Layer 2 security for Precision time protocol frames for Automotive Ethernet

Verification challenges & solutions for PTP over MacSec.

Krunal Patel – Principle Product Engineer

Shubham Agarwal - Principal Software Engineer

Date: 09/11/2022

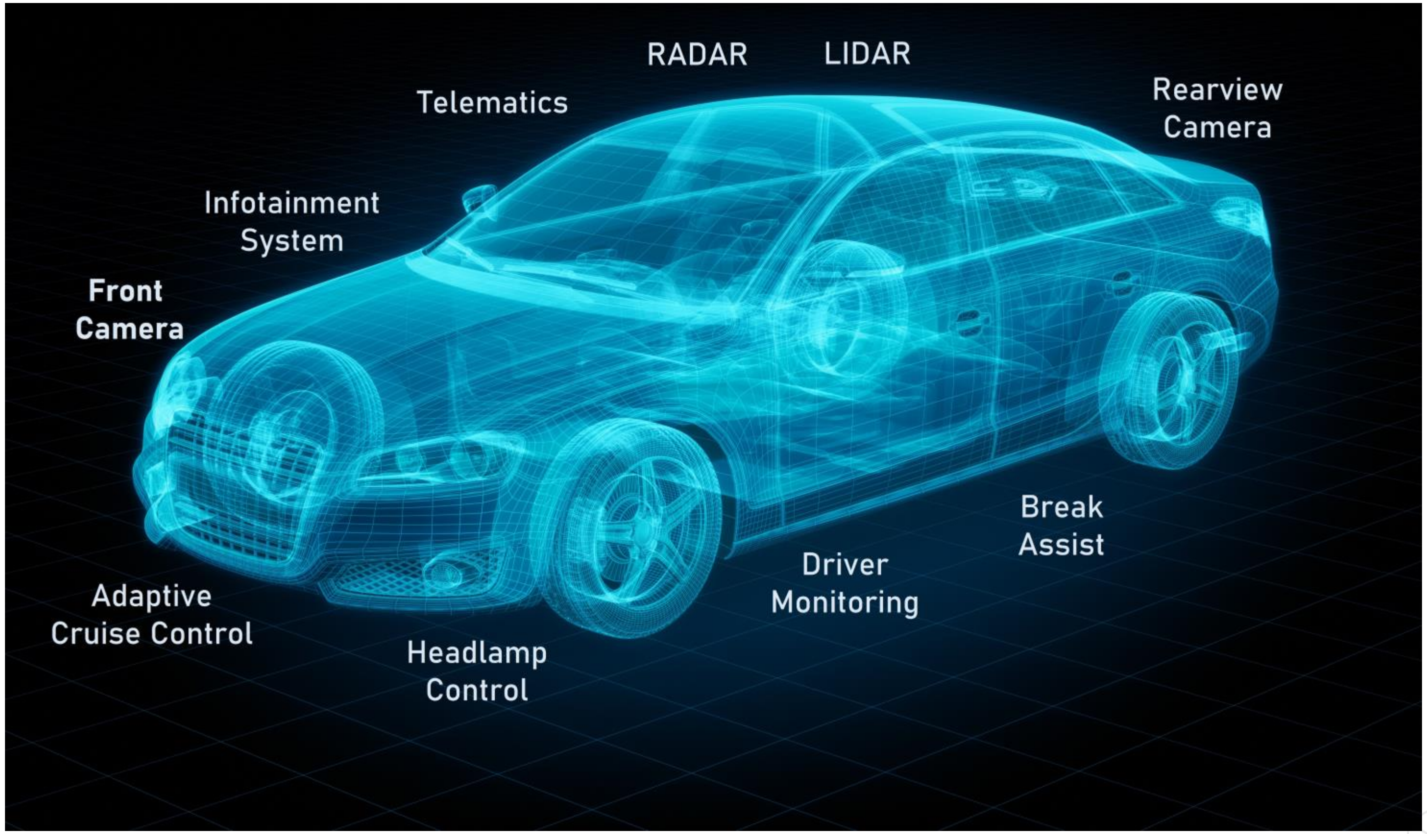
cadence®

Agenda

- Time Synchronization in Automotive Ethernet Networks
- Introduction to PTP
- Common security threats for Automotive Ethernet Network
- Introduction to MacSec
- MacSec overview and frame format
- Why does PTP over MacSec require in Automotive Ethernet
- Use Case: How PTP over MacSec can avoid the potential threat while maintaining timing accuracy
- Verification challenges for PTP over MacSec IPs
- Solution

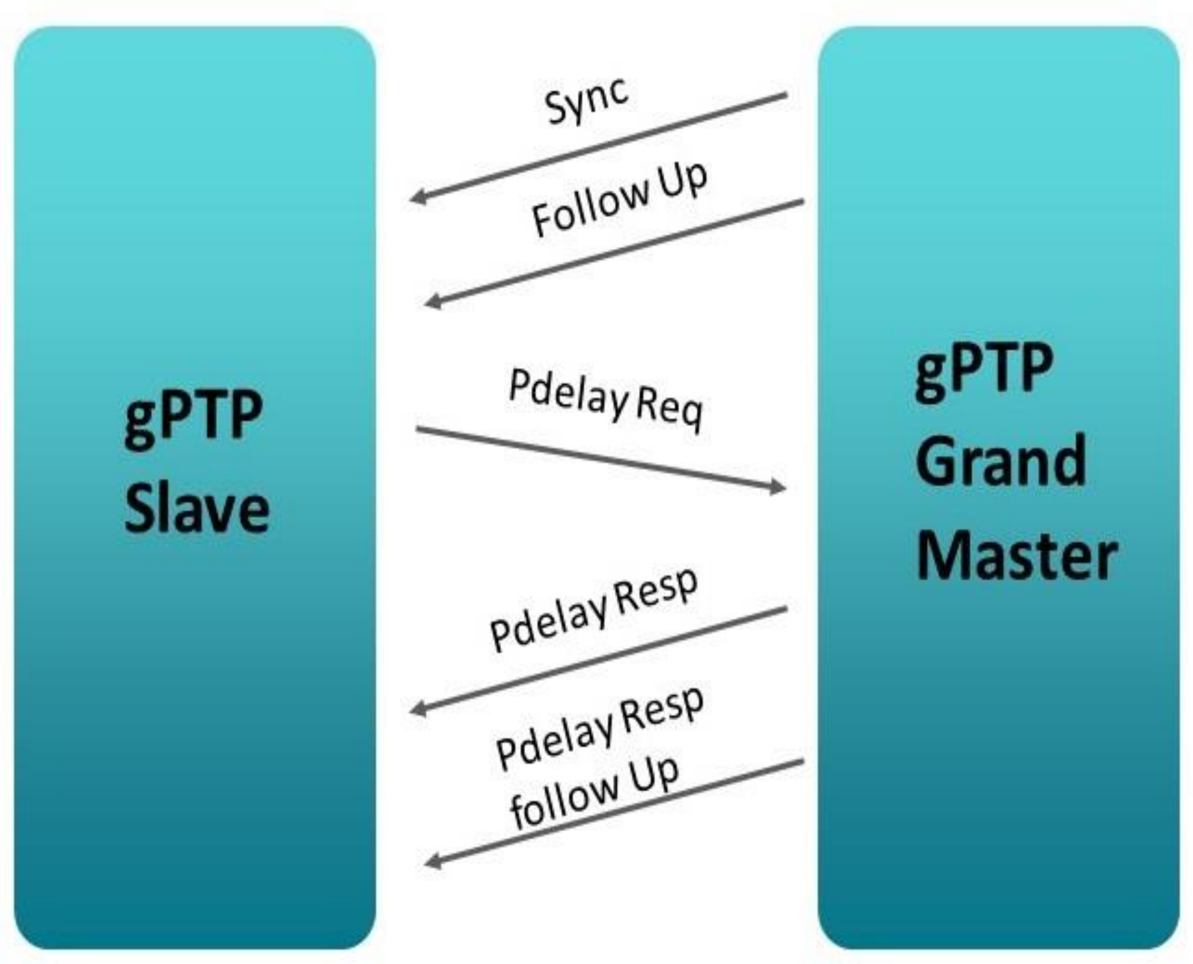
Time Synchronization in Automotive Ethernet Networks

- Time-critical Ethernet applications in the automobile
- Critical and time-sensitive components should be synchronized and have deterministic latencies
- Ethernet network should be synchronized with other Physical systems like CAN and FlexRay



PTP for Automotive Ethernet Networks

- “Generalized Precision Time Protocol” (gPTP) based on IEEE 802.1AS for time-synchronization
- SyncUp and FollowUp messages for synchronized time
- Pdelay messages to measure time between two node and “Time Aware System” detection
- Best Master Clock Algorithm (BMCA) to determine Grand Master



cādence®

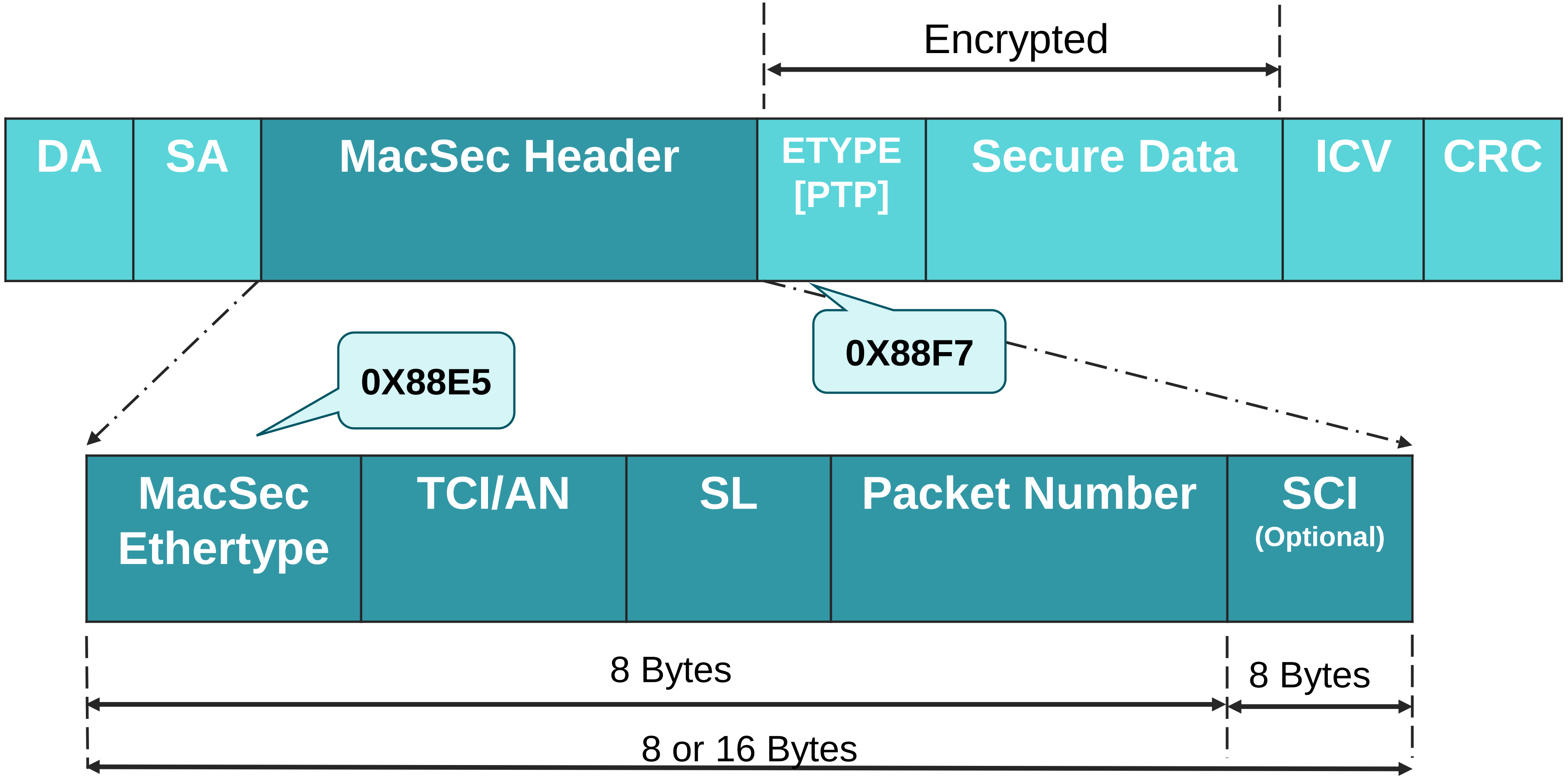
Common security threats for Automotive Ethernet Network

- Modifying frames/messages
- Sending random messages
- Replaying recorded messages
- Snooping data/messages and corruption
- Exploiting software bugs for attacks
- Installing harmful software/code

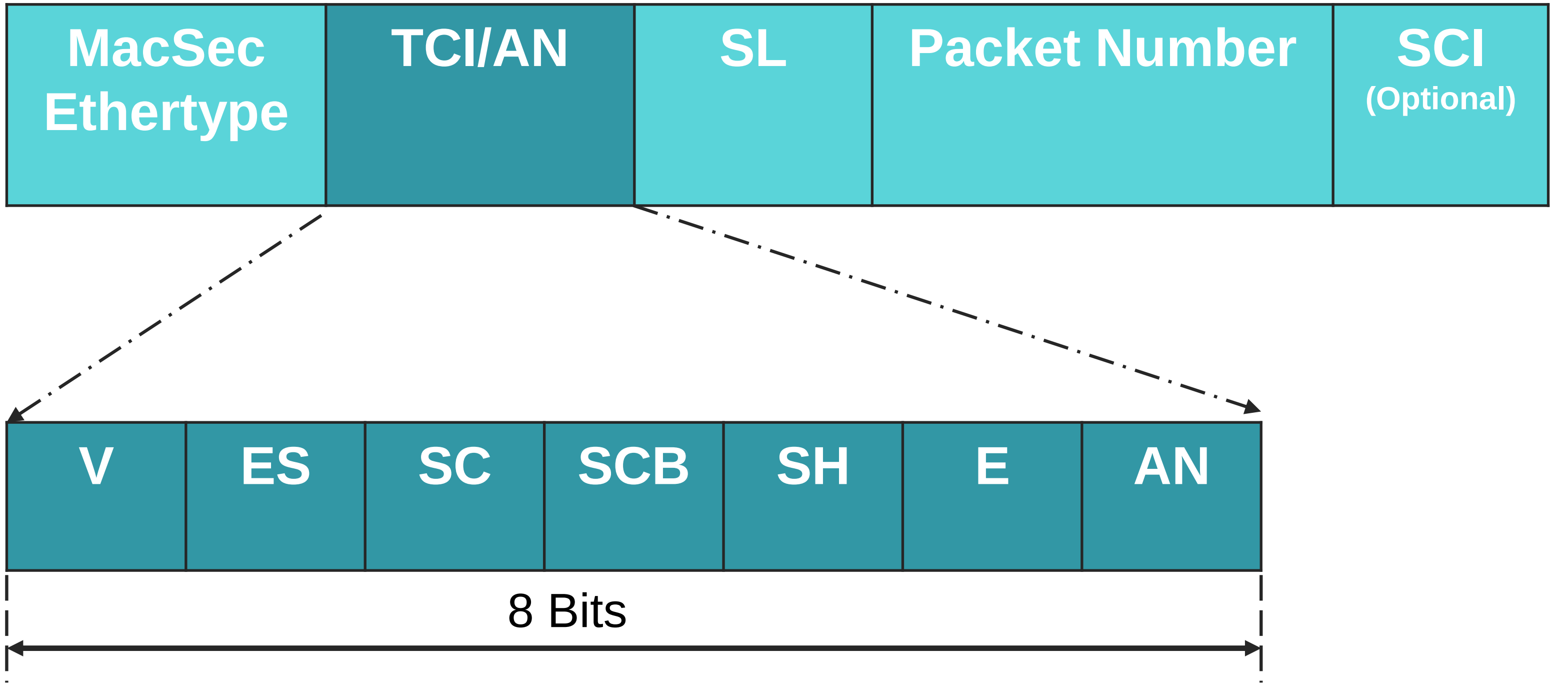
Introduction to MacSec

- MacSec stands for Media Access Control Security and is defined in IEEE 802.1AE provides Layer 2 (OSI data link layer) security.
- MacSec provides a bi-directional secure link between two devices
- In the Automotive Ethernet network, MacSec provides the link to link encryption and protection to the data passing over Electronic Control Units (ECUs) within the Vehicle
- MacSec facilitates the authorized system in a network to maintain the confidentiality of frame data and take action against a security breach.
- The MACsec protocol uses AES-GCM AES-GCM-128, AES-GCM-256, AES-GCM-XPN-128, AES-GCM-XPN-256
  AES-GCM (Advanced Encryption Standard, Galois Counter Mode)
  AES-GCM-XPN (Advanced Encryption Standard, Galois Counter Mode extended PN)

PTP Over MacSec Frame Format



TCI/AN Frame Format



MacSec Ethertype	TCI/AN	SL	Packet Number	SCI (Optional)

V	ES	SC	SCB	SH	E	AN

8 Bits

Why does PTP over MacSec require in Automotive Ethernet

- In Automotive networks, a need arises to protect the data transported on Electronic Control Units (ECUs).
- Automotive networks are prone to third-party wiretapping, infiltration, man-in-the-middle, and playback attacks due to inline connectors and internet/cloud connectivity of Vehicles.
- It is highly desirable to avoid disruption and data loss/leakage due to unauthorized transmission and reception in the automotive network.
- Since it’s not sensible to protect the entire network from physical access, one can save the network by layer security.

Why does PTP over MacSec require in Automotive Ethernet

- MacSec provides the link to link encryption and protection to the data passing over Electronic Control Units (ECUs) within the Vehicle.

- MACsec (IEEE 802.1AE standard) facilitates the authorized system in a network to maintain the confidentiality of frame data and take action against a security breach.

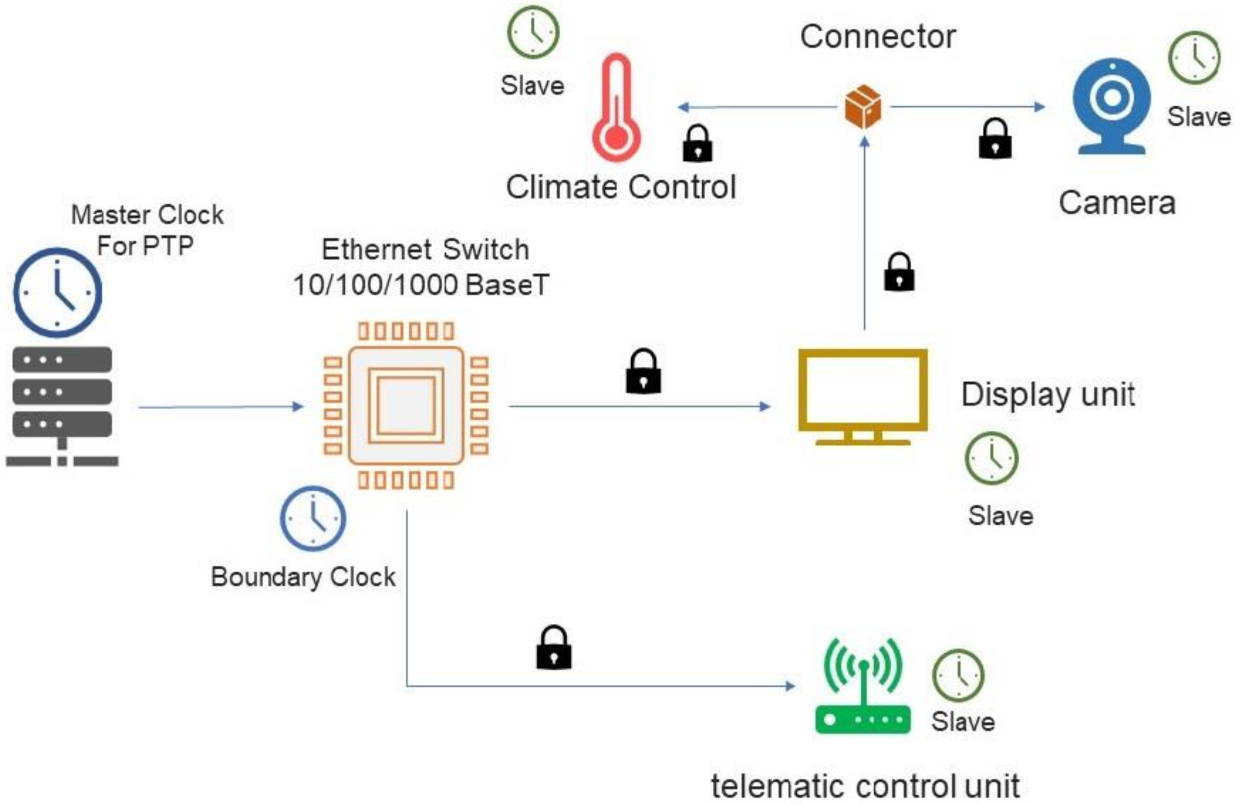
- MacSec protocol adds Security TAG (SecTAG), ICV (Integrity Check Value), Packet number fields, and encryption.

- Let’s check how these MacSec fields secure the network using these fields by a Use Case scenario.

Use Case : PTP over MacSec

when an attacker/ Hacker tries to snoop the data from the connector or tries to attack the device by pushing the false data/modify the information, MacSec will protect the network by,

- Data integrity
  - Checking ICV, the receiving node makes sure that data has not been changed/modified.
- Reply protection
  - using packet number, MacSec assigns a unique packet number to each packet and prevents sending duplicate messages.

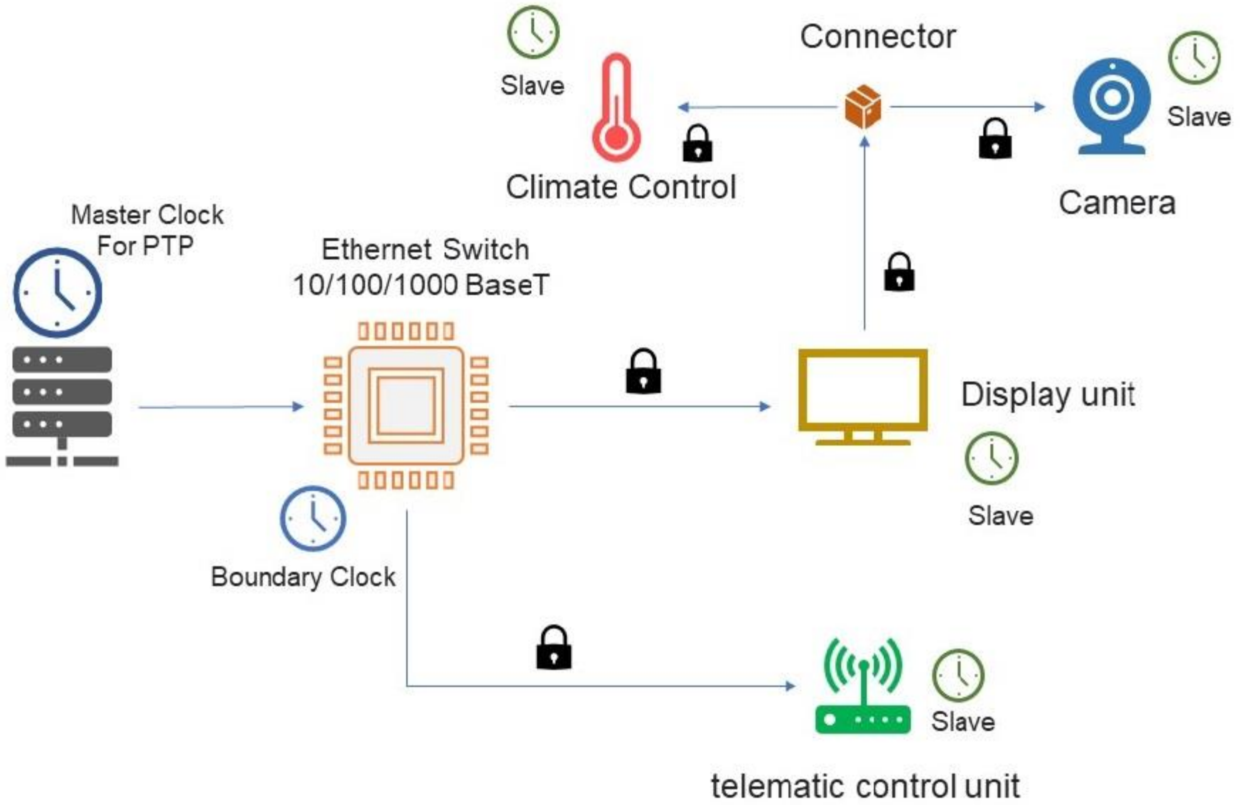


Security threat aversion using PTP Over MacSec for Automotive Ethernet

Continue…

Use Case : PTP over MacSec

- The Authenticity of link partner
    - Using Security tags, the receiving node ensures that an authentic link partner has sent data while identifying the third-party intrusion.
- Data encryption
    - The attacker will not be able to steal the information since it is encrypted. The transmitting node encrypts the payload using industry-standard cipher suites AES-GCM-128/256 and AES-GCM-XPN-128/256; only the nodes that possess the key can decrypt the data, hence Providing confidentiality.



Security threat aversion using PTP Over MacSec for Automotive Ethernet

Verification challenges for PTP over MacSec IPs

Considering data security and Time sensitiveness, “PTP over MacSec” IP is a crucial component of the Ethernet network, and flowless functional verification is expected. While discussing verification challenges of IP, the Verification engineer may face,

- MacSec encryption introduces highly variable delays, affecting the accuracy of PTP latency prediction.
- Length type issue, since Ethernet packets have one length type field, this field value is different for MacSec and PTP frames. So, accommodating both length type values in an ethernet frame is the topic of discussion.
- Placement and boundary identification of PTP frame within encrypted MacSec Ethernet frame payload creates challenges.

Continue…

Verification challenges for PTP over MacSec IPs

- Data integrity check & debugging of encrypted data.
- Thorough encryption logic verification is expected with all possible key values.
- All types of negative testing and verifying IP against possible network threat scenario is mandatory.
- Complete coverage closer, verification accuracy, and delay measurement are required for this IP.
- Debugging issues in latency-related scenarios on top of encryption logic may create challenges.

Solution

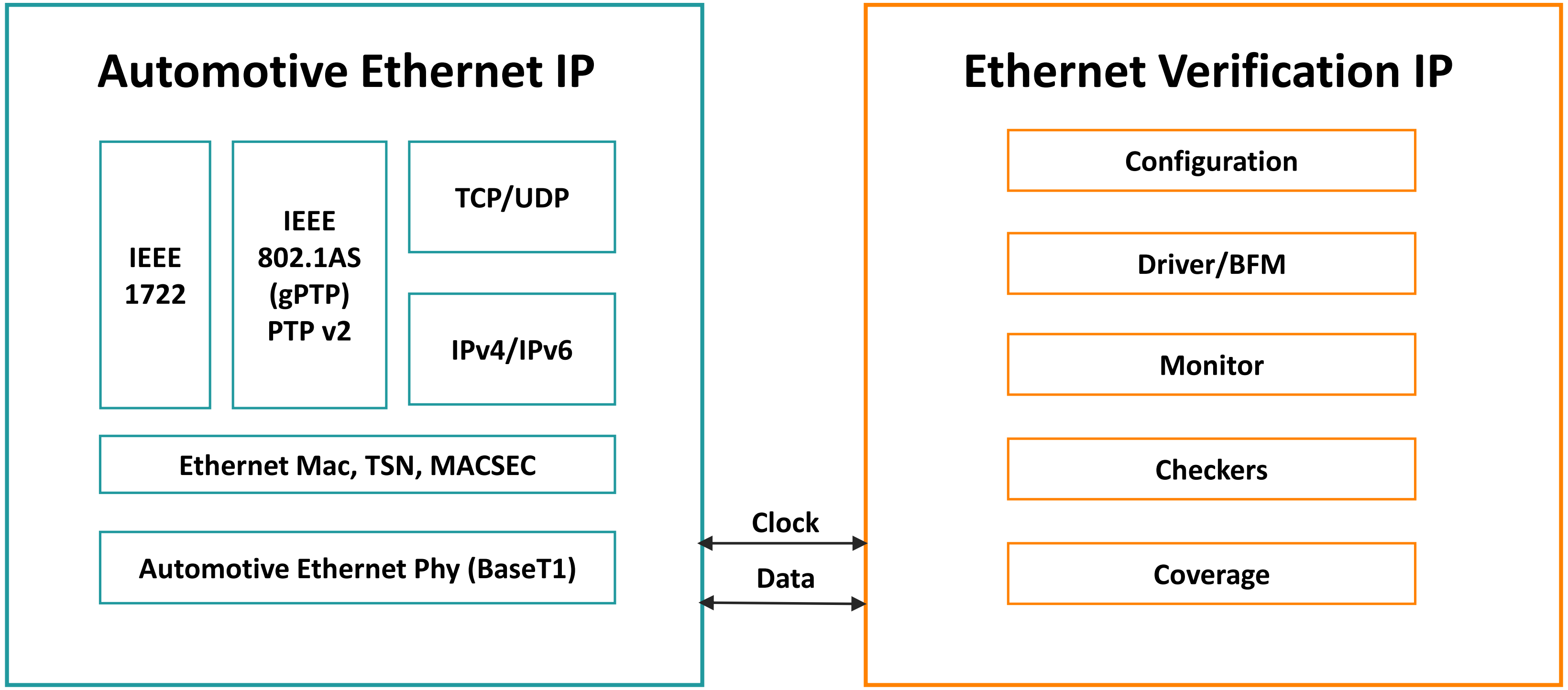
- Length-type issues can be resolved with mutual understanding. The Ethernet frame’s length type field can be set with MacSec values; while the PTP frame will be sent as a part of the Ethernet frame payload, the PTP length type field can be set as the first two-byte frame payload.

- Probes with complete control over ethernet packets at various levels of Verification IP can help the verification engineer snoop on the data for data integrity checks, debugging the complex issues, and error injection.

- Fully configurable security key and frame fields with the ease of randomization will help the varication engineer test the IP thoroughly.

- Inbuilt a rich set of coverage groups, automatic coverage report generation, and support from protocol experts make life easy for verification engineers.

Automotive Ethernet IP Verification Environment



Conclusion

With the Rapid adaptation of PTP over MacSec in Automotive Ethernet, a mature, competent and compliance verification solution for Automotive Ethernet helps reduce time to test, accelerate verification closure, and ensure end-product quality.

cadence®

Krunal Patel
Principle Product Engineer
krunalku@cadence.com
Cadence design systems
https://www.linkedin.com/in/krunal-patel-94a2104b

Shubham Agarwal
Principle Software Engineer
agarwals@cadence.com
Cadence design systems
https://www.linkedin.com/in/shubham-agarwal-8843a678