

# New Requirements and Challenges of Network Link Security

Weiqiang Cheng, China Mobile

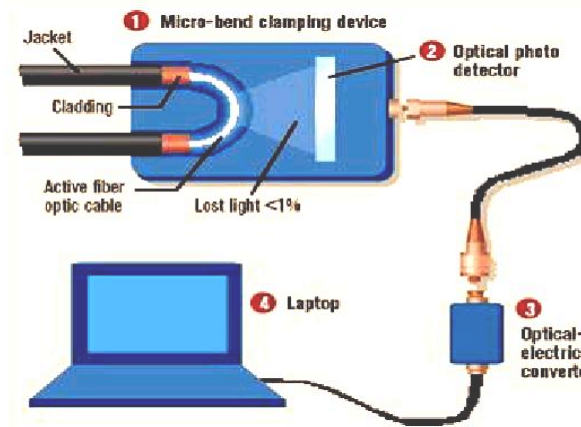
Haojie Wang, China Mobile

Jin Yang, China Mobile

# Network attacks may be anywhere and anytime



1100+ cyber attacks happened per second [1-2]



Eavesdropping by optical fiber bending [4]

**Eavesdropping is easy!**

Only **3** steps

- ① **Interception:** bending to refract light
- ② **Conversion:** optical signal to electrical signal
- ③ **Analysis**

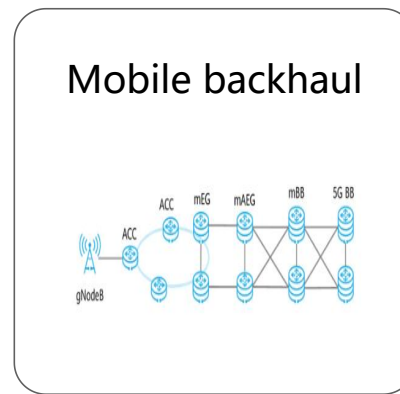
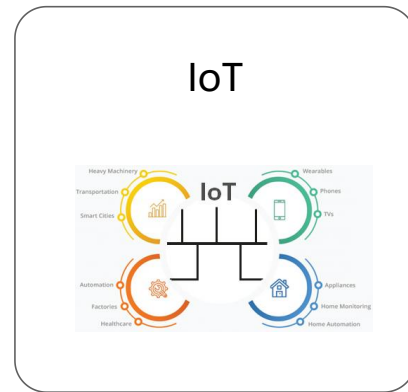
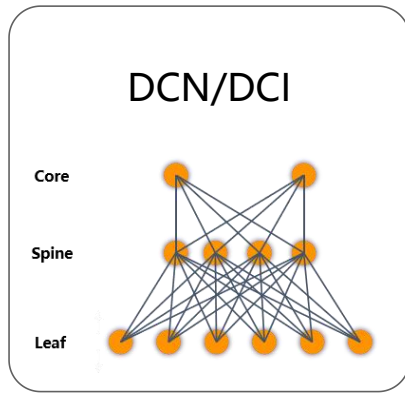
- *Network security is essential to protect network links and devices from potential threats. These threats can lead to network outages or sensitive data breaches.*

[1] <https://www.ciena.com/insights/articles/unlocking-the-macsec-puzzle.html> [2] <https://www.balbix.com/insights/attack-vectors-and-breach-methods/>

[3] <https://www.youtube.com/watch?v=0PXJH2UrcPA> [4] *Securing Fiber Optic Networks and Designed According to the Security Standards*

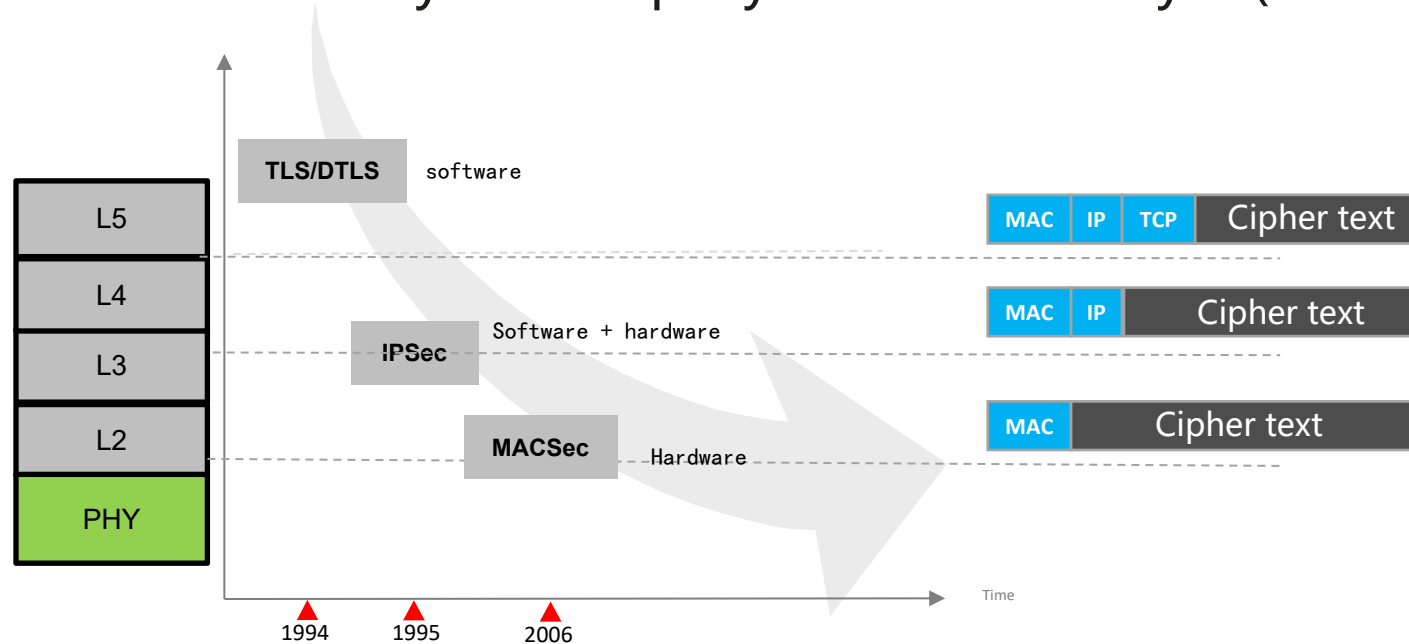
# Security requirements of many classical scenarios

- Many classical scenarios such as DCN/DCI, IoT, mobile backhaul, campuses, and telecom networks, etc., need security protection.
- More other scenarios...



# Existing standard security mechanisms

- Existing standard security mechanisms: TLS、IPSec、MACSec、...
- Trend:
  - Optimization of security in the same layer (e.g., MACSec, 802.1AE-→802.1AEdk)
  - Implementation of security from top layer to bottom layer (TLS-→IPSec-→MACSec).



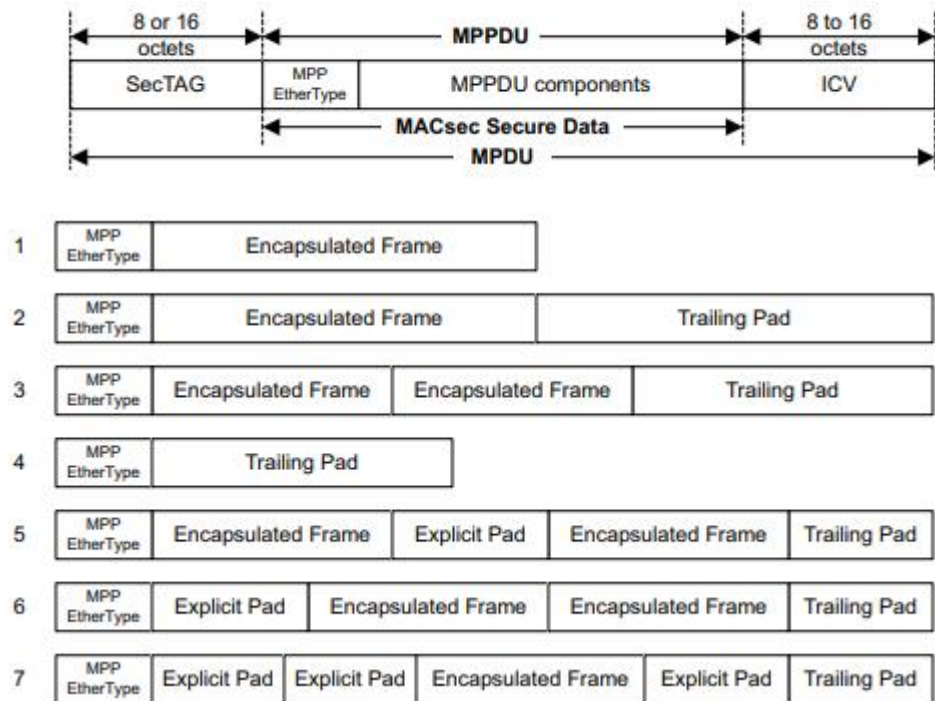
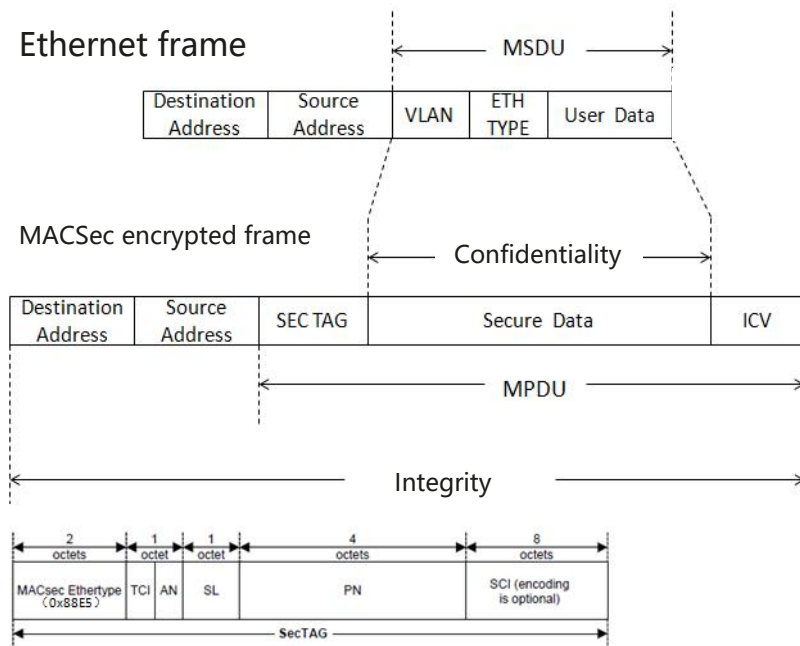
# IPSec and TLS

- IPSec/TLS are widely used in end-to-end scenarios.
- Usually software-based implementation. Not easy to chip implementation.
- After the rate reaches 100 Gbit/s+, the encryption capability cannot match the line-rate.  
The link throughput limitation imposed by encryption has become the biggest bottleneck for encryption application (<70%@1400B packet).

# Network Link Security: MACSec

## MACSec

- Has been used wildly in Ethernet at layer 2, standardized in 2006. Provides confidentiality, data integrity, replay protection, and data origin authenticity.
- Latest standard amendment of MACSec is 802.1AEdk, published in August 2023, to enhance the privacy protection.

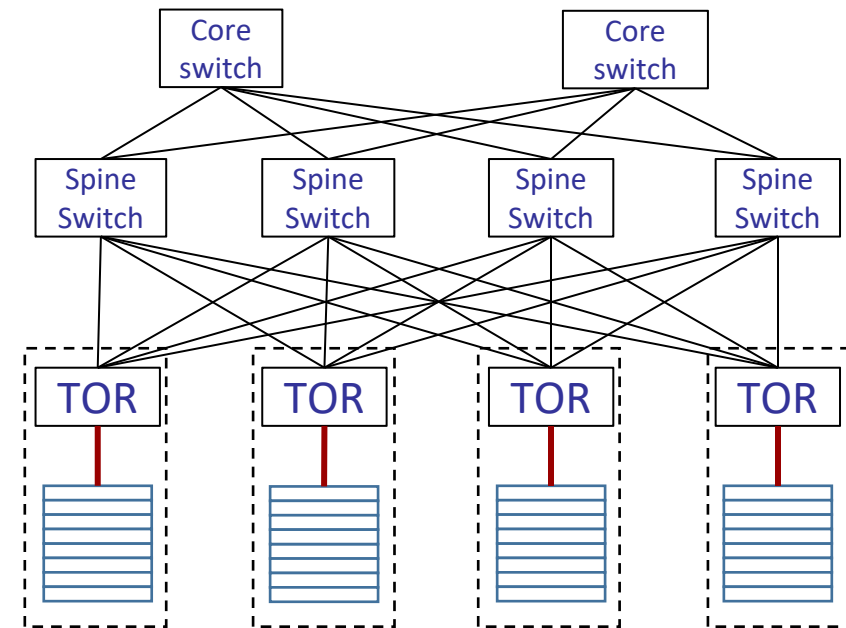


# New security requirements of AI Data center

- Security requirements:
  - Traditional data centers do not have security protection for eastbound-westbound traffic. After evolving to the AI data center, their sensitive assets such as models, parameters, and data may be disclosed.
  - Due to communication link and device port exposure, security protection needs to be enhanced in typical scenarios, such as network expansion and upgrade, frequent O&M, and **multi-tenant networking**.

**New scenario:  
intra-connection of AI  
Data center**

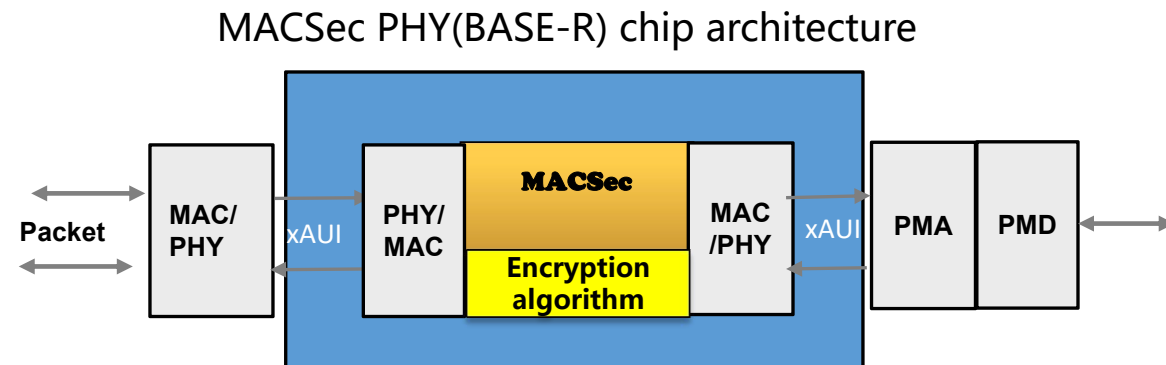
AI data center



- Performance requirements: **low latency (ns level)** and **high throughput (>95%)**

# Challenges

- ✓ MACSec can satisfy the security requirements.
- MACSec cannot satisfy the performance requirements of intra-connection in AI data center .
  - Have an impact on computing efficiency. latency  $>100\text{ns}@400\text{G}$ ; bandwidth utilization  $72.4\%@64\text{B}$
  - 802.1AEdk hides channel privacy at the cost of some added latency and additional chip resources.





# Future

- How to solve the link security problem with high performance requirements (such as AI data center, low latency, high throughput, low overhead)?

Thank you !