17th International Conference on Space Operations, Dubai, United Arab Emirates, 6 - 10 March 2023.

SpaceOps-2023, ID # 96

The information and communication architecture in the lunar orbit

Jamel Metmati

[a] *Department of Cyber : djamel.metmati@thalesgroup.com*

Abstract

The missions to the Moon increase the assets number on the lunar orbit. It includes the spacecrafts, the satellites, the futur Space station, the robots already on the surface. This context needs to understand the key parameters to built the permanent network covering the missions cycles to the Moon. It concerns the Artemis mission and the first telecommunication satellites applied to lunar orbit. The purpose being to manage data with a stable network between the Moon and the Earth orbit and the ground segment at its surface. Anticipated by the LunaNet, the architecture shall take account the cybersecurity requirements applicable through the specificity of the transmission from the context of the vacuum at long distance to ground stations on Earth. The Apollo missions demonstrated the capacity to emit and to receive data from the Moon. The Lunar Gateway and the satellites like Lunar reconnaissance orbiter or Cislunar High patrol System introduce new aspect of telecommunication outer the terrestrial orbit. Indeed, the Space assets on the Moon create the condition of an IoT concept in which the information system should fuse from different means and technologies with the capacity to monitor them. By the way, the understanding of the matter information theory provides the methodology to design, to built and to run the elements of this architecture with the new requirements linked with the human presence on the Moon

Keywords: Moon, information, communication, orbit

1. Introduction

The objectives of this work is to provide the features of the Moon information and communication system including a different design thinking.

2. Methods

The methodology is to describe the networks applicable in Space with the requirements of human presence with the activity.

3. Results

3.1 The Space of Things in Space networks

The Space incident response require the processing to support the work of the assets supporting on the Moon. And The interfaces already in Space need also a gateway to communicate with Earth. It means the safety and security operating center on Earth shall operate the fusion networks applying with a signal management taken account the equipments, the signal itself, the flags identified to manage the data transmission. Three level should be taken account the ground segment activities, the Space activities, the Moon activities.

The signal management [1] is known as Space exploration done on Mars with the probes on the ground. This through the Deep Space Networks and the fusion networks including IoT protocol, data relay satellite on Orbit and the connection to the Earth by the DSP antennas. Except in the Moon context, the model of IoT thanks to assets on orbit introduce the Space incident organisation on orbit. Even more for the Moon where the orbit is not the same as Mars. It means the trajectory of assets on the Moon orbits needs correction or else any objects is going down on the surface.

The connection with the information and communication on orbit should need to be thinking with the Space Object Things concept understanding the requirement of the missions. The parameters shall be taken account for these objects should include the functions from the safety and security operating center : the identification and access management, Bot Agent to control the workflow of the system and the data for the command and control, the signal management in the context of vacuum. This last parameter defines the capacity to manage optic signal [2] with classic radio frequency, the workflow to be sent on Earth through the atmosphere.

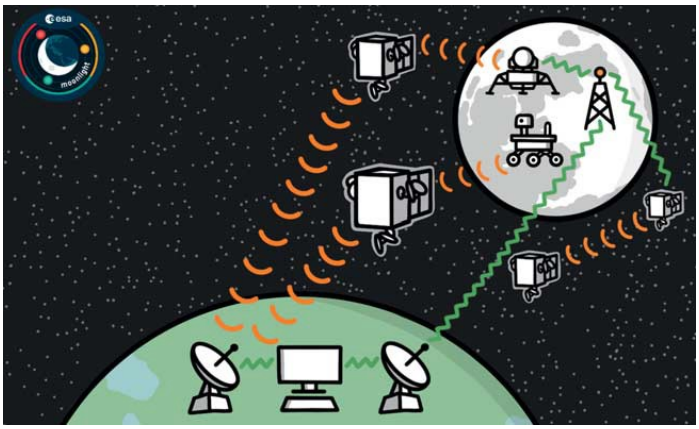

Figure 1 : Telecommunication on Moon Orbit

In these network monitoring missions, the characteristics of the ground segment include a novel and complex incident response. However, the main points can be seen from the point of view of the current operation of the control centres of navigation systems or ground observatories.
The case of the Entoto observatory [3] demonstrates how LunaNet could fit into this signal supervision posture. The optical telescope of this observatory is connected to a command and control unit based on a navigation system. This same unit is connected to several interfaces based on a client-server relationship to users, external entities and a data-center for the backup link. The dome, the telescope, and the weather station rely on this client-server relationship through a software interface.
The network must ensure the continuity of the system to fulfil the functions of the following segments: user interface for monitoring and tracking, for the data management system, for the telescope, for the control and command module. While these separate services are interdependent, they share the same architecture for the optical sensors, the active network elements and the software process. In the event that this process is no longer available, the Kenyan space agency would lose the ability to connect to the LunaNet segment.

3.2 The safety and the security in Space
The chain of transmissions to the Moon therefore requires a novel application of operational cyber security concepts. This is especially true given that security is linked to the widespread introduction of digital techniques in the operation of spacecraft and telecommunications. This space cybersecurity [4] has two components. The first part concerns the way in which it is applied by crews in orbit or on the lunar surface. The second part deals with securing the signal between the Moon and Earth to provide warning and telemetry services for the ground segment. The first point is the properties of cyberspace to be considered. Signal transmission and reception passes through several media in the C and K bands: the ether, the atmosphere, the Earth's electromagnetic field, the relative vacuum of space, gravitation and space weather.
In addition, other Telecom deployment conditions are emerging in the space telecommunications architecture. The Starlink broadband Internet service, which, from 600 active satellites in low orbit for a target of 42,000, with a launch authorisation for 12,000 satellites in 2020, a test transmission reaching a downstream/upstream rate of 60.24 Mbits/s and 17.64 Mbits/s for an announced latency of 20ms, demonstrates an unprecedented network for transmission security constraints: taking into account roaming, the movement of the satellite with the receiving terminal, laser synchronisation between satellites, terrestrial routing with ground stations, inter-satellite routing, The terminal's 0.48-metre antenna rod may be subject to jamming and man-of-the-middle attacks. The second point concerns the vulnerability of the transport layer during the transmission and reception of the signal between the orbital objects and the ground stations.
The comand and control systems are based on known input and output protocols and schemes: Internet interface, shell, UDP, TCP, Wireshark. In addition, there is Red Team and Green Team hardware: DVB card, decoder, satellite dish. The analysis of IP datagrams and UDP datagrams shows multiple fields that can be summarised as IDs, type of encryption, satellite orbit, frequency, polarisation, synchronisation. The 3D visualization models then allow to work on the time cycles of the satellite in orbit to better connect. The use of the "US catalog of

space objects" completes the analysis by providing the satellite's orbital data. The widespread provision of business-critical services via space networks also encourages on-board space cybersecurity [5].
It describes the digital systems on board shuttles, modules, launchers and satellites, which are the most numerous. There are few cybersecurity standards applied to satellites. They have a launch mass, altitude control, solar panels for electrical power, an orbit with periods, an inclination, an antenna mast, on-board instruments.
And to master the processes of automatic execution of the tasks requested by the ground station or the crews, each command must respond to an identified action for which an on-board computer or electronic circuits perform calculations. During the last Hack-a-Sat organised in 2020 by the Air Force and the Digital Defense Service, control of the tracker mechanism made it possible to change the orientation of the test satellite and take pictures of the Moon. Just as in 1998 when the ROSAT had its solar panels changed orientation towards the sun. Other similar cases took place during the 2000s. It also deals with the man-machine interface, where cognitive safety enables the correct interpretation of terminal data to be carried out on the ground or in space.
During the Apollo 11 mission, alarm codes from the on-board computer appeared during the final descent of the lunar module, and the astronauts' radio report mentioned an alarm that only the ground station could interpret. The astronauts, being in their positions, were under the tunnel effect of the landing pilot. These were alarms 1201 and 1202, which Jack Garman, computer engineer, and Steves Bales, navigation officer, had encountered during simulations. The alarms were due to a problem with the landing radar calculation cycle and the throttle control algorithm. And the computer's 72 KB of memory was having difficulty processing the amount of commands coming in. This event shows the Space operations should be managed at distance with a constant link with the teams in Space and on the ground with in addition teams able to maintain the stability of complex networks. The LunaNet, marking the first inter-planetary network, integrates known issues into a new operational deployment context that includes applying cybersecurity principles in space too.

4. Discussion

4.1 The Moon design networks

LunaNet is defined as a telecommunications network capable of supporting human exploration and scientific missions to the Moon. The first building blocks of the telecommunications system will be nodes for lunar deployment and the first permanent installations. The features of this network combine a set of interoperable systems with government and commercial partners. And the aim of the system is to support the Artemis III, Artemis IV and commercial missions involved in the IOC and EOC phase.
The structure of the LunaNet network is a first in human space exploration as it lays the foundation for interplanetary communications for the presence of human civilisation outside Earth. The LunaNet design encompasses all systems providing time, navigation, and communications services to users around the Moon and to Earth. In other words, the network equipment will be located both in lunar orbit and on the surface of the Moon. For the lunar segment, a specific chain is envisaged for which an interface could be implemented to the ground segments of the Earth.
A relay system between the two segments is being studied in which the exchane cinfiguration would be based on a private link. To establish the link between the two segments, the LunaNet will be built through a combination of LunaNet access providers who will themselves be service providers. The interfaces between the segments can be divided into several categories. The first includes the physical interfaces and protocols between a user and a provider. The second concerns the interfaces between different access providers.
The declination of interfaces is then divided into a series of connections involving typologies of interfaces: linkage between the lunar and terrestrial system, linkage between lunar surface users, linkage between surface users and those in lunar and terrestrial orbit, linkage between service providers according to linkage use cases. Permanent data transmission is achieved through a communication in space and a link from the lunar ground. Users will be able to establish communications through these two channels according to known standards and protocols. Thus, the Internet protocol could join the Bundle protocol in the Consultative Committee on Space Data Standards, the Advanced Orbiting Systems, and the IETF.
This Space Internet is based on three space telecommunication characteristics: real time, time shifting, and service messages. The applications supporting this transmission chain are related to alerts, position navigation times and service acquisition. Thus, the LunaSAR service corresponds to the Search and Rescue signal of the navigation satellite constellations in Earth orbit. This service offers the ability to monitor the distress signal from any equipment and infrastructure on the Moon. Other services include space weather monitoring and the use of optical and radio links for measurement missions from Earth.

4.2 Support the Moon activity

Together this creates an inter-planetary architecture in which Earth-Moon telecommunication use X, Ka, or optical bands to connect to relay nodes inlunar orbit. These nodes, connected to each other with a complementary band[5] communicate with spacecraft in lunar orbit and entities on the surface of the Moon. The existing ground stations will transmit and receive the lunar signal from the constellation of navigation satellites.

This means that terrestrial infrastructures will have to be able to supervise and monitor the state of the network by taking into account new parameters. These include the ability to manage integrated architectures with different systems and protocols, to understand the effect of the space environment on signal processing, to ensure signal availability within acceptable performance times for crews in orbit and on the lunar surface.

The design of the networks to the Moon out from radio communication as known in the Apollo Mission supports the future activities on its surface. The primary topics could be to perform humans and robots at sites across the Moon, to deploy and operate a global network connected with Earth, to deploy and operate a global network of space small stations, to measure biological and physiological effects of the lunar environment, to prepare, to search Helium 3 resources, demonstrating production of oxygen as done for Mars.

It shall added the capacity to ensure the communication test beds on the Moon surface and the building of small modules to be able to stay couples of days with the use of solar panel on the surface. The design of the networks should provide the way to send and to receive data from Earth.

The datasets [6] shall be useful for the primary components on the Moon surface. Moreover, it will give the support to monitor on remote the assets in case of failure or damage. The last point is also the means to provide a backup communication solution to ensure the safety and the security of the missions. Others purpose could be useful thanks to the design of these networks. The antenna field with the architecture is a potential tool of detection against the astroid detection. The quantum antenna being the capacity to detect the electromagntic field of the Earth should be able to record the unexpected particles move in the vacuum. The overview of the design can be illustrated by th Lunar Pathfinder. It will be launched by NASA in 2024, using the Commercial Lunar Payload Service (CLPS) programme. With a store and forward architecture, a proximity link allowing for two simultaneous links with lunar missions in S-band and UHF, and backup link to Earth in X-band, a data-relay satellite will be able to solve both direct line of sight and performance limitation due to distance between the Earth and the Moon. In addition, an ESA GNSS receiver capable of detecting weak signals coming from the Earth GNSS infrastructure (GPS and Galileo) will be hosted onboard Lunar Pathfinder, demonstrating GNSS's potential role in Lunar navigation and other services applicable for the activities on the Moon.

Conclusion :

The information and communication architect for the lunar orbit is close to the one used for Mars. The purpose engaged for permanent presence on the Moon changes the requirements of the architecture applying the means to manage through the infrastructurres all specific aspects in the fusion networks. This through Space of Things on orbit able to get the functionalities of safety and security operating center or able to be connected with the same infrastructure on Earth.

References

Reference to a journal publication:

[1] M. P. Howarth et al. "Dynamics of Key Management in Secure Satellite Multicast". In: *IEEE Journal on Selected Areas in Communications* 22.2 (Feb.2004), pp. 308–319.

[2] Hengqing Wen et al. "Countermeasures for GPS Signal Spoofing".
In: *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*. International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS). Long Beach, CA, 2005, pp. 1285–1290. url: https://www.ion.org/publications/abstract.cfm?articleID=6325.

Reference to a conference/congress paper:

[3] Ackermann, M. R., et al. (2015). A Systematic Examination of Ground-Based and Space-Based Approaches to Optical Detection and Tracking of Satellites. 31st Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America.

[4] Julio Vivero and Luca del Monte. "Space Missions Cybersecurity". In: *AIAA SpaceOps 2014*. SpaceOps 2014 Conference. 2014, p. 1765.

[5] Robert Lemos. "Satellite Control Codes Stolen by Hackers". In: *ZDnet* (Mar. 7, 2001). url: https://www.zdnet.com/article/satellite-control-codesstolen-by-hackers/ (visited on 02/07/2019).

[6] H. Cruickshank et al. "Securing Multicast in DVB-RCS Satellite Systems". In: *IEEE Wireless Communications* 12.5 (Oct. 2005), pp. 38–45.