February 2020

IMPLEMENTING GMP-SEC USING STUFFING BYTES TO PROVIDE SECURITY OVER 400ZR AND OTHER OPTICAL STANDARDS

Gilberto Loprieno

Davide Codella

Emanuele Giacometti

IMPLEMENTING GMP-SEC USING STUFFING BYTES TO PROVIDE SECURITY OVER 400ZR AND OTHER OPTICAL STANDARDS

AUTHORS:

Gilberto Loprieno
Davide Codella
Emanuele Giacometti

ABSTRACT

Presented herein are techniques for providing security to networks operating in accordance with the 400ZR standard. Currently, there is no specification relating to how traffic should be encrypted and authenticate by this standard. In addition, the techniques presented herein support the possibility of encrypting and authenticating every single 100GBASE-R or 200GBASE-R stream when they are mapped inside 400ZR. GMP-Sec can be used in any application which relies on the Generic Mapping Procedure (GMP), with the only recommendation that client rates must be lower than 0.21% of container frequency. Moreover, the techniques presented herein can be applied to the Optical Transport Network (OTN) layer, in particular when packets are mapped over OTN (100GBASE-R over OPU4, 200GBASE-R and 400GBASE-R over OPUCn). Other solutions require tag frames (hence adding bytes and increasing line frequency) or require overwriting of many Overhead and Operational bytes, which may impact the customer's ability to manage the network (like OTNSec). In the techniques presented herein, GMP-Sec replaces unused stuffing bit, filled by fixed pattern and not carrying payload traffic.

DETAILED DESCRIPTION

The Generic Mapping Procedure (GMP) is a mechanism to map any client traffic (or constant bit rate) over a generic frame by inserting stuffing bits to adjust the delta frequency between the client traffic and the frame (or container). GMP is widely used when client traffic is not subject to deep inspection and the client is transparently transported, i.e. client traffic is transported as it was generated without any modification, also preserving inter-packet gaps. In this way, the frequency of the source at which the traffic is generated is preserved.

GMP also introduces stuffing bytes inside the payload in a way that they are "equally" distributed over the payload and not concentrated over a single portion of the frame. That is, the stuffing words are distributed throughout the OPU payload such that they fill completely the frame and match the client traffic frequency. The receiver applies the same rules and detects stuffing.

The stuffing bits do not carry payload traffic and, when the client traffic is not enough to fill the payload, the GMP algorithm inserts the needed stuffing. In addition, GMP inserts stuffing inside a frame payload following an arithmetical rule that allows receiver to easily identify payload data from stuffing. The stuffing bits are filled by a fixed pattern.

The techniques presented herein define GMP Security to the data path by replacing GMP stuffing with GMP-Sec Overhead (Secure Header Field (SHF) and Secure Check Field (SCF)). SHF transports security information (such as Key in Use, Key exchange, Secure Frame Counter, etc.) and SCF is used to transport the signature of the previous frame, allowing the authentication of the received frame.

For simplicity, it is assumed that GMP Secure Overhead mimics MACSEC by adding 32 bytes for each frame (16 bytes for SHF and 16 bytes for SCF). It has been determined that the container frequency (frame) must be greater than 0.21% compared to client frequency in order to allow more than 32 bytes of stuffing. Any mapping respecting this rule is eligible for GMP-Sec.

GMP was originally defined to support OTN mapping, but now it is used in multiple applications including the Optical Internetworking Forum (OIF) 400ZR standard, specified in oif2017.245.14. The 400ZR standard is a new technology designed to transport 400GBASE-R over coherent optics pluggable modules and it does not provide any specification to support security on the 400ZR payload.

In operation, the 400GBASE-R is asynchronously mapped into a 400ZR container by GMP. Since mapping is asynchronous, the 400GBASE-R stream is treated as CBR data (including preamble and IPG). Data and timing transparency is preserved by the GMP mapping. The GMP Justification Control bytes (JC1-6) are carried in the first of the four 320-bit OH instances, and present in the 2nd, 3rd, and 4th frames of a 400ZR 4-frame multi-frame, as specified by oif2017.245.14. The 4 frames are identified by MFAS bits 7 and 8 being 00, 01, 10 and 11. For the purpose of 400ZR, GMP parameters shall be defined as:

- Block : Minimal GMP granularity transporting data/stuff (m) = 4 x 257 = 1028 bit;
- Number of Blocks inside a multiframe (Pm,server) = 10220.

- Number of Blocks requested to transport 400GBASE-R (Cm) ($10214 \leq Cm \leq 10218$)

That is, four 400ZR frames are combined together and the 400ZR payload is grouped into 4x257 bits block (one block is 1028 bits). The multiframe is based on 10220 blocks. In the worst case scenario (when 400GBASE-R is +100ppm and 400ZR payload is -20ppm), the 400GBASE-R requires a maximum of 10218 blocks so at least two blocks are always available. It is proposed to use the first block (first 32bytes of first block, i.e. 256 bits) to transport Secure Header (SHF) and Secure Check Field (SCF).

Another application addressed by this idea is related to aggregation mode for 400ZR. Certain companies have presented a method for 100GE/200GE multiplexing over 400ZR. This proposal is based on dividing 400ZR into 4 interleaved time slots, each one made of 257 bits. Each 400ZR time slot (257 bits) is dedicated to transport a single 100G stream. Each 100G client (in particular 100GBASE-R but potentially also FlexO) is GMP mapped over its dedicated time slots.

While 400ZR was transporting OH only of first 32Bytes, the interleaved version uses 32 bytes x 4 transporting OH1, OH2, OH3, OH4. In this way, each client has its own OH bytes and its own GMP Justification Control bytes (JCx). As a result, all Justification Control bytes are independently available for each stream. In this case, a single 100G client requires a maximum of 10218 blocks (consisting of 257 bits each) over a total of 10220 blocks available. Consequently, at least two blocks are always available for each client. It is proposed to use the first block of 257 bits for each time slot to transport Secure Overhead (SHF and SCF). Each of the 4 time slots can be independently Encrypted and Authenticated. Alternatively, the payload can be encrypted and authenticated as per 400ZR mode. In case of 200GBase-R, the block size is selected as 2x257 bits, but the description is the same as 100GBASE-R. Also in this case GMP-Sec security overhead are inserted in first block.

More generally, the techniques presented herein can be applied to any mapping in which GMP is used. The techniques presented herein also work well when packet mapping is applied over OTN hierarchy (100GBASE-R over OPU4 , 200GBASE-R, 400GBASE-R over OPUCn). In these scenarios, the number of stuffing bits available for each frame is more than the required 32 bytes.

Even if not optimized for already deployed ASICs, the techniques presented herein can be also applied to ODUk time-division multiplexing, where GMP is adopted (ODUj into OPUk and ODUk into OPUCn mapping, G709 chapter 7.4). However, such arrangements require some

modification to G709 standard. Security at optical level can be provided by OTNSec but, since it replaces OH bytes planned for OTN Operation and Management, it reduces the functionalities of OTN layer. Differently, GMPSec replaces unused bits/bytes otherwise filled by fixed pattern, not carrying payload traffic.

The following description illustrates different example scenarios employing the techniques presented herein.

The GMP parameters required for 400GE mapping are between a minumum of 10214 blocks (Cm,min) and a maximum of 10218 (Cm,max). In addition, the Justification Overhead is transported inside the first 40 bytes of OH inside the 400ZR frame. In the OIF 400ZR Multiframe structure, block 1 is always filled by stuffing bits and, for 400GBASE this block is based on 4x257 bits (1028) The techniques presented herein propose to replace only the first 257 bits (32 bytes) of Block 1 with GMP-Sec Overhead.

In the worst case analysis for a 400G-ZR frame, there are 10220 of 4x257 blocks. For mapping 400GBASE inside 400G-ZR there are requested a maximum of 10217,136 blocks. Assuming the maximum of blocks used equal to 10218, there are at least 2 blocks available on each frame. As for, to support GMP-SEC, 32 bytes are requested so a single block is more than enough.

In summary of OIF 400ZR, 400GBASE-R can be transported over 400ZR frame and a maximum of 10218 blocks are requested as calculated by IA # OIF-400ZR-0.12 Draft. This occurs when 400GBASE-R is +100ppm while 400ZR frame is -20ppm (Worst case scenario). This means that a maximum of 10218x4x257 client bits are transported over a multiframe (10504104 bits over 10505132 available). Any 400GBASE-R requires a number of blocks (Cm) between 10214 and 10218. The GMP block 1 is always filled by stuffing so available to GMP-Sec Overhead. As such, in all possible scenarios of GMP mapping inside 400ZR frame, it is possible to include secure information in the first block of 4x257 bits (1028 stuffing bits).

In GMP-SEC with the so-called “Aggregation mode,” companies have proposed 4x100G and 2x200G Multiplexing over 400ZR. The advantage of this multiplexing scheme is to allow 100G/200G without OTN layer. The 400ZR frame has a payload based on 10220 blocks of 4x257 bits and companies have proposed to split the 400ZR payload into 4 time slots, each one based on 257 bits, allowing client interleaving. In that way, 400ZR blocks can now support four (4) time

slots each of 257 bits. The techniques presented herein propose to provide security to each of the four 400ZR time slots.

In multiplexing 4 x 100G (FlexO) over 400ZR, the 400ZR.ts frame in channelized mode is built as:

- OH and alignment markers are added as per 400ZR specs but divided into 4 groups.
- Payload is divided into 4 time slots (each one dedicated to transport a 100G traffic).

In addition, each client has its own OH (OH1, OH2, OH3, OH4) and its own GMP justification control information (JC1/2/3/4/5/6). In this way each (of the 4) 100G can be asynchronously mapped by GMP inside the 400ZR payload. Each block transports Client data or stuffing. The client can be FlexO frame or 100GBASE (both are transported as CBR traffic).

The 400ZR payload blocks are 10220 and are based on 4x257bits block. In a 400ZR.ts (channelized) each block is divided by four (i.e. into 257 bits blocks) (i.e., ts is channelized to support 4 time slots). Each of the four 257 bits blocks transports a single 100G traffic. The mapping of client inside the time slots is managed by GMP mapping and follows the same rules of 400ZR. Additionally, 400ZR OH is also divided into 4 x320-bits (4x 40Bytes) and each OH1 is dedicated to Client 1, OH2 to Client 2, OH3 to Client3 and OH4 to Client4. The GMP Justification Control (JC) are defined as per 400ZR but they are transported over OH1. OH2, OH3 and OH4, therefore each client can be asynchronously GMP mapped over its own time slots.

While 400ZR was transporting OH only of first 32Bytes, the interleaved version uses 32 bytes x 4 transporting OH1, OH2, OH3, OH4. In this way, each client has its own OH bytes and its own GMP Justification Control bytes (JCx). As a result, all Justification Control bytes are independently available for each stream. In this case, a single 100G client requires a maximum of 10218 blocks (consisting of 257 bits each) over a total of 10220 blocks available. Consequently, at least two blocks are always available for each client. It is proposed to use the first block of 257 bits for each time slot to transport secure header (SHF and SCF). Each of the 4 time slots can be independently Encrypted and Authenticated. Alternatively, the payload can be encrypted and authenticated as per 400ZR mode. It is noted that, for 200GBASE-R the description is the same but each block must be based on 2x257 bits.

In packet mapping over OTN, i.e., GMP-Sec with 400GBASE-R / 200GBASE-R over OTN hierarchy, 400GBASE-R and 200GBASE-R are mapped over ODUFlex . ODUFlex

ısporting packets has a bandwidth much lower rather than OPUCn and requires multiple GMP

stuffing. Based on calculations, it is requested that mapped clients have a bandwidth < 0,21% OPUCn and this is fully supported.

With GMP-Sec and 100GBASE-R, 100GBASE-R (103,125Gbit/s) is mapped over OPU4 as CBR traffic (including Alignment Markers) over OPU4 104,355975330 Gbit/s. OPU4 is filled by 32 stuffing bytes. In this way 3800 OPU4 bytes are available over 3808. Real OPU4 available bandwidth is 104,1367 Gbit/s that is 0,97155% more than 100GBASE-R frequency. In a nominal case, 15052,32466 bytes are required for transporting 100GBASE-R over a frame (Stuffing bytes are 147,655 bytes for frame). In a worst case scenario, taking into account OPU4 +/-20ppm and 100GBASE-R +/-100ppm resulting as:

145,869 ≤ Stuffing bytes ≤ 149,481

This can be rounded up to 145 ≤ Stuffing bytes ≤ 150.

As such, the stuffing bytes are more than 32 require to support GMP-Sec Secure Overhead.

GMP mapping is used to multiplexing low order to High Order container (ODUj into OPUk and ODUk into OPUCn). The number of stuffing is usually enough to support MSH (Message Secure Header) and MIC (Message Integrity Check) for encryption and authentication (as shown below in FIG. 1 in the “green” highlighting color). Only 3 cases require to be further analysed (highlighted in “yellow” in Figure 1), namely:

- (*) ODU2e mapped over OPU4
    - instead of 8 time slots of 1,25G, 9 time slots are requested to support GMP-SEC
- (**) ODU3 mapped over OPU4
    - instead of 31 time slots of 1,25G, 32 time slots are requested to support GMP-SEC
- (***)ODU4 mapped over OPUCn
    - instead of 20 time slots of 5G, 21 time slots are requested to support GMP-SEC

		5G Tributary PT=22	1,25G Tributary PT=21		
		OPUCn	OPU2	OPU3	OPU4 (*)
	ODU0	na	GMP	GMP	GMP
	ODU1	na	AMP	AMP	GMP
	ODU2	GMP	na	AMP	GMP
	ODU2e	GMP	na	GMP	GMP (*)
	ODU3	GMP	na	na	GMP (**)
	ODU4	GMP (***)	na	na	na
200GBASE-R	ODUFlex	GMP			
400GBASE-R	ODUFlex	GMP			

Figure 1

In summary, GMP-Sec can be used in any application in which GMP is used with the only recommendation that client rates must be lower more than 0,21%, rather than frame payload frequency in which client is transported. The techniques presented above provide security to 400ZR, where the OIF standard currently does not specify any method to encrypt and authenticate 400ZR. The proposed techniques are also applicable to aggregation of 100GBASE-R or 200GBASE-R when they are mapped inside 400ZR. In that scenario the clients are independently encrypted/authenticated. Moreover, the techniques presented herein can be applied to the OTN layer, especially when packets are mapped over OTN (100GBASE-R over OPU4, 200GBASE-R and 400GBASE-R over OPUCn). Finally, the techniques presented herein can be used in Low Order OTN multiplexing over High Order container (ODUj into OPUk and ODUk into OPUCn), but in some cases the number of tributary slots requested to map ODUk are greater than the number specified by G.709.