Encryption

Eva María Urbano González

October 8, 2016

Chapter 1

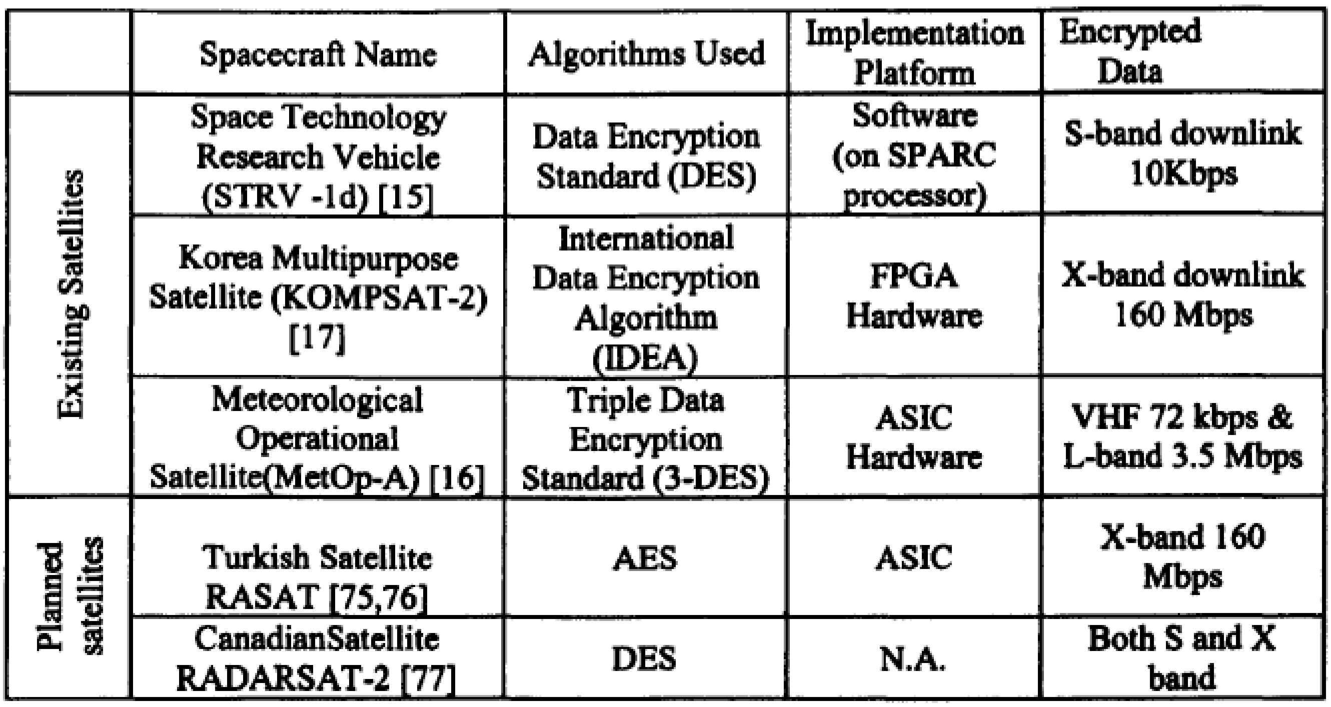
Encryption

1.1 Is encryption necessary in satellites?

In the light of latest intrusions into satellite data the demand to protect the sensitive and valuable data transmitted from satellites to ground has increase and hence the need to use encryption on-board [?]. Currently, only few satellites are equipped with on-board encryption to protect the data transmitted to ground satation, but more and more organizations are planning to have on-board encryption as a security mesure.

1.2 Satellite On-Board Encryption

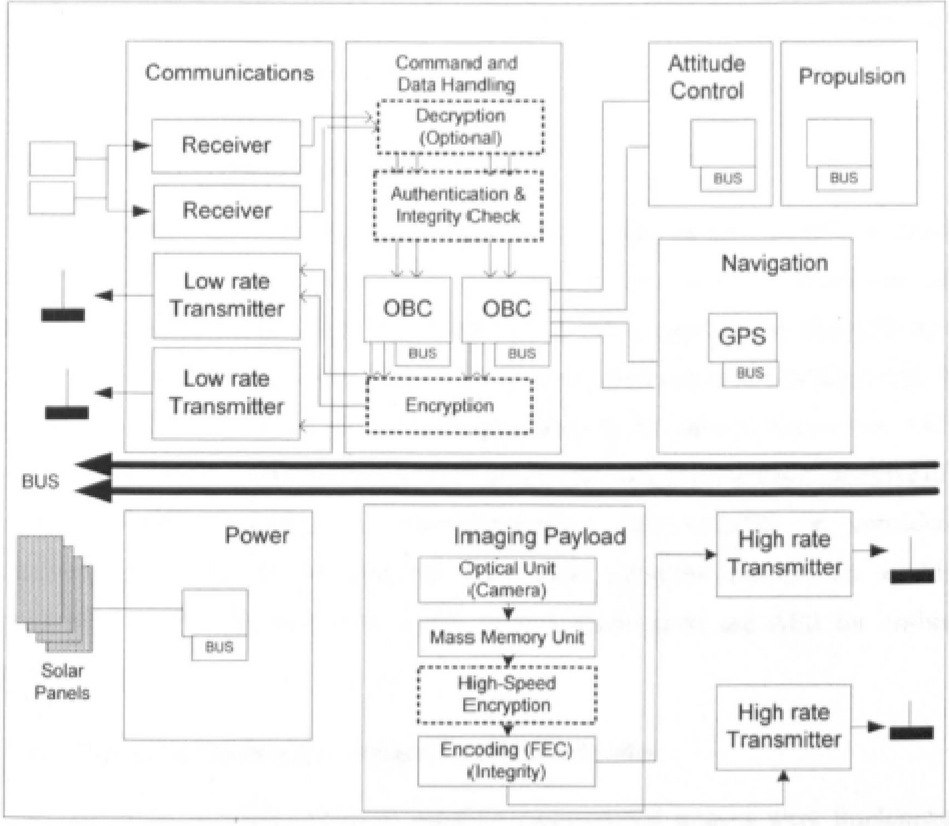
Due to limited computational resources on-board, the encryption technology used in spacecrafts is very different that the one used in terrestrial systems. In the following table we can see a brief description of each of the existing planned satellites with encryption on-board.



	Spacecraft Name	Algorithms Used	Implementation Platform	Encrypted Data
Existing Satellites	Space Technology Research Vehicle (STRV -1d) [15]	Data Encryption Standard (DES)	Software (on SPARC processor)	S-band downlink 10Kbps
	Korea Multipurpose Satellite (KOMPSAT-2) [17]	International Data Encryption Algorithm (IDEA)	FPGA Hardware	X-band downlink 160 Mbps
	Meteorological Operational Satellite(MetOp-A) [16]	Triple Data Encryption Standard (3-DES)	ASIC Hardware	VHF 72 kbps & L-band 3.5 Mbps
Planned satellites	Turkish Satellite RASAT [75,76]	AES	ASIC	X-band 160 Mbps
	CanadianSatellite RADARSAT-2 [77]	DES	N.A.	Both S and X band

1.3 Security services for Uplink Commands

The uplink or telecommand should **always** be checked for integrity and authentication in order to protect the satellite from being taken over by unauthorized people. There must exist and authentication and integrity block which provides protection to the satellite by ensuring that the on-board data handling system receive unmodified telecommands from authorized ground station. Data authentication is usually achieved by appending an extra unit of information to the original message (the digital signature). The digital signature identifies the origin of the data. Many digital signature generation mechanisms require the use of an asymmetric cryptographic algorithm where senter and receiver do not hold the same cryptographic keys. An integrity service is used to ensure that unauthorized users have not manipulated the data in any way. Integrity of data is achieved by appending an Integrity Check Value (ICV) to the data structure in a manner similar to the way a digital signature is appended, but in this case thee ICV is always a function of the data itself. All these telecommands may also be encrypted by ground station depending on the level of security required. Here we can see an example of a block diagram of the the on-board security architecture. In this case the satellite is an small EO satellite.



1.4 Security services for downlink data

This information is related with satellite health, control information (AOCS), temperature, etc.

1.5 Encryption of Payload information

The usual algorithms to use is AES. The most popular modes of AES are: ECB, CBC, OFB, CFB, CTR. They are carried out using a purpose-build software simulator developed in JAVA.