Follow-up Discussion of Ethernet Link Security for Datacenter interconnection

Weiqiang Cheng, CMCC

Haojie Wang, CMCC

Jieyu Li, CMCC

Recap

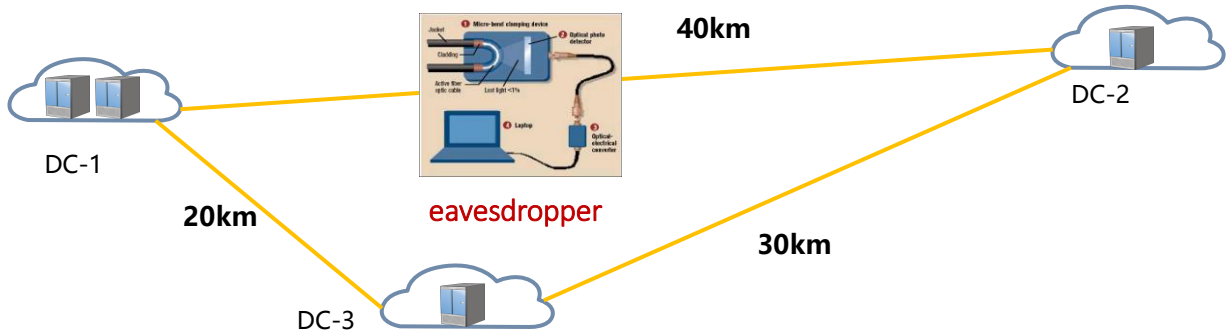
- The topic of DCI link security underwent the discussions within the framework of the AICN item during 802 Nendica July's sessions.
  - July 10: Further Discussion of Link Security Requirements and Challenges on 800G Coherent Interface (**scenarios**, **requirements and challenges, potential PHY layer solution)**

- **This contribution intends to**:
  - more specify security requirements, gap analysis, and potential solution at Ethernet DCI applications,
  - meanwhile hope that the security scenarios and requirements should be discussed within the scope of 802.1, and try to get feedbacks and achieve some consensus,
  - and thus as a input to advance subsequent discussions of potential PHY layer solution within 802.3.

Security Requirements on DCI links

- **Massive data over DCI links is valuble and privacy-sensitive.** Datacenters are a critical infrastructure for cloud computing and AI/ML application, storaging and processing mass sensitive data[1,2]. These valuable data also need to be transimitted bewteen DCs in some application senarios, and become potential eavesdropping targets over DCI links.

- **DCI links is vulnerable in secruity.** Eavesdroppers can intercept optical signals and acquire sensitive data by bending optical fibers, posing a threat to the security and privacy of DCI links exposed to the open physical environment[3].



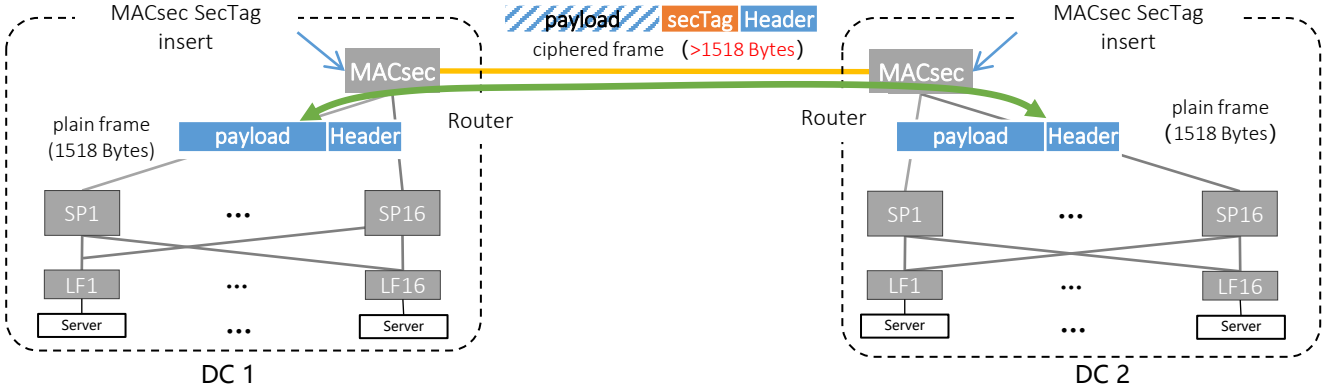
- **Encryption of DCI links should be mandatory.** The possible methods used to encrypt data of DCI links include MACsec, etc.

[1]. Security risk assessment within hybrid data centers: A case study of delay sensitive applications
[2]. Data Center Secure Communication via DNA Hyperchaotic Encryption
[3]. Eavesdropping G.652 vs. G.657 fibres: a performance comparison

Gap Analysis of Prior Mechanisms

① **MACSec's header overhead may lead to reduced bandwidth efficiency of DCI.**

- Given the high utilization of inter-DC links[1,4], such extra security overhead in the traffic can cause congestions, conversely to degrade the utilization of inter-DC links.



② **MACsec isn't easy to be deployed at the existed devices without MACsec.** MACsec requires parsing upto the MAC layer. Implementing MACsec upgrades necessitates replacement of PHY chips or routing/switching hardware, which entails substantial upgrade costs.

What encryption we need:

- **Low Overhead**: maximizing data transmission proportion, minimizing SecTag overhead, reducing data transmission costs.
- **Simplified Deployment**: Compatibility with existing device platforms, avoiding the replacements of costly network devices.

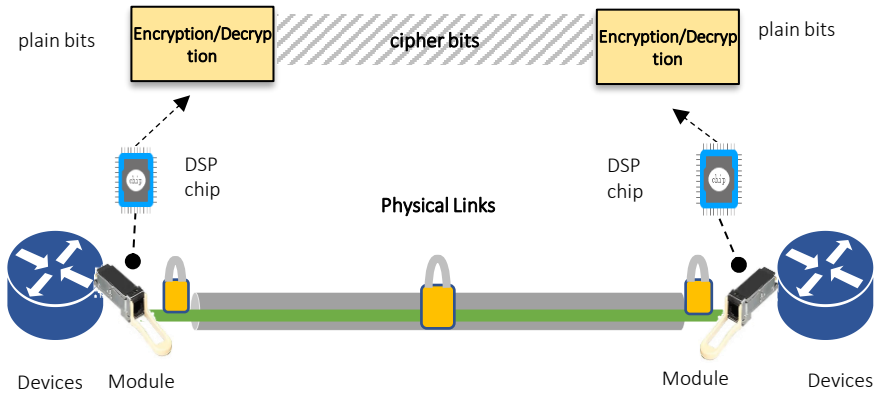
[1] Predicting Inter-Data-Center Network Traffic Using Elephant Flow and Sublink Information
[2] Understanding Data Center Traffic Characteristics
[3] Alibaba hpn: A data center network for large language model training
[4] A Survey on Resource Scheduling for Data Transfers in Inter-Datacenter WANs

Potential solution: pluggable security in PHY layer

- The interface technologies targeting DCI links are currently standardized by **IEEE P802.3dj with pluggable coherent optical modules**, named as **800GE ER1-20 and ER1** objectives. Defining a **PHY layer pluggable security mechanism (encryption on the bitstream)** in these coherent optical modules has the below benefits:

  ① **Not expand frames despite of the addition of SecTag and ICV**. Inserting security context in the reserved PAD field, and not need extra space.

  ② **Pluggable implementation.** Being implemented in a DSP chip of an optical module, providing a pluggable solution that supports the rapid upgrade of link security in existing networks..



An existing OTN PHY layer security reference: OTN has incorporated physical-layer cryptographic security capabilities (i.e. **FlexOsec**), which uses EOH for security overhead.

Discussion

Dicsussions as for the following points are desired to reach consensus. Any other contents are welcomed.

#1 Are the security requirements of DCI links clear? Do you tend to support this requirement?

#2 Is the gap analysis of the current solution in DCI links reasonable?

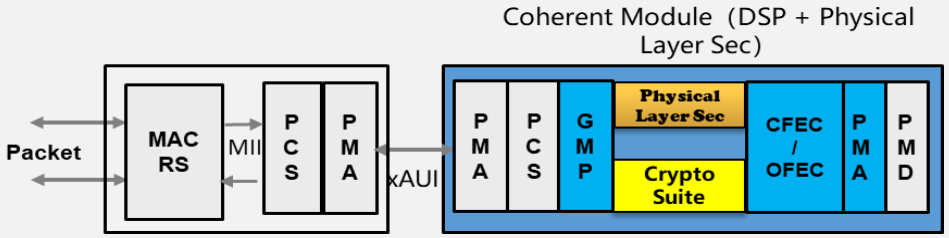
#3 Would you like to support develop a low-overhead and easily deployable security solution in Ethernet PHY layer?

Q&A!

Feasibility Analysis of Confidentiality and Integrity at Coherent Ethernet Physical Layer

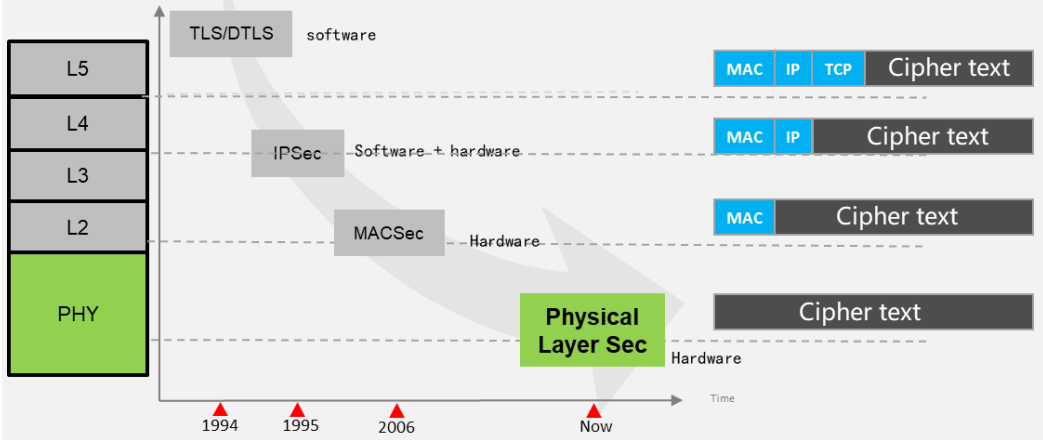
Proposed Architecture Design

- Pluggable security in coherent Ethernet physical layer applies the standardized cryptographic suites (e.g., AES-GCM) to encrypt and integrity-protect bitstreams.
- With the inherent FEC capability in the coherent module, integrity verification works with no problem.



- Leveraging the 802.3dj framework, the PAD field within the frame structure may be redefined to carry security encryption parameters (MACSec similar): TCI, AN, PN, SCI, ICV…

Physical Layer Security Advantages



	TLS/DTLS	IPsec	MACsec	Physical Layer Sec
Confidentiality Layer	L4	L3	L2	L1
Overhead	Packet / Frame header consumption			0
Latency	High	High	Medium	Low
Deployment	Device Software / Hardware Update			Optical Module Replacement / Update