the unpredictable part of the short segment in the spread spectrum code .

In this case, one of the choices of the deceiver is signal interference. The signal jammer records the real GNSS signal as in a conventional receiver and replays the signal through a transmitter with sufficient gain to drown the real signal on the antenna of the victim receiver. The deceiver may deceive any GNSS signal, even encrypted military signals.

If the unpredictable part of the signal is only in the low-rate bit, it is possible to complete deception without interference. Instead, spoofers can use a secure code estimation and replay (SCER) attack: spoofers estimate unpredictable bits and broadcast them immediately after obtaining reliable estimates. Before broadcasting them, it can broadcast random guesses of these bits or its own best estimates.

* Advanced-form spoofing

Nowadays, with the continuous advancement of the research works of various spoofing defense technologies, the means of spoofing are also improving daily. An advanced technique is called zeroing. The spoofer sends two signals for each spoofing signal. One is the spoofing signal, which works in conjunction with all other spoofing signals to cause incorrect location/timing positioning. The other is the negative value of the real signal, which is used to cancel the real signal at the receiver. The zeroing attack will delete all traces of the real signal. However, the principle of many current defense measures is to look for signs that two signals from the same satellite are received. They may look for different signals with sufficient spread between their coding phases or carrier Doppler shifts. Alternatively, they may look for interfering signals with similar code phase and carrier Doppler shift. In either case, clearing will eliminate all signs of duplicate signals, and defense measures relying on these signs will not be able to detect such attacks.

The other is used to combat advanced spoofing with multiple-antenna victim receivers. This method generally uses multiple independent spoofing transmitting antennas and matches each antenna to the corresponding receiver antenna. Moreover, the deceiver must be close enough to the victim, and the gain pattern of each antenna must be obtained and reduced sufficiently so that each victim antenna receives only the signal from the deceiver antenna. This technology will enable the deceiver to control the difference between the beat carrier phase of each spoofing signal received at different antennas of the victim receiver in the time axis.

These and other high-level forms of spoofing usually do not change the location or time of the victim too quickly. Otherwise, the victim can identify the attack through physical properties. For example, an inertial measurement unit (IMU) can be used as a physical anti-spoofing detection, which further limits the possible growth rate of deception navigation. If the growth rate is too high to be suspected, the conventional IMU drift level cannot be used to explain this anomaly. The same is true of the increase in the clock offset of the victim receiver.

**PRACTICAL DIFFICULTIES OF SPOOFING**

Covert operations

Knowledge of the exact location of the relevant antenna and make and model of the GNSS receiver it is connected to, and its spoofability, would be essential for the attackto have any realistic chance of success. If an off-the-shelf simulator was chosen, police forces could use the record of purchase to track down the offender if the attack was detected. Thiscould result from simultaneous disruption of mobile GNSS services in the vicinity, through mobile jamming detectors, or through direct detection by sensor networks.

Inverse square law

One of the major problems faced by the would-be spoofer is the simple inverse square

law:

Where is the transmitted power, the received power, and d the distance between the receiving and transmitting antennas. As the distance between spoofer and target varies even by a small amount, for example, when spooﬁng a navigation receiver in a vehicle, the received signal strength varies more widely, in accordance with the term. As a result the spoofer must either maintain a precise distance to the target or vary signal strength to compensate. Otherwise, the receiver may detect the unexpectedly strong signal and report loss of lock, or will fall back onto the legitimate signals. In either case the spoofer would have to start all over again, but would not know that the attack had failed. The signals from legitimate satellites also vary with the inverse square law, but their distance from the receiver doesn’t vary signiﬁcantly for distances of several kilometres on the earth’s surface, but such variations make a very big difference in the spooﬁng case because the transmitter and receiver are much closer together. Some of the variations that do occur in the legitimate signals depend on known factors such as satellite elevation, but received power can also vary by as much as ±6dbW due to the orientation of the transmitting antenna and changes in altitude of the SV. All of the cited spooﬁng experiments carried out in the laboratory have emphasized this need for closely controlling signal strength for a spooﬁng attack to succeed.

Moving targets

One consequence of the inverse square law is the difﬁculty of spooﬁng a moving target such as a ship, aeroplane or car. In order to maintain correct signal strength it would be necessary for the spoofer also to be moving with the target. Similarly, in order to spoof a truck’s navigation system, Warner had to follow 15 feet behind the target truck after ﬁrst disabling the its GPS satellite lock and establishing a fake one at close proximity for several minutes. Kerns notes the need for accurate tracking of aircraft for spooﬁng to succeed, requiring the use of the aircraft’s own ADS-B broadcasts. Jafarnia and Wesson note that for a synchronous spooﬁng attack (the precise alignment of the legitimate and spoofed PRN sequences) to avoid detection through the vestigal signal defense requires precise “centimetre level knowledge” of the position of the spoofer in relation to its target. Ideally, a spooﬁng device needs to be either physically on the receiving antenna or at a ﬁxed distance from it. Although these were experiments, or theoretical scenarios, these kinds of limitations make the remote spooﬁng of vehicles very difﬁcult in many cases, and in the case of ground-based vehicles jamming is often easier, more reliable and far cheaper.

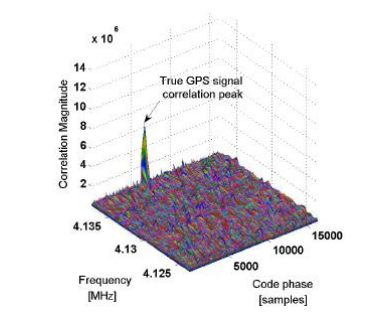
Direct line of sight

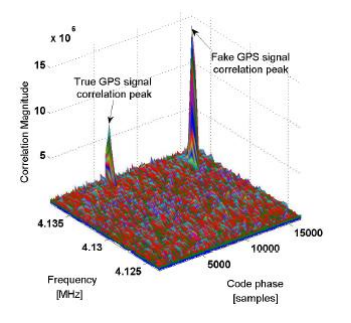
The most common GNSS signals are transmitted around 1.5 GHz (GPS L1, etc.), which has a wavelength of just 20cm. As a result, GNSS signals do not bend much around obstacles. Hence a spoofer would have to be in direct line of sight with the target’s antenna. Aircraft are already considered immune from ground-based GNSS interference when in ﬂight, because of the shielding effect of the aircraft underside, while the antenna is typically situated on the top of the aircraft. Terrestrial broadcasting of spooﬁng signals inside a city or in uneven terrain would also likely fail because of shielding from buildings and hills.

**Overview of Anti-Spoofing Technology**

*5.1.* **Power detection technology**

When the receiver was on the ground, the received satellite signal power was generally below the maximum power. Without occlusion, the received signal power level is low. For example, the maximum receiving power of GPS signal will not exceed -150dBW, and the receiving power of L1, L2 and L5 frequency points was generally between -150dBW and - 162dBW. Deception attack made the receiver to capture and track deceptive signals incorrectly, and the deceptive signal power was generally larger than the real signal power, so that deceptive signals can be detected and identified by limiting the signal power through a reasonable power upper limit. Signal power can be measured by capturing peak value, tracking correlation value and carrier-to-noise ratio. However, not only signal power, but also interference and noise power affected the above three detection statistics. Acquisition was a two-dimensional search procedure for PN phase and carrier frequency of GNSS satellite signal for a specific PRN number. The acquisition peak value was the correlation between the GNSS spatial signal and the aligned local signal, and its peak value reflected the signal power and noise power. Therefore, the acquisition peak spoofing detection algorithm can be formed. For the tracking correlation value of I and Q branch, which reflected the signal power and noise power. Therefore, the tracking correlation value spoofing detection algorithm can be formed. Carrier-to-noise ratio (C/N0) reflected the relationship between signal power and noise power, and was an important index to describe the signal quality of receivers. The correlation signal power was mainly reflected in the I branch and the correlation noise power was mainly reflected in the Q branch. Carrier-to-noise ratio (C/N0) was usually determined by the correlation values of I and Q paths. Because the carrierto-noise ratio of GNSS satellite signal was affected by the correlation between noise and other jamming signals, the carrier-to-noise ratio (C/N0) deception detection algorithm can be formed by using the distribution of carrier-to-noise ratio (C/N0) of GNSS satellite signal under receiving noise.

 the correlation peaks without jamming

 the correlation peaks with jamming

*5.2. Anti-Spoofing Technology Based on Encryption*

Such technologies use encryption to create unpredictable parts of the transmission signal that make it difficult for the deceiver to make the above estimation and replay the deception. The strongest defense measure is to encrypt the whole extension code  with a symmetric key.

One method is to use symmetric encryption. A GNSS signal encrypted with a symmetric key can be used to detect spoofing in a civil GNSS receiver without accessing the private key. It is not necessary to distribute the key to the civil receiver, but it can use the known relationship between the open civil extension code and the encrypted military code. In GNSS, they are quadrature modulated on the same carrier. Under this method, the receiver uses its civil code tracking system to record the noisy baseband version of encryption coding. This is done on a potential victim receiver and another receiver that can prevent spoofing. The two noisy versions of the encrypted code are then interacted to find the correlation peak that will exist if the signal in the potential victim is real. If the correlation peak is very high, it indicates that the signal is true; otherwise, an alarm will be issued. However, this needs a secure receiver network to generate a noisy “real” version of the encrypted code. It also requires a secure communication network to bring real and unverified versions of the encrypted code to a common signal processing unit that can check the correlation. The purpose of this is to check the authenticity of the signal.

Another method is to use delayed symmetric key encryption. In the spreading code, the short segment of the symmetrically encrypted spread spectrum security code (SSSC) is interleaved with the long segment of the predictable spreading code. The receiver uses the known part to track the signal and records the unknown part. Shortly after the unpredictable SSSC is broadcast, bitstream data containing the key arrives, which can be used to generate the SSSC. The key is digitally signed, so it can be reliably traced back to the relevant GNSS control segment. After verification, the key is used to synthesize the unknown spreading code, and the receiver associates the code with its recorded signal part to verify the authenticity of the signal. However, the technology using this method will involve a large number of detection delays when waiting for a complete digital signature, which may take a few seconds to a few minutes.

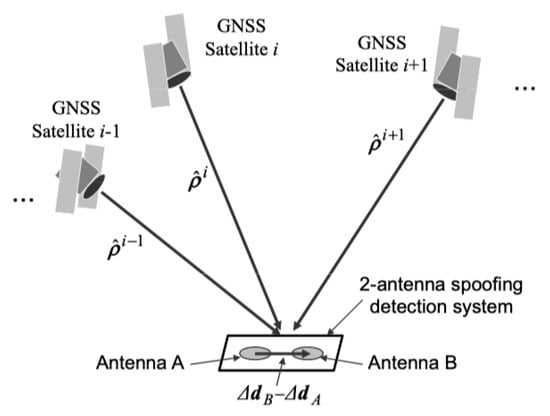
The third method is asymmetric private/public key navigation message authentication (NMA). A subset of the broadcast data stream  contains an unpredictable digital signature generated using the private key of the control segment. This signature signs the rest of the data in . The receiver knows the position of these bits in the demodulated data stream. It collects all the numbers needed to check the signature and verifies it with a known public key. The implementation of a delayed symmetric key SSSC method and asymmetric private key/public key NMA method are needed to modify the satellite signal. This is difficult or impossible for existing GNSS satellites and expensive for future satellites.

*5.3. Anti-Spoofing Technology Based on Drift*

Drift-based anti-spoofing technologies aim to find abnormal changes in receiver position or clock. If spoofing causes the receiver clock error to change too fast, the victim receiver can detect that the clock drift rate is greater than a reasonable value of its oscillator category. IMU or other motion sensors can impose similar constraints on the reasonable drift rate of the position. Similarly, the rolling constraint of the vehicle and its known maximum values of speed, acceleration and turn rate can be used to check whether there is excessive drift. As with clock drift, if an untrue motion track is detected, the receiver will issue a deception alarm. However, the deceiver can avoid being detected by the drift detection method by slowly establishing the wrong clock offset and wrong position.

*5.4. Anti-Spoofing Technology Based on Signal/Geographical Location*

Signal location techniques monitor the direction of arrival of the signal by considering the received beat carrier phase. The receiver can use interferometry by using three or more different antennas to sense Δd(t) offsets or by using the direction of arrival vector as measured by a single antenna’s Δd(t)motion curve.



**Figure.** Schematic diagram of interferometry model.

*5.5. Complementary Strategy of Multiple Anti-Spoofing Technologies*

At present, in order to avoid the likelihood of the target detecting the attack to the greatest extent, spoofers usually use a complex attack method combining multiple spoofing strategies rather than a single method. Based on this situation, it is a relevent yet difficult point for researchers to develop more effective detection methods that can adapt to complex spoofing scenes.

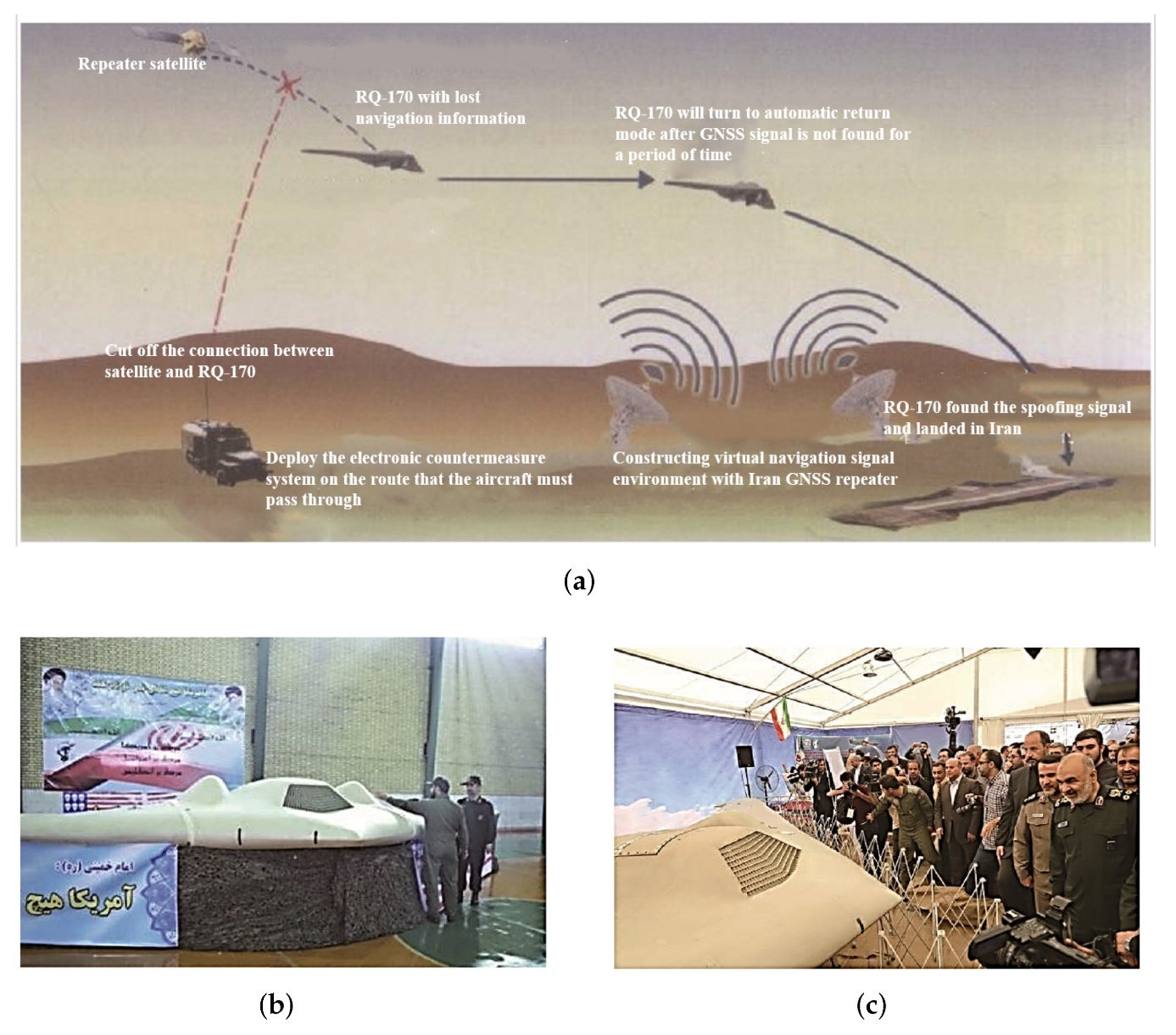
For example, one of the combination strategies is that the spoofer can choose to use a higher carrier amplitude to avoid the obvious distortion of complex correlation function in the process of drag off. If the defense object checks the complex correlation at many stages when implementing received power monitoring (RPM), which views the total received power in absolute proportion, it can detect the beginning of the attack, regardless of how much power the spoofer uses. If the clock offset drift rate and position drift rate are also monitored, the spoofer will be forced to perform a slow drag-off operation so that the receiver has more time to detect the distortion of the complex correlation function or the high received power level.

Another combination strategy is to use the unpredictable data bits of NMA to monitor the distortion of those bits, plus IMU and clock drift monitoring. IMU and clock drift monitoring will force spoofer to launch attacks slowly. This restriction will prevent the formation of dangerous position or timing errors in the latency of NMA-based spoofing detection. If the spoofer implements an SCER attack to estimate and replay unpredictable NMA bits, the victim will be able to detect the initial uncertainty of these bits. Because clock-drift monitoring will limit the initial ability of the spoofer to use the delay, this will allow a reliable estimation of the bits before starting the broadcast.

**Example of spoofing**

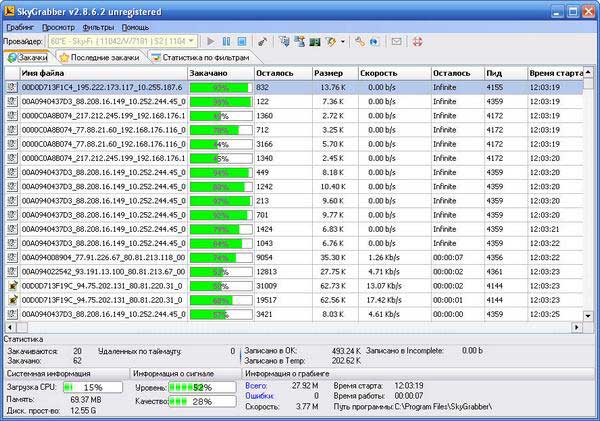
**RQ-170**

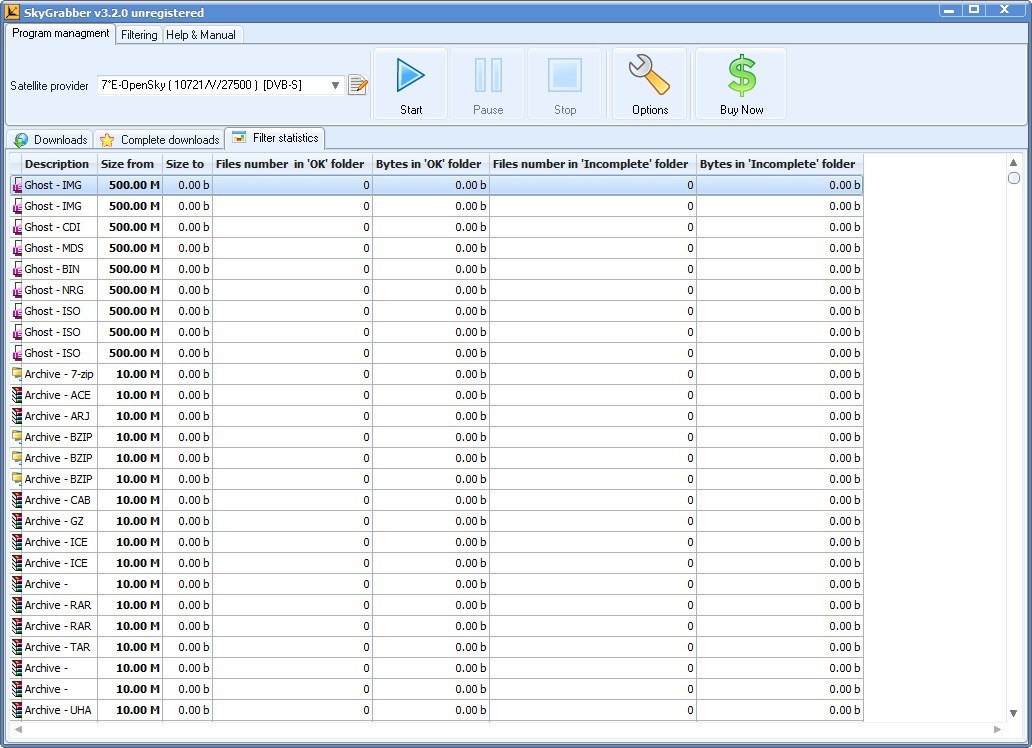
On 4 December 2011, Iran announced the capture of a U.S. stealth unmanned reconnaissance aircraft RQ-170. A participating Iranian engineer said they took advantage of the weakness of the UAV navigation system. First, through interference, they shielded the communication link of the UAV, cut off its connection with the ground command and control center, and cut off the data connection with the GNSS satellite, forcing the UAV to enter automatic driving state. Then, they sent navigation spoofing signals and reconstructed the coordinates of the GNSS. By such means, they induced the drone to land in the Tabas desert area of Iran, 140 km away from the U.S. military base, but the drone mistakenly thought it was landing at the U.S. military base designated by the U.S. military.



**The technology behind this attack**

SkyGrabber is a software application designed to intercept satellite signals for personal use. It is commonly used to capture digital satellite television or internet signals, and it can be purchased online for a relatively low cost. The software can be installed on a computer, and with the use of additional hardware, it can intercept and decrypt satellite signals. However, SkyGrabber has also been used for illegal purposes, such as intercepting sensitive military and government communications. In some cases, it has been used by terrorist organizations to monitor and intercept sensitive information. Because of its potential for misuse, some countries have banned the sale and use of SkyGrabber. Also it is not officially reported that SkyGrabber used in RQ-170 attack but in some resources we can find this information.

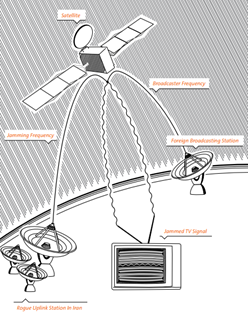




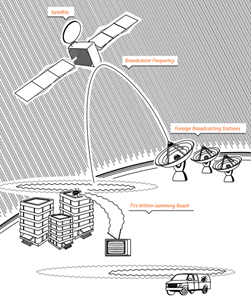
**JAMMING**

When a GNSS tracking device is jammed, most devices report their last known location, rather than raise an alarm. Loss of lock can occur for legitimate reasons such as when a vehicle goes through a tunnel or in heavily built-up areas. In such cases, sending an alarm signal would be more of an annoyance than help as it happens so often. However, this weakness can also be exploited by attackers to falsify the where abouts of a truck carrying valuable cargo, as reported by Economist in 2011 and ABC in 2013. This can have a significant impact on vehicles in the vicinity, including emergency vehicles. Therefore, it is important to have appropriate security measures in place to prevent such attacks. The two forms of satellite jamming are “orbital” and “terrestrial”:

* In orbital jamming, the attacker sends a beam of contradictory signals directly toward a satellite via a rogue uplink station. The jamming signals are mixed with the legitimate signals, thus interfering with them. The jamming signals are able to override the legitimate transmission, blocking its transmission to the recipient.



In terrestrial jamming, the attacker transmits rogue frequencies in the direction of terrestrial targets (ground satellite dishes). Rather than targeting the satellite itself, as is the case in orbital jamming, terrestrial jamming involves transmitting rogue frequencies in the direction of local consumer-level satellite dishes. The jamming frequencies are limited to a specific area and are able to interfere only with the frequency emanating from the satellite in a specific location. Small, portable terrestrial jammers are easy to purchase and use; they typically have a range of 3-5 kilometers in urban areas, while in rural areas their range can increase to up to 20 kilometers.

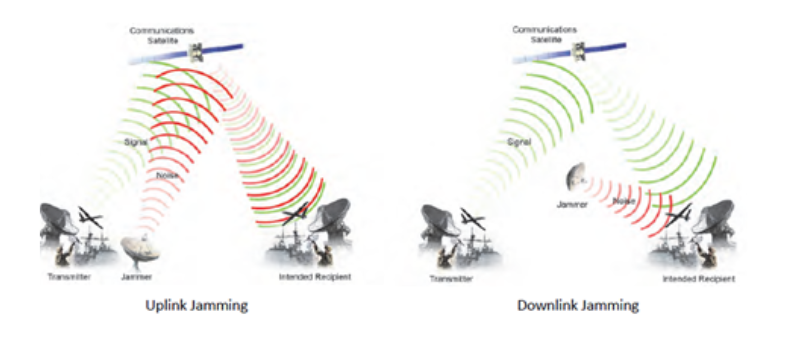


**Uplink Jamming**

Uplink jamming against a payload signal is an attractive electronic attack strategy because all recipients of the target transmission are affected. The jamming uplink signal is a radio frequency (RF) signal of approximately the same frequency as the target uplink signal. It is transmitted up to the satellite onto the same transponder as the target signal and affects the transponder’s ability to distinguish the true signal from the jamming signal. Note that the target uplink source and signal are not affected; the inability of the satellite’s transponder to distinguish between the signals results in a loss of downlink or corrupted downlink. The effectiveness of uplink jamming is extremely dependent on obtaining detailed information on the target signal. This can be done through formal signals intelligence (SIGINT) processes or (in some cases) open-source intelligence (OSINT) research. Once this is gathered and analyzed, the uplink jamming source must be able to acquire the proper satellite and transponder, as well as produce a signal with the correct characteristics andpower necessary to overcome the signal to be jammed. Targets of uplink jammers are the satellites’ radio receivers, including their sensors and command receivers. Uplink jamming is more difficult, since considerable jammer transmitter power is required. However, its effects may be global, since the satellite or space system could be impaired for all users.

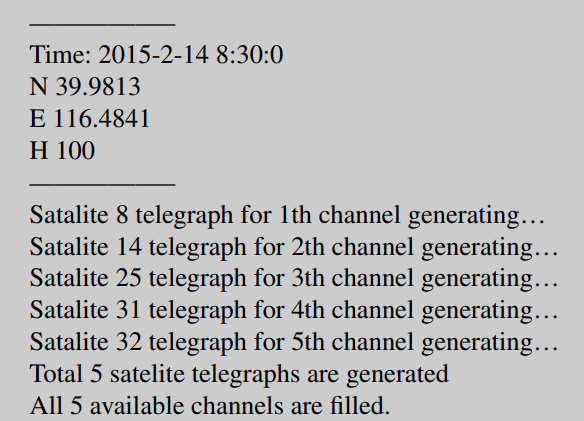
**Downlink Jamming**

There are two main targets for downlink jamming: SATCOM broadcasts and navigation satellite (NAVSAT) broadcasts. In a downlink jamming scenario, the objective of the elctronic attack is to disrupt or temporarily keep the spacecraft’s transmission (communication or navigation signal) from being received by select ground users. A downlink jamming system accomplishes this by broadcasting an RF signal of approximately the same frequency as the targeted downlink signal but with more power. This jamming signal is transmitted toward a terrestrial (ground-based) or airborne satellite downlink reception antenna where it overpowers the satellite’s signal. With smart jamming (vicebruteforce jamming), the jamming signal attempts to emulate the satellite’s signal and, if successful, can provide the targeted user with false data or information. The effectiveness ofdownlink jamming is dependent upon the jammer being able to operate within line of sight (LOS) of the ground site and within the field of view of the ground site’s antenna; effectiveness is also dependent upon the jamming signal being processed by the SATCOM receiver. LOS restrictions can be overcome to a degree by utilizing an airborne platform; the altitude gained by the airborne platform expands the coverage and aids in overcoming ground-based obstacles. It is difficult toassess the effectiveness of downlink jamming as this normally requires monitoring the output ofthe targeted receiver (often not possible). The targets of downlink jammers are ground-based satellite data receivers, ranging from large, fixed ground sites to handheld GPS user sets. Downlink jamming only requires a very low-power jammer, though its effects are local (from tens to hundreds of miles, depending on the power ofboth the jammer and downlink signal). Since downlink telemetry contains the mission informationand health and status information, successfully attacking the downlink directly attacks informationflow and, therefore, has a more immediate effect on denying or disrupting the satellite’s mission Sophisticated technologies for jamming satellite signals are emerging.



**An experience of spoofing**

BladeRF and GPS-SDR-SIM are GPS SDR applications that can be used to generate GPS signals for testing and research purposes. By using these tools, researchers can send out fake GPS data which generated from Matlab. In this example we have specified geographical location: latitude 39.9813, longitude 116.4841, and altitude 100 m. PRN: 8, 14, 25, 31 and 32 are part of the signals of 5 satellites. With this basic process we can distort the location and time information of the devices.



Various experiments have been conducted using different devices, such as phones, cars, dual-mode positioning chips, drones, and others, to test the accuracy and effectiveness of these tools. For example, experiments have shown that a car parked in a parking lot in China can be made to appear as if it is in the middle of an ocean in another country. Similarly, drones can be made to appear as if they are flying in restricted areas where they are actually not allowed to fly.

These experiments demonstrate the potential for GPS spoofing attacks, where false GPS signals are generated to deceive GPS receivers and manipulate their behavior. It highlights the need for improved GPS signal authentication and security measures to prevent such attacks from occurring.

**COUNTERMEASURES**

6.1. Signal processing based defenses

There are several stages to signal processing by a digital GNSS receiver before the navigation and time solutions can be computed. The incoming analog RF signal from the antenna is ﬁrst ampliﬁed, then down-converted toa lower frequency, and its signal strength adjusted via AGC (automatic gain control). After digital conversion, a replica PRN code, plus the computed Doppler shift (caused by the relative motion of the receiver and the satellite vehicle), is used to separate the individual satellite signals. The digital data of the individual channels, including their in-phase (I) and quadrature (Q) components is then available for computing the navigation and time solutions. As discussed in the following sections, at various stages in this process it is possible to monitor the acquisition and tracking of signals for anomalies that may indicate a spooﬁng attack is in progress. These approaches differ from cryptographic and physical defences, in that they do not require physical modiﬁcations to existing equipment or signal protocols, but only the updating of the device ﬁrmware.

6.1.1. RAIM

Receiver autonomous integrity monitoring (RAIM) is the oldest and mostwidely used anti-spooﬁng strategy in GNSS receivers. This checks all available GNSS signals for spatial consistency, and can exclude aberrant satellites. For example, the ephemeris data predicts the location of satellites in advance, and should closely agree with their reported positionin the navigation message and external sources. In the case of au-thentic signals, the frequency changes due to the Doppler effect, and the PRN codeis delayed to maintain signal lock. A low quality spoofer might not be able to keepthis correlation. Another RAIM-like check is for clockconsistency between times of other satellites not currently being tracked. The basic weakness of RAIM is that it assumes any spooﬁng attack will be conﬁned to one or two aberrant satellites, not an entire constellation. The owner of a timer also has no detailed knowledge of which sanity checks are performed, and hence cannot assess the degree of protection they provide.

6.1.2. Absolute Power.

Absolute power monitoring involves monitoring the received signal strength (RSS) versus expected signal levels. Some researchers argues that using absolute power level rather than SNR considerably reduces receiver vulnerability to spooﬁng. However, signal levels vary due to atmospheric and solar interference. They may also be changed by the AGC in the receiver (unless the changes are detected in the AGC controller itself), and only moderately increased signals levels of +1-2dB are required to executea “lift”. Also, the risk of false alarms would be a serious problem for this technique, which would be therefore limited to detecting only highly elevated signals.

6.1.3. Doppler shift detection. Due to satellites’ high orbital speeds relative to a receiver, the Doppler effect: the shortening of wavelengths when moving towards, or lengthening when moving away, induces detectable effects in the received frequency of GNSS signals. These effects are normally corrected for in the receiver, and vary in a predictable way for each satellite. Hence a defence based on detecting anomalies in Doppler shift between real and simulated constellations, might be an effective spooﬁng detection technique. In the Volpe report [Volpe 2001] detection of such anomalies was listed as a defence, but it was also observed that simulators regularly provide controlover Doppler shift. However, such simulation might leave tell-tale traces that could beused as the basis for detection, even in the case of a sophisticated spoofer. There are identiﬁed two kinds of Doppler simulation: consistent Doppler attacks, where the spoofer keeps the code delay rate and frequency consistent with one another, and attack where the spoofer locks the Doppler frequency of the spooﬁng signal to that of the authentic signal. Both scenarios, however, leave strong traces of an attack such as ﬂuctuation in signal strength caused by interactions between the spoofed and authentic signals. This form of signal analysis, therefore, already tested in the laboratory by seeral researchers, seems one of the most promising detection techniques.

6.1.4. Correlation Peak Monitoring. Cavaleri investigated the feasibility of using this tech-nique as a means of spooﬁng detection. Under the name “vestigal signal defense” (VSD) it has also been evaluated. How-ever, authentic GNSS signals frequently suffer from multipath signals reﬂected offbuildings in a similar way to spoofed signals.

**Digital signatures**

Digital signatures can be used to add a layer of security to GPS transmissions and prevent spoofing attacks. In fact, the current GPS system already uses a form of digital signatures called the "Public Key Infrastructure" (PKI) to authenticate the signals from GPS satellites.

The extensible ephemeris messages (EEMs) that are transmitted by GPS satellites contain information about the satellite's orbit and clock corrections, which are used by GPS receivers to calculate their own positions. By adding digital signatures to these messages, it would be possible to verify that the messages are authentic and have not been tampered with by a spoofing attacker.

However, implementing digital signatures on a large scale would require significant changes to the current GPS infrastructure, including updates to both the GPS satellites and receivers. Additionally, digital signatures are not foolproof and can also be susceptible to attacks if the private key used for signing the messages is compromised. Therefore, a combination of different security measures would be necessary to effectively prevent spoofing attacks.

**Multi-mode Chips**

The normal positioning process is carried out by receiving signals from 4 satellites and calculating the intersection points of these signals. A multi-mode positioning device can perform position calculation by using signals from different satellite systems (GPS, Galileo, Beidou, etc.). When the positioning chip is multi-mode, we can determine the position by combining other systems supported by the chip in order to avoid fragility of single-mode positioning. Although it does not provide full protection against spoofing attacks alone, a multi-mode positioning chip is one of the measures that can be taken.

REFERENCES:

Dessiatnikoff, A., Deswarte, Y., Alata, E., & Nicomette, V. (2012). Potential Attacks on Onboard Aerospace Systems. IEEE Security & Privacy, 10(4), 71–74. doi:10.1109/msp.2012.104

Tedeschi, P., Sciancalepore, S., & Di Pietro, R. (2022). Satellite-based communications security: A survey of threats, solutions, and research challenges. *Computer Networks*, 109246.

Meng, L., Yang, L., Yang, W., & Zhang, L. (2022). A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sensing*, *14*(19), 4826.

Bardin, J. (2013). Satellite cyber attack search and destroy. In *Computer and Information Security Handbook* (pp. 1173-1181). Morgan Kaufmann.

Yang, Q., & Huang, L. (2018). *Inside Radio: An Attack and Defense Guide* (pp. 1-369). Springer.

Schmidt, D., Radke, K., Camtepe, S., Foo, E., & Ren, M. (2016). A survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Computing Surveys (CSUR)*, *48*(4), 1-31.

Kodheli, O., Lagunas, E., Maturo, N., Sharma, S. K., Shankar, B., Montoya, J. F. M., ... & Goussetis, G. (2020). Satellite communications in the new space era: A survey and future challenges. *IEEE Communications Surveys & Tutorials*, *23*(1), 70-109.

Santamarta, R. (2018). *Last call for SATCOM security*. Seattle, WA: IOActive.

|  |
| --- |
|  |

Santamarta, R. (2014). A wake-up call for satcom security. *Technical White Paper*.

Shuli, D., Taotao, Z., & Min, L. (2019, May). A GNSS Anti-Spoofing Technology Based on Power Detection. In *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)* (pp. 1134-1137). IEEE.

Lohani, S., & Joshi, R. (2020, February). Satellite network security. In *2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3)* (pp. 1-5). IEEE.

Zidan, J., Adegoke, E. I., Kampert, E., Birrell, S. A., Ford, C. R., & Higgins, M. D. (2020). GNSS vulnerabilities and existing solutions: A review of the literature. *IEEE Access*, *9*, 153960-153976.

Hudaib, A. A. Z. (2016). Satellite network hacking & security analysis. *International Journal of Computer Science and Security (IJCSS)*, *10*(1), 8.