

基于国密算法的车载以太网控制器身份认证方法

郭辉^{1,2}, 罗勇³, 郭晓潞³

(1. 清华大学车辆与运载学院, 北京 100084; 2. 智己汽车科技有限公司, 上海 201804; 3. 联合汽车电子有限公司, 上海 201206)

摘要: 随着智能网联汽车的发展, 车载以太网的信息安全成为汽车行业关注的重点。安全认证是保证车载以太网信息安全的关键技术之一。现有的车载以太网认证技术难以兼顾安全性和车载控制器性能要求。国密算法在车载网络信息安全的应用逐渐成为趋势, 但在车载以太网领域的应用研究还处于起步阶段。为了满足车载控制器相对较低的性能和车载以太网的安全要求, 提出了基于国密算法的两阶段信任链车载以太网控制器身份认证方法。该身份认证方法可适用于车载以太网不同的网络拓扑架构, 通过基于认证凭证的信任链将车载以太网控制器身份认证的初始化阶段和车辆使用阶段进行关联。初始化阶段认证在整车下线首次安装控制器或售后更换控制器时, 由整车厂诊断仪触发。在初始化阶段, 基于复杂的 SM2 国密算法和身份证书建立完整认证。车辆使用阶段认证在每次车辆重新上电或网络唤醒时, 由以太网网关触发。在车辆使用阶段, 基于 SM4 对称国密算法和认证凭证信任链建立快速认证。认证凭证通过认证凭证函数生成, 并且每一次认证凭证都基于之前成功认证的随机会话编号动态产生, 形成信任链。基于车载以太网控制器进行了测试验证, 测试结果表明, 该方法资源占用较低并具有较高的安全性, 能够同时满足车载以太网控制器身份认证性能和安全两方面的需求。

关键词: 车载以太网; 身份认证; 两阶段信任链; 国密算法

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022079

Automotive ethernet controller authentication method based on national cryptographic algorithms

GUO Hui^{1,2}, LUO Yong³, GUO Xiaolu³

1. School of Vehicle and Mobility, Tsinghua University, Beijing 100084, China

2. IM Motors Technology Co., Ltd, Shanghai 201804, China

3. United Automotive Electronic Systems Co., Ltd., Shanghai 201206, China

Abstract: With the development of intelligent and connected cars, cyber security of automotive ethernet becomes the focus of automotive industry. Authentication is one of the key technologies for automotive ethernet security. The existing authentication methods have shortcomings to meet the requirements of both safety and electronic controllers' performance. Besides, national cryptographic algorithms are becoming a trend for automotive network

收稿日期: 2022-05-05; 修回日期: 2022-09-05

通信作者: 郭辉, guohuil8@mails.tsinghua.edu.cn

引用格式: 郭辉, 罗勇, 郭晓潞. 基于国密算法的车载以太网控制器身份认证方法[J]. 网络与信息安全学报, 2022, 8(6): 20-28.

Citation Format: GUO H, LUO Y, GUO X L. Automotive ethernet controller authentication method based on national cryptographic algorithms [J]. Chinese Journal of Network and Information Security, 2022, 8(6): 20-28.

security, while the related research in automotive ethernet area is still in starting phase. In order to balance the limited computing performance of electronic controllers and high security requirements of automotive ethernet, a two-stage trust chain authentication method based on national cryptographic algorithms was proposed. The method can be used in different automotive ethernet topologies. A trust chain was built up based on authentication credentials, which linked the two authentication stages, namely the initial stage and the vehicle using stage. The initial stage was triggered by diagnosis instrument at end of line or controller replacement. It deployed complete authentication based on SM2 algorithm and certificates in the initial stage. The vehicle using stage was triggered by ethernet gateway at vehicle power-on or network wakeup. In this stage, the method deployed fast authentication based on SM4 algorithm and authentication credential trust chain. The authentication credentials for trust chain were generated by credential functions. In order to ensure security, each credential was generated based on last successful authentication parameters dynamically. The test results on automotive ethernet controllers show that the method has lower computing cost and higher security level, and it can guarantee both performance and security.

Keywords: automotive ethernet, authentication, two-stage trust chain, state cryptographic algorithms

0 引言

随着智能网联汽车的发展, 车内网络对数据传输的网络带宽需求持续上升。传统汽车主干网通常使用 CAN 总线, 带宽可以达到 5 Mbit/s, 但已经不能满足智能网联汽车中摄像头图像、激光雷达点云、信息娱乐高清视频等高带宽数据传输要求; 而车载以太网可以实现 1 Gbit/s 甚至更高的网络带宽, 逐渐成为车内主干网^[1-2]。与此同时, 智能网联汽车对信息安全提出了更高要求^[3]。相较于传统汽车, 智能网联汽车的攻击入口更多, 并且被黑客攻击后破坏效果更大, 有可能导致车毁人亡, 甚至是大面积道路交通瘫痪^[4-5]。因此, 相关信息安全标准日趋严格。我国《汽车产业中长期发展规划》中明确提出以网络安全为重点。同时, 汽车行业正在积极推动国密算法和相关芯片的应用, 这对于提升汽车行业的整体网络安全有着积极意义。

车载以太网作为车内主干网, 其信息安全成为行业关注的重点。与互联网领域的以太网应用相比, 车载以太网的应用环境有其自身的特点。1) 由于成本受限, 车载控制器的计算性能相对较低。2) 智能网联汽车的信息安全要求高。安全认证是保证车载以太网信息安全的关键技术之一。

本文提出了一种基于国密算法的两阶段信任链认证方法来保证车载以太网的信息安全, 并且能够在性能有限的控制器上有效运行, 满

足车载以太网控制器身份认证性能和安全两方面的需求。

1 研究现状

1.1 车载以太网认证技术现状

车载以太网认证技术目前主要包括两种类型。第一种是通过消息认证码实现通信数据认证。典型代表是 AUTOSAR 标准中推荐的 SecOC 方法^[6], 针对需要保护的通信数据基于对称加密生成消息认证码, 接收方通过校验消息认证码实现认证。其优点是简单, 并且认证信息与通信数据可以同步传输; 缺点是基于对称加密, 安全性较低, 并且没有对通信内容加密, 难以防止窃听攻击。

第二种类型是基于认证协议对车载以太网控制器进行身份认证。目前行业内研究的车载以太网身份认证协议主要参考互联网领域认证协议, 如口令认证协议、挑战握手认证协议、可扩展认证协议(EAP-TLS/TTLS)及 Kerberos 协议等。口令认证、挑战握手等协议简单但安全性低, 难以满足车载以太网安全要求。EAP-TLS/TTLS^[7-9]、Kerberos^[10-11]等协议安全性高, 但认证过程复杂, 在车载以太网控制器资源有限的情况下, 难以满足应用实时性要求。为了保证安全, 在汽车使用阶段至少需要在每次车辆上电时完整进行一次以太网控制器身份认证。车辆上电到车辆启动运行的时间通常需要控制在 500 ms 以内^[12], 超出此时间范围会直接影响驾驶员操作。Zelle 等^[9]基于

TLS 协议在车载以太网中的应用进行了研究, 基于 ECC 非对称加密算法进行身份认证, 建立认证的握手时间超过 2 s。

1.2 汽车领域国密算法应用现状

国家密码管理局于 2012 年正式发布了自主设计的国密算法行业标准 (包括 SM2 椭圆曲线公钥密码算法、SM3 密码杂凑算法、SM4 分组密码算法等), 该标准于 2016 年成为国家推荐标准^[13-15]。国密算法首先在金融领域应用, 并逐步在互联网、工业控制、汽车等各个领域开始推广应用。近年来, 中国汽车厂商在车载网络信息安全需求中开始加入国密算法的需求, 国密算法的应用成为趋势。在国密算法车载应用方面, 吴志红等^[16]基于英飞凌 Aurix 芯片对 SM2、SM4 等国密算法与国际密码算法 ECC256、AES 进行了对比研究。修志鹏等^[17]结合 SecOC 研究了 SM4 国密算法在 CAN 总线通信数据加密方面的应用。国密算法在车载以太网相关应用领域尚处于起步阶段。

2 基于国密算法的车载以太网身份认证

为了保证车载以太网的信息安全, 本文提出了一种基于国密算法的车载以太网控制器身份认证方法, 该方法能够在性能有限的车载控制器上有效运行。本文的研究基于图 1 中的以太网拓扑架构 1 进行, 同时适用于更加集中的架构 2 和架构 3。

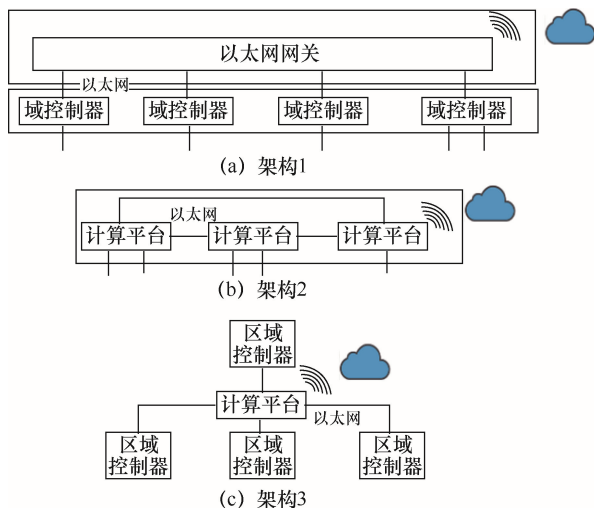


图 1 身份认证方法适用的车载以太网架构
Figure 1 Automotive ethernet network topologies applicable to method authentication

将车载以太网控制器作为研究对象, 结合威

胁建模和攻击树分析方法, 识别出的车载以太网安全风险清单见表 1^[18-19]。车载以太网控制器身份认证作为必要的基础防护措施, 可以实现对篡改、窃听、拒绝服务、重放和注入攻击的安全防护。

表 1 车载以太网安全风险清单
Table 1 Automotive Ethernet security risk list

编号	攻击类型	攻击路径	攻击影响
1	篡改	篡改通信程序/数据	植入恶意代码/数据
2	窃听	接入窃听控制器	窃取秘密数据
3	拒绝服务	发送大量无效消息	无法正常通信
4	重放	播放录制消息	触发错误的响应
5	注入	注入错误消息	触发错误的响应
6	拦截	断开连接/时延发送	无法/时延正常通信

针对车载以太网的特点, 本文提出了基于国密算法的两阶段信任链安全认证方法: 在初始化阶段, 基于 SM2 国密算法和身份证书建立完整认证; 在使用阶段, 基于 SM4 对称国密算法和认证凭证信任链建立快速认证; 初始化阶段和使用阶段与基于认证凭证的信任链相关联, 每一次认证凭证都基于之前成功认证的随机会话编号生成。

该方法的车载以太网安全身份认证系统如图 2 所示。由汽车整车厂建立一套密钥管理服务器, 实现智能网联汽车系统和零部件 (包括诊断仪、以太网网关、域控制器) 的数字证书签发和密钥管理工作, 整车厂公私钥由整车厂密钥管理服务器生成和存储, 此服务器安全性符合 ISO 27001 要求。诊断仪、以太网网关和域控制器中具有硬件安全芯片, 带有硬件安全模块 (HSM, hardware security module), 具备防数据非法篡改和读取能力。诊断仪和车辆生产时, 在诊断仪、以太网网关和域控制器安全芯片中基于 SM2 算法生成公私钥, 并将公钥导出给整车厂密钥管理服务器, 使用整车厂私钥签名生成证书, 并发放给对应零部件, 写入安全芯片中。本文提出的车载以太网身份认证功能通过诊断仪、以太网网关、域控制器之间的交互来实现。诊断仪发送指令触发以太网网关和域控制器进入初始化阶段身份认证模式, 并在初始化完成后将身份认证切换为使用阶段身份认证模式。以太网网关作为车内认证中心, 车内各个域控制器分别与以太网网关完成身份认证, 以此为信任基础实现以太网域控制器之间的身份认

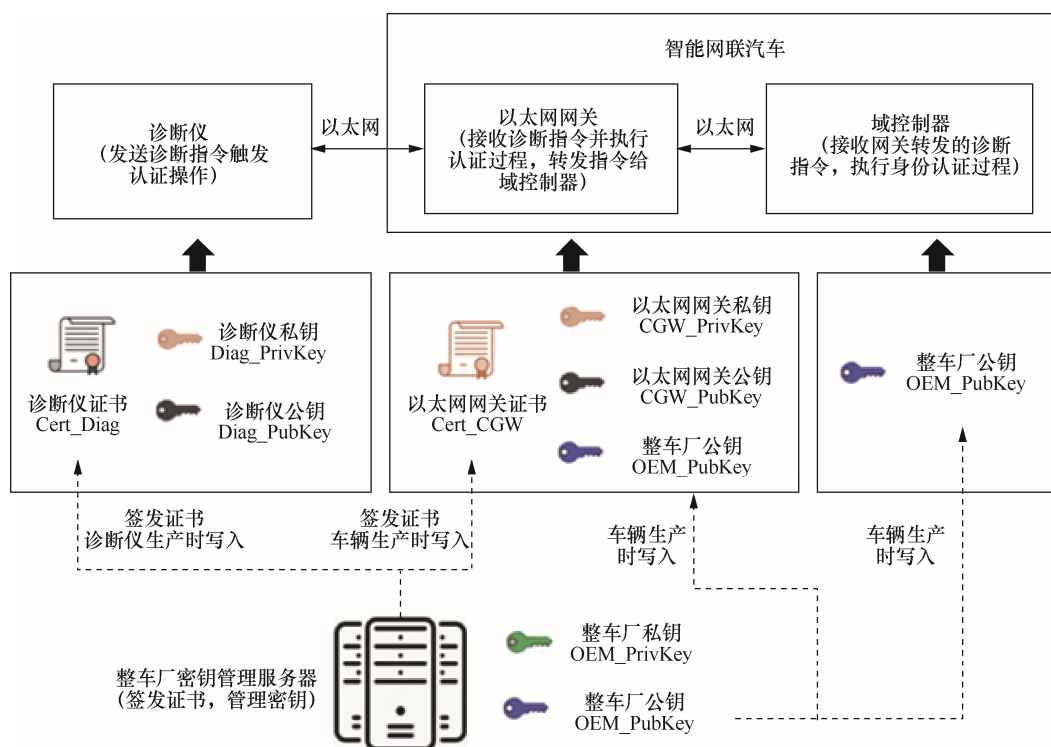


图2 车载以太网安全身份认证系统
Figure 2 Automotive ethernet authentication system

证。以太网网关和域控制器在初始化阶段身份认证模式生成初始认证凭证，并建立认证凭证信任链，使用阶段每次认证都会在时间窗口内基于认证凭证信任链进行身份认证，认证不成功时触发身份认证错误响应机制。通过使用 ISO 14229 诊断协议中的功能寻址命令进行“一对多”的通信，可以实现以太网网关和多个域控制器之间身份认证的并行。

2.1 初始化阶段身份认证

初始化认证之前，在车载以太网控制器（包括以太网网关和域控制器）的安全存储区域中写入基于 SM2 算法的整车厂公钥 OEM_PubKey 和身份认证凭证函数表，如表 2 所示；在以太网网关的安全存储区域中写入基于 SM2 算法的网关证书 Cert_CGW（基于整车厂私钥 OEM_PrivKey 对以太网网关公钥 CGW_PubKey 签名得到）。

身份认证凭证函数表中， $f(N)$ 和 $f'(N)$ 分别用于计算认证过程中通信双方所使用的认证凭证。其中， N 为通信双方所使用的随机会话编号。如果控制器之间为双向通信，则使用相同的认证凭证函数， $f'(N) = f(N)$ 。在以太网网关作为车内认证中心的架构中，域控制器之间可以不需要

认证凭证函数。函数预置在控制器中，通信双方预先知道双方的认证凭证函数；若某两个控制器不需要进行通信，则不需要写入相应的认证凭证函数。

表 2 认证凭证函数
Table 2 Authentication credential functions

接收方/发送方	以太网网关	域控制器 1	域控制器 2	域控制器 n
以太网网关	—	$f_1(N)$	$f_2(N)$	$f_n(N)$
域控制器 1	$f_1(N)$	—	$f_{21}'(N)$	$f_{n1}'(N)$
域控制器 2	$f_2(N)$	$f_{21}(N)$	—	$f_{n2}'(N)$
域控制器 n	$f_n(N)$	$f_{n1}(N)$	$f_{n2}(N)$	—

初始化阶段身份认证发生在整车下线首次安装控制器或售后更换控制器之后，进入初始化阶段身份认证过程如图 3 所示。

由整车厂诊断仪触发控制器（包括以太网网关和域控制器）进入初始化阶段身份认证模式。诊断仪向控制器发送认证请求 Request 和诊断仪证书 Cert_Diag。诊断仪证书由整车厂私钥 OEM_PrivKey 对诊断仪公钥 Diag_PubKey 签名得到。

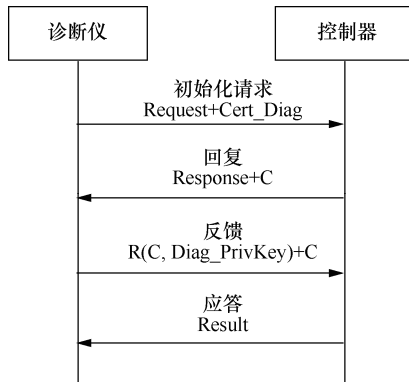


图 3 初始化阶段身份认证过程
Figure 3 Initialization stage initial authentication process

控制器使用内部安全存储区域存储的整车厂公钥 OEM_PubKey ，对诊断仪证书 $Cert_Diag$ 进行校验。校验通过则可以从中提取诊断仪公钥 $Diag_PubKey$ ，并发送回复 $Response$ 和随机数 C 给诊断仪。

诊断仪收到回复之后，基于诊断仪私钥 $Diag_PrivKey$ 对随机数 C 签名得到 $R(C, Diag_PrivKey)$ ，将结果和随机数 C 一起反馈给控制器。

控制器首先判断所收到的随机数与之前发送给诊断仪的随机数是否一致，如果两者一致再利用诊断仪公钥 $Diag_PubKey$ 校验随机数 C 的签名是否正确。两步校验通过则将应答 $Result$ 发给诊断仪，并进入初始化认证模式。

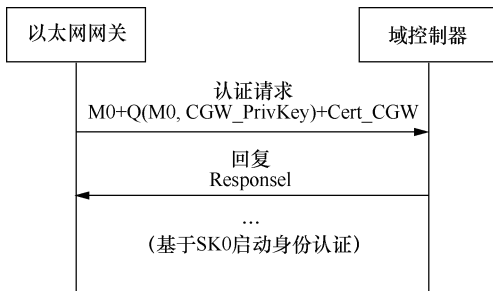


图 4 初始化阶段身份认证
Figure 4 Initialization stage authentication

进入初始化认证模式后，由以太网网关发起与域控制器的初始化认证过程。以太网网关生成随机会话编号 $M0$ ，并使用其私钥 $CGW_PrivKey$ 对 $M0$ 进行签名得到 $Q(M0, CGW_PrivKey)$ ，然后发送 $M0$ 、 $Q(M0, CGW_PrivKey)$ 以及网关证书 $Cert_CGW$ 给域控制器。

域控制器 n 在收到以太网网关发起的认证请求后，通过预置的整车厂公钥 OEM_PubKey 对以

以太网网关证书 $Cert_CGW$ 进行验证，验证通过则确认以太网网关身份。之后通过从以太网网关证书提取得到以太网网关公钥 CGW_PubKey ，对 $Q(M0, CGW_PrivKey)$ 进行验证，验证通过则提取随机会话编号 $M0$ 。最后以 $M0$ 为输入，基于安全认证凭证函数 $f_n(M0)$ 计算得到初始化认证凭证 $SK0$ 并记录，回复结果 $Response1$ 给以太网网关。

以太网网关随后以 $M0$ 为输入计算，基于相同的认证凭证函数，得到初始认证凭证 $SK0$ 并记录。接下来，基于 $SK0$ 完成控制器初始化身份认证，后续认证过程与使用阶段身份认证相同。

2.2 使用阶段身份认证

使用阶段身份认证在每次车辆重新上电或网络唤醒后触发。认证凭证信任链如图 5 所示，以第 i 次认证为例 ($i \geq 0$, $i=0$ 对应初始化阶段身份认证相应过程)，本次身份认证使用的认证凭证为 SK_i ，身份认证成功以太网网关和域控制器将基于本次认证随机会话编号 M_i 生成下一次认证凭证 $SK(i+1)$ 。认证凭证存储在安全芯片中，保存最近 K 次认证凭证信息 (K 可以配置)。每一次认证凭证都基于之前成功认证的随机会话编号动态生成，形成信任链。

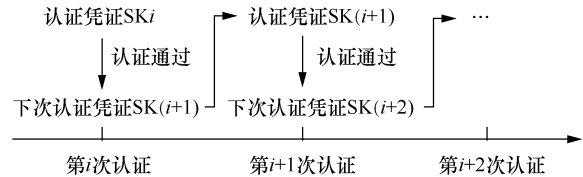


图 5 认证凭证信任链
Figure 5 Authentication credential trust chain

使用阶段身份认证过程如图 6 所示。

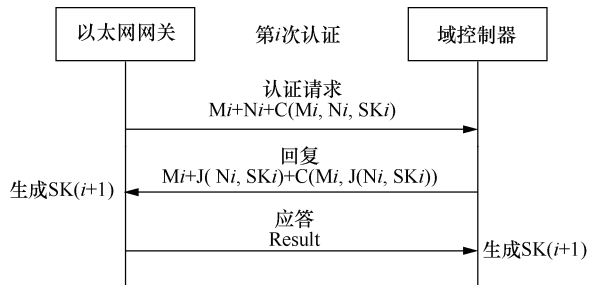


图 6 使用阶段身份认证
Figure 6 Application second stage authentication

由以太网网关发起认证，以太网网关生成随机会话编号 M_i 和随机数挑战码 N_i ，并基于存储

的认证凭证 SK_i 使用 SM4-CMAC 算法生成认证码 $C(M_i, N_i, SK_i)$, 然后将 M_i, N_i 和 $C(M_i, N_i, SK_i)$ 发送给域控制器。

域控制器使用自己存储的认证凭证 SK_i 校验认证码 $C(M_i, N_i, SK_i)$ 。通过后, 基于认证凭证 SK_i 使用 SM4-CBC 算法进行加密生成 $J(N_i, SK_i)$ 作为挑战应答, 并基于认证凭证 SK_i 使用 SM4-CMAC 算法生成认证码 $C(M_i, J(N_i, SK_i), SK_i)$, 然后将 $M_i, J(N_i, SK_i)$ 和 $C(M_i, J(N_i, SK_i), SK_i)$ 回复给以太网网关。

以太网网关必须在认证时间窗口内收到正确回复才判断为认证成功。收到回复后, 首先基于认证凭证 SK_i 校验认证码 $C(M_i, J(N_i, SK_i), SK_i)$ 。通过后, 对挑战应答 $J(N_i, SK_i)$ 解密得到回复 N_i , 判断收到的回复与之前发送给域控制器的随机数挑战码是否一致, 确认一致则完成身份认证。以 M_i 为输入基于认证凭证函数 $f_n(M_i)$ 生成下一次认证凭证 $SK_{(i+1)}$, 并发送认证成功结果 Result 反馈给域控制器。域控制器收到成功反馈后, 生成下一次认证凭证 $SK_{(i+1)}$ 并记录。下次身份认证将基于认证凭证 $SK_{(i+1)}$ 。

2.3 认证错误响应机制

如果在认证过程中认证失败, 控制器将记录认证错误信息并进行重试, 重试认证将利用上一次的认证凭证进行。如果重试若干次连续失败, 则触发认证系统报警, 通过人机交互界面通知驾驶员和后台, 并禁止与未通过认证的控制器进行通信。如果未在认证时间窗口中发送正确的认证回复, 则记录超时认证错误信息并重试, 若连续超时超过 300 ms, 则触发系统报警, 并通知车主和后台。在认证错误响应中, 还可以根据整车厂安全需求, 在系统报警的同时, 增加禁止车辆起动的错误响应。

3 测试

3.1 测试环境

搭建的测试环境如图 7 所示, 包括诊断仪, 一个车载以太网网关及两个域控制器。以太网网关和域控制器均使用汽车电子行业常用的英飞凌 TC387 芯片作为主芯片, 包含 3 个计算核, 芯片主频为 300 MHz, 计算能力为 1800 DMIPS, 可以代表汽车控制器典型计算性能。



图 7 测试环境
Figure 7 Test environment

测试环境中, TC387 的一个计算核被分配用于实现国密算法和配套认证逻辑。按照两阶段信任链安全认证方法编译出的二进制代码占用 13 kB 程序存储空间, 身份认证相关程序运行占用 2 kB RAM 空间。程序代码所占用的存储资源相对于 TC387 芯片提供的存储资源(程序存储空间 16 MB, RAM 空间 6912 kB) 占比很小, 可以满足车载应用的需求。

测验环境中, 以太网网关和域控制器 IP 地址配置如下。

- 1) 以太网网关: 192.168.1.8。
- 2) 域控制器 1: 192.168.1.100。
- 3) 域控制器 2: 192.168.1.120。

3.2 测试结果

基于以上测试环境, 对两阶段信任链安全认证的身份认证耗时进行了测试。

首先对本文方法中使用的加密算法性能进行测试。对 16 字节的数组, 分别进行 SM2 签名、SM2 验签、SM4-CBC 加密、SM4-CMAC 的计算, 平均耗时结果如表 3 所示。从测试数据来看, SM2 非对称算法的签名和验签在未使用硬件加速下平均耗时分别为 0.9 s 和 1.3 s。在本文提出的身份认证方法中, 基于 SM2 算法的身份验证发生在整车下线首次安装控制器或售后更换控制器的初始化阶段, 耗时可以满足这种非实时场景下的需求。对于 SM4 对称算法的相关运算, SM4-CBC 和 SM4-CMAC 在未使用硬件加速下平均耗时分别为 40 μ s 和 106 μ s, 能够满足车载以太网控制器身份认证场景下的实时性需求(当前车载以太网应用环境中报文的发送周期最短 1 ms)。

表 3 国密算法性能测试结果
Table 3 Cryptography performance test results

运算	平均耗时
SM2 签名	0.9 s
SM2 验签	1.3 s
SM4-CBC	44 μ s
SM4-CMAC	106 μ s

两阶段信任链安全认证的身份认证耗时测试过程如图 8 和图 9 所示, 图 8 和图 9 中标出了初始化阶段身份认证和使用阶段认证对应的各个步骤, 根据其时间差可以计算出身份认证耗时, 测试结果见表 4。诊断仪触发控制器进入初始化模式平均耗时 3.3 s, 之后的初始化身份认证平均耗时 3.4 s。初始化认证阶段发生在整车下线或售后维修环节, 由操作人员通过诊断仪执行认证过程, 对身份认证的实时性要求不敏感, 其耗时可以满足应用要求。而使用阶段身份认证平均耗时仅 75.4 ms, 相较于 Zelle 等^[3]基于 TLS 身份认证协议的耗时降低了 96%, 完全可以满足车辆使用过程中车载以太网身份认证实时性要求。

针对安全性, 由独立的攻击测试团队进行了篡改、重放、窃听等入侵测试, 测试结果表明, 被攻击的控制器不能通过控制器身份认证, 确保了安全性。

篡改攻击过程测试案例如图 10 所示。在完成使用阶段的某个会话过程身份认证后, 攻击者在下次会话身份认证过程发送篡改后的身份认证请求(篡改图 6 的随机会话编号字段, 其余字段跟上次会话过程保持一致)给被测控制器。

由于攻击者无法获得上次会话过程的身份认证凭证, 被测控制器不响应身份认证请求。

Time	Bus	Dir	Len	Data
100.972961	ETH2	Tx	0	
100.973052	ETH2	Rx	0	
100.973058	ETH2	Tx	0	
100.974946	ETH2	Rx	0	
100.974953	ETH2	Tx	0	
100.975022	ETH2	Rx	0	
100.975029	ETH2	Tx	0	
100.976946	ETH2	Rx	0	
100.976953	ETH2	Tx	0	
100.982951	ETH2	Rx	6	FE 0F A1 EE B0 16 352.168.1.8 → 192.168.1.100
100.983026	ETH2	Tx	0	
101.015815	ETH2	Rx	8	FE 20 49 F9 69 DA 352.168.1.100 → 192.168.1.8
101.016959	ETH2	Tx	0	
101.052947	ETH2	Rx	6	FE 2F BF 0D CA 3D 352.168.1.8 → 192.168.1.100
101.053022	ETH2	Tx	0	

图 9 使用阶段身份认证过程

Figure 9 Application stage authentication process

表 4 身份认证耗时测试结果
Table 4 Authentication time test

阶段	平均耗时
进入初始化模式	3.3 s
初始化身份认证	3.4 s
使用阶段身份认证	75.4 ms

Time	Bus	Dir	Len	Data
72.694103	ETH2	Rx	6	FE 0F A0 C6 BF DA 352.168.1.8 → 192.168.1.100
72.694262	ETH2	Tx	0	
72.734050	ETH2	Rx	6	FE 20 A0 C6 BF DA 352.168.1.100 → 192.168.1.8
72.734183	ETH2	Tx	0	
72.774171	ETH2	Rx	6	FE 2F F8 B6 B6 9D 352.168.1.8 → 192.168.1.100
72.774358	ETH2	Tx	0	
72.774551	ETH2	Rx	0	
成功完成认证				
:				
260.976915	ETH2	Rx	0	
260.976932	ETH2	Tx	0	
260.982910	ETH2	Rx	6	FE FF A1 EE B0 16 352.168.1.8 → 192.168.1.100
260.983863	ETH2	Tx	0	
261.015851	ETH2	Rx	0	
261.016993	ETH2	Tx	0	
261.052976	ETH2	Rx	0	
261.053823	ETH2	Tx	0	

图 10 篡改攻击测试案例

Figure 10 Tampering attack test case

一种重放攻击测试案例如图 11 所示。在完成使用阶段的某个会话过程身份认证后, 攻击者在下次会话身份认证过程重放之前的身份认证报

Time	Chn	Dir	Prot...	Payload Data	Destination...	Source IP	Destination IP	Source...	Destination...
2478.274519	Eth 1.2	Tx	tcp		CA:CA:CA:23:...	192.168.1.8	192.168.1.100	000C	1392
2478.275333	Eth 1.2	Rx	tcp		CA:CA:CA:23:...	192.168.1.100	192.168.1.8	1392	000C
2478.275554	Eth 1.2	Tx	tcp		CA:CA:CA:23:...	192.168.1.8	192.168.1.100	000C	1392
2774.097868	Eth 1.2	Tx	tcp	31 01 57 01 01 01 00 48 C0 16 A9 F0 A2 A8 5C AD C7 50 56 D0 ...	CA:CA:CA:23:...	192.168.1.8	192.168.1.100		
2774.098665	Eth 1.2	Rx	tcp		CA:CA:CA:23:...	192.168.1.100	192.168.1.8	1392	000C
2774.104668	Eth 1.2	Rx	tcp		FF FF FF FF ...				
2776.084546	Eth 1.2	Rx	tcp	31 01 57 01 AA 01 00 20 01 02 03 04 05 06 07 08 01 02 03 04 05 ...	CA:CA:CA:23:...	192.168.1.100	192.168.1.8		
2776.181364	Eth 1.2	Tx	tcp		CA:CA:CA:23:...	192.168.1.8	192.168.1.100	000C	1392
2810.586790	Eth 1.2	Tx	tcp	31 01 57 02 01 01 00 66 01 02 03 04 05 06 07 08 01 02 03 04 05 ...	CA:CA:CA:23:...	192.168.1.8	192.168.1.100		
2810.588380	Eth 1.2	Rx	arp		FF FF FF FF ...				
2810.588409	Eth 1.2	Rx	tcp		CA:CA:CA:23:...	192.168.1.100	192.168.1.8	1392	000C
2810.588900	Eth 1.2	Tx	arp		CA:CA:CA:23:...				
2811.952304	Eth 1.2	Rx	tcp	31 01 57 02 AA 01 00 01 01	CA:CA:CA:23:...	192.168.1.100	192.168.1.8		
2812.050485	Eth 1.2	Tx	tcp		CA:CA:CA:23:...	192.168.1.8	192.168.1.100		
2849.060330	Eth 1.2	Tx	tcp	31 01 57 03 00 01 01 01	CA:CA:CA:23:...	192.168.1.8	192.168.1.100		
2849.061095	Eth 1.2	Rx	tcp		CA:CA:CA:23:...	192.168.1.100	192.168.1.8		
2852.679769	Eth 1.2	Rx	tcp	31 01 57 03 00 01 01 01	CA:CA:CA:23:...	192.168.1.100	192.168.1.8		
2852.771177	Eth 1.2	Tx	tcp		CA:CA:CA:23:...	192.168.1.8	192.168.1.100	000C	1392

图 8 初始化阶段身份认证过程

Figure 8 Initialization stage authentication process

文数据给被测控制器。由于攻击者重放会话的身份认证凭证和当前被测控制器的身份认证凭证不相同,身份认证请求无效,被测控制器不响应身份认证请求。

me	Bus	Dir	Len	Data	
72.694103	ETH2	Rx	6	FE 0F A0 C6 8F 9A	192.168.1.8 → 192.168.1.100
72.694262	ETH2	Tx	0		
72.734050	ETH2	Rx	6	FE 20 A0 C6 8F 9A	192.168.1.100 → 192.168.1.8
72.734383	ETH2	Tx	0		
72.774171	ETH2	Rx	6	FE 2F FB B6 B6 90	192.168.1.8 → 192.168.1.100
72.774358	ETH2	Tx	0		
72.774551	ETH2	Rx	0		成功完成认证
重放数据					
273.343601	ETH2	Rx	6	FE 20 A0 C6 8F 9A	192.168.1.8 → 192.168.1.100
273.344506	ETH2	Tx	0		
273.383215	ETH2	Rx	0		192.168.1.100 → 192.168.1.8
273.383699	ETH2	Tx	0		
273.414517	ETH2	Rx	0		192.168.1.8 → 192.168.1.100

图 11 重放攻击测试案例
Figure 11 Replay attack test case

一种窃听攻击测试案例如图 12 所示。攻击者将非法控制器连入车载以太网,企图伪装成域控制器发送正常以太网通信报文,窃取通信内容。由于不具备合法的身份认证凭证,非法控制器无法建立与其他域控制器的通信,无法收到交互节点的应答回复,无法窃取通信内容。

	Bus	Dir	Len	Data	
12.698112	ETH2	Rx	0		非法控制器请求无法建立通讯
12.736083	ETH2	Rx	6	FE 20 A0 C6 8F 9A	192.168.1.100 → 192.168.1.120
12.774071	ETH2	Rx	0		
12.813051	ETH2	Rx	0		
12.858058	ETH2	Rx	0		
12.888040	ETH2	Rx	6	FE 20 A0 C6 8F 9A	192.168.1.100 → 192.168.1.120
12.926026	ETH2	Rx	0		
12.964013	ETH2	Rx	0		
13.002071	ETH2	Rx	0		

图 12 窃听攻击测试案例
Figure 12 Eavesdropping attack test case

4 结束语

本文分析了车载以太网身份认证技术的现状和面临的挑战,基于车载控制器性能有限的应用场景,提出了基于国密算法的两阶段信任链安全认证方法。① 在对认证时间不敏感的初始化阶段,基于复杂的非对称国密算法 SM2 进行身份认证;而在对认证时间敏感的使用阶段,基于对称国密算法 SM4 进行身份认证,节省了身份认证时间。② 在初始化阶段和使用阶段的身份认证之间,以及在使用阶段的每一次认证之间,基于认证凭证建立了信任链,上一次的认证结果会影响下一次认证,相对于现有的控制器身份认证协议提高了认证安全性。基于车载控制器的实验证明,该方法资源占用较少并具有较高的安全性,能够

同时满足车载以太网控制器身份认证性能和安全两方面的应用需求。

后续研究可以考虑:① 将车辆识别代码(VIN 码)加入认证凭证生成过程,进一步提高安全性;② 使用硬件安全模块对加解密算法进行硬件加速,或者在使用阶段身份认证中将控制器身份认证与控制器业务数据交互过程同步执行,进一步提高性能,缩短认证时间;③ 使用防侧信道攻击的安全芯片来存储车辆的密码材料,提升存储安全性;④ 功能安全设计,如使用环形网络及冗余硬件/软件,在单点故障时确保控制器身份认证功能的可用性。

参考文献:

- [1] MATHEUS K. Automotive ethernet[M]. Cambridge: Cambridge University Press, 2015.
- [2] 呼布钦, 秦贵和, 刘颖, 等. 下一代汽车网络: 车载以太网技术现状与发展[J]. 计算机工程与应用, 2016(24): 29-36.
HU B Q, QIN G H, LIU Y, et al. Next generation automotive network: technology status and development of automotive ethernet in-vehicle network[J]. Computer Engineering and Applications, 2016, (24): 29-36.
- [3] 李克强, 戴一凡, 李升波, 等. 智能网联汽车(ICV)技术的发展现状及趋势[J]. 汽车安全与节能学报, 2017, 8(1): 1-14.
LI K Q, DAI Y F, LI S B, et al. State-of-the-art and technical trends of intelligent and connected vehicles[J]. Automotive Safety and Energy. 2017, 8(1): 1-14.
- [4] LIN C W, YU H. Cooperation or competition? Coexistence of safety and security in next-generation ethernet-based automotive networks[C]//IEEE Design Automation Conference. 2016.
- [5] RAY S, WEN C, BHADRA J, et al. Extensibility in automotive security: current practice and challenges[C]//Proceedings of the Design Automation Conference, 2017.
- [6] 罗超. 面向网联汽车车内网络的防御技术研究[实现[D]. 成都: 电子科技大学, 2020.
LUO C. Research and implementation of defense technology for in-vehicle network of connected vehicle[D]. Chengdu: UESTC, 2020.
- [7] IEEE standard for local and metropolitan area networks[R]. 2004.
- [8] FUNK P, BLAKEWILSON S. EAP tunneled TLS authentication protocol (EAP-TTLS)[R]. 2004
- [9] ZELLE D, CHRISTOPH K, HUBERT S, et al. On using TLS to secure in-vehicle networks[P]. Availability, Reliability and Security, 2017.
- [10] KOHL J, NEUMAN C. The kerberos network authentication service (V5)[S]. RFC Editor, 1993.
- [11] MUNDHENK P, PAVERD A, MROWCA A, et al. Security in automotive networks[J]. ACM Transactions on Design Automation of Electronic Systems, 2017.
- [12] 程安宇. 乘用车网络控制系统中调度算法的研究与实现[D]. 武汉: 武汉大学, 2014.
CHENG A Y. The research and implementation of scheduling algo-

- rithm in passenger vehicle network control system[D]. Wuhan: WHU, 2014.
- [13] GB/T 32918-2016. 信息安全技术 SM2 椭圆曲线公钥密码算法[S]. 北京:中国质检出版社, 2016.
- GB/T 32918-2016. Information security technology— public key cryptographic algorithm SM2 based on elliptic curves[S]. Beijing: China Quality Press, 2016.
- [14] GB/T 32905-2016. 信息安全技术 SM3 密码杂凑算法[M]. 北京: 中国质检出版社, 2016.
- GB/T 32905-2016. Information security technology— SM3 cryptographic hash algorithm[S]. Beijing: China Quality Press, 2016.
- [15] GB/T 32907-2016. 信息安全技术 SM4 分组密码算法[M]. 北京: 中国质检出版社, 2016.
- GB/T 32907-2016 Information security technology— SM4 block cipher algorithm[S]. Beijing: China Quality Press, 2016.
- [16] 吴志红, 赵建宁, 朱元, 等. 国密算法和国际密码算法在车载单片机上应用的对比研究[J]. 信息网络安全, 2019(8): 68-75.
- WU J H, ZHAO J N, ZHU Y, et al. Comparative study on application of chinese cryptographic algorithms and international cryptographic algorithms in vehicle microcontrollers[J]. Netinfo Security, 2019(8): 68-75.
- [17] 修佳鹏, 田超宇, 杨正球, 等. SecOC 安全机制中国密算法应用方案研究[J]. 信息安全研究, 2020, 6(9): 775-782.
- XIU J P, TIAN C Y, YANG Z Q, et al. Research on application scheme of national secret algorithm SecOC security mechanism[J]. Journal of Information Security Research. 2020, 6(9): 775-782.
- [18] AL-JARRAH O Y, MAPLE C, DIANATI M, et al. Intrusion detection systems for intra-vehicle networks: a review[J]. IEEE Access, 2019: 1-10.
- [19] 胡鑫鑫, 刘彩霞, 刘树新, 等. 移动通信网鉴权认证综述[J]. 网络与信息安全学报, 2018, 4(12): 1-15.
- HU X X, LIU C X, LIU S X, et al. Overview of mobile communica-

tion network authentication[J]. Chinese Journal of Network and Information Security, 2018, 4(12): 1-15.

[作者简介]



郭辉 (1981-), 男, 重庆人, 清华大学博士生, 主要研究方向为车载网络信息安全、汽车功能安全。



罗勇 (1990-), 男, 江西新余人, 联合汽车电子有限公司工程师, 主要研究方向为车载网络信息安全。



郭晓潞 (1970-), 男, 上海人, 联合汽车电子有限公司教授级高级工程师, 主要研究方向为汽车电子控制器。