基于改进差分算法的汽车ECU远程升级回滚策略

胡 杰[1,2,3]，邓佳慧[1,2,3]，徐文才[1,2]，岳意娥[4]，范志容[4]

（1. 武汉理工大学 现代汽车零部件技术湖北省重点实验室，武汉 430070；
2. 新能源与智能网联汽车湖北省工程技术研究中心，武汉 430070；
3. 武汉理工大学 人工智能与新能源汽车现代产业学院，武汉 430070；
4. 东风汽车集团有限公司研发总院，武汉 430058）

摘 要：针对汽车ECU远程升级失败时，现有回滚方法效率低下、鲁棒性弱的问题，设计了一种高效且稳定的升级回滚策略。提出优化的回滚备份方法和完备的安全校验策略，以提升回滚过程的稳定性。考虑传统全量回滚耗时较长，提出采用改进Bsdiff差分算法的差分回滚技术，利用压缩性能更高的LZMA2压缩算法，并优化差分包的数据格式，显著提升回滚效率。在实车上对所设计的策略进行测试，结果表明，采用改进差分算法的回滚策略能将回滚时间缩短84.69%，测试用例通过率为100%，确保汽车ECU在升级失败时车辆功能不受影响，同时提高了回滚效率。

关键词：空中在线升级技术；差分算法；车载ECU；回滚策略

中图分类号：U461 **文献标志码：**A **DOI：**10.3969/j.issn.2095–1469.2025.04.07

Rollback Strategy for Remote Automotive ECU Upgrades Based on Improved Differential Algorithm

HU Jie[1,2,3]，DENG Jiahui[1,2,3]，XU Wencai[1,2]，YUE Yie[4]，FAN Zhirong[4]

（1. Hubei Key Laboratory of Advanced Technology for Automotive Components，Wuhan University of Technology，Wuhan 430070，China；2. Hubei Technology Research Center of New Energy and Intelligent Connected Vehicle Engineering，Wuhan 430070，China；3. Artificial Intelligence and New Energy Vehicle Modern Industrial College，Wuhan University of Technology，Wuhan 430070，China；
4. Dongfeng Motor Corporation Research & Development Institute，Wuhan 430058，China）

Abstract: To address the inefficiency and weak robustness of existing rollback methods when a remote update of automotive ECU fails, this paper designs an efficient and stable upgrade rollback strategy. Firstly, an optimized rollback backup method and a comprehensive security-verification strategy are proposed to enhance rollback stability. Then, to avoid the long duration of traditional full rollback, a differential rollback technique based on an improved Bsdiff algorithm is proposed. The improved algorithm can significantly increase rollback efficiency by using the higher-ratio LZMA2 (Lempel-Ziv-Markov chain-Algorithm 2) compression and optimizing the patch format. Finally, the proposed strategy is tested on real-vehicles. The results show that the rollback strategy using the improved differential algorithm reduces rollback time by

收稿日期：2024–04–29 **改稿日期：**2024–06–20 **网络首发日期：**2024–07–03

基金项目：湖北省中央引导地方科技发展专项（2023CGB005）

参考文献引用格式：

胡杰，邓佳慧，徐文才，等.基于改进差分算法的汽车ECU远程升级回滚策略[J].汽车工程学报，2025，15(4)：497–507.

HU Jie，DENG Jiahui，XU Wencai，et al.Rollback Strategy for Remote Automotive ECU Upgrades Based on Improved Differential Algorithm[J].Chinese Journal of Automotive Engineering，2025，15(4)：497–507.(in Chinese)

84.69%, and achieves a 100% test-case pass rate. The proposed strategy preserves vehicle functionality when an ECU upgrade fails while improving rollback efficiency.

Keywords: over-the-air technology; Bsdiff algorithm; in-vehicle ECU; rollback strategy

汽车空中在线升级（Over-the-Air，OTA）技术是当前汽车行业的一个重要组成部分，该技术使汽车 ECU 通过远程升级不断获得新的功能和改进，但同时也面临着升级稳定性的挑战。《关于批准车辆的软件升级和软件升级管理体系统一规定的法规》（R156）中提出要对 OTA 系统进行升级失败处理测试[1]，旨在确保车辆远程升级失败的情况下将系统恢复至原稳定版本，防止因控制器升级失败导致整车功能无法正常使用[2-3]。因此，需要设计一套安全高效的回滚策略，确保在升级过程中出现问题时，系统能迅速恢复至之前已验证且运行稳定的版本，这对于新一代智能网联汽车至关重要。

回滚策略的概念源于计算机科学，通过将系统回退至之前正确运行的状态来解决[4]系统更新失败所引发的崩溃问题。针对 ECU 升级失败回滚策略，现有研究主要聚焦在回滚策略稳定性方面。王俊秀[5]设计了基于外扩内存的 A/B 交换升级方案的回滚恢复机制，在更新异常时能及时回滚至旧版本，但是未考虑某些控制器不适用 A/B 交换升级的方案。王栋梁等[6]在探讨控制器的回滚重刷策略时，综合考虑了两种不同类型的控制器，对于搭载诸如 Linux 等智能操作系统的控制器，采用 A/B 备份的方式；而对于配备传统实时操作系统（RTOS）的控制器，则提出了 FLASH 备份方法，即调用存储在网关 FLASH 中上一版本的回滚策略。王樱蓓[7]设计了一种备份机制，在云端服务平台备份旧版本程序，待平台收到回滚通知后，下发相应回滚包，实现终端设备稳定版本回滚。马伯祥等[8]在车内远程通信模块中增加任务队列和判断机制，解决了多任务升级失败的问题。周恒等[9]提出了一种双分区升级技术，设计了同面启动和异面启动升级系统，并通过测试验证了系统的稳定性和回滚时分区切换的有效性。回滚作为一种可靠性技术，能确保系统的稳定性，上述相关研究尽管涵盖了不同类型控制器的回滚方式、云端备份机制和双分区升级等回滚技术，能确保系统远程升级的稳定性，但并未充分考虑回滚的效率问题。

目前，行业内单个 ECU 升级失败后的回滚时间一般在几十秒到十几分钟不等，具体回滚时间取决于固件大小、网络速度和回滚机制等因素[10]。用户所能接受的回滚时间一般在 30 min 以内[11]，然而，车企在进行 OTA 升级任务推送时，通常会同时升级多个 ECU，当遇到多 ECU 升级失败需要回滚时，回滚时间可能会远超用户期望时间。因此，如何尽可能减少 ECU 的回滚时间，提升回滚速度是当前研究的一个重点和难点。

在回滚效率方面，数据压缩技术的提升可以减小 ECU 更新包的大小，从而加快回滚速度。李汨江[12]使用车载终端的诊断数据对 Huffman、LZ77（Lempel-Ziv 1977）和 LZW（Lempel-Ziv-Welch）三种无损压缩算法进行了对比试验，结果表明，LZ77 算法的压缩比最高，但其解压缩时间相对较长。为优化 LZ77 算法性能，BELL 等[13]提出改进版本 LZMA（Lempel-Ziv-Markov Chain-Algorithm）算法，该算法可以获得比 Bzip2 算法更高的压缩性能与效率。GOYAL 等[14]提出了基于循环神经网络的无损数据压缩技术，虽然其压缩比远高于传统压缩算法，但是不适用于计算资源有限的车端。

综上所述，本文为解决汽车 ECU 远程升级失败后回滚效率低下的问题，从回滚策略与差分算法优化两个角度设计了一种基于改进差分算法的汽车 ECU 远程升级回滚策略，以提升汽车 ECU 在回滚过程中的效率和鲁棒性。在回滚策略方面，提出一种改进的云端备份方法，引入差分回滚，提升回滚效率、节省内存空间，并加入安全校验措施保证回滚稳定性。在差分算法方面，采用压缩性能更高并且更适用于车端的 LZMA2 压缩算法，代替原 Bsdiff 算法中 Bzip2 压缩算法，并将差分包的数据格式序

列化，进一步提升回滚效率。实车测试验证表明，基于新算法的回滚策略能大幅缩短回滚时间，同时保证回滚的稳定性。

1　回滚策略设计

1.1　回滚流程

在汽车 ECU 远程升级中出现新版本固件安装失败或不能正常使用时，需要通过回滚操作将系统恢复至之前的稳定状态[15]。回滚流程如图 1 所示，首先擦除已刷写失败区程序，然后将备份区的回滚包刷写至运行区，使运行区能正常工作；回滚成功后，删除备份区回滚包，以减少空间占用，避免影响后续升级。当 ECU 升级成功未触发回滚时，备份区的回滚包也会相应地被删除，以免占据存储空间。OTA 云端在配置 ECU 升级策略时，会为升级任务配置回滚机制，待升级失败时，云端服务器发送回滚指令，车端接收到指令后按上述流程进行回滚操作。基于上述回滚流程，本文回滚策略的设计主要考虑回滚备份方式、回滚方式和回滚安全性 3 个方面，下面将详细阐述设计方案。

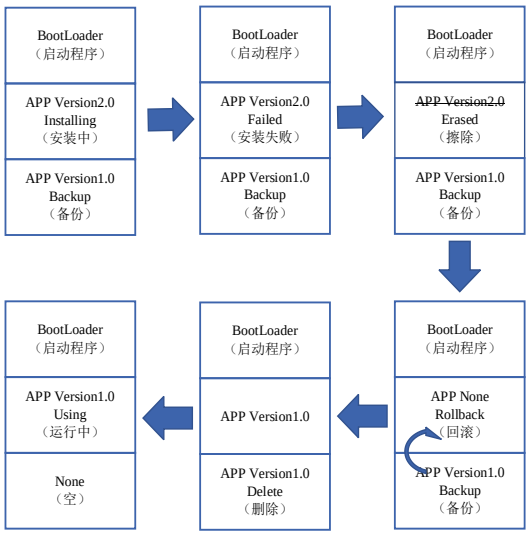

图 1　回滚流程

1.2　回滚备份方式

回滚的实现需要备份设备状态和数据，包括设备的固件版本、配置文件和用户数据等，以便在需要时进行回滚。目前常用的备份方式为云端备份，如文献［7］所提及的，这种方式是在云端存储程序和信息升级前的版本。当车端需要回滚到之前版本时，车端会向云端平台发送回滚请求，云端平台收到请求后，会将相应的回滚包发送至车端，之后由车端完成回滚包的下载与安装。云端备份可以节省车端的内存空间，但需要稳定的互联网连接。由于用户进行 OTA 升级的地点无法完全保证网络信号的稳定性，该方式存在因网络异常导致回滚包下载失败，进而无法执行回滚操作的风险，可能造成车辆无法恢复至升级前安全状态的严重后果。因此，为了应对网络风险并提高回滚操作的可靠性和鲁棒性，本文调整了云端备份方案中回滚包下发的时间节点。在部署 OTA 升级任务时，云端需同步配置 OTA 升级任务信息及其对应的回滚包，并将这些信息与回滚包随 OTA 任务一并传送至车端的主控程序（Updater Control Master，UC-Master），即将回滚包的下发时间节点提前至 OTA 升级任务发布之时；随后，UC-Master 负责解析接收到的 OTA 任务信息，从中提取安装信息以及回滚包。图 2 为改进前和改进后的备份方式对比，当回滚操作触发时，回滚过程可以立即开始，无需向云端请求下发回滚包。虽然这种备份方式会在下载升级任务时相应地增加回滚数据传输量和传输时间，但相较于升级失败后无法及时恢复的高风险，改进的备份方式可以保证车辆在升级失败时迅速、安全地进行回滚操作，有效规避了网络不稳定性的隐患，对用户用车安全和系统鲁棒性具有明显优势。

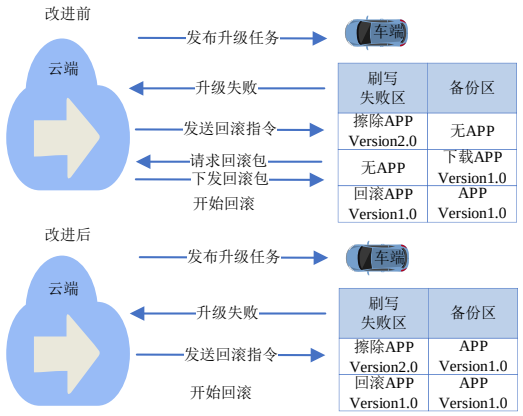

图 2　备份方式改进对比

1.3 差分回滚

传统的回滚方式需要下载备份整个系统或应用程序的相关信息，对于智能控制器这种带有操作系统的设备，由于其数据量和代码处理量较大，会消耗大量计算资源和内存空间。因此，为了提升回滚速度，降低资源消耗，本文引入差分回滚技术。差分回滚通过比较新旧版本之间的差异，使用差分压缩算法生成相应的差分回滚包，应用差分回滚包将新版本回退到旧版本。差分回滚仅传输和存储有差异部分的数据，避免了冗余数据的空间占用，对带宽和存储空间受限的车端适用性好[15]。

差分回滚具体实现过程如图3所示，车端向云端上报当前软件版本号，云端将差异部分编码生成目标回退版本的差分包，根据OTA升级策略配置随升级任务一并下发至车端；差分回滚机制触发时，车端首先按照回滚包校验流程对差分包进行校验，校验通过后，车端结合当前版本软件包和差分包还原出目标版本的软件包；为确保使用正确的目标版本软件包进行回滚，需校验还原出的软件包；最后应用目标版本软件包进行回滚安装，完成后上报回滚信息至云端。

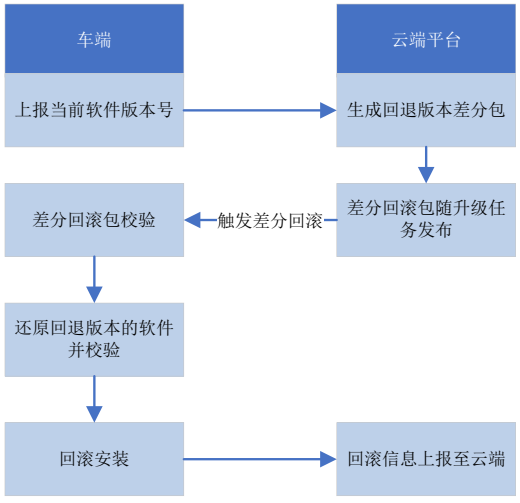

图3 差分回滚过程

差分回滚的核心是根据差分回滚包执行回滚操作，差分回滚包通常为二进制文件，因此需要选择合适高效的差分算法。文献[16]中比较了Xdelta、RTPatch、Exediff、Bsdiff四种用于二进制文件的差分算法，结果表明，在压缩性能方面，Exediff算法压缩率最高，其次是Bsdiff算法，但是Exediff算法有特定的应用场景，跨平台性能较差，不适用于汽车OTA升级，而Bsdiff算法可独立于平台运行，并且差分性能优良，因此，本文采用Bsdiff算法生成差分回滚包。

1.4 回滚安全性策略

为保证回滚的准确性和安全性，防止使用被篡改过或不符合预期目标的回滚包影响控制器功能的正常使用，回滚包需要严格的校验流程。常见回滚包的校验方法有校验和算法、哈希函数、数字签名、安全证书[17]。校验和算法与哈希函数都不具备身份验证能力，数字签名和安全证书分别依赖于公钥和第三方信任机构，当公钥或第三方机构出现漏洞或其他问题时会影响签名和证书的可信性。上述方法可以单独使用，但是相比组合使用策略，单独使用其中一种校验方法的可靠性较低。因此，本文采取安全证书、数字签名和哈希函数组合校验策略。哈希函数可以检测数据的完整性，数字签名可以防止数据被冒充，安全证书可以确保公钥的真实性，提供更全局的信任链机制，三者结合使用实现三重验证机制，可以提供更强大、更全面的数据完整性和身份验证功能。

具体校验流程如图4所示，在校验开始前，车端从升级任务信息中读取软件原包、原包签名以及签名安全证书；读取成功后，首先校验回滚包签名安全证书的合法性，云端在创建回滚包时，使用第三方可信证书颁发机构签发的数字安全证书对回滚包进行签名，车端UC-Master调用公开密钥基础设施（Public Key Infrastructure，PKI）接口，将签名安全证书发送给PKI模块，PKI模块校验证书的合法性，若证书验证通过，则进入下一步；若证书不合法，则回滚包校验失败；回滚包的解签是从签名证书中提取公钥，使用公钥对回滚包签名进行解密，此过程若解密失败，则回滚包校验失败；解密回滚包得到原包哈希值（H1），该哈希值是由云端计算生成的，车端计算拆分得到的原始回滚包的哈希值（H2），比较H1和H2的值，若二者一致，则表明回滚包校验成功；反之，回滚包校验失败。

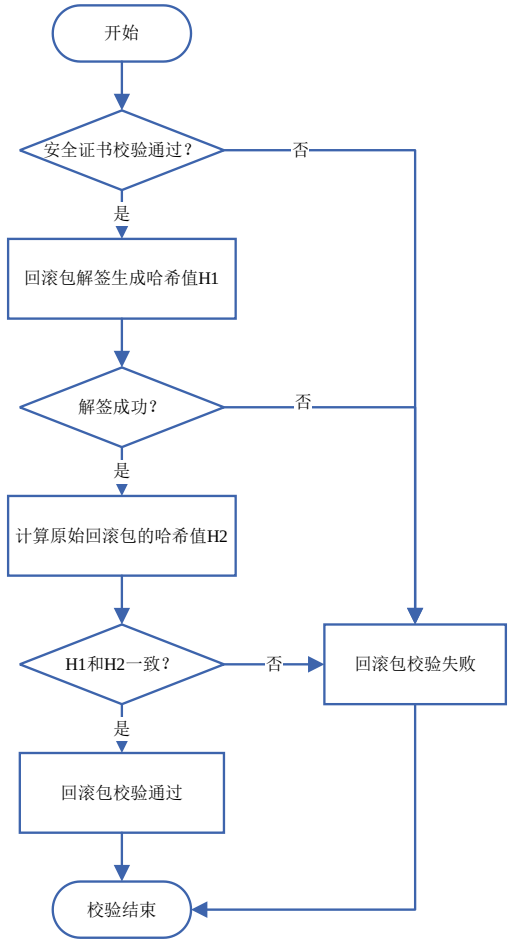

图 4　回滚包校验流程

2　差分算法分析

2.1　Bsdiff 差分算法

Bsdiff 是一种二进制差量更新算法，该算法可分为差分和还原 2 个阶段，第 1 阶段在云端运行 Bsdiff 算法生成差分包，第 2 阶段在车端运行 Bspatch 算法，将原始软件包和差分包合成为目标版本软件包。

在第 1 阶段，Bsdiff 算法通过后缀数组生成字典序，采用二分查找法查找一段完全相同的数据段，并向前和向后拓展找到最长的近似匹配数据段，该段数据即为差分数据 diff string，在两段近似匹配数据段之间的数据为完全不匹配数据，即为新增数据 extra string [18]。Bsdiff 算法差分包的数据由数据头、控制数据、差分数据 $diff_i$ 和新增数据 $extra_j$ 四部分组成。控制数据中，x_i 为 $diff_i$ 的字节数，y_j 为 $extra_j$ 的字节数，z_k 为相对于原文件中的偏移量。由于控制数据和差异数据的高度结构化，并且差分数据中含有大量冗余零值，所以可以被高效压缩。Bsdiff 算法使用 Bzip2 压缩算法来对差分包进行压缩，生成最终向车端发送的差分包，具体伪代码见表 1。

表 1　Bsdiff 算法伪代码

Bsdiff 算法伪代码
输入：新文件，原文件 输出：差分包 1 qsufort（）；//生成字典序 2 while scan 指针未遍历完新文件 3　len = search（）；//二分法查找最大匹配长度 4　matchlen（）；//原文件和新文件完全匹配长度 5　calculate oldscore； 6　if len > oldscore + 8 7　diff string = backward-extension + completely　matched area + forward-extension； 8　extra string = completely mismatched area； 9　else continue； 10 end while 11 diff file = ｛［header］，［x_i，y_j，z_k］，［$diff_1$，…，$diff_i$］，［$extra_1$，…，$extra_j$］｝； 12 差分包 = Bzip2［diff file］；

第 2 阶段如图 5 所示，车端首先创建一个新文件，利用 Bzip2 算法解压缩差分包，提取原文件中与 $diff_i$ 对应的数据至新文件，依据偏移量 z_k 将相应 x_i 个字节的差分数据 $diff_i$ 插入到原文件对应的数据中，将 y_j 个字节的新增数据 $extra_j$ 以复制的方式写入新文件中 [19]，遍历差分包中的所有数据，生成的新文件即目标版本软件包。

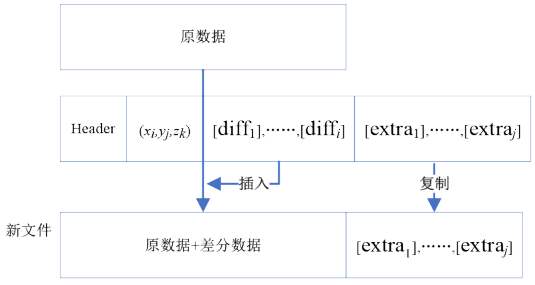

图 5　目标版本软件包还原过程

2.2　Bsdiff 差分算法改进

将 Bsdiff 差分算法应用于前文提出的差分回滚中，进行解压缩差分包时，传统 Bsdiff 算法使用 Bzip2 压缩算法，该算法的解压速度较慢，会影响软件包的还原速度；此外，现有差分包的数据格式

在还原过程中，需频繁查找和计算所需的新增数据和差分数据的偏移量，导致计算量较大，影响差分还原的速度。因此，本文从压缩算法和差分包数据格式两方面对Bsdiff差分算法进行改进。

本文提出采用具有高解压速度和压缩比的LZMA2压缩算法来代替原Bsdiff算法中使用的Bzip2压缩算法[20]。LZMA2是一种基于LZ77的无损数据压缩算法，利用滑动窗口和范围编码实现高压缩比。相比LZMA，LZMA2支持多线程压缩与解压缩，可以并行处理多个数据块。在当前多核处理器广泛应用于车载系统的背景下，LZMA2能充分利用这些硬件资源，提高数据处理效率；同时，LZMA2改进了内存管理，使其在不同的硬件环境下更具灵活性，可以根据实际情况优化内存使用，非常适用于资源有限的车端。因此，本文采用LZMA2算法代替原Bzip2算法，以满足车载系统对数据压缩的高性能需求，具体压缩与解压算法步骤分别如图6和图7所示。

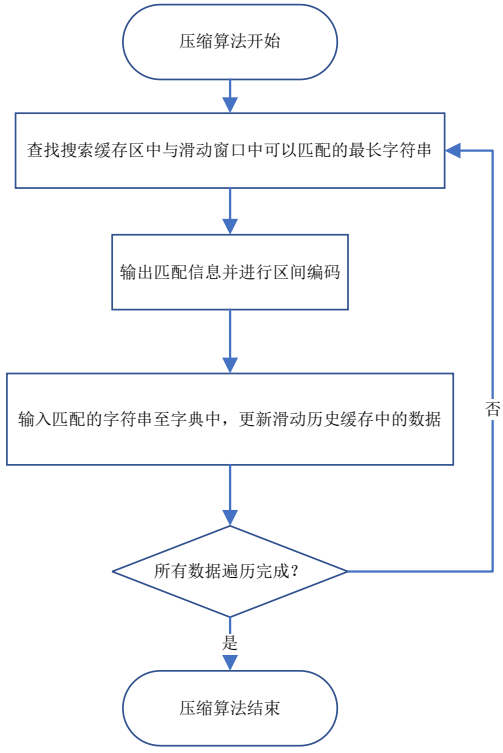

图6 LZMA2压缩算法流程

压缩算法步骤为：

1）构建一个固定大小的滑动窗口字典，该字典主要用于保存输入数据以及查找和处理重复字符串；

2）在搜索缓存区中，使用基于二叉树的哈希搜索匹配算法，在滑动窗口中寻找与之匹配的最长字符串；

3）根据匹配到的最长字符串，输出匹配信息并进行区间编码，匹配信息包括相匹配数据首个字节间的匹配距离和匹配长度；

4）将匹配的字符串输入到字典中，更新滑动历史缓存中的数据，进行下次匹配查找；

5）重复步骤2～4直至所有数据压缩完成，将压缩后的数据写入输出文件。

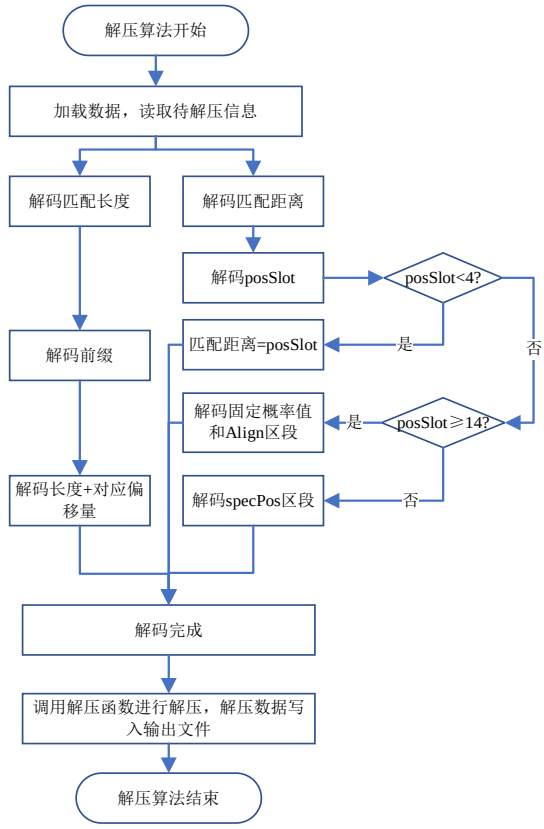

图7 LZMA2解压算法流程

解压算法步骤为：

1）加载待解压的文件至工作内存中，读取需解析的信息。

2）解码压缩文件中的匹配长度和匹配距离。在匹配长度解码中，首先对前缀进行解码，其中不同的前缀代表了不同级别的长度，具体分为low、mid和high三个级别，之后将解码出的匹配长度加

上其对应的偏移量。在匹配距离解码中，首先要解码一个名为 posSlot 的中间变量，当 posSlot 小于 4，则匹配距离等于 posSlot；当 posSlot 在 4～14 之间，匹配距离需要通过解码 specPos 区段来获得；当 posSlot 超过 14，则需要解码固定概率值部分和 Align 区段来得到匹配距离[21]。

3）根据解码的匹配信息调用解压函数对压缩文件中的数据进行解压，将解压完毕的数据写入输出文件中。

原差分包的数据格式将控制数据、差分数据和新增数据分在不同的数据块中，使用时需在控制数据中查询和计算对应字节长度和偏移量，并将所需数据从差分数据块和新增数据块中提出。本文提出差分包数据序列化的方法[16]，如图 8 所示，将每一个控制数据、差分数据和新增数据依次有序放置在一起，每一个数据块包含一条完整的差分数据信息，在进行还原时，仅需在原文件中找到与 $diff_i$ 和 $extra_j$ 对应的数据，依次遍历差分包中每一个数据块，即可完成目标文件还原。优化后的数据格式使算法无需再进行频繁查询和计算，缩短了车端还原目标软件包的时间，改进后的 Bsdiff 差分算法伪代码见表 2。

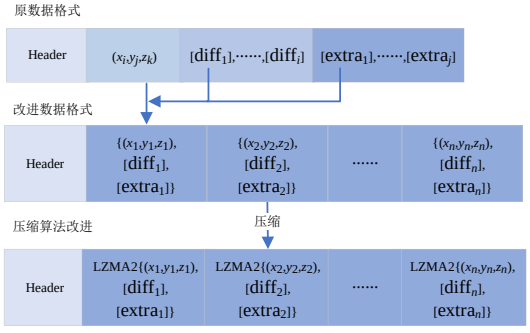

图 8　改进后差分包数据格式

3　测试验证

3.1　测试方案

将本文设计的回滚策略在实车上进行测试验证，根据目前 OTA 市场推送统计数据，国内各车企

表 2　改进后 Bsdiff 算法伪代码

改进后的 Bsdiff 算法伪代码
输入：新文件，原文件 输出：差分包 1 qsufort（）；//生成字典序 2 while scan 指针未遍历完新文件 3　len = search（）；//二分法查找最大匹配长度 4　matchlen（）；//原文件和新文件完全匹配长度 5　calculate oldscore； 6　if len > oldscore + 8 7　diff string = backward-extension + completely matched area + forward-extension； 8　extra string = completely mismatched area； 9　else continue； 10 end while 11 diff file = ｛[header]，[（x_1，y_1，z_1，diff$_1$，extra$_1$）]，[…]，[（x_i，y_j，z_k，diff$_i$，extra$_j$）]｝； 12 差分包 = LZMA2［diff file］；

每年进行 OTA 升级推送的次数一般不超过 10 次，按 5 年的使用周期，一辆智能网联汽车最多进行 50 次 OTA 升级[22]。因此，本文选取 2 台测试车辆，分别进行 50 次回滚测试。测试设备包括实测车辆、笔记本电脑、CANalyst 分析仪和 CANTest 软件，如图 9 所示。实测车辆作为 OTA 车端用于进行 ECU 升级；笔记本电脑作为 OTA 云端，测试人员可在其中的 OTA 云端管理系统制作与上传升级包和回滚包，为测试车辆配置并发布 OTA 升级和回滚任务，升级结束后可在云端查看升级结果、升级时间、回滚结果、回滚时间和日志信息；CANalyst 分析仪结合 CANTest 软件用于采集升级过程中的 CAN 报文信息，并向被升级 ECU 发送诊断指令。

图 9　测试设备

为全面评估回滚策略的有效性，需要验证与测试以下 4 点：

1）当升级错误时，系统是否能正确回滚到原来的版本；

2）当回滚包出现错误时，系统是否能识别错误，终止本次回滚，并重新向云端请求下发新回滚包以完成本次回滚；

3）回滚过程出现网络异常时，是否不影响回滚操作执行，升级失败的ECU仍可以回滚成功；

4）对比改进前的整包回滚、使用原Bsdiff差分算法的回滚和基于改进差分算法的回滚这3种回滚方式的效率。回滚效率的评价指标为压缩率（Compression Ratio，CR）和回滚时间，其中，压缩率越高、回滚时间越短，则回滚效率越高。

压缩率计算式为：

$$CR = (S_{target} - S_{patch})/S_{target} \circ \quad (1)$$

式中：S_{target}为目标版本软件包大小；S_{patch}为差分包大小。

针对上述前3点，设计了如表3所示的测试用例，以验证回滚策略的稳定性与鲁棒性。

表3 回滚策略测试用例

序号	测试点	预置条件	测试步骤	预期结果
1	刷写过程中升级失败	云端发布ECU升级任务并配置回滚策略	发送1次诊断指令给被升级ECU，触发升级异常	触发回滚，ECU升级失败，回滚成功，ECU可按原版本正常工作
2	新版本不可使用	1.云端发布ECU升级任务并配置回滚策略 2.配置下发的目标升级版本不能正常使用	等待安装失败	触发回滚，ECU升级失败，回滚成功，ECU可按原版本正常工作
3	回滚包安全校验	1.云端发布ECU升级任务并配置回滚策略 2.云端配置的回滚包为假包	发送1次诊断指令给被升级ECU，触发升级异常	触发回滚，回滚包校验失败终止本次回滚，请求云端下发新回滚包，二次回滚成功
4	回滚网络异常	云端发布ECU升级任务并配置回滚策略	1.发送1次诊断指令给被升级ECU，触发升级异常 2.断开车辆网络连接	触发回滚，ECU升级失败，回滚成功，ECU可按原版本正常工作

3.2 测试结果与分析

根据上述测试方案进行回滚策略测试，可在云端实时查看升级包信息、回滚包信息、每辆车的升级进度、升级结果和OTA日志。经过50次测试后，2辆测试车的测试用例数据统计见表4，各用例的通过率均达到了100%。

表4 回滚策略测试用例结果统计

测试用例序号	测试车①通过率/%	测试车②通过率/%
1	100	100
2	100	100
3	100	100
4	100	100

图10为上述3种回滚方式下4组回滚包大小和压缩率对比。为充分验证算法的有效性，本文选取了来自4个不同ECU的软件包进行对比试验。由于这些ECU在功能需求、操作系统特性以及版本更新中的改动幅度上存在显著差异，其软件包大小也呈现出较大的差异。当ECU版本更新改动的数据

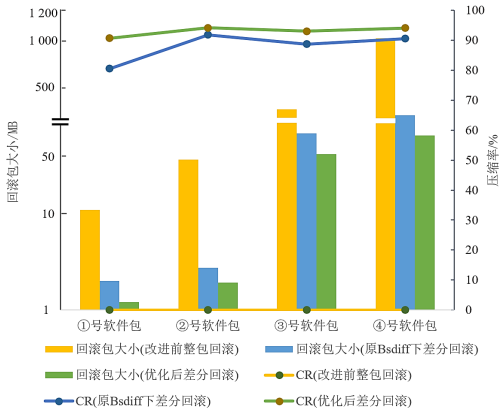

图10 不同回滚方式回滚包大小与压缩率对比

内容越少，数据结构性越高，其差分效果越好，得到的差分包相对原文件更小。改进后的Bsdiff差分算法相比原Bsdiff差分算法在压缩率上平均提高了5.11%，其中，1号软件包效果提升最显著，共提升10.19%，主要原因是1号软件包的数据结构性高，其二进制数据内容相较于其他3个软件包更简单，使改进后的算法能对其进行更高效的压缩，因此体现出更好的差分效果。改进后的Bsdiff差分算法压

缩率最高可达 94.18%，平均压缩率为 93.02%，压缩率的提升减少了数据传输量与传输时间，从而有效降低了车端缓存中需要存储的数据量和内存中的数据读写量，达到节约内存空间的效果。

表 5 为在 3 种不同回滚方式下，4 组软件包经过 50 次测试的平均回滚时间，在相同网络环境下，本文提出的回滚方式相对于改进前的整包回滚方式，回滚时间最高可缩短 92.64%；相对于原 Bsdiff 下差分回滚方式，回滚时间最多可缩短 36.32%。总体而言，优化后回滚方式相对于改进前整包回滚方式平均回滚时间可缩短 84.69%，相对于原 Bsdiff 下差分回滚方式平均回滚时间可缩短 26.38%。

表 5　三种回滚方式回滚时间对比

软件包序号	文件大小/MB	整包回滚时间/s	原 Bsdiff 下差分回滚时间/s	优化后差分回滚时间/s	相对整包回滚时间缩短率/%	相对原 Bsdiff 下差分回滚时间缩短率/%
1	10.01	36	12	10	72.22	16.67
2	32.15	101	21	15	85.15	28.57
3	522.06	958	142	108	88.73	23.94
4	944.48	1 740	201	128	92.64	36.32

测试结果表明，本文所提出的回滚备份方式以及回滚安全性策略可以保证车辆在 OTA 升级失败后，安全有效地回退至升级前使用的稳定版本，回滚过程不受网络信号因素的影响，提升了回滚过程的鲁棒性；同时，基于 LZMA2 压缩算法的差分回滚方式可以缩短回滚时间，大幅提升了回滚效率，解决了传统回滚方法效率低下的问题。

4　结论

本文针对汽车 ECU 远程升级失败，现有回滚策略效率低下的问题展开研究，设计了一套安全高效的回滚策略，主要在以下 2 个方面做出了改进与优化。

1）在回滚策略设计中提出改进的回滚备份方式，将回滚包同升级软件包一同下发至车端，引入差分回滚技术，同时提出使用安全证书、数字签名以及哈希函数的组合校验策略来确保回滚的安全性。

2）对差分回滚中使用的差分算法进行优化，从提升车端回滚效率考虑，提出将差分包数据格式序列化，并将原 Bsdiff 使用的 Bzip2 压缩算法更换为压缩性能更高、解压时间更短的 LZMA2 压缩算法。

实车测试表明，基于改进差分算法的回滚策略测试用例通过率达到 100%，压缩率较原 Bsdiff 差分算法平均提高了 5.11%，回滚时间相比原整包回滚方式平均缩短了 84.69%，充分验证了所设计的回滚策略能保证 ECU 在升级失败后安全回滚至原版本，同时提升了回滚效率。

参考文献（References）

[1] 林波，董红磊，林烨，等. 中国汽车软件在线升级（OTA）现状及管理建议[C]//2023 中国汽车工程学会年会论文集（6）. 北京：机械工业出版社，2023：95-100.
LIN Bo, DONG Honglei, LIN Ye, et al. Automobile OTA Update Situations and Management Suggestions in China [C]// Proceedings of the 2023 Annual Conference of the China Society of Automotive Engineering (Vol. 6). Beijing: China Machine Press, 2023: 95-100. (in Chinese)

[2] ZHANG Ji, LV Yu, LIAO Zhi. Research on Automotive ECU Remote Update and It's Security [J]. Journal of Physics: Conference Series, 2018, 1074 (1): 012133.1-012133.9.

[3] 张海强. 智能网联汽车安全远程升级技术的研究与实现[D]. 成都：电子科技大学，2018.
ZHANG Haiqiang. Research and Implementation of Intelligent Remote Upgrade Technology for Intelligent Network Connection Vehicles [D]. Chengdu: University of Electronic Science and Technology of China, 2018. (in Chinese)

[4] 谢建洲. 计算机系统容错技术研究[J]. 电脑知识与技术，2016，12（6）：250-252.
XIE Jianzhou. Research on Fault Tolerance Technology

for Computer Systems [J]. Computer Knowledge and Technology, 2016, 12(6): 250-252.(in Chinese)

[5] 王俊秀.矿用智能车载终端远程升级OTA系统设计[J].煤矿机械,2023,44(8):207-209.(in Chinese)
WANG Junxiu. Design of Remote Upgrading OTA System for Mining Intelligent Vehicle Terminal [J]. Coal Mine Machinery, 2023, 44(8): 207-209.(in Chinese)

[6] 王栋梁,汤利顺,陈博,等.智能网联汽车整车OTA功能设计研究[J].汽车技术,2018(10):29-33.
WANG Dongliang, TANG Lishun, CHEN Bo, et al. The Research of OTA Function Design for Intelligent and Connected Vehicle [J]. Automobile Technology, 2018 (10): 29-33.(in Chinese)

[7] 王樱蓓.基于优化差分算法的车载CAN网络ECU远程刷写[D].长春:吉林大学,2023.
WANG Yingbei. ECU Remote Swipe for In-Vehicle CAN Networks Based on Optimized Differential Algorithm [D]. Changchun: Jilin University, 2023.(in Chinese)

[8] 马伯祥,李志宁,聂泽宇,等.OTA系统远程固件升级问题分析[C]//2020中国汽车工程学会年会论文集(4).北京:机械工业出版社,2020:319-323.
MA Boxiang, LI Zhining, NIE Zeyu, et al. OTA System Remote Firmware Upgrade Problem Analysis [C]// Proceedings of the 2020 Annual Conference of the China Society of Automotive Engineers (Vol.4). Beijing: China Machine Press, 2020: 319-323.(in Chinese)

[9] 周恒,梁贵友,柳旭,等.基于实时操作系统的车载ECU双分区软件空中下载升级技术[J].汽车工程学报,2023,13(6):803-809.
ZHOU Heng, LIANG Guiyou, LIU Xu, et al. A Dual-Slot Software OTA Upgrading Technology Based on RTOS of Vehicle Electronic Control Unit [J]. Chinese Journal of Automotive Engineering, 2023, 13 (6): 803-809. (in Chinese)

[10] 张远威.支持应用程序动态更新的车载多媒体系统设计与实现[D].长春:吉林大学,2022.
ZHANG Yuanwei. Design and Implementation of Vehicle Multimedia System Supporting Dynamic Update of Application Programs [D]. Changchun: Jilin University, 2022.(in Chinese)

[11] 刘俊,马云林,刘平,等.基于电子电器架构的整车OTA设计研究[C]//重庆汽车工程学会2022年论文汇编.重庆长安汽车软件科技有限公司,2023:42-47.
LIU Jun, MA Yunlin, LIU Ping, et al. Research on Vehicle OTA Design Based on Electronic and Electrical Architecture [C]//Compilation of Papers of Chongqing Automotive Engineering Society 2022. Chongqing Chang'an Automobile Software Technology Company, 2023: 42-47.(in Chinese)

[12] 李汨江.基于传感网和分布式诊断的电力机车故障分析系统[D].北京:北京交通大学,2022.
LI Gujiang. Fault Analysis System for Electric Locomotives Based on Sensor Network and Distributed Diagnosis [D]. Beijing: Beijing Jiaotong University, 2022.(in Chinese)

[13] BELL T C, WITTEN I, CLEARY J G. Modeling for Text Compression [J]. ACM Computing Surveys, 1989, 21(4): 557-591.

[14] GOYAL M, TATWAWADI K, CHANDAK S, et al. DeepZip: Lossless Data Compression Using Recurrent Neural Networks [C]//2019 Data Compression Conference (DCC), Mar. 26-29, 2019, Snowbird, Utah, USA. Piscataway NJ: IEEE, c2019: 1-10.

[15] KOMANO Y, XIA Z, KAWABATA T, et al. Efficient and Secure Firmware Update/Rollback Method for Vehicular Devices [C]// Information Security Practice and Experience: 14th International Conference, Sept. 25-27, 2018, Tokyo, Japan. Springer International Publishing, 2018: 455-467.

[16] TERAOKA H, NAKAHARA F, KUROSAWA K. Incremental Update Method for Resource-Constrained in Vehicle ECUs [C]// 2016 IEEE 5th Global Conference on Consumer Electronics, Oct. 11-14, 2016, Kyoto, Japan. Piscataway NJ: IEEE, c2016: 1-2.

[17] 钱枫,易齐,祝能,等.基于改进Bsdiff算法的车载诊断系统远程升级系统[J].汽车安全与节能学报,2023,14(3):329-337.
QIAN Feng, YI Qi, ZHU Neng, et al. Remote Upgrade System for the On-Board Diagnostic System Based on an Improved Bsdiff Algorithm [J]. Journal of Automotive Safety and Energy, 2023, 14(3): 329-337.(in Chinese)

[18] 王莹.智能网联车载终端OTA软件升级技术研究[D].西安:长安大学,2022.
WANG Ying. Research on Over-the-Air Technology for the Terminal of Intelligent Connected Vehicles [D]. Xi'an: Chang'an University, 2022.(in Chinese)

[19] 王豫新,高美凤.一种改进的固件增量更新算法[J].计算机工程,2020,46(10):210-215.
WANG Yuxin, GAO Meifeng. An Improved Incremental Update Algorithm for Firmware [J]. Computer Engineering, 2020, 46(10): 210-215.(in Chinese)

[20] LI Zhihao, QIN Guihe, LIANG Yanhua, et al. BSDIFF Difference Algorithm Based on LZMA2 for In-Vehicle ECUs [C]//7th International Conference on Computing, Control and Industrial Engineering, Feb. 25-26, 2023,

Hangzhou, China. Singapore: Springer Nature Singapore, 2023: 719-725.

[21] 郑子瑶. 基于BLE的物联网设备固件升级系统研究与设计[D]. 广州: 华南理工大学, 2022.
ZHENG Ziyao. Research and Design of Firmware Upgrade System for Internet of Things Devices Based on BLE [D]. Guangzhou: South China University of Technology, 2022.(in Chinese)

[22] 郭健忠, 汪子林, 闵锐, 等. 基于QNX/Linux的汽车ECU安全升级模式的研究[J]. 电子器件, 2019, 42(4): 1070-1075.
GUO Jianzhong, WANG Zilin, Min Rui, et al. Research on Safety Upgrade Mode of Automotive ECU Based on QNX /Linux [J]. Chinese Journal of Electron Devices, 2019, 42(4): 1070-1075.(in Chinese)

作者简介

胡杰（1984-），男，湖南永州人，博士，教授，主要研究方向为汽车控制与诊断、车联网与大数据、智能驾驶与智能底盘。
E-mail：auto_hj@163.com