Securing the Space Link
a Crucial Component of Space
Mission Security Architecture

I. Aguilar Sánchez
Laurel, MD
11/06/2013
Outline

- Introduction: Securing Space Missions
- Data Link Layer Security
- Physical Layer
- Conclusions and Follow-on
- Acknowledgements
- References
INTRODUCTION

SECURING SPACE MISSIONS
Two security problems are identified and differentiated when considering how to secure a space mission.

- The first one concerns the protection of the space mission assets and their infrastructure, e.g., the satellite or the constellation when more than one satellite is involved, the ground stations, the operations control centre(s), the mission control centre(s), the networks that interconnect them and the interface with the user(s).

- The second security problem corresponds to the protection of the mission products, that is, the signals and/or data produced by the spacecraft.
CIA Requirements

Confidentiality needed for:
1. Key protection while cryptographic key uploading (TC);
2. Protection Sensitive parameter of security unit in TM, if any;
3. Telecommand protection (optional).

Integrity/Authentication needed for:
1. Transmission error protection;
2. Anti-spoofing/Command source authorization;
3. Complement to Encryption (optional).

Availability needed for:
1. Protection of Telecommand transmission (spread spectrum, null-steering antennas, high-power up-link).
Space asset protection

- Main Threats:
  - Unauthorized access to spacecraft control;
  - Denial-of-service on command link;
  - Traffic analysis.

- Specific mission risk assessment will dictate the adoption of Protection measures like:
  - Command authentication;
  - Command and telemetry encryption;
  - Anti-jam techniques (e.g. cryptographic spread spectrum, antenna null-steering);
  - Spacecraft autonomy, ground station diversity.
Mission products protection

- **Main Threats:**
  - Unauthorized access to mission data or mission signal on space link;
  - Unauthorized access to mission processed data at payload data ground segment.

- **Protection measures:**
  - Mission data encryption on space link; decryption keys distributed to authorized users;
  - User identification, authentication, access control, encryption when interacting with payload data ground segment for mission processed data.
Spacecraft end-to-end security (1)
Single space link topology
Spacecraft end-to-end security (2)
Separate payload link topology
DATA LINK LAYER
SECURITY
At the **Data Link Layer** the following two features can be addressed:

**Confidentiality** needed for:
1. Key protection while cryptographic key uploading (TC);
2. Protection Sensitive parameter of security unit in TM, if any;
3. Telecommand protection (optional).

**Integrity/Authentication** needed for:
1. Transmission error protection;
2. Anti-spoofing/Command source authorization;
3. Complement to Encryption (optional).
Experience in previous and ongoing ESA projects has benefited ESA contribution to CCSDS SDLS. Following projects can be mentioned:

- Automated Transfer Vehicle
  - Telecommand Segment Encryption (3-DES CFB)
- Global Monitoring for the Environment and Security (GMES) Sentinel-1, -2 and -3 satellites
  - Telecommand Segment Authentication (AES CMAC)
  - Authentication Key Encryption (OTAR)
ESA precedents (2)

- Telecommunication Missions Telecommand protection
  - Thales Alenia Space (AES)
  - Astrium (AES)
- SEOSAT (Spanish Earth Observation satellite)
  - Telecommand Authentication/Encryption
  - Housekeeping Telemetry Encryption
  - Payload Telemetry Encryption
- EUMETSAT Meteosat Third Generation (MTG)
  - Telecommand Authentication
  - Payload Telemetry Encryption
Cryptography

➤ Security primitives and corresponding Cryptographic algorithms are at the core of data security services. ESA approach is the following:

qn Civilian Space Missions,

▪ Promote and adopt relevant international standards (e.g. ISO, NIST, CCSDS).
  ➥ AES in its various modes for Authentication (CMAC), Encryption (CTR) and Authenticated Encryption (GCM).

▪ Study adaptation and particulars of the space mission context (e.g. protocols, intermittent communications, safety).

qn Institutional Missions,

▪ Driven by ESA Security Regulations;
▪ European National Security Authorities.
CCSDS Security effort: Data link security

1. Several reports and standards like
   a. The Application of CCSDS Protocols to Secure Systems;
   b. Cryptographic Algorithms;

2. Space Data Link Security (SDLS) protocol.
   This security protocol offers
   a. security services to the three Space Data Link protocols previously standardized by CCSDS;
   b. security services: authentication, encryption and authenticated encryption;
   c. flexibility in the selection of services and cryptographic algorithms.
   d. ‘Baseline modes’ in SDLS and their companion cryptographic algorithms as recommend in another key CCSDS standard on security: Cryptographic Algorithms.
Security objectives not covered by SDLS:

- protection against denial of service,
  - can be dealt with by TRANSEC methods (physical layer security).

- protection against traffic analysis,
  - typically not required for civilian missions.
## CCSDS SDLS

### Protected SLP Services

<table>
<thead>
<tr>
<th>User Services</th>
<th>Type of Service Data Unit</th>
<th>Protection by SDLS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TC Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple Access Point (MAP) Packet</td>
<td>Packets with authorized Packet Version Number (PVN)</td>
<td>Protected</td>
</tr>
<tr>
<td>MAP Access</td>
<td>Variable-length private data</td>
<td>Protected</td>
</tr>
<tr>
<td>Virtual Channel (VC) Packet</td>
<td>Packets with authorized PVN</td>
<td>Protected</td>
</tr>
<tr>
<td>VC Access</td>
<td>Variable-length private data</td>
<td>Protected</td>
</tr>
<tr>
<td><strong>TM Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet</td>
<td>Packets with authorized PVN</td>
<td>Protected</td>
</tr>
<tr>
<td>VCA</td>
<td>Variable-length private data</td>
<td>Protected</td>
</tr>
<tr>
<td><strong>AOS Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet</td>
<td>Packets with authorized PVN</td>
<td>Protected</td>
</tr>
<tr>
<td>VCA</td>
<td>Variable-length private data</td>
<td>Protected</td>
</tr>
<tr>
<td>Bitstream</td>
<td>Bitstream</td>
<td>Protected</td>
</tr>
<tr>
<td>Insert</td>
<td>Short fixed-length data</td>
<td>Not Protected</td>
</tr>
</tbody>
</table>
**SDLS Requirements**

- Two operational modes: Clear and Secure
- Coexistence of clear and secure logical channels on a physical channel
  - Secure logical channel being a set of VCs (TM/AOS) or MAPs (TC)
- Compatible with following Key Management schemes:
  - Scheme 1: all session keys pre-loaded before launch
  - Scheme 2: both pre-loaded and in-flight up-loaded keys (OTAR)
  - Scheme 3: both preloaded and on-board generated keys
- Command and monitoring support:
  - TC security control directives managed either:
    - as in-band commands (interpreted and executed internally by the on-board security processor)
    - or as out-of-band commands (executed at application level)
- Protocol overhead strictly limited: 32 octets max / frame
SDLS Key drivers (1/2)

- Compatibility with CCSDS SDL protocols (TM, TC and AOS)
  - No impact on data structures or protocol operation;
  - Minimum impact due to integration of security protocol in existing TM/TC data handling (ground, on-board).

- Compatibility with Space Link Extension (SLE) Services (F-CLTU, F-TCF, RAF, RCF)
  - SDLS protocol should be invisible for SLE services processing.
    - All transfer frame headers and trailers should be readable.

- Flexibility
  - Security services selectable in accordance to mission needs (risk assessment and security policy)

- Independence from cryptographic algorithms
  - Preference for standard algorithms as recommended by CCSDS but
  - Switching to new algorithm to cater for obsolescence,
  - Possibility to implement ad-hoc algorithms (operator specific).
SDLS Key drivers (2/2)

- Interoperability (CCSDS main goal)
  - should support cross-support scenarios like:
    - Outsourced secure LEOP operations,
    - Agency A satellite operated by agency B (typical of international cooperation).

- Decoupling of SDL and SDLS data integrity performance
  - should allow for easy distinction and identification of the nature of errors
    - Non-intentional transmission errors (detected and dealt with by SDL protocol);
    - Intentional security errors (detected and dealt with by SDLS protocol).
  - needed for correct operation of S/C FDIR and TC COP
SDLS Protocol design: Security Associations

- **Concept**
  - borrowed from IPSec but notably simplified for TM/TC space links;
  - defines a simplex (one-way) stateful cryptographic session between the sending and receiving ends:
    - includes cryptographic parameters to be used for the session (e.g.: key, security service: authentication, encryption, authenticated encryption),
    - maintains state information for the duration of the session (e.g.: anti-replay counter).

- **Operation**
  - sender and receiver must create an SA, associate it with key(s) and activate it before transferring securely frames over the space link,
    - SA may be pre-loaded before launch or created dynamically as needed.
  - all Transfer Frames sharing the same SA constitute a Secure Channel,
    - a secure Channel consists of one or more Virtual Channel (VC) or Multiplex Access Points (MAP).
  - the Security Parameter Index (SPI) is an in-line transmitted value that uniquely identifies the SA applicable to a Transfer Frame.
SDLS Protocol Data Structures

Security header

Encryption done on Frame Data Only

MAC computed over TF headers, Security Header and Frame Data

Security trailer (MAC)
(computed over full transfer frame minus OCF, ECF and masked subfields of TF headers)
SDLS Baseline Implementation Modes

- To promote multi-mission implementations:
  - 3 recommended profiles have been defined covering security requirements of most missions w.r.t. TC, TM and AOS links

- Baseline mode for TC
  - **Authentication only**, using AES/CMAC, 128-bit key, 32-bit ARC, 128-bit MAC (22-octet overhead (8%))

- Baseline mode for TM and AOS
  - **Authenticated encryption**, using AES/GCM, 128-bit key, 96-bit initialization vector, no seq. # needed, 128-bit MAC (30-octet overhead (2.5%))
The SDLS functions are shown both at sending and receiving ends. They are tightly coupled to the Virtual Channel Generation and Reception functions. However, they are placed outside the COP-1 loop/procedures (FOP-1 on sending end, FARM-1 on receiving end).
Symmetric Key Infrastructure (1/2)

- Key management (KM) is described in several documents (CCSDS, NIST, etc.). However, there is a lack of literature on KM tailored for space-missions,
  - Crucial parameters such as key length and cryptoperiod are usually not specified.

- Particularities of space systems:
  - High reliability, long communication delays, integrity of cryptographic material and processing, “Keep it simple” rule.

- Some ESA missions have gone through parameters definition (e.g. GMES Sentinels).
  - Further scientific substantiation for current approaches
  - How would the threats progress?

- ESA and University of Waterloo (Canada) are working together to tackle the following objectives:
  - Optimize the design and implementation of security functions for space missions by focusing on sound cryptographic key management;
  - Evaluate higher levels of spacecraft autonomy which can provide temporary operational independence from ground-based Certificate Authorities and Trust Authorities. This may be necessary in specific contingency situations where interactive ground communications for key establishment may not be available.
Symmetric Key Infrastructure (2/2)
Key results of first phase & follow-on

- Minimal security for a 20-year mission: **115 bits** (given the assumptions on attacker’s capabilities taken for the study).

- Worst case authentication cryptoperiod (TM PL, CER=10-6):
  - LEO: 9 hours
  - GEO: 59 mins

- Proposed models flexible enough to support different mission and communication scenarios, advances in cryptanalysis, and computational power availability.

- Second phase draft final report recently received and under evaluation.
  - Focus on space networks key management and
  - Use of trusted recovery modules.
Data Link Layer Security
Follow-on

- CCSDS SDLS
  - Validation of Core protocol;
  - Extended Procedures for SA Management, Cryptographic Key Management and Monitoring & Control;
  - Integration with Space Link Protocols (TC, TM and AOS Blue Books).

- Cryptographic Key Management
  - Solid guidelines for future missions concerning Symmetric Key Infrastructure (e.g. key hierarchy, roles, cryptoperiods);
  - Extension to space networks.

- ESA prototypes
  - Developments proceeding to support future missions.

- Cryptography:
  - Authenticated Encryption MAC is ‘limited’ to 128-bits (AES GCM). This potential long-term concern has been expressed to the Cryptographic Research community (DIAC 2012).
PHYSICAL LAYER SECURITY
CIA Requirements

At the Physical Layer the priority is to take care of the following security feature.

**Availability** needed for:

1. Protection of Telecommand transmission (spread spectrum, null-steering antennas, high-power up-link).

Current research on physical layer security providing Secrecy and Authentication for radiofrequency signals, while intense at the mobile communications research community, is not yet sufficiently mature to allow for implementation on space missions. However, the topic is being monitored given its attractiveness.
Spread Spectrum Modulation (1)

The so-called 'Jamming Margin' reflects the ratio between Jammer and wanted signal powers. It is formulated as follows:

\[ J_m = G - L_{sys} - \frac{E_b}{N_o} \]

\[ G = \frac{B_{RF}}{R} \]

Where

- **G**, itself the ratio between signal radiofrequency bandwidth \((B_{RF})\) and information bandwidth \((R)\), is known as the **Processing Gain** of the spread spectrum signal;
- **\(E_b/N_o\)** reflects the required energy-per-bit vs. noise power spectral density and is chosen considering the particular modulation and coding technique;
- And **\(L_{sys}\)** gathers the system implementation losses, that is, the deviations between actual (physical) and theoretical performance; among those for instance one can mention modem imperfections.
Spread Spectrum Modulation (2)
DS-SS CDMA

Direct-Sequence Spread-Spectrum modulation provides an efficient interference-robust modulation solution for TT&C space communications links with limited bandwidth expansion, multi-user capability and technical complexity as well as need for ranging.

- NASA’s Tracking and Data Relay Satellite System (TDRSS) is the precursor for civilian space missions.
- The defunct ESA HERMES project included the provision of spread spectrum communications with Data Relay.
- Later on and out of the Automated Transfer Vehicle (ATV) and European Data Relay experiences ESA has promoted the development of spread spectrum technology for TT&C application in Europe.
- The European Telecommunications Standard Institute (ETSI) established a derived standard for TCR (TT&C for Telecommunication Satellites).

NASA pictures
Spread Spectrum Modulation (3)
DS-SS CDMA Enhancements

However, Direct-Sequence Spread-Spectrum modulation as specified on those systems has two fundamental weaknesses:

- Relatively short pseudo-noise sequences, which does not allow to fully exploit theoretical processing gain with respect to interference/jamming; and provides almost no resistance to signal interception.
- Relatively poor complementary channel coding (with no interleaving) as per CCSDS/ECSS Channel Coding standards (see references).

Hence, enhancements for such modulation to mitigate those weaknesses have been and continue to be addressed with:

- Cryptographic pseudo-noise sequences with corresponding synchronization techniques;
- Advanced TC coding/interleaving.
Key requirements sought for cryptographic sequences are:

- Autocorrelation geared to support synchronization;
- Multi-user support, which in turn implies controlled cross-correlation between any pair of sequences;
- Resistance to interception.

Cryptographic Sequence structure is based on the Hadamard product of a multiple access sequence and a cryptographic sequence.
Cryptographic Pseudo-noise Sequences – Synchronization (1)

Parallel Searching Capability: L+1 Code Phases

On Board Code Shift = (L +1) Code Phases

N = Incoming and Local Block Size (samples)
L = Zero Padding Length (samples)
D = Doppler Compensation Sub-ranges
W = Non-Coherent Integration length
\( R_{C,ACQ} \) = Local Code Rate during Acquisition
\( F_S \) = Sampling Frequency = 4\( R_C \)
\( R_C \) = Code rate
\( F_{IF} \) = Intermediate Frequency
\( F_S \) = Sampling Frequency

N = 8192 samples = 4071 chips
L ≈ 6500 ± 7000 samples = 3250 ± 3500 chips
Cryptographic Pseudo-noise Sequences – Synchronization (2)

Frequency-domain digital synchronization techniques, capable to provide a several order of magnitude improvement against classical time-domain serial search, have been explored. Basic algorithms (e.g., Generalized Zero Padding) have been evaluated in various typical mission scenarios like:

- LEO,
- MEO,
- GEO,
- ISL,
- HEO.

\[
P_d = 99\% \text{ for } J/S \leq 27\text{dB}, \text{ Data Modulation Degradation}=1\text{dB}
\]

Average Code Acquisition Time (Code Length \(L_{\text{code}}=2^{24}\) chips) lower than 18s

Average Code Acquisition Time (Code Length \(L_{\text{code}}=2^{22}\) chips) lower than 6s
Cryptographic Pseudo-noise Sequences – Synchronization Summary

- A Novel PN Codes On-Board Synchronization Processing has been developed and optimized for GSO, MEO and LEO Satellite for Telemetry Tracking and Command Secure Link Applications.

- A very Long PN Code (Code Length: $2^{24} - 2^{26}$ chips, $2^{16}$ times longer than the ETSI Standard) can be synchronized Blindly in a few seconds in a very hostile environment characterized by large Doppler (up to 60-kHz for LEO scenario) ad high Jammer over Signal Power Ratio (J/S=30dB).

- The proposed Synchronizer Architecture allows adopting a Secure TT&C Spread Spectrum link not only for GSO Mission but also for more challenging MEO and LEO missions.
Advanced TC Coding (1)

- Limits of TC BCH coding and decoding.
- Suboptimal for channels with interference
  - Poor performance under error bursts leading to TC frame rejection.
  - Suboptimal concatenation with convolutional (7,1/2) not a long term solution.
- Suboptimal for DS-SS modulation.
  - Potential processing gain/performance degraded by burst errors
- Need to study, evaluate and compare novel coding/interleaving concepts for TC where physical layer security is required.
Pulsed jamming impact for TC BCH

![Graph showing the impact of pulsed jamming on TC BCH](image-url)
AWGN performance for TC BCH code
Advanced TC Coding (2)
AWGN performance new codes/decoders

Here is a plot showing an example of code performance under AWGN.
Advanced TC Coding (3)
Performance under jamming

- The same codes and decoding algorithms have been evaluated against generic jamming signals:
  - CW;
  - Pulsed signal;
  - PRN.

- **Interleavers** to improve performance under burst errors (pulsed signal) have also been studied.

- The presence/absence of ideal **Jammer State Information (JSI)** detector has been considered.

- Results are under evaluation.
Interleaver effect (Turbo code)
Advance TC Coding
Some preliminary findings

- Coding:
  - the current BCH(63,56) coding scheme is not very powerful; new codes can guarantee a much better protection against jamming.

- Interleaver:
  - Results show that the use of an interleaver at CLTU level can strongly improve the protection against pulsed jamming.

- DS-SS:
  - G = 10 looks too small to guarantee a good protection against pulsed, CW and PN jamming
  - G = 100 (or, better, G =1000) can significantly improve the system protection
CONCLUSIONS AND FOLLOW-ON
CONCLUSIONS

- This presentation has provided an overview of the Space Link Security concepts, techniques and solutions being researched and defined by ESA
  - in cooperation with the international space community (CCSDS) as well as ESA-member state research institutions for the Data Link layer and
  - in cooperation with European companies for the physical layer techniques and technologies (DS-SS with cryptographic sequences).

- This portfolio of space link security concepts, techniques and technologies should be able to accommodate the security needs of many future space missions with a relatively simple network topology.
FOLLOW-ON (1/2)

- Data Link Security
  - Application of Core SDLS,
    - Prototypes evaluation;
    - Flight qualification.
  - Completion of SDLS Extensions,
    - Key Management
      - Guidelines for symmetric key infrastructure.
    - Monitoring and Control,
      - Directives;
      - Status reports.
    - Security Association Management.
  - Integration with SLE Management?
    - SLE Adaptations.
Physical Layer Security:
- Detailed specification of robust PN Sequences;
- Advanced coding evaluation; integration in TC protocol (e.g. CLTU delimitation);
- Link acquisition concepts;
- Key Management;
- Standardization?
  - TC novel codes;
  - Cryptographic Sequences.

Network Security.
ACKNOWLEDGEMENTS

The author is indebted to the members of the CCSDS Security Working Group and the CCSDS Space Data Link Security Working Group for their leadership and contribution to the production of relevant security reports and standards like CCSDS SDLS. Special thanks to:

- C. Biggerstaff, H. Weiss, E. Greenberg, NASA;
- D. Fischer, G.P. Calzolari, M. de Lande Long, ESA;
- G. Moury, B. Saba, CNES;
- M. Pilgram, D. Richter, DLR.

Furthermore, the author is grateful to the many ESA colleagues and contractors involved on the activities reported in this presentation. The list would be too numerous to be completely included here. In particular, the following are mentioned:

- Symmetric Key Infrastructure:
  - M. Juliato, C. Gebotys, University of Waterloo (CDN).

- Cryptographic Pseudo-noise Sequences:
  - J. Massey, Massey Consulting (DK);
  - G. Fittipaldi, L. Simone, Thales Alenia Space (I).

- Advanced TC coding:
  - R. Garello, Politecnico di Torino (I);
  - F. Chiaraluce, M. Baldi, M. Bianchi, Università Politecnica delle Marche (I);
  - S. Cioni, M. Bertinelli, ESA.
ESA activities (Final reports publicly available)

REFERENCES (2/8)

- IEEE Wireless

- ESA TT&C Workshop 2004
  - Aguilar Sánchez, I.; *The TTC Concept for the GALILEO Constellation*, ESA 3rd International Workshop on Tracking, Telemetry and Command Systems for Space Applications, 7-9 September 2004, ESOC, Darmstadt, Germany.

2007

REFERENCES (3/8)


- Aguilar Sanchez, I.; *Securing ESA Space missions: some conclusions after recent generic and project-specific security activities*, ESA 4th International Workshop on Tracking, Telemetry and Command Systems for Space Applications, 11-14 September 2007, ESOC, Darmstadt, Germany.


REFERENCES (4/8)

2010


REFERENCES (5/8)


- AFCEA-IEEE Military Communications Conference (MILCOM)

- IEEE Aerospace Conference (AEROSP) 2012

- Data Systems in Aerospace (DASIA)
REFERENCES (6/8)

- ECRYPT Workshop *Directions in Authenticated Ciphers* (DIAC) 2012

- IEEE AESS ESTEL 2012

- IEEE Vehicular Technology Conference (VTC) 2013 (approved for presentation)
  - Baldi, M.; Bianchi, M.; Chiaraluce, F.; Garello, R.; Aguilar Sanchez, I.; Cioni, S.; *Advanced Channel Coding for Space Mission Telecommand Links*, Las Vegas, USA.
REFERENCES (7/8)

- International Standards and Reports (e.g. CCSDS, ETSI, GAO)
  Consultative Committee of Space Data Systems (CCSDS)

- European Telecommunications Standard Institute (ETSI)

- United States Government Accounting Office (GAO)
REFERENCES (8/8)

Selected Books:

CCSDS background

- Civilian space agencies cooperate for the development of security concepts applicable to their space missions through CCSDS.
  - Blue Books (standards)
  - Green Books (reports)

- CCSDS has developed over 25 years a set of standard communication protocols & services supporting data transfers within space systems & interoperability:
  - 60+ standards published;
  - Serving 500+ space missions.
## SDLS Summary of Protocol and Services Support (1)

<table>
<thead>
<tr>
<th>User Services</th>
<th>Type of Service Data Unit</th>
<th>Protection by SDLS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TC Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple Access Point (MAP) Packet</td>
<td>Packets with authorized Packet Version Number (PVN)</td>
<td>Protected</td>
</tr>
<tr>
<td>MAP Access</td>
<td>Variable-length private data</td>
<td>Protected</td>
</tr>
<tr>
<td>Virtual Channel (VC) Packet</td>
<td>Packets with authorized PVN</td>
<td>Protected</td>
</tr>
<tr>
<td>VC Access</td>
<td>Variable-length private data</td>
<td>Protected</td>
</tr>
<tr>
<td>COP Management</td>
<td>N/A</td>
<td>Not protected</td>
</tr>
<tr>
<td>VC Frame</td>
<td>Transfer Frame</td>
<td>Not protected</td>
</tr>
<tr>
<td>MC Frame</td>
<td>Transfer Frame</td>
<td>Not protected</td>
</tr>
</tbody>
</table>
### SDLS Summary of Protocol and Services Support (2)

<table>
<thead>
<tr>
<th>User Services</th>
<th>Type of Service Data Unit</th>
<th>Protection by SDLS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TM Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet</td>
<td>Packets with authorized PVN</td>
<td>Protected</td>
</tr>
<tr>
<td>VCA</td>
<td>Variable-length private data</td>
<td>Protected</td>
</tr>
<tr>
<td>VC_FSH</td>
<td>Fixed-length data</td>
<td>Authentication Only</td>
</tr>
<tr>
<td>VC_OCF</td>
<td>Fixed-length data</td>
<td>Not protected</td>
</tr>
<tr>
<td>VC Frame</td>
<td>Transfer Frame</td>
<td>Not protected</td>
</tr>
<tr>
<td><strong>MC Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MC_FSH</td>
<td>Fixed-length data</td>
<td>Not protected</td>
</tr>
<tr>
<td>MC_OCF</td>
<td>Fixed-length data</td>
<td>Not protected</td>
</tr>
<tr>
<td>MC Frame</td>
<td>Transfer Frame</td>
<td>Not protected</td>
</tr>
</tbody>
</table>
### SDLS Summary of Protocol and Services Support (3)

<table>
<thead>
<tr>
<th>User Services</th>
<th>Type of Service Data Unit</th>
<th>Protection by SDLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOS Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet</td>
<td>Packets with authorized PVN</td>
<td>Protected</td>
</tr>
<tr>
<td>Bit stream</td>
<td>Bit stream</td>
<td>Protected</td>
</tr>
<tr>
<td>VCA</td>
<td>Variable-length private data</td>
<td>Protected</td>
</tr>
<tr>
<td>VC_OCF</td>
<td>Fixed-length data</td>
<td>Not protected</td>
</tr>
<tr>
<td>VC Frame</td>
<td>Transfer Frame</td>
<td>Not protected</td>
</tr>
<tr>
<td>MC Frame</td>
<td>Transfer Frame</td>
<td>Not protected</td>
</tr>
<tr>
<td>Insert</td>
<td>Short fixed-length data</td>
<td>Not protected</td>
</tr>
</tbody>
</table>
## Cryptographic Key Management

### Mission Scenarios

<table>
<thead>
<tr>
<th>Mission Type</th>
<th>Link Type</th>
<th>Scenario</th>
<th>Data rate [kbps]</th>
<th>Frame size [bits]</th>
<th>Contact Time [min/day]</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEO</td>
<td>TC</td>
<td>Nominal</td>
<td>64</td>
<td>1024</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency</td>
<td>1</td>
<td>1024</td>
<td>400</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fixed Attacker</td>
<td>64</td>
<td>1024</td>
<td>400</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distributed Attacker</td>
<td>64</td>
<td>1024</td>
<td>1440</td>
</tr>
<tr>
<td>HK TM</td>
<td></td>
<td>Nominal/Attacker</td>
<td>2048</td>
<td>8192</td>
<td>10</td>
</tr>
<tr>
<td>PL TM</td>
<td></td>
<td>Nominal/Attacker</td>
<td>819200</td>
<td>8192</td>
<td>400</td>
</tr>
<tr>
<td>GEO</td>
<td>TC</td>
<td>Nominal</td>
<td>4</td>
<td>1024</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency</td>
<td>1</td>
<td>1024</td>
<td>1440</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attacker</td>
<td>4</td>
<td>1024</td>
<td>1440</td>
</tr>
<tr>
<td>HK TM</td>
<td></td>
<td>Nominal/Attacker</td>
<td>2048</td>
<td>8192</td>
<td>10</td>
</tr>
<tr>
<td>PL TM</td>
<td></td>
<td>Nominal/Attacker</td>
<td>2097152</td>
<td>8192</td>
<td>1440</td>
</tr>
</tbody>
</table>