车载异构网络节点消息认证协议设计

徐国胜[1], 李逸静[2], 汪梓撼[1], 王晨宇[1]

[1] 北京邮电大学网络空间安全学院 北京 中国 100876
[2] 中国信息通信研究院安全研究所 北京 中国 100083

摘要 消费者对汽车安全性、舒适性和智能性的需求推动着汽车工业的不断发展, 目前大多数创新都集中在汽车电子和软件领域, 这一点在车载网络架构以及电子控制单元(ECU)和车内节点之间交换的消息数量增长中表现得非常明显。一方面, 推动着汽车电子系统不断升级, 另一方面, 也不可避免地引入了额外安全风险, 其中最突出的就是消息缺乏认证, 面临的关键挑战之一是如何利用有限的计算和通信资源来验证总线内的消息, 其主要目的是确保数据传输的可靠性和新鲜性。目前的方案主要问题在于实际应用开销大, 需要在通信节点之间维护多个字段来验证消息新鲜性, 这导致整体通信负载较大。为弥补这一缺陷, 本文提出了一种新的车载网络消息认证方案, 我们提供了理论证据, 证明该方案可以有效抵御重放和欺骗等攻击, 同时提高对去同步化的抵抗能力。在理论分析的基础上, 我们使用专业仿真软件开发了一个模拟环境, 并设计了一系列对比实验来验证方案的有效性。实验结果表明, 该方案不仅能够有效地抵抗重放和欺骗等常见攻击, 还具备良好的安全性、抗去同步性和鲁棒性。该方案通过基于时间间隔的新鲜性机制, 消除了用于同步的计数器开销, 进而降低了消息认证的整体时间开销。与现有方案相比, 本方案在确保数据传输的可靠性和新鲜性方面可以显著提升车内消息认证的效率和安全性, 在实际应用中具有较高的价值, 能够为车载网络提供更为安全、可靠的消息认证服务。

关键词 车载异构网络; 消息认证; 电子控制单元; 控制域网络
中图法分类号 TP311 DOI 号 10.19363/J.cnki.cn10-1380/tn.2026.01.01

Design of Message Authentication Protocol for Vehicle Heterogeneous Network Nodes

XU Guosheng[1], LI Yijing[2], WANG Zihan[1], WANG Chenyu[1]

[1] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] China Academy of Information and Communications Technology, Beijing 100083, China

Abstract Consumer demand for automotive safety, comfort, and intelligence drives continuous development in the automotive industry. Currently, most innovations are focused on automotive electronics and software, which is particularly evident in vehicle network architecture and the increasing number of messages exchanged between the electronic control units (ECUs) and in-vehicle nodes. On one hand, it propels continuous upgrading of automotive electronic systems; on the other hand, it inevitably introduces additional security risks, the most prominent of which is the lack of message authentication. One of the key challenges is how to verify messages within the bus using limited computing and communication resources, with the main goal of ensuring the reliability and freshness of data transmission. The main problem of current solutions is the high practical overhead due to the demand of maintaining multiple fields between communication nodes to verify message freshness, resulting in a high overall communication load. To compensate for this deficiency, this paper proposes a novel in-vehicle network message authentication scheme. We provided theoretical evidence to demonstrate that the scheme is effective in resisting replay and deception attacks while enhancing the resistance to desynchronization. Based on theoretical analysis, we developed a simulation environment using professional simulation software and designed a series of comparative experiments to verify the effectiveness of the proposed scheme. Experimental results indicate that the proposed scheme not only effectively resist common attacks such as replay and deception, but also has good security, anti-desynchronization, and robustness. This scheme eliminates the counter overhead for synchronization through a freshness mechanism based on time intervals, thereby reducing the overall time overhead for message authentication. Compared to existing solutions, this scheme significantly improves the efficiency and security of in-vehicle message authentication by ensuring the reliability and freshness of data transmission. This scheme is of high practical application value, providing a more secure and reliable message authentication service for in-vehicle networks.

Key words In-vehicle heterogeneous networks; message authentication; ECU; CAN

通讯作者: 徐国胜, 学历: 博士, 职称: 副教授, Email: guoshengxu@bupt.edu.cn。
本课题得到国家重点研发计划项目(No. 2021YFB3101500)和中央高校基本科研业务费专项(No. 2023RC69)资助。
收稿日期: 2024-03-26; 修改日期: 2024-08-01; 定稿日期: 2025-12-05

1 引言

汽车自 1886 年诞生以来, 已有近 140 年的历史。从工业 1.0 的机械化、工业 2.0 的电动化到工业 3.0 的信息化, 关于汽车的研究几乎伴随着人类工业化的所有阶段。汽车工业紧跟发展步伐, 许多最新技术不断应用于汽车的设计和制造中。近年来, 工业向 4.0 时代迈进, 逐步向智能化、互联互通方向迁移。汽车行业也开始朝着这个方向发展, 在可预见的未来, 智能网联汽车将成为主要汽车领域争夺的制高点。

目前, 一些高端机型的软件代码量已超过 1 亿行[1], 并有持续增加的趋势。这些代码分布在 100 多个电子控制单元(Electronic Control Unit, ECU)[2]中, 正是它们使现代汽车更安全、更舒适、更智能。ECU 数量的快速增长给汽车总线网络带来了巨大的通信压力, 一些研究计算了汽车中的通信信号数量, 当 ECU 数量达到 70 个时, 它产生的通信信号已经达到 4716[3], 文献[4-5]也对此进行了讨论。面对这种情况, 传统的分布式总线架构已经无法承载智能网联汽车所需的通信流量, 因此汽车总线网络的架构也发生了变化。

经过几十年的发展, 汽车工业已经形成了一个完整的基于控制域网络(Controller Area Network, CAN)总线协议的开发框架。尽管汽车总线网络的架构已经发生了变化, 但大多数车辆仍然依赖 CAN 协议进行内部通信。因此, 在新的通信协议成为车辆行业标准之前, 有必要通过安全协议在现有的总线环境中实现安全通信。目前, 总线安全领域的研究人员面临的关键挑战之一是如何利用有限的计算和通信资源来验证总线内的消息, 其主要目的是确保数据传输的可靠性和新鲜性。在传统的 CAN 总线中, 攻击者很容易发起重放和欺骗攻击, 因此大多数现有的方案都选择在总线上传输的消息中添加身份验证和新鲜性验证。然而, 目前的许多方案在确保数据传输的可靠性和新鲜性的同时, 普遍增大了实际应用中通信负载开销。本文提出了一种新的基于时间戳和消息认证码(Message Authentication Code, *MAC*)的消息认证方案, 对方案的安全性进行分析。一方面我们的方案弥补现有车载网络消息认证开销大的不足, 另一方面也展示了其抵抗常见攻击的能力, 证明其完全能够满足相关的安全要求。

本文第 1 节对车载异构网络节点消息认证方法的背景进行总述, 给出了本文研究的问题所在; 第 2 节针对当前消息认证方法的国内外研究现状阐述; 第 3 节详述提出的车载网络消息认证方案; 第 4 节分析设计的消息认证方案的安全性, 论证其是否能够满足常见的安全要求, 并具备抵御常见攻击的能力; 第 5 节对所提出的方法进行实验验证和分析比对; 第 6 节总结全文。

2 相关工作

CAN 总线网络被设计为一个封闭网络, 为工业设备或控制器提供通信能力。尽管网络协议本身存在许多安全漏洞, 但由于网络本身与外界相对隔离, 因此几乎不存在安全风险。然而, 自 2007 年 Hoppe 和 Dittman[6]通过 CAN 总线攻击成功控制电动车窗的升降以来, 许多学者相继发表了关于 CAN 总线网络攻击的研究。在目前的成果中, 许多研究人员的攻击是通过各种方法获得对 CAN 总线的访问权限, 然后篡改总线中的消息来实现的。例如, 通过使用虚假 ID 或伪造的 CAN 帧来控制 ECU, 或者通过拦截以前的 CAN 帧进行重放攻击。在针对车载网络的攻击实验中, Miller 和 Valasek[7]在车辆的停车辅助过程中回放了先前截获的 CAN 帧。由于这些框架中包含的进入停车位的速度和角度不正确, ECU 最终接收到这些信息并向动力和转向系统发送了不正确的控制信号。最终, 车辆在停车辅助系统启动的情况下发生碰撞事故。

哈希(Hash)函数[8-10]是将任意长度输入映射为固定长度输出的函数, 用于数据完整性验证和数字签名。它具有确定性、快速计算、抗碰撞性和抗预镜像性。消息认证码(*MAC*)[8-10]结合哈希函数和密钥生成, 用于验证消息完整性和认证。发送方计算 *MAC* 并附加在消息上, 接收方用相同密钥验证, 防止消息被篡改或伪造。典型的 *MAC* 算法包括 *HMAC*。

目前, 对车载网络消息认证的研究已经取得了一定的成果。2008 年, Nissen 等[11]提出了一种应用于总线的延迟消息认证机制, 该机制使用 64 位 *MAC*, *MAC* 被拆分并在 4 个帧中单独发送。这种解决方案可以在一定程度上解决总线消息缺乏身份验证的问题, 但如果攻击者发送伪造的消息, 系统需要接收所有 4 个数据包才能被发现。Miller 等[7]提出了 CANAuth 方案, 该方案通过基于哈希的消息认证码(Hash-based Message Authentication Code, HMAC)和计数器机制对消息进行认证, 这样可以减少注入攻击和重放攻击的可能性。然而, 它使用 CAN+协议, 以避免 CAN 协议本身对数据负载的限制, 并通过将数据插入 CAN 协议物理层的非采样部分来增加总线上的数据承载能力。它对总线上设备的采样精度有一定的要求, 不能应用于仅满足 CAN 协议物理层要求的设备。

除了使用安全协议进行消息验证外, 一些研究人员还通过检测总线内的攻击来确保消息传输的可信度。Cho 等[12]在 2016 年提出了一种基于时钟的入侵检测系统(Intrusion Detection System, IDS)方案, 该方案通过检测设备硬件指纹来识别 ECU, 并利用总线内定期发送消息的特性来识别恶意消息。然而, 这种方法不能识别周期性的消息注入, 因此攻击仍然是可能的。

2017 年, Schmandt 等[13]统计了试驾丰田普锐斯后 12.27 min 内在公交车上捕获的 15768 条公交车信息, 发现大约 61%的信息只使用了 8 字节数据负载中的 4 字节。基于这一统计结果, 该研究进一步提出了一种微型 CAN 机制, 通过将 *MAC* 放置在未使用的 4 字节数据有效载荷中来实现消息认证。尽管微型 CAN 可以在不增加通信开销的情况下完成消息身份验证, 但该机制并不是为验证数据负载超过 4 字节的消息而设计的。

由于 CAN 总线的每一帧所能承载的数据量都很小, 因此如何在不改变负载大小和响应延迟的情况下提高总线网络的安全性是 CAN 总线安全研究的重点[12]。

3 车载网络消息认证方案设计

为了更好地解释该方案的详细过程和具体算法, 所使用的符号如表 1 所示。

表 1 消息认证方案符号定义

Table 1 Symbol definition of message authentication scheme

符号	含义
A	*MAC* 计算过程的中间参数, 表示哈希运算的结果
K	会话密钥
T_n	n 时刻的时间
TC_n	n 时刻的时间间隔计数器
Δt	时间间隔
M	消息明文
offset	取数据时的偏移量
MAC	消息认证码
/	除法运算(舍去余数)
$H()$	哈希运算
‖	连接运算符
&	与操作运算符
$[m]$	数据的第 m 字节
$[m:n]$	数据的第 m 到 n 字节

为了尽可能保持与 CAN 总线协议的兼容性, 我们使用 *MAC* 来替换 CAN 帧中的原始循环冗余校验(Cyclic Redundancy Check, CRC)字段。此更换过程不会改变 CAN 协议中指定的框架结构, 所以它可以在符合 CAN 总线标准的网络中正常运行。此外, CAN 协议自开发以来已有多个版本, 包括 CAN-FD 等升级协议, 尽管这些协议具有不同的帧格式, 但它们都具有 CRC 字段。因此, 只需要针对不同的协议进行适当修改, 就可以非常便利地将本方案迁移到各种 CAN 协议当中, 这使得本方案具有较强的可迁移性。

传统的消息新鲜性需要在通信参与方之间维护若干个字段, 对于每一次验证都需要改变这些字段的值, 给整体通信增加了不小开销。本方案设计基于时间间隔的新鲜性机制, 消除了用于同步的计数器开销, 进而降低了消息认证的整体时间开销。

3.1 引入 *MAC* 字段

本节以经典 CAN 总线协议为例展示 *MAC* 替换 CAN 帧内 CRC 字段的原理。如图 1 所示, 在一帧 CAN 报文内, 可以传输 8 字节数据, 同时还有 15 比特长度的 CRC 字段用来进行错误检测。CRC 码是一种具有检错和一定程度纠错能力的校验码, 在早期通信技术中有着较广泛的应用。但是 CRC 的计算过程公开且不包括身份信息, 所以攻击者可以轻易为恶意消息生成一段合法的 CRC 码来通过 ECU 的验证。

使用 *MAC* 对消息进行认证较 CRC 而言有着较高的安全性, 通过将密钥等信息附加在 *MAC* 生成时的明文内, 还可以实现消息来源认证等功能。所以本文所提方案选择使用 *MAC* 替代 CRC 来为 CAN 帧附加消息来源认证功能, 经过改进后的经典 CAN 协议帧如图 2 所示, 只有 CRC 字段被替换为 *MAC*, 其他结构和长度并未受到影响。

由于 *MAC* 的生成依赖哈希函数, 而几乎所有哈希函数的运算结果都远大于 CAN 帧所提供的 15 比特空间[9], 所以方案需要对 *MAC* 结果进行处理和缩减, 用到的具体方法将在 3.3 节中介绍。

3.2 基于时间间隔的新鲜性机制

车内总线网络内部节点大多由功能单一的 ECU 构成, 车辆正常运行状态下向总线中发送的消息内容一般比较固定, 且各 ECU 都有自己的消息发送周期[13]。如果某些 ECU 的功能是监控汽车部件运行状态并报告, 则有更大可能周期性发送内容相同的报文, 在这种应用场景下, 仅使用密钥和消息明文生成 *MAC* 会发生认证部分重复的情况。此外, 缺乏消息的实效性验证还可能导致重放攻击, 严重威胁车内总线网络的安全。

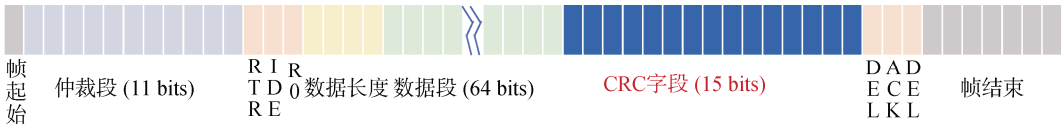

图 1　传统 CAN 帧结构

Figure 1　Traditional CAN frame structure

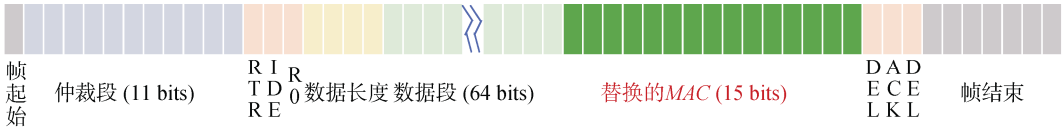

图 2　改进后的 CAN 帧结构

Figure 2　Improved CAN frame structure

目前常见的消息新鲜性机制有基于计数器和基于时间两种类型。两种机制在运行时都需要在通信双方之间同步地维护一个或多个字段: 对于基于计数器的新鲜性验证, 需要对消息进行计数, 每次发送或接收消息都对计数器进行更新; 基于时间的新鲜性验证要求通信双方的时间同步, 消息根据发送或接收的时间去进行新鲜性验证。对于车内网环境来说, 保持 ECU 之间的消息计数器同步需要更大的代价, 因为 CAN 总线协议不能保证消息的可靠传输, 如果发生超时或其他原因导致的消息未送达, 就会发生消息计数不同步的问题。所以本方案选择了基于时间间隔的新鲜性机制, 并通过设定时间间隔来扩大对通信、数据处理等流程所产生的时延的宽容度。

车内总线网络具有的典型特征就是在车辆点火时进行初始化, 即各 ECU 设备的上电时间可以基本保持一致, 借助这一特征就可以在总线网络节点间维护一个从零开始的定时器, 通过这一定时器可以实现各 ECU 节点之间的时间同步, 进而实现方案内新鲜性字段的生成和验证。

如果使用精确时间计算新鲜性字段, 很有可能因为发送方与接收方之间传输、处理信息的时间差造成新鲜性校验失败的情况, 为了解决这一问题, 本方案使用时间计数器 TC 来代替精确时间, 计算方法如式(1)。

$$TC = T / \Delta t \tag{1}$$

通过该计算方法可以将一段时间划分为长度为 Δt 的时间间隔, 处于同一时间间隔内的消息计算得到的 TC 值也相同, 从而增大了新鲜性字段对时延的宽容度。并且 Δt 的大小可以根据实际情况动态调整: 如果总线负载较低, 通信时延较短可以缩小 Δt 的值以增强安全性; 而在网络负载较高, 通信环境复杂的情况下则需要适当增大 Δt 来提高消息新鲜性校验的通过率。

在实际使用所提方案进行新鲜性校验时, 可能发生如图 3 所示的两种情况, 其中①表示正常情况下新鲜性字段计算时间点 T_0 和验证时间点 T_1 处在同一时间间隔内, 这种情况下计算得到的 TC_0 和 TC_1 是相等的, 所以可以通过新鲜性校验; 而在②情况下, T_0 和 T_1 分散在了两个时间间隔内, 此时通过式(1)计算得到的 TC_0 和 TC_1 不相等, 出现了合法消息的新鲜性校验不通过的现象。

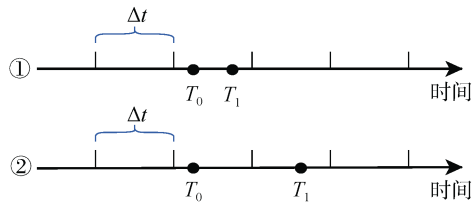

图 3　时间间隔机制

Figure 3　Time interval mechanism

合法消息出现新鲜性校验不通过大多是因为新鲜性字段生成和校验时间点跨越了两个时间间隔。为了解决这一问题, 方案引入了时间间隔补偿字段 c, 当校验时计算得到的 TC_0 和 TC_1 不相等时, 会加入补偿字段 c 重新计算, 计算方法为式(2)。补偿字段 c 的大小也可以根据实际情况动态调整: 如果总线负载较低, 通信时延较短, 此时可以减小 c 的值以增强安全性; 而在网络负载较高, 通信环境复杂的情况下则需要适当增大 c 的值来提高消息新鲜性校验的通过率。

$$TC_1 = (T_1 / \Delta t) \pm c \tag{2}$$

接收方校验新鲜性时会按顺序计算 TC_1+1, TC_1–1, TC_1+2, TC_1–2 等结果, 直到校验通过或计算到 TC_1+n, TC_1–n,这里 n 为补偿字段 c 的阈值, 即校验的最大尝试次数, 超过此阈值则会判定新鲜性校验不通过。通过引入补偿字段 c, 该方案具有了时间上的宽容度, 可以允许新鲜性生成与校验间最多相差 n

个时间间隔的消息通过新鲜性校验, 因此在实际应用中, 需要根据网络环境选择合适的阈值 n, 过大的 n 可能会将较短时间前截取的报文包含进合法时间间隔内, 增大了重放攻击成功的可能性。

3.3 *MAC* 的生成和校验

本方案中 *MAC* 的计算需要用到通过认证和密钥交换协议后得到的会话密钥 K、使用式(1)计算得到的时间间隔计数器 *TC* 以及本条消息传输的明文 M。首先, 将三者拼接后通过哈希运算得到中间量 A, 此处使用的哈希算法为 SHA256[8], 将得到 32 字节的运算结果, 如式(3)所示:

$$A[0:31] = H(K||TC_0||M) \tag{3}$$

由于 32 字节(256 比特)的哈希结果远大于 CAN 数据帧中 CRC 字段的 15 比特, 因此在对 CRC 字段进行替换前需要对 A 进行处理和裁剪。为了增加每条消息间裁剪的随机性, 本方案使用如下方法从 A 中裁剪出最终的 *MAC* 值:

$$offset = A[31]\&0x1e \tag{4}$$

$$MAC = (A[offset]<<4+A[offset+1]\ mod\ 2^{15} \tag{5}$$

等式(4)对中间值 A 和 $0x1e$ 的最后一个字节执行 AND 运算, 然后将结果记录为偏移量, 偏移量的大小在 0~30 之间, 正好代表哈希结果 A 的第 0 到第 30 个字节。后续过程如式(5)所示。首先, 截取 A 中的偏移量和偏移量+1 字节, 以获得两个字节的总共 16 比特的数据。在去除最高有效位(Most Significant Bit, MSB)之后, 获得最后的 15 位 *MAC* 值。最后, 将原来 CAN 帧中的 CRC 字段替换为该 *MAC*, 完成认证字段的生成。

当接收方收到 CAN 帧时需要进行消息认证来验证发送方的合法性和消息的新鲜性。首先根据接收消息的时刻 T_1 计算出时间间隔计数器 TC_1, 然后与会话密钥 K、消息明文 M 拼接后计算出 $A'=H(K||TC_1||M)$。随后对 A'的值进行处理和裁剪就可以得到 *offset* 和 *MAC'*。最后, 将接收方本地计算出的 *MAC'*和消息中携带的 *MAC* 进行比较, 若相等, 则表示消息发送方的身份合法, 且消息未过期, 可以接受消息; 不相等则认证失败, 舍弃该条消息。

4 方案安全性分析

本章将解释所设计的消息认证方案的安全性, 并分析该方案是否能够满足常见的安全要求以及可能的攻击。

4.1 欺骗攻击

在原有 CAN 协议下, 攻击者可以轻易对总线网络发起欺骗攻击, 因为 CAN 标准规定每一帧的数据完整性由 CRC 字段进行保护, 而攻击者可以轻易使用恶意数据替换报文中的合法数据并根据恶意数据重新计算 CRC 值。此时接收方根据 CRC 段校验数据时仍然会通过, 接受报文中的恶意数据。本方案下使用 *MAC* 验证代替 CRC, *MAC* 在生成时除需要消息明文外, 还需要认证阶段交换得到的会话密钥和时间间隔计数器, 攻击者无法获得会话密钥, 也就无法计算出消息对应的 *MAC* 值。

为了在不更改 CAN 帧结构的前提下用 *MAC* 替换 CRC 字段, 最终的 *MAC* 值被裁剪为了 15 比特的长度, 攻击者使用暴力破解需要尝试 2^{15} 种可能性, 对于现代计算设备, 该数量级下的秘密可以轻松被破解, 但由于每种可能性的检验都要向接收方发送消息, 所以实际的破解速度受限于 CAN 总线网络的传输速度, 攻击者将很难在一个设置合理的时间间隔内尝试出合法的 *MAC*。

通过以上分析, 可以认为该方案能够满足总线网络内消息来源和完整性验证的安全需求, 并且具有抵御欺骗攻击的能力。

4.2 重放攻击

传统 CAN 帧中并没有关于新鲜性的校验机制, 只要帧 ID 在 ECU 的 ID 接收列表中有记录, 该帧就会无条件被接收。在本章所提方案中, 在 *MAC* 生成时引入了一个基于定时器时间间隔的计数器 *TC*, 借助这一参数, 方案能够在不同时间间隔内产生不同的 *MAC*。如果攻击者记录了以前的帧并重新发送, 就会由于 *TC* 与当前时刻接收方计算出的 *TC* 不匹配而导致 *MAC* 验证不通过。

需要注意的是, 为了保证因为通信或处理时延而被分割在两个时间间隔中的消息也能顺利通过新鲜性验证, 方案设计了补偿值 c, 并规定了 c 的阈值 n, 当 TC_0 满足 $TC_{1-n}<TC_0<TC_{1+n}$ 时都可以通过验证。如果重放攻击的报文也满足这一要求, 也会被认为是合法报文而被接收。所以对于方案中自定义的时间间隔补偿阈值 n 和时间间隔 Δt, 都要根据实际应用时总线网络的速度合理设置, 以防止发生在合理时间间隔内的重放攻击。

上述分析表明, 本章所提方案能够满足消息新鲜性验证的安全需求, 在时间间隔补偿阈值 n 和时间间隔 Δt 设置合理的前提下可以抵御重放攻击。

4.3 抵御去同步化

CAN 总线中, 能够实现新鲜性验证的方案大多需要在网络的所有节点间维护一个同步的参数, 常见的有消息计数器和定时器。消息计数器对网络的稳定性要求较高, 如果发生丢失报文的情况, 就会

发生去同步化, 导致后续验证全部失败, 而且去同步化后重新同步的代价也很高。本方案选择使用基于时间间隔的计数器, 在车辆上电时统一对网络内节点的定时器进行初始化, 后续同步所依赖的硬件晶振也具有较高的计时精度, 因此该机制发生去同步化的概率较低。对于由 *MAC* 计算和验证分隔在不同时间间隔所导致的去同步化, 也有补偿值 c 来进行处理。所以本方案所采用的新鲜性校验机制具有抵御去同步化的能力。

5 实验设计

本章对我们的消息认证方案的功能和安全性进行实验验证, 主要验证消息结构的变化、时间间隔计数器的变化以及最终的消息认证结果。在车辆总线网络安全研究领域, 大多选择软件仿真进行验证。在文献[14]和[15]中, 研究人员在 Vector 的 CANoe[16]的帮助下完成了对所提出方案的实验验证。在文献[17]中, 研究人员使用 CAN 分析仪将模拟 ECU 节点的硬件连接到主机, 然后分析实验期间生成的 CAN 消息, 以验证该方案的功能。本章将参考文献[14, 15, 17], 使用本研究领域广泛认可的软件构建实验环境, 并在仿真环境中对本文提出的方案进行实验验证。

5.1 实验环境

CANoe[16, 18]是德国 Vector 公司专门为汽车行业提供的总线开发和测试工具, 自 1996 年推出以来, 它已成为主要汽车制造商和 ECU 供应商首选的总线开发工具。CANoe 最初只支持 CAN 总线的调试和开发, 经过版本迭代, 它几乎支持所有的车载总线协议, 包括 CAN、LIN、FlexRay 和汽车以太网。同时, CANoe 还可以通过硬件连接到真实的总线环境, 提供网络分析和测试功能。我们将使用 CANoe 提供的模拟总线功能, 建立一个包含 4 个节点的 CAN 总线网络, 在这些节点中实现协议, 并通过软件专用的 CAPL 语言和动态链接库接口进行测试。模拟的网络结构如图 4 所示。在实验环境中, 我们选择的 CAN 总线参数是 500k 波特率, 单通道, 传输负载为 8 字节的标准 CAN 帧, 消息认证和新鲜性验证实验将在这个模拟环境中进行。

5.2 实验验证

CRC 字段是在 CANoe 中自动计算的, CANoe 没有向用户提供相关的修改接口, 因此需要通过编写 C 语言代码来完成对消息认证方案的模拟验证。实验将验证该方案中的新鲜性验证机制, 并模拟攻击者在总线上发起重放攻击, 以验证该方案的安全能力。

在验证实现代码中, 我们定义了一个简化的 CAN 帧, 它只包括数据字段和 *MAC* 验证字段。此外, 发送方和接收方的本地存储已适当简化, 双方仅包括通过密钥交换获得的共享密钥。最后, 在代码中定义了 3 个函数来模拟协议中发送方、接收方和攻击者的行为, 如表 2 所示。我们设置了 3 个实验来验证所提出方案的有效性。

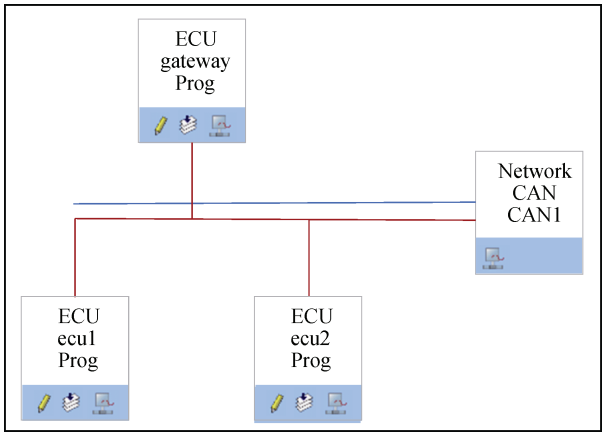

图 4 模拟网络结构图

Figure 4 Simulated network structure diagram

表 2 消息认证方案实验的主要功能

Table 2 The main functions of the message authentication scheme experiment

函数声明	具体功能
sender()	模拟发送方进行 *MAC* 计算和消息传输
receiver(CAN_frame)	模拟接收器的 *MAC* 验证
attacker(CAN_frame)	模拟攻击者对解决方案发起各种攻击

实验一是测试正常通信条件下消息认证的可靠性, 利用 SHA-256 算法生成 *MAC* 值进行验证。在标准 CAN 帧环境下, 随机生成的 16 字节对称密钥被分发给双方, 发送方构造包含数据负载和 *MAC* 值的 CAN 帧, 接收方则通过密钥和时间间隔重新计算 *MAC* 值进行比对, 以确认消息的真实性。

实验二则聚焦于时间间隔不一致情况下的消息认证。在模拟时间延迟后, 接收方首先尝试用当前时间间隔验证 *MAC* 值, 若失败, 则使用时间间隔补偿机制重新验证, 以此测试该机制的效用。

实验三旨在检测系统在重放和欺骗攻击下的防御力。在此实验中, 我们引入了一个攻击者角色, 该角色会截获并稍后重放正常的 CAN 帧。由于时间间隔的不匹配, 接收方应能识别该重放攻击。同时, 由于密钥的保密性, 攻击者无法构造有效欺骗帧, 从而证明了系统对欺骗攻击的防御能力。通过这 3 个精心设计的实验, 我们全面验证了所提出方案在各

种情况下的有效性和合理性, 展示了系统在正常通信、时间间隔变化和恶意攻击下的稳定性和安全性。

实验结果将通过终端窗口打印出来, 如图 5 所示。时间戳是在程序开始运行时记录的, 当发送方或接收方使用新鲜性机制时, 可以通过从实验开始时的时间戳中减去当前时间的时间戳来获得计时器。对于跨时间间隔的消息验证, 实验使用 sleep()函数使接收器延迟验证来模拟这种情况。在模拟重放攻击时, 攻击者将首先保存发送方发送的正常消息, 然后在延迟后将其重新发送给接收方。对于欺骗攻击, 由于攻击者无法获得通信双方的会话密钥, 因此无法计算合法的 *MAC*。发送消息时, 原始 CRC 字段将被保留, 不会被 *MAC* 取代。为了便于分析实验数据, 根据式(2)的设计, 这里我们将时间间隔设计为 1s, 并且补偿 c 的阈值 n 被设置为 1。表 3 列出了上述实验场景和实验结果。

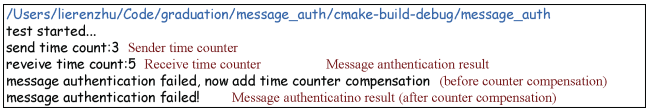

图 5 消息认证方案的实验输出

Figure 5 Experimental output of message authentication scheme

表 3 消息认证方案的实验场景和结果

Table 3 Experimental scenarios and results of message authentication scheme

实验场景	实验设置	认证结果
实验一: 正常时间间隔	通信双方时间计数器同步	通过
实验二: 跨时间间隔	通信双方时间计数器相差 1	未通过, 引入补偿值 c=1 后通过
实验三: 重放攻击	报文与接收方时间计数器相差 4	未通过
实验三: 欺骗攻击	保留原 CRC 字段	未通过

6 总结

本文首先介绍了车内网络的发展现状和对 CAN 总线攻击的研究成果, 进一步强调了 CAN 总线中消息认证的重要性。然后对现有的 CAN 总线消息认证方案进行分析, 总结了它们在实际开销大以及应用迁移性差等方面的缺点, 随后给出相应的解决方案。我们的方案具体包括 3 个部分: 替换 CRC 字段为 *MAC* 字段, 用于改善迁移性差的问题; 基于时间间隔的新鲜性机制, 用于改善实际开销大的缺陷; *MAC* 生成机制, 包括具体对 *MAC* 字段的使用。最后对该方案的安全性进行分析, 证明其不仅能有效防御重放与欺骗等网络攻击, 还提升了系统的安全性、抗去同步化能力和整体的鲁棒性, 不仅如此, 我们的方案还具有一定的协议迁移性。此外, 我们在专业软件 CANoe 中建立了仿真环境, 并设计了对比实验进行实际测试, 以进一步证明该方案的真实性和有效性。

参考文献

[1] Mössinger J. Software in automotive systems[J]. *IEEE Software*, 2010, 27(2): 92-94.

[2] Goswami D, Schneider R, Masrur A, et al. Challenges in Automotive Cyber-Physical Systems Design[C]. *2012 International Conference on Embedded Computer Systems*, 2013: 346-354.

[3] Xie Y, Liang W, Li F R, et al. A vehicle CAN signal packaging algorithm suitable for the Internet of Vehicles environment [J]. *Journal of Software*, 2016, 27(9): 2365-2376.

[4] Anwar A, Anwar A, Moukahal L, et al. Security assessment of in-vehicle communication protocols[J]. *Vehicular Communications*, 2023, 44: 100639.

[5] Ben Chehida Douss A, Abassi R, Sauveron D. State-of-the-art survey of in-vehicle protocols and automotive ethernet security and vulnerabilities[J]. *Mathematical Biosciences and Engineering*, 2023, 20(9): 17057-17095.

[6] Hoppe T, Dittman J. Sniffing/Replay Attacks on CAN Buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy[C]. *Proceedings of the 2nd workshop on embedded systems security,* 2007: 1-6.

[7] Miller C, Valasek C. Remote exploitation of an unaltered passenger vehicle[J]. *Black Hat USA*, 2015, 2015(S 91): 1-91.

[8] Gilbert H, Handschuh H. Security Analysis of SHA-256 and Sisters[M]. Selected Areas in Cryptography. Berlin, Heidelberg: Springer, 2004: 175-193.

[9] Menezes A J, van Oorschot P C, Vanstone S A. Handbook of Applied Cryptography[M]. Boca Raton: CRC Press, 1996.

[10] Bellare M, Canetti R, Krawczyk H. Keying Hash Functions for Message Authentication[C]. *Advances in Cryptology — CRYPTO '96*, 1996: 1-15.

[11] Nissen I. Adaptive Systems for Mobile Underwater Communications with a P (oste) riori Channel Knowledge. *FWG Report* 59 (2008).

[12] Cho K T, Shin K G. Fingerprinting Electronic Control Units for Vehicle Intrusion Detection[C]. *The 25th USENIX Conference on Security Symposium*, 2016: 911-927.

[13] Schmandt J, Sherman A T, Banerjee N. Mini-MAC: Raising the bar for vehicular security with a lightweight message authentication protocol[J]. *Vehicular Communications*, 2017, 9: 188-196.

[14] Radu A I, Garcia F D. LeiA: A lightweight authentication protocol for CAN[C]. *Computer Security – ESORICS 2016* 2016: 283-300.

[15] Song H M, Kim H R, Kim H K. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network[C]. *2016 International Conference on Information Networking*, 2016: 63-68.

[16] Vector.CANoe[EB/OL].https://www.vector.com/at/en/products/products-a-z/software/canoe/, 2022.

[17] Woo S, Jo H J, Lee D H. A practical wireless attack on the connected car and security protocol for in-vehicle CAN[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2015, 16(2): 993-1006.

[18] Li J Z. Design of Network Security Protocol for Vehicle CAN Bus Gateway [D]. Yanbian *University*, 2022. DOI:10.27439/d.cnki.gybdu.2022.001089.

徐国胜 于 2008 年在北京邮电大学信息安全专业获得博士学位。现任北京邮电大学网络空间安全学院副教授, CCF 会员。研究领域为移动安全、人工智能。研究兴趣包括: 现代密码学、人工智能安全、车联网等。Email: guoshengxu@bupt.edu.cn

汪梓撼 于 2022 年在北京交通大学信息安全专业获得学士学位。现在北京邮电大学网络空间安全专业攻读硕士学位。研究领域为密码算法、车联网。研究兴趣包括: 轻量级密码算法、车内网络安全等。Email: wzh@bupt.edu.cn

李逸静 于 2022 年在北京邮电大学信息与通信工程专业获得工科博士学位。现任中国信息通信研究院安全研究所任工程师。研究领域为车联网、网络安全。研究兴趣包括: 大数据通信、车联网隐私等。Email: liyijing@caict.ac.cn

王晨宇 于 2020 年在北京邮电大学网络空间安全专业获得博士学位。现任北京邮电大学网络空间安全学院特聘副研究员, CCF 会员。研究领域为安全协议、身份认证。研究兴趣包括: 人工智能安全、车联网安全等。Email: wangchenyu@bupt.edu.cn