Consideration on a new solution of network link security

Weiqiang Cheng, China Mobile

Haojie Wang, China Mobile

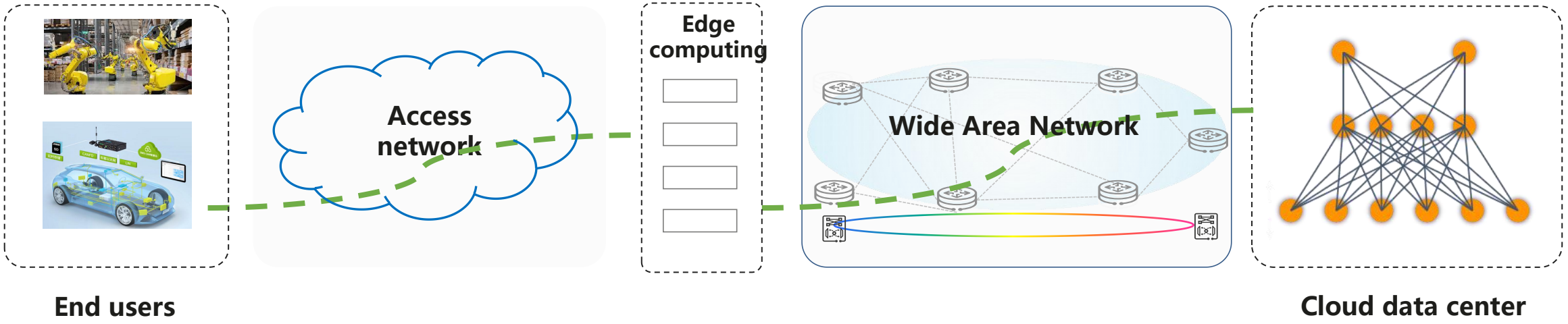
Jin Yang, China Mobile

Overview

- In July’s meeting, we have presented the new requirements and challenges of network link security from the emerging application.
- In this contribution, we will quickly recap the scenario requirements for network link security.
- Giving the consideration on the implementation of a security mechanism at the Ethernet physical layer, along with the advantages it offers.

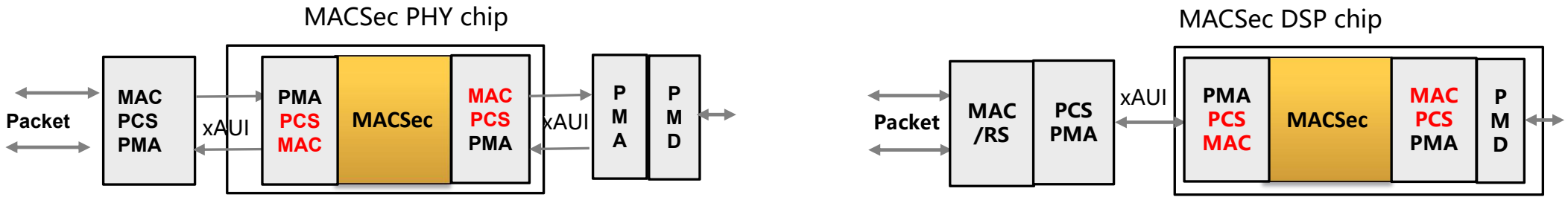
Requirements of network link security

- The risk of link eavesdropping and data leakage is increasing with the emergence of various applications.
  - End users like industrial internet of things and in-vehicle network are exposed in uncontrollable environments.
  - Access and wide area network may consist of wireless, optical, routers and so on. Not all paths are secure.
  - Within data centers, a vast amount of sensitive data, such as customer information, financial data, business transaction details, and more, is being hosted and interacted between different nodes and zones.
- From the perspective of network operators, there is a greater preference for rapidly upgrading link security capabilities while maintaining compatibility with existing network infrastructure.



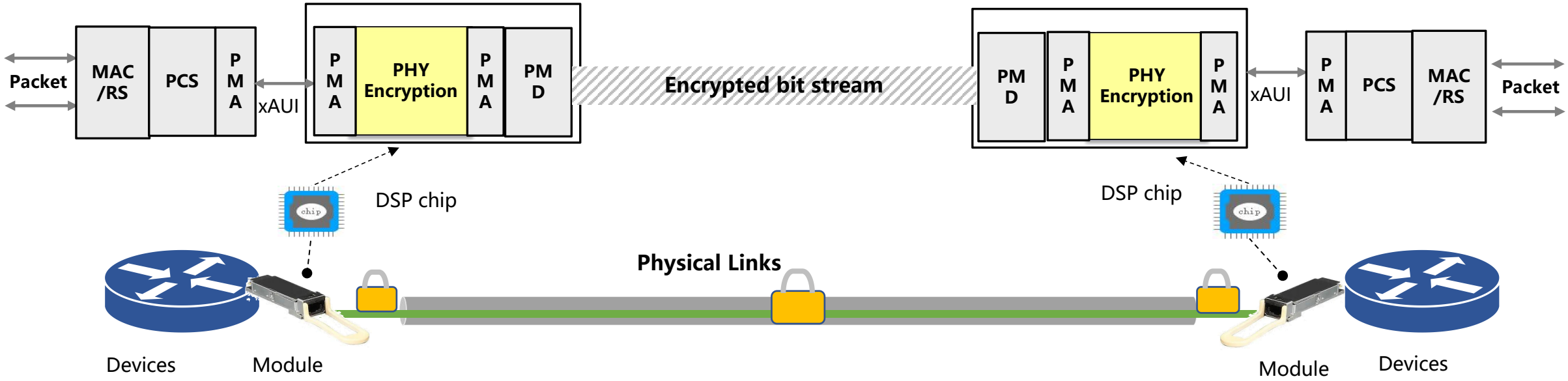
The existing solution: MACSec

- MACSec provides link security solution including confidentiality, data integrity, and data origin authenticity.
- The existing MACSec is mostly offloaded on the PHY chip to improve performance. It can even be implemented through the DSP chip of high-speed optical modules, such as 400GE or 800GE optical modules.
- However, it is necessary to perform back-to-back conversion (PCS and MAC) from bitstream to MAC frames in the chip, which will introduce additional implementation complexity, chip resources and conversion latency.
- SecTAG of MACSec also need encapsulation overhead. Especially in short-frame scenarios, it will significantly occupy bandwidth and affect the efficiency of high-bandwith services such as AI training.



The proposed solution: Security into PHY layer

- Physical layer encryption is not a novel idea. OTN has already implemented link encryption at its physical layer.
- The physical layer of Ethernet should also have its own security mechanisms. Integrating traditional cryptography methods with the Ethernet physical layer, where it involves encrypting and decrypting the bit stream.
- DSP of optical modules. Security features in plug and play, directly compatible with the current network equipment, enabling a rapid upgrade of the secure capabilities for the communication link.



Advantages

- **Full encryption of data link and other upper layers**. All packet data at the link and upper layer can be encrypted, including PFC/pause frame. Hiding the traffic frame length and transmission frequency
- **Lower latency**. There is no back-to-back conversion, and can be implemented with latency as low as tens of nanoseconds.
- **Without bandwidth overhead**. Using the reserved padding such as alignment marker to carry en/decryption parameters.
- **Compatible with existing devices**. Being implemented based on a DSP chip of an optical module, providing a pluggable solution that supports the rapid upgrade of link security in existing networks.

Summary

- Ethernet link security is becoming more and more important. New security mechanisms are needed to address these security requirements.
- Implementing data encryption and decryption at the physical layer of Ethernet can avoid back-to-back conversions, offering the extremely low latency, lower power consumption, and reduced costs.
- By implementing this in optical modules, it is possible to have plug-and-play security features, allowing for the rapid establishment of link security.

Thank you !