Reordering the COP and SDLS Functions in TC Space Data Link Protocol (CCSDS 232.0)

A Proposal from NASA GSFC & JPL

Email Thread of Discussion prior to Fall 2022 CCSDS Meeting in Toulouse, FR

Sept. 18, 2022

**Purpose**

Both GSFC and JPL personnel are providing the following evidence in order to convince the SDLS WG to concur on changing the order of processing in Chapter 6 (SDLS chapter) of TC Space Data Link Protocol (CCSDS 232.0) as follows, because for the following reasons we believe it to be technically incorrect.

I’ve captured the discussion via the email thread below, so that we have it recorded in one place.

**Proposal**

FROM:

SDLS – FOP – Encode …..(space link)…. Decode – FARM – SDLS

TO:

FOP – SDLS – Encode …..(space link)…. Decode – SDLS – FARM

**Proposed Action**

At the fall CCSDS meeting in Toulouse in October, unless we have misunderstood something, we plan to generate RIDs after the discussion of this topic at the joint SLP/SDLS WG meeting against the TC Space Data Link Layer Protocol book (CCSDS 232.0-B-4) in Chapter 6 namely, “ORDER OF PROCESSING BETWEEN TC, COP-1, AND SDLS PROTOCOLS”, Figure 6-3, and Table 6-1 to change the order of processing between COP and SDLS as proposed. Our goal is to obtain consensus that this RID needs to be written.

Rational for this Change: (Please follow the thread of this discussion so far below)

1. First from Marc Sanchez Net (NASA/JPL)

[MARC] I have some thoughts on the current order of processing:

* COP-1, being a go-back-N retransmit protocol, will eventually replay TC transfer frames. SDLS provides anti-replay. Therefore, if FOP is applied before SDLS at the sending end, and SDLS before FARM at the rx end, then SDLS at the rx will discard all replayed frames by COP-1, thus defeating COP.

[MARC] I don’t actually agree with this. At the transmitter, the FOP may re-transmit a copy of the transfer frame (TF) because it has received, via the downlink, indication that it must do so. This copy of the TF will then go through the SDLS encryption procedure which, internally, contains a persistent replay counter that is copied into each TF while being encrypted. This replay counter is incremented every time something is run through the encryption procedure, be it a re-transmission or not (in fact the encryption procedure has no way of knowing this). Therefore, at the rx, SDSL would see an incremented replay counter, validate the TF, and provide it to the FARM, which could then determine if the TF is correct or not with the CRC (and signal re-tx accordingly). See diagram below.

[MARC & GREG & BRENT] The anti-replay function of SDLS DOESN’T prevent re-transmissions by the FOP.



* *SDLS at rx end checks integrity of TC frame by checking the MAC. Therefore, all errors detected by SDLS are counted as security events rather than channel errors due to noise*

[MARC] Yes, this is true, it is a good reason to close the COP-1 loop before SDLS

* *SDLS at rx end checks integrity of TC frame by checking the MAC. Therefore, COP-1 will replay those SDLS rejected frames because the FARM will never see them. Those replayed TC frames will be rejected as replay by SDLS*

[MARC} This statement has two parts:

***COP-1 will replay those SDLS rejected frames because the FARM will never see them*:**Thisis true, but the operation of COP-1 will be very inefficient. In particular, if SDLS fails to authenticate/decrypt a TF it will simply discard it and, possibly, the FARM will not be notified that this happened. Therefore, the FARM will never issue re-transmission requests in response to an error. It will, however, issue retransmission request the COP-1 timers expire. So, instead of pro-actively requesting re-tx whenever there is a channel error, we will just rely on timers for re-transmissions, which is brittle and possibly inefficient if we misconfigure them. (timers are notoriously difficult to configure)…

[Greg’s input] In this case, SDLS uses authentication and the MAC is a much stronger error detector than either the BCH or LDPC codes. So SDLS in this mode, will potentially detect more frame errors and discard those frames, so COP will not see those discarded frames – that means that SDLS in effect will slow down the forward progress of the go-back-N protocol. It will force FARM to go back to the last good frame received +1 and ask for retransmission from that point, independent of the timers. So even in this case, COP is still working as it normally does. [Greg Stop]

* ***Those replayed TC frames will be rejected as replay by SDLS*: [MARC}** This goes back to my statement (1), which I do not believe is true.
* Technically speaking, there is a way to run COP-1 after SDLS and the system does work.

End (of Marc Sanchez Net 1)

1. Gilles Moury – CNES … In response to the email above

After discussion of your proposal with Ignacio, we gathered the following points :

* discriminating between transmission and security errors is very important since:
* They do not have the same probability of occurrence (transmission errors are hopefully more frequent than security !)
* They do not require the same handling (transmission errors recovery can be automated (COP), security errors recovery not)
* False alarm on security will be much more disruptive for operations than resynchronizing the COP by sending a setV(R) command.

* your proposal has pros and cons:
	+ Pros : COP stays synchronized and guarantees in sequence delivery of type A frames to the OBDH
	+ Cons : No discrimination between transmission errors and security events
* With the recommended order of processing (1), in case of security event, the reporting to ground is done through the FSR. The MCC reaction cannot be automated and will require human analysis. In the meantime, the OBDH should reject resulting out of sequence TC frames or packets as is normal practice for TC sequence execution. When operation resumes, COP will need to be resynchronized but this seems acceptable since security events are rare (hopefully!) and their handling will require human analysis and complex procedures anyway.

* The order of processing is in our view correct. On the receive side, first transmission control for all frames. Afterwards, security verification for those carrying protected data:
	+ Inverting the order may lead to false alarms when the legal operator is communicating with the spacecraft. This is a burden, in particular for missions with certain level of security. We should not care much about the behavior for the attacker.

* We have two somewhat independent reports concerning transmission control (CLCW) and security (FSR):
	+ However, we agree with you and the other NASA colleagues that there might be an issue between the coherency and consistency of both reports and implicitly a not-so-independent relationship between protocols

* We think the action as currently formulated is not appropriate:
	+ The action(s) should focus on defining first the real problem that we are trying to solve as well as the identification of potential solutions with corresponding trade-off criteria. There might be other solutions than inverting the order of processing.

* Reliably differentiating security events from transmission errors is for us a paramount constraint. Minimizing impact on existing implementation is another one.

End (of Gilles Moury 2 response)

1. Brent Andres – GSFC … in response to Gilles email

**[Brent]** I have 2 concerns with the current SDLS-FOP-FARM-SDLS ordering:

First, as already stated, that ordering allows the possibility of a frame being accepted by the FARM as in-sequence and then subsequently rejected by SDLS, either because of a security event or because of un-corrected transmission errors.  The COP-1 protocol would be unaware that a gap has been created in the sequence and, depending on what the contents are, that gap may not be detected by the flight software.  Even if the gap is detected, the service guarantee of the COP will not be completely reliable.

Second, with the current ordering of functions the security counter (or IV when using option b) in 355.0 section 2.3.2.3.4 , I’ll refer to either here as the Nonce to distinguish them clearly from the frame sequence number used by the COP for frame sequencing), will be incremented based on the order of the frames presented to the SDLS on the ground which may not be in the order presented to SDLS on the spacecraft, possibly leading to false authentication failures.  For example if a string of type AD frames is transmitted with frame sequence numbers ranging from 1 to 100  followed by a type BD expedited frame, the sequence of nonces for those frames would range from 1 to 100 (assuming they started at 1) with the type BD frame having a nonce of 101.  Once the BD frame is accepted then the current nonce value on the spacecraft will be set to 101.  If, for some reason though, AD frame 1 was not accepted, then all re-transmission attempts of frames 1 to 100 by the FOP will be accepted by the FARM but rejected by the SDLS on the spacecraft because their nonces are less than 101.  The COP however will not be aware of that failure.

With the current ordering I don’t understand why placing the FARM ahead of SDLS on the spacecraft would enable the system to differentiate between security events and un-corrected transmission errors.  If you could provide an example or a more detailed explanation that would be helpful.  Similarly, I don’t understand why recovery from authentication failures can’t be automated by the COP.  At any rate, the use of the optional FECF to detect transmission errors and differentiate them from security events would seem to work with either ordering since the CRC is computed based on the entire, secured transfer frame minus the FECF itself and therefore the current ordering is not required on that basis.

An alternative ordering of functions would be:

FOP

SDLS (encrypt data, increment nonce, compute MAC - which excludes the FECF field as an input)

FECF (optional - compute CRC based on secured TF minus the FECF itself per 6.3.7 of 232.0 for secured TFs)

FEC encoding at the Coding and Synch layer

Physical channel

FEC Decoding

FECF CRC check (frames with detected transmission errors are trashed)

SDLS (check for incremented nonce, provide decryption/authentication, rejected frames are trashed)

FARM

* This order does not preclude re-transmission by the FOP since the MAC for each frame will be computed based on an incremented nonce.
* The nonce for each frame will be incremented based on the order of transmission regardless of the frame type (AD or BD)
* Only frames which pass FEC and SDLS will be presented to the FARM maintaining the synchronization of the COP
* Frames with transmission errors could be detected by the optional FECF and removed prior to authentication, allowing differentiation between the two types of errors
* Recovery from both events is automated by the COP

End (of Brent Andres response 3)