DOI：10.7652/xjtuxb201805014

车载控制器局域网络安全协议

刘毅[1]，秦贵和[2,3]，赵睿[1]
（1.吉林大学计算机科学与技术学院，130012，长春；2.吉林大学符号计算与知识工程教育部重点实验室，130012，长春；3.吉林大学软件学院，130012，长春）

摘要：针对汽车智能化、网联化快速发展，攻击者通过逐渐开放的接口向汽车发动攻击，严重威胁驾驶者的人身和财产安全，进而引发的车载信息安全问题，提出了一种车载控制器局域网络安全协议(SPOCAN)。SPOCAN包含2个模块，启动阶段的安全模块采用公钥体系认证机制，在车辆点火启动的过程中进行初始化认证，保证了待通信节点身份的真实性；通信阶段的安全模块采用对称加密算法及信息摘要算法，在车辆正常运行时保障了节点间通信的安全，保证了数据机密性、消息正确性和数据完整性，并通过递增的序列号实现了防重放保护。通过搭建控制器局域网络车载控制系统的硬件平台对所提出的安全协议进行评估，实验结果表明，该协议能够从汽车点火启动阶段到运行通信阶段有效地为车载控制器局域网络提供安全保障，提高了网络的信息安全级别。

关键词：车载信息安全；控制器局域网络；安全协议
中图分类号：TP399 **文献标志码**：A **文章编号**：0253-987X(2018)05-0094-07

Security Protocol for On-Board Controller Area Network

LIU Yi[1], QIN Guihe[2,3], ZHAO Rui[1]
(1. College of Computer Science and Technology, Jilin University, Changchun 130012, China;
2. Symbol Computation and Knowledge Engineer of Ministry of Education, Jilin University, Changchun 130012, China;
3. College of Software, Jilin University, Changchun 130012, China)

Abstract: A safety protocol for on-board controller area networks (SPOCAN) is proposed to solve the problem that attackers can launch attacks on vehicles through the gradually opening interfaces caused by the rapid development of auto intelligence and networking, while these attacks will cause serious threat to driver's personal and property safety, and trigger the cyber security of vehicles furthermore. The SPOCAN contains two modules, SNIA and CNEP. SNIA uses the public key system authentication mechanism, and executes the process of initialization of certification in the vehicle ignition stage to ensure the authenticity of the identity between the communicated nodes. CNEP uses a symmetric encryption algorithm and an information digest algorithm to guarantee data confidentiality, message correctness, data integrity, and the safety of communication among nodes in the vehicle communication stage. At the same time, the anti-replay protection is achieved through the increasing sequence number. A hardware platform of CAN network vehicle control system is built to assess the proposed security protocol, and experimental results show that the protocol effectively provides CAN bus security from the vehicle ignition stage to the vehicle communication stage, and improves information security of

收稿日期：2017-10-15。 作者简介：刘毅(1993—)，男，硕士生；秦贵和(通信作者)，男，教授，博士生导师。 基金项目：吉林省重点科技攻关资助项目(20150204034GX)。
网络出版时间：2018-03-27 网络出版地址：http://kns.cnki.net/kcms/detail/61.1069.T.20180327.0847.002.html

the CAN bus.

Keywords: in-vehicle information security; controller area network; security protocol

随着智能网联汽车的发展，自主驾驶、车队管理、智能交通管理等技术应运而生[1]，这些技术的应用提升了驾驶的舒适性与便捷性，但同时越来越多开放的接口也使得汽车的风险指数逐渐增加。攻击者可以通过 WiFi、蓝牙、OBD-II 等接口对汽车发动长距离或短距离、有线或无线的攻击，严重威胁驾驶者的人身和财产安全，因此网联汽车信息安全问题亟待解决。车载网关承担着车内总线网络和车外网络的信息交互，仅仅在车载网关上增加防火墙的方式并不能提供足够的安全防护，网联汽车的信息安全问题更需要保护车内总线网络的信息安全[2]。

车载控制器局域网络(CAN)总线因其灵活性、实时性、可靠性已成为车内总线网络的标准[3]，并且 CAN 总线在未来一段时间内也将是车载总线技术的基础。CAN 总线虽然有着得天独厚的优势，CAN 总线协议却没有考虑到信息安全问题。CAN 协议不能对连接到总线上的节点提供身份认证，不能对总线上传输的数据提供加密保护，也不能支持保障数据正确性与完整性的校验机制，由此造成的严重后果是攻击者可以轻易地窃听、伪造、篡改数据，发动重放攻击。考虑到网联汽车的出现及 CAN 总线安全漏洞，CAN 总线的信息安全问题成为现实中亟需解决的问题。

近年来，欧盟等相关机构积极资助并开展汽车信息安全项目，例如车辆电子安全入侵检测应用项目(EVITA)、开放式车辆安全平台项目(OVERSEE)等。EVITA 项目[4]定义了安全需求并且提供了应用于车载网络的方法，其中中量级硬件安全模块保障了电子控制单元之间通信环境的安全；OVERSEE项目提供了标准的软件架构和车辆运行的内部环境，保障了信息的安全性和可靠性[5-6]，但是这些项目并没有给出具体的安全措施，也没有有效的安全协议。

对于车载网络安全协议的研究中，文献[7-9]的安全协议考虑了 CAN 总线的广播特性，并利用数据域长度受限的特点设计协议以降低总线负载。由于上述协议没有考虑到车辆启动阶段的初始化身份认证，也不能提供车辆通信阶段的防重放保护，因此不能很好地为车载 CAN 总线提供安全保障。

在 CAN 总线协议特点和安全需求的基础上，设计了一种车载控制器局域网络的安全协议(SPOCAN)，深入研究并分析 CAN 总线协议的特点、网联汽车攻击接口及 CAN 总线安全需求；考虑到受限车载资源和 CAN 协议的特点，设计了 CAN 总线的安全协议 SPOCAN，SPOCAN 包含 SNIA 和 CNEP 2 个模块，SNIA 模块提供待通信节点身份的真实性保证，在车辆点火启动阶段保障节点的身份安全，CNEP 模块保障了数据机密性、消息正确性、数据完整性和数据新鲜性，在车辆运行通信时保障节点间通信安全；为了验证所提安全协议的有效性，基于飞思卡尔 MPC5646C 网关和 MC9S12XDT512 开发板搭建了 CAN 网络车载控制系统的硬件平台，在汽车点火启动阶段和车辆运行通信阶段分别进行了测试，验证了 SPOCAN 协议能够有效地提供安全保障。

1　CAN 总线及网联汽车信息安全分析

1.1　CAN 总线

在车载总线网络中，CAN 总线是目前使用最广泛的总线技术，因为它使用双绞线传输信号，显著地降低了通信线缆的数量，并且提供了更高的通信可靠性。CAN 总线协议根据 ID 域的不同，分为 CAN 2.0A 标准格式和 CAN 2.0B 扩展格式 2 部分[10]，由于 CAN 2.0B 支持 CAN 2.0A，所以对 CAN 2.0B 解释说明。CAN 2.0B 数据帧中的 ID 域用于设置消息的优先级，其 29 位 ID 域分为标准 ID 和扩展 ID 2 个部分，IDE 域决定是否使用 18 位扩展 ID，数据域包含 0～8 个字节数据，循环冗余校验(CRC)域提供传输过程中的错误检测，这也是 CAN 协议中唯一与安全相关的校验机制，但这种简单的校验机制无法满足网联汽车的安全需求。

1.2　网联汽车攻击接口

网联技术的发展使汽车开放的接口越来越多，这些接口可能成为攻击者对汽车发动攻击的入口[11]。图 1 给出了整个汽车电子系统可能的攻击接口，根据攻击者的连接方式，这些接口可以分为以下 3 类：①物理访问接口。攻击者通过直连的方式或者使用第三方工具访问汽车内部网络，例如车载诊断系统的外部接口 OBD-II、用于娱乐系统的 USB 接口和开放的充电桩接口等；②短距离无线访问接口。在物理连接难以实现的情况下，攻击者通过非物理接触、近距离的方式访问接口，这种短距离访问

一般通过在距离汽车 5～300 m 的范围内放置发射器与接收器的方式来实现[12]，这类典型接口包括蓝牙、WiFi、无钥匙进入系统、车载雷达等；③长距离无线访问接口。攻击者通过无线电、卫星导航 GPS/北斗等通信距离超过 1 km 的接口实现长距离访问攻击[13]。

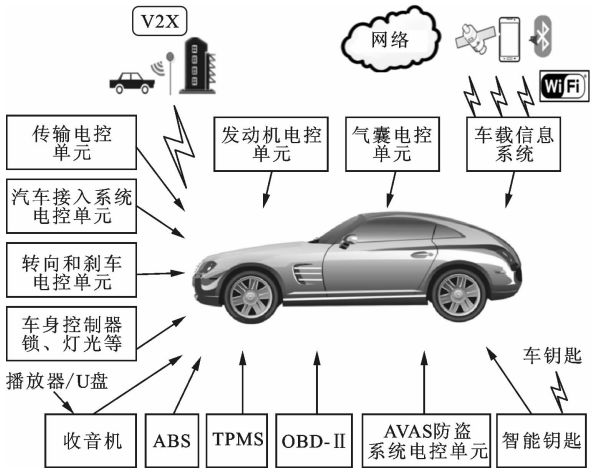

图 1 网联汽车的攻击接口

2 CAN 总线安全需求

结合 CAN 总线特点设计控制器局域网络安全协议需要满足以下 5 点安全需求：①身份真实性。CAN 总线系统中通信双方在建立通信前，需要确认双方的有效身份，防止攻击者利用虚假身份进行通信；②数据机密性。CAN 总线网络由于其广播发送、明文传输的特性，极易泄露数据，尤其当信息是与驾驶员的生命安全息息相关时，数据加密与语义安全的保障显得尤为必要；③消息正确性。CAN 总线上节点间相互通信时，接收方需要确认该消息来自于正确的发送方而不是攻击节点发送的伪造信息；④数据完整性。CAN 总线上消息的接收方需要确保消息在传输过程中没有被攻击者更改，一般地，数据完整性通过消息认证[14]来保证；⑤数据新鲜性。在 CAN 总线上传输的数据需要保证是最近发送的，而不是一个已经在总线上发送过的数据，对数据新鲜性的保证能够防止重放攻击。

3 SPOCAN 协议

为了在车载控制器局域网络中满足上述安全需求，在 CAN 总线协议的基础上，增加了汽车点火启动阶段的安全模块 SNIA 和通信阶段的安全模块 CNEP，实现了车载控制器局域网络安全协议 SPOCAN。SNIA 模块采用基于公钥体系认证方法的身份认证技术，保障了待通信节点的身份真实性，在汽车点火启动阶段保障了节点之间的通信安全；CNEP 模块采用了加密通信、消息检验及序列号技术，保障了 CAN 总线上节点间信息传递时的数据机密性、消息正确性、数据完整性和数据新鲜性。SPOCAN 基于这 2 种安全模块，能够在汽车启动阶段和通信阶段阻止基于消息窃听、信息伪造、消息篡改、数据重放等攻击手段，有效地保障车载 CAN 总线网络上节点间的通信安全。

3.1 SNIA 模块

SNIA 模块提供了 CAN 总线网络中节点的身份认证方法。考虑到 CAN 总线广播发送的特性，若采用私钥体系的认证方法，其中任何一个接收节点都可以模仿发送节点伪造消息给其他接收节点，因此 CAN 总线需要非对称的认证机制来完成广播认证。SNIA 模块采用基于公钥体系认证方法，在车辆点火启动的过程中进行初始化身份认证[15]，身份认证只进行一次并在认证结束后更新密钥，以备在下次初始化过程中使用。

身份认证过程是连接到总线上的各个电子控制单元(ECU)向网关 G 请求身份认证，认证通过后得到由网关分发的保障数据机密性的加密密钥 K_e 和消息校验阶段的认证密钥 K_a。在所提方案中使用 RSA-64 位非对称加密算法[16]，E 为加密函数，D 为解密函数，身份认证过程具体分为以下 5 个步骤。

步骤 1 第 i 个 ECU 通过查询证书 C_i 将其标志 I_i 用网关公钥 G_u 加密得到密文 C_1 发送到 CAN 总线上。证书中包含节点标志、节点的密钥和节点的其他信息，不同节点的公钥通过查询获得，私钥是每个节点独有的，除节点自身外其他节点无法获取。为保证安全性，证书由车场刷写 ECU 固件时写入

$$C_1 = E(G_u, I_i) \tag{1}$$

步骤 2 网关 G 用私钥 G_r 解密收到的消息得到 P_1，读取其标志 I_i，G 在证书 C_g 中查找此 I_i 对应的节点公钥 E_u，并产生一个挑战值 N_k，用此公钥 E_u 将挑战值 N_k 加密发送到 CAN 总线上，得到 C_2

$$P_1 = D(G_r, C_1) \tag{2}$$

$$C_2 = E(E_u, N_k) \tag{3}$$

步骤 3 该 I_i 对应的 ECU 利用私钥 E_r 解密收到的消息后得到 P_2，读取数据 N'_k，将该数据再次利用网关公钥 G_u 加密发送到 CAN 总线上，得到 C_3

$$P_2 = D(E_r, C_2) \tag{4}$$

$$C_3 = E(G_u, N'_k) \tag{5}$$

步骤 4 网关 G 利用私钥 G_r 解密 C_3 后得到 P_3，读

取数据。若数据中的挑战值等于步骤 2 中网关 G 产生的挑战值 N_k，则网关把该 ECU 对应的 I_i 加入到其信任列表中，表明网关已信任该节点并可以与它进行通信

$$P_3 = D(G_r, C_3) \tag{6}$$

步骤 5　网关 G 与第 i 个 ECU 认证成功后，则以非对称加密方法颁布用于通信的加密密钥 K_e 和用于消息校验的认证密钥 K_a。若认证不成功，则不会给节点颁布密钥

$$C_4 = E(E_u, K_e) \tag{7}$$

$$C_5 = E(E_u, K_a) \tag{8}$$

上述认证过程中密钥 K_e 和 K_a 只能由网关生成，身份认证过程只在芯片上电后进行一次。为了保证认证后节点间的通信安全，节点间通信密钥由网关定期更新。

至此，初始化身份认证阶段结束，在系统内网关确认了待通信节点的身份并生成了通信阶段加解密密钥及消息校验密钥。

3.2　CNEP 模块

汽车点火启动阶段的初始化认证结束后，节点间通信的安全保障通过 CNEP 模块实现。在所提方案中使用 DES-64 位对称加密算法和 MD5-32 位消息摘要算法[16]保证了数据机密性、消息正确性和数据完整性，并且通过序列号递增的方法提供了防重放保护。序列号是系统初始化时约定的，在每次使用后递增，并要足够大才能避免不同的消息产生相同的序列号。

发送方在发送数据前需要经过如下 4 个步骤。

步骤 1　发送方将待发送数据 T 与第 j 个序列号 C_j 进行或运算得到 T'。考虑到车载通信的大部分数据帧数据域的长度在 3～4 个字节，所以 C_j 仅在第 7 个字节中存储

$$T' = T \parallel C_j \tag{9}$$

步骤 2　将通过 SNIA 协议认证得到的密钥 K_e 与接收端保持一致的随机数 S_j 异或后得到新密钥，再利用新密钥对 T' 加密得到 C_6，并对 S_j 更新

$$C_6 = E((K_e \oplus S_j), T') \tag{10}$$

步骤 3　利用密钥 K_a 发送方对 C_6 计算消息认证码

$$M_j = E(K_a, C_6) \tag{11}$$

步骤 4　C_6 存储在 CAN 协议数据帧的前 7 个字节中，M_j 存储在最后 1 个字节中，将密文 C_6 和 M_j 一同发送到 CAN 总线上

$$C_7 = C_6 \parallel M_j \tag{12}$$

接收方在收到消息后需要经过如下 4 个步骤。

步骤 1　接收方收到消息 C_7 后，利用 C_7 的前 7 个字节通过 K_a 计算消息认证码 M_j'。若生成的 M_j' 与 C_7 中第 8 个字节的 M_j 不一致，则识别出这是一个伪造信息，并发出报警信号

$$M_j' = E(K_a, C_7) \tag{13}$$

步骤 2　消息校验通过后，利用 K_e 与随机数 S_j 异或，对 C_7 的前 7 个字节解密得到 P_4 并更新 S_j

$$P_4 = D((K_e \oplus S_j), C_7) \tag{14}$$

步骤 3　分解 P_4 得到 T 和发送端序列号 C_j'

$$P_4 = T \parallel C_j' \tag{15}$$

步骤 4　比较得到的序列号 C_j' 与本地序列号 C_j 是否一致。若一致，则使用数据并更新序列号；若不一致，则发生了重放攻击，进行危险警告。

CNEP 模块通过随机数 S_j 随机化加密，提供了语义级别的安全保护，S_j 每次加密后发生变化且不会重复，这种强安全协议阻止了攻击者从窃听到的加密消息推断出明文；由于使用了消息认证码进行校验，在不影响正常通信的前提下增强了系统的防伪造特性；采用序列号技术进行端到端的计算，提供弱新鲜性防护以及防重放攻击保护。

4　安全协议有效性评估的实验

为了对所提安全协议进行有效性评估，本文基于飞思卡尔 MPC5646C 网关和 MC9S12XDT512 开发板搭建了 CAN 网络车载控制系统的硬件平台，其中 1 块 MPC5646C 作为网关 G，4 块 MC9S12XDT512 作为与该网关相连的节点 a、b、c、d，同时使用 USB-CAN-II 模拟一个攻击节点 S 对总线发动攻击。实验从点火启动阶段和通信阶段分别模拟攻击场景，在 PC 机上使用 CodeWarrior 环境编程并使用 CANTest 软件显示总线上传输的数据。

4.1　点火启动阶段安全测试分析

点火启动阶段的安全性是指在 ECU 上电后，需要确定 CAN 总线系统中所有待通信节点身份的真实性，在初始化阶段阻止基于身份欺骗的攻击，该阶段实验设置了 3 个攻击场景，验证了节点身份的真实性。

在初始化认证阶段，系统内各节点需要向网关节点 G 申请认证，假设一个攻击节点 S 在车辆启动前就已经连接到总线上，准备发动攻击。

场景 1　S 并没有获得总线上传输的信息，只是伪造了认证请求消息并发送给 G，希望得到网关的认证。由于 S 作为相对于内部车载控制系统的外部节点，没有车场统一刷写的证书，因此无法通过查询

获得 G 的公钥 G_u，不能将伪造的认证请求加密发送到 CAN 总线上。网关收到消息后无法正确解密进而无法识别出这个请求认证消息，所以请求身份认证无效。

场景 2 S 通过窃听总线上的消息，获得了节点 b 请求身份认证的报文，并在此基础上将部分信息篡改后发送到 CAN 总线上。如表 1 的第 6 号所示，虽然 S 在正确请求认证报文的基础上篡改信息，但 G 仍会识别出这是一个无效的身份认证请求，如表 1 的第 7 号所示。S 的篡改使得正确的请求认证消息发生了变化，该消息不再是由网关公钥加密后的正确信息；同时，消息的篡改也使得 G 无法正确分析出所请求认证的节点标志，进而也无法通过查询确定所请求节点的公钥，G 识别出 S 是一个攻击节点。

场景 3 S 通过窃听总线上的消息，获得了节点 a 请求身份认证的报文，此时 S 不做任何修改，将消息再次发送到 CAN 总线上，如表 1 的第 14 号所示。G 为了验证该节点的身份，发出表 1 中第 15 号的验证帧，S 收到该消息后，无论是通过伪造、篡改还是再次将窃听到的节点 a 的反馈帧发送给 G，G 在这 3 种情况下都不会通过 S 的身份认证。在前 2 种情况下，G 无法正确识别出反馈帧，进而不能正确解密消息并确定所请求节点标志。在最后一种情况下，如表 1 的第 16 号所示，因为 G 发送的验证帧中利用节点 a 的公钥 E_u 加密发送了一个挑战值 N_k，由于每次加密的挑战值是不同的，使得本次验证帧中的挑战值与 S 重放的节点 a 的反馈帧中的挑战值不一致，因此 G 能识别出基于身份欺骗的攻击。

4.2 通信阶段安全测试分析

通信阶段安全性是指在车辆启动后，各个 ECU 通过身份认证后开始通信，攻击者除了在车辆初始化阶段发动攻击外，还有可能在车辆通信时通过 OBD-II 等通信接口发动攻击。该阶段实验设置了 4 个攻击场景，分别验证了消息正确性、数据机密性、消息完整性、数据新鲜性。

场景 1 S 没有通过窃听得到总线上的消息，只是通过消息伪造向节点 d 发送攻击数据，如表 2 的第 2 号所示。S 企图接收到节点 d 响应的数据信息，此时节点 d 发出了警报帧，如表 2 中的第 5 号所示。这是因为 S 并没有参与节点启动过程的初始化身份认证，进而无法得到通信时的加解密密钥 K_e 和消息校验密钥 K_a。S 可以伪造消息却无法伪造这 2 个密钥，节点 d 接收到消息后，无法正确接收并进行消息校验与解密处理，因此识别出这是一个攻击节点发送的伪造消息。

场景 2 由于攻击节点是在汽车启动后以直接或间接的方式连接到车上，没有经过点火启动阶段的身份认证，从而并没有通信阶段的加密密钥，因此 S 企

表 1 车辆启动阶段的攻击测试

序号	传输方向	帧 ID	帧格式	数据长度	数据							
1	接收	0x00000001	数据帧	0x08	00	00	00	00	03	00	08	06
2	接收	0x00000004	数据帧	0x08	00	00	00	00	00	06	09	05
3	接收	0x00000001	数据帧	0x08	00	00	00	00	02	03	00	04
4	接收	0x00000004	数据帧	0x08	00	10	75	f4	f9	09	0f	76
5	接收	0x00000004	数据帧	0x08	01	0f	c8	11	15	f7	00	15
6	发送	0x00000001	数据帧	0x08	00	00	00	00	03	07	06	04
7	接收	0x0000001e	数据帧	0x08	ff	ff	ff	ff	ff	ff	ff	ff
8	接收	0x00000003	数据帧	0x08	01	16	24	82	b7	1c	7c	71
9	接收	0x00000001	数据帧	0x08	00	00	00	00	01	03	08	07
10	接收	0x00000003	数据帧	0x08	00	00	00	00	00	02	00	04
11	接收	0x00000001	数据帧	0x08	00	00	00	00	00	03	09	09
12	接收	0x00000003	数据帧	0x08	00	ec	15	ee	d0	ea	9c	45
13	接收	0x00000003	数据帧	0x08	01	9c	f7	a8	6f	d6	02	7e
14	发送	0x00000001	数据帧	0x08	00	00	00	00	01	03	08	07
15	接收	0x00000003	数据帧	0x08	00	00	00	00	02	01	04	07
16	发送	0x00000001	数据帧	0x08	00	00	00	00	00	03	09	09
17	接收	0x0000001e	数据帧	0x08	ff	ff	ff	ff	ff	ff	ff	ff

图监听总线上的一系列消息，并希望通过足够数量的加密密文推断出明文。虽然攻击者知道了部分数字 0 和数字 1 加密后对应的数字或字符，但是并不能判断出一个新加密的字符是用 0 加密的还是用 1 加密的。CNEP 模块的发送方利用了一个随机数 S_j 和密钥 K_e 异或后加密数据，由于这个 S_j 每次加密后都是不同的，使得相同的消息在不同的会话通信时加密后的数据是不同的。攻击者即使知道了部分明文密文对，也无法推断出加密前的消息。

场景 3　S 窃听总线上的消息，如表 2 的第 8 号所示，并在窃听到的消息的基础上篡改消息中的部分控制位数据然后发送给节点 b，如表 2 的第 11 号所示，企图控制节点 b 执行相关操作。CNEP 模块采用的消息检验技术可以保护消息传递过程中的数据完整性，由于数据段发生了更改，节点 b 收到消息后对数据段进行消息校验时，会检测到不一致的消息检验码，检测出此消息在发送的过程中发生了变化，则会拒绝接受此消息并发出报警帧如第 13 号。

场景 4　S 通过窃听总线消息，不做任何修改，只是重复发送一个已经在总线上发送过的消息，准备发动重放攻击以使 CAN 总线系统不能正常提供服务。如表 2 的第 18 号所示，S 重放了表 2 中的序号为 15 的帧。由于 CNEP 模块采用了序列号技术，重放消息的序列号 C_j 并没有发生改变，按照 CNEP 模块执行时，接收端就会检查到不一致的序列号，检测到重放攻击，并发出警报帧如第 21 号。

本文基于搭建 CAN 网络车载控制系统的硬件平台，对 SPOCAN 协议的有效性进行了完整且充分地评估。通过对 2 个阶段分别进行模拟攻击，完整地考虑了从汽车点火启动阶段到运行通信阶段的安全需求，保障了实验测试的完整性。通过对启动阶段设计的 3 个攻击场景，充分考虑了在该阶段对 ECU 身份真实性的可能发动的伪造攻击、篡改攻击以及重放攻击；通过对通信阶段设计的 4 个攻击场景，充分考虑了在该阶段对消息正确性、数据机密性、消息完整性、数据新鲜性可能发动的伪造攻击、窃听攻击、篡改攻击以及重放攻击，保障了实验测试的充分性。通过对 2 个阶段 7 种攻击场景的实验测

表 2　车辆通信阶段的攻击测试

序号	传输方向	帧 ID	帧格式	数据长度	数据							
1	接收	0x00000005	数据帧	0x08	12	cf	d8	00	6a	bb	77	5e
2	发送	0x00000004	数据帧	0x08	24	0a	6f	e3	2b	36	5b	43
3	接收	0x00000001	数据帧	0x08	47	13	40	11	b4	1a	41	90
4	接收	0x00000002	数据帧	0x08	24	04	16	45	00	23	15	96
5	接收	0x0000001d	数据帧	0x08	ff	ff	ff	ff	ff	ff	ff	ff
6	接收	0x00000003	数据帧	0x08	14	6f	73	48	17	2a	7f	12
7	接收	0x00000001	数据帧	0x08	02	14	37	54	96	bb	13	7a
8	接收	0x00000005	数据帧	0x08	43	2b	9a	18	63	09	17	66
9	接收	0x00000001	数据帧	0x08	b7	54	36	27	09	b6	71	e4
10	接收	0x00000002	数据帧	0x08	3b	41	3f	4b	20	71	34	17
11	发送	0x00000005	数据帧	0x08	43	2b	9a	11	96	09	b3	10
12	接收	0x00000001	数据帧	0x08	13	72	0a	48	33	90	14	62
13	接收	0x0000001f	数据帧	0x08	ff	ff	ff	ff	ff	ff	ff	ff
14	接收	0x00000001	数据帧	0x08	d2	d4	90	91	6f	92	7e	aa
15	接收	0x00000002	数据帧	0x08	bb	9f	b3	94	96	bb	02	5d
16	接收	0x00000001	数据帧	0x08	7f	3f	92	c4	8b	0c	6a	ee
17	接收	0x000000ff	数据帧	0x08	79	9d	03	8k	76	91	04	00
18	发送	0x00000002	数据帧	0x08	bb	9f	b3	94	96	bb	02	5d
19	接收	0x00000002	数据帧	0x08	06	y4	7f	34	89	b5	08	72
20	接收	0x00000005	数据帧	0x08	5a	9b	76	44	03	a5	47	70
21	接收	0x00000020	数据帧	0x08	ff	ff	ff	ff	ff	ff	ff	ff
22	接收	0x00000001	数据帧	0x08	80	ff	bc	27	14	bf	ca	91

试,结果表明,该 SPOCAN 协议能有效地为 CAN 总线提供安全保障。

5 结 论

针对汽车网联化所带来的车载 CAN 总线的信息安全问题,本文提出了一种车载控制器局域网络安全协议 SPOCAN,该协议包含 SNIA 和 CNEP 2 个模块。SNIA 模块提供车辆启动阶段 ECU 间的身份认证,保障待通信节点的身份真实性;CNEP 模块提供了车辆启动后通信阶段的安全保障,提供数据机密性,消息正确性、数据完整性和数据新鲜性保护。本文从汽车点火启动阶段和通信阶段对该协议进行了有效性评估,实验结果验证了该协议能够为 CAN 总线提供良好的安全保障。

参考文献:

[1] 张亚萍,刘华,李碧钰,等. 智能网联汽车技术与标准发展研究 [J]. 上海汽车,2015(8):55-59.
ZHANG Yaping, LIU Hua, LI Biyu, et al. Research on intelligent network technology and standard development of automotive technology [J]. Shanghai Automotive, 2015(8): 55-59.

[2] 于赫. 网联汽车信息安全问题及 CAN 总线异常检测技研究 [D]. 吉林:吉林大学,2016:15-31.

[3] 田希晖,张玘,张连超,等. CAN 总线及其应用技术 [J]. 微计算机信息:测控仪表自动化,2002(9):3-5.
TIAN Xihui, ZHANG Qi, ZHANG Lianchao, et al. CAN bus and its application technology [J]. Microcomputer Information: Measurement and Control Instrumentation Automation, 2002(9): 3-5.

[4] HENNINGER O. E-safety vehicle intrusion protected applications (EVITA) project [EB/OL]. (2008-07-31)[2017-10-05]. http// www. evita-project. org.

[5] GROLL A, HOLLE J, RULAND C, et al. OVERSEE a secure and open communication and runtime platform for innovative automotive applications [C]// Proceedings of the 19th Intelligent Transport Systems World Congress. Washington D C, USA: ITS, 2012: EU-00690.

[6] HOLLE J, PLATSCHEK A, SANCHEZ J, et al. OVERSEE: a secure and open in-vehicle ITS station [C]// Proceedings of the 19th ITS World Congress. Washington D C, USA: ITS, 2012: EU-00469.

[7] LIN C W, SANGIOVANNI-VINCENTELLI A. Cyber-Security for the controller area network (CAN) communication protocol [C]// Proceedings of the International Conference on Cyber Security. Piscataway, NJ, USA: IEEE Computer Society, 2012: 1-7.

[8] NILSSON D K, LARSON U E, JONSSON E. Efficient in-vehicle delayed data authentication based on compound message authentication codes [C]// Proceedings of the Vehicular Technology Conference. Piscataway, NJ, USA: IEEE, 2008: 1-5.

[9] GROZA B, MURVAY S. Efficient protocols for secure broadcast in controller area networks [J]. IEEE Transactions on Industrial Informatics, 2013, 9(4): 2034-2042.

[10] 王莉,刘德新,刘书亮. 汽车网络标准总线 CAN [J]. 世界汽车,2001(1):15-17.
WANG Li, LIU Dexin, LIU Shuliang. Automotive network standard bus CAN [J]. World Automotive, 2001(1): 15-17.

[11] CHECKOWAY S, MCCOY D, KANTOR B, et al. Comprehensive experimental analyses of automotive attack surfaces [C]// Proceedings of the Usenix Security Symposium. Berkeley, CA, USA: Usenix, 2011: 6.

[12] EZAKI T, DATE T, INOUE H. An analysis platform for the information security of in-vehicle networks connected with external networks [C]// Proceedings of the International Workshop on Security. Berlin, Germany: Springer, 2015: 301-315.

[13] NIGHSWANDER T, LEDVINA B, DIAMOND J, et al. GPS software attacks [C]// Proceedings of the ACM Conference on Computer and Communications Security. New York, USA: ACM, 2012: 450-461.

[14] SVAMSIKRISHNA T R, HARIHARAN R H. VANET-based vehicle tacking on message authentication and secure navigation route [J]. International Journal of Computer, 2015, 113(7): 32-40.

[15] LIU H, LIANG X, FANG L, et al. A secure and authentication protocol based on identity based aggregate signature for electric vehicle applications [C]// Proceedings of the International Conference on Wireless Communication and Sensor Network. Piscataway, NJ, USA: IEEE, 2015: 353-357.

[16] 胡向东. 应用密码学 [M]. 2 版. 北京:电子工业出版社,2011:87-88.

(编辑 武红江)