Technical White Paper

利用 MACsec 增强汽车以太网数据的机密性和完整性

Avtar Dhaliwal

摘要

随着现代车辆越来越依赖以太网进行关键通信，确保数据安全以防止未经授权的访问和篡改势在必行。汽车行业不断发展，以满足由先进电子系统和连接功能驱动的日益增长的网络安全需求。MACsec（媒体访问控制安全）通过加密和完整性检查提供强大的安全性，保护通过汽车以太网传输的数据。

随着车辆数据传输速度和带宽要求的提高，传统的安全措施已显得力不从心。MACsec 通过防止窃听、重放攻击和未经授权的器件访问来应对这些挑战，从而增强了车辆通信的安全性，并有助于实现更安全的驾驶体验。

内容

插图清单

表格清单

商标

1 MACsec 简介

媒体访问控制安全 (MACsec) 可确保以太网连接器件之间交换的数据受到保护。MACsec 由 IEEE 标准 802.1AE 定义，允许授权系统连接到网络中的 LAN 并进行互连，从而保持传输数据的机密性，并针对未经授权的器件传输或修改的帧采取措施。

MACsec 在 OSI 模型的第 2 层（数据链路层）运行。数据从之前的非结构化数据打包成帧，在数据链路层定义数据的格式。

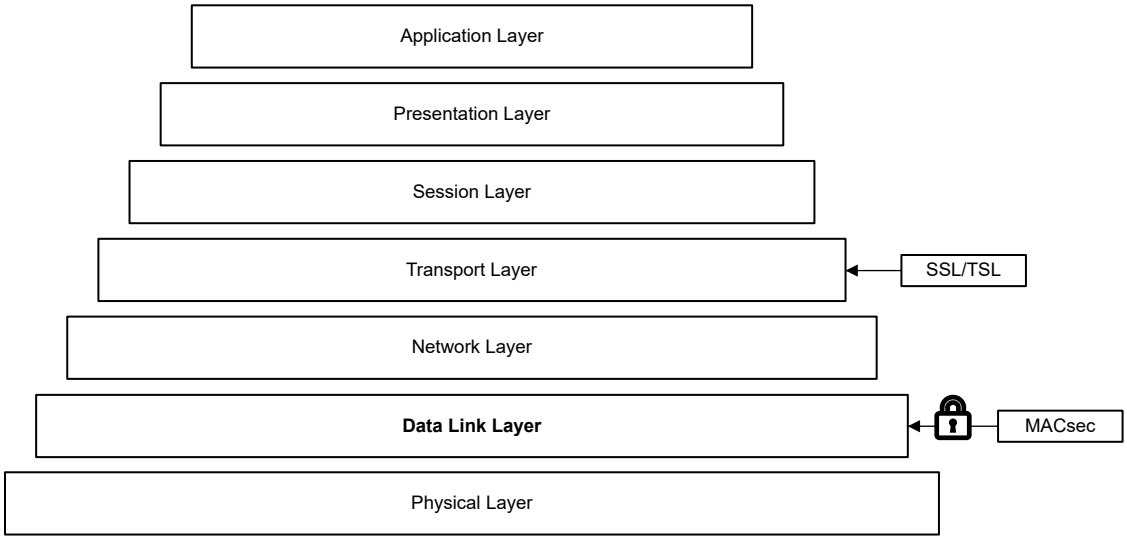

图 1-1. OSI 网络堆栈

在 MACsec 之前，SSL 和 TLS 等安全协议已被广泛使用，但其在软件层运行，这带来了挑战。这些协议需要 SoC 提供大量的 CPU 和内存资源，因此可能降低性能。

如果启用 MACsec，在两个连接的器件之间交换和验证安全密钥后，会建立双向安全链路。利用数据完整性检查和加密的组合来保护传输的数据。

发送器件将唯一的 MACsec 标头附加到所有要发送的以太网帧，对帧内的数据有效载荷进行加密。接收器件会检查标头和尾部的完整性。如果检查失败，流量会被丢弃。如果检查成功，帧则会被解密。

2 MACsec 在汽车安全中的关键作用

2.1 实际应用

在汽车行业，对以太网通信的日益依赖产生了许多可以利用的漏洞：

- **电子控制单元 (ECU)**
  控制制动、转向和发动机管理等车辆基本功能的各种 ECU 之间的通信。
- **高级驾驶辅助系统 (ADAS)**
  实时数据交换，实现防撞、车道保持辅助和自适应巡航控制等功能。
- **车身控制**
  监测和控制车身的各种电子配件。锁上车门、安全带警告系统或调暗车内照明。

2.2 常见安全威胁

在当今互连的世界中，以太网应用容易受到多种外部安全威胁的影响：

- **窃听**
  拦截未知方通过网络传输的数据。
- **中间人攻击**
  插入两个器件之间的通信，可能会篡改或窃取数据。
- **重放攻击**
  捕获和重新传输数据包，产生未经授权的效果。
- **未经授权的访问**
  没有适当凭据的器件访问网络，可能会获取敏感信息。

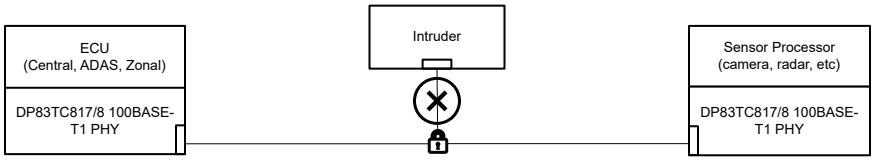

图 2-1. 外部威胁

2.3 MACsec 安全措施

- **加密**
  MACsec 会在数据链路层加密数据，以防止窃听，确保未经授权的各方无法读取截获的数据。
- **完整性检查**
  MACsec 会对所有数据帧进行完整性检查，检测任何未经授权的修改，确保数据在传输过程中未被篡改。
- **身份验证**
  MACsec 会在建立安全链路之前要求器件进行身份验证，防止未经授权的器件加入网络。
- **重放保护**
  MACsec 会在数据帧中添加序列号和时间戳，以 降低重放攻击的风险。

3 MACsec 如何在系统中工作

MACsec 在链路层提供加密功能，而 IEEE 802.1X 则提供了一种对希望加入网络的器件进行身份验证的方法，确保只有受信任的器件才能访问网络。MACsec 使用一种称为 EAPOL 的协议来处理身份验证过程，在 MACsec 中，MKA 协议有助于安全交换密钥以进行加密通信。

为使 MACsec 正常工作，SoC 必须具有专用数据库来存储连接关联密钥 (CAK) 和连接关联密钥名称 (CKN)。在许多实现中，SoC 依靠 WPA Supplicant 来管理 CAK-CKN 数据库，以便与更高级别的身份验证协议和网络安全标准集成。

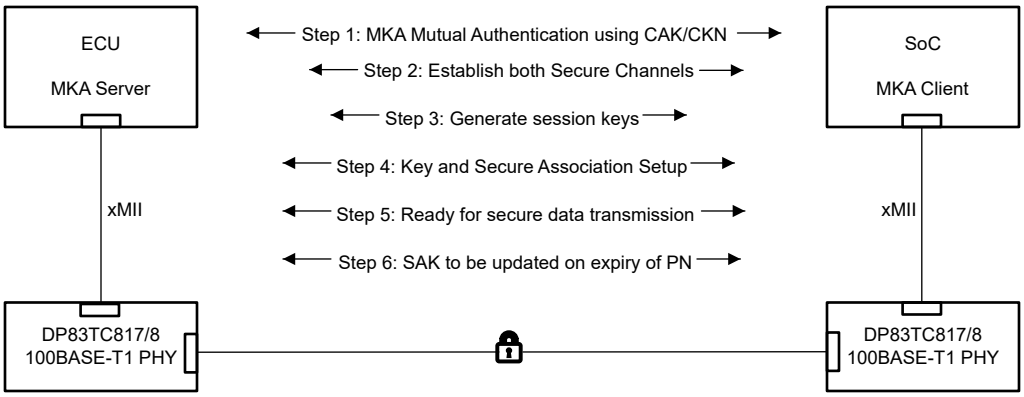

图 3-1. MACsec 系统架构

表 3-1. MACsec 关键术语

MACsec 术语	定义
CKN/CAK	CKN（连接关联密钥名称）和 CAK（连接关联密钥）由用户配置，必须在链路两端匹配才能初始启用 MACsec。这必须在两个处理器上预设。CAK 是一个 32 十六进制或 64 十六进制密钥。CKN 是长度不超过 32 个字符的十六进制数字字符串。
SecY	表示网络器件上启用 MACsec 的端口或接口的实体。
安全通道 (SC)	通常是两个节点之间的逻辑连接。该连接为 MACsec 提供了安全的通信路径。负责管理 MACsec 密钥和多个 Secy 的安全关联。
安全通道标识符 (SCI)	与每个 SC 关联。这是传输器件的 MAC 地址和端口标识符的组合。与每个 SecY 关联，用于标识 MACsec 会话中的参与者。
安全关联 (SA)	表示两个 MACsec 器件之间的安全关联，SA 定义了用于保护器件之间通信的算法和密钥等安全参数。每个安全通道包含两个安全关联。还包含数据包编号。
安全关联密钥 (SAK)	用于保护 SA 中器件的加密密钥。SAK 是动态生成的，在器件之间分发。SAK 使用 AES-GCM 算法对数据帧进行加密和解密，在 MKA 过程中推导出来，且在特定安全通道中是唯一的。

4 MACsec 块

以太网帧是数据链路层的数据单元，是底层以太网物理层传输机制。每个以太网帧都以以太网标头开始，其中包含目标和源 MAC 地址作为前两个字段。帧的中间部分是有效载荷数据，包括帧中携带的其他协议的标头。帧以帧校验序列 (FCS) 结束，该序列用于检测任何传输中的数据损坏。

- 目标 MAC 地址：6 字节 - 标识收件人。
- 源 MAC 地址：6 字节 - 标识发件人。
- EtherType 或长度：2 字节 - 指示有效载荷的类型或长度。
- 有效载荷：N 字节 - 正在传输的数据。
- 帧校验序列 (FCS)：4 字节 - 确保数据完整性的错误检查代码。

MACsec 为标准以太网帧增加了安全功能。以下是 MACsec 帧的结构：

- 目标 MAC 地址：6 字节
- 源 MAC 地址：6 字节
- SecTAG：8-16 字节 - 安全标签，包括关键信息和安全参数。
- 有效载荷：N 字节（加密数据）
- 完整性检查值 (ICV)：8 或 16 字节 - 确保数据的完整性。
- 帧校验序列 (FCS)：4 字节

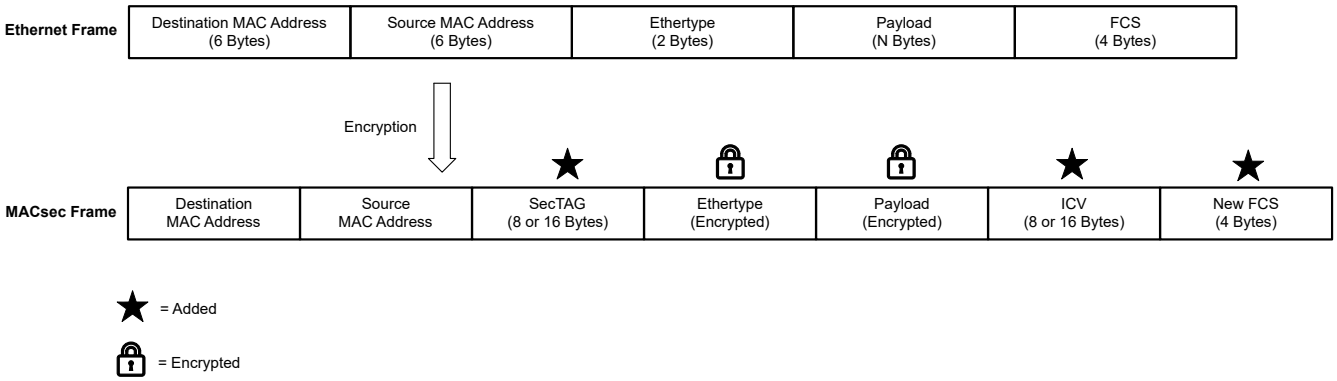

图 4-1. 未加密的以太网帧与 MACsec 以太网帧

SecTAG 是 MACsec 帧的关键组成部分，提供了基本的安全信息。包含以下内容：

- EtherType：2 字节 - 表示该帧是 MACsec 帧。MACsec ethertype 为 0x88e5。
- TAG 控制信息 (TCI/AN)：1 字节 - 包含多条信息，例如加密/机密性存在和关联号。
- 数据包编号 (PN)：4-6 字节 - 通过对帧进行编号来防止重放攻击。
- 短长度 (SL)：1 字节 - 指示有效载荷的长度（可选）。
- SCI（安全通道标识符）：8 字节 -唯一标识安全通信通道。

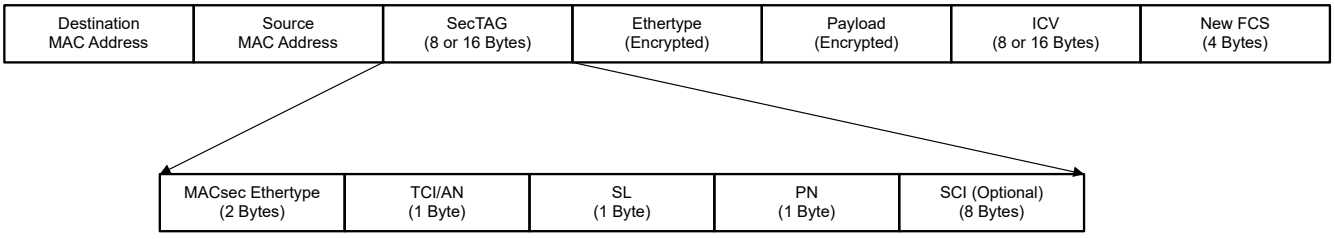

图 4-2. MACSEC SecTAG

在 MACsec 帧中实现的 MACsec 功能：

- EtherType：在普通帧和 MACsec 帧中，EtherType 字段表示有效载荷的类型。对于 MACsec，它明确标识该帧包含 MACsec 数据。
- SecTAG：

  - SCI：安全通道标识符确保帧属于特定的安全通道。
  - AN：区分同一通道内的不同安全关联，允许同时进行多个安全连接。
  - PN：确保每个帧都有唯一的编号，防止重放攻击。
- 有效载荷：在 MACsec 帧中，有效载荷是加密的。确保传输数据的机密性。
- ICV：通过确保帧在传输过程中未被更改，来确保完整性。使用预共享密钥在整个帧（FCS 除外）上计算加密校验和。

5 物理层 MACsec

DP83TC817 可在物理层实现稳健的 MACsec，在整个系统中提供了显著的优势。

- 从 SoC 卸载加密和解密任务可减少系统资源消耗，从而降低成本并释放 SoC 用于其他关键功能。
- 在物理层上实施 MACsec 可优化整体性能，提供更精简、更安全的数据流，同时最大限度地减少延迟。

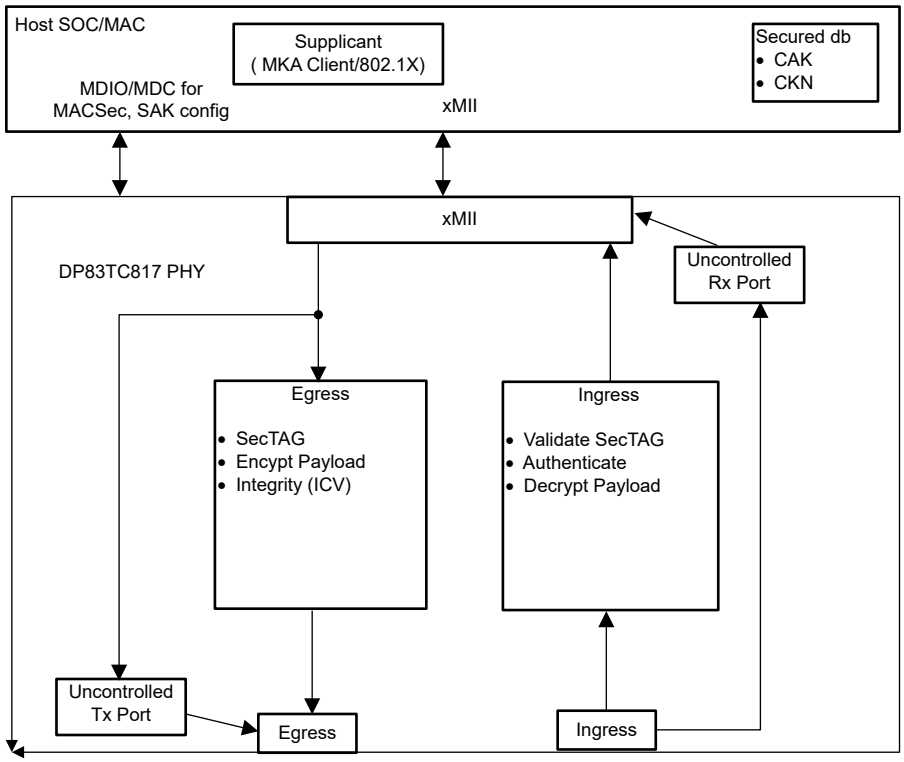

图 5-1. MACsec 以太网物理层

DP83TC817 支持的 MACsec 功能：

- 线速身份验证和加密
- 密码套件：GCM-AES-XPN-128/256、GCMAES-128/256
- 安全通道：总共 16 个 SAK，实现 8 个 Tx/Rx SC
- 支持 SAK 自动翻转
- 窗口重放保护

6 结语

随着汽车行业朝着集成更多电子系统和复杂连接功能的方向发展，对强大安全性的需求变得更加重要。

MACsec 为汽车以太网网络安全提供了全面的设计，提供加密和完整性检查来保护数据安全。通过解决窃听、重放攻击和未经授权访问等漏洞，MACsec 可确保车辆内通信的安全性和可靠性。

重要通知和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的相关应用。 严禁以其他方式对这些资源进行复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265