工程与管理科学
Engineering and Management Science
第 7 卷◆第 12 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

STB-90V 船载数字加密电台终端系统

柯跃前
泉州师范学院物理与信息工程学院　福建泉州　362000

DOI:10.12238/ems.v7i12.16438

［**摘　要**］为应对我国船载通信电台在国际市场上“卡脖子”的技术难题，设计了一种具有自主知识产权的新型船载智能数字加密电台。该电台针对海上通信中存在的三大技术难题——覆盖范围受限、频谱资源易受干扰、通信安全和隐私保护，提出了一种综合性解决方案。关键技术路径包括：应用无线自组网技术以扩大通信覆盖范围并消除盲区；设计抗干扰物理层传输技术，以适应高动态信道环境，提升传输的可靠性。采用 256 位 AES 对称加密算法，实现通信数据加密、角色认证以及“一次一密”功能，确保通信安全，为我国船舶的海上安全生产与应急通信能力提供核心装备支持。

［**关键词**］通信系统；数字化加密；电台；船载终端；STB-90V

1 引言

目前，船舶实时通信主要依赖海上无线电通信电台，然而该领域的关键设备与技术长期被国外厂家垄断，这不仅使我国航运业面临潜在的技术封锁风险，更对国家海上安全与应急响应能力构成了严峻挑战。近年来，多起海上突发事件凸显了拥有自主、可靠通信能力的极端重要性。例如，2022 年 1 月，香港附近水域“东方之星”轮沉没后的搜救行动，以及 2023 年 3 月，在台风“马勒卡”影响下，于南海失联的“福景 001”轮工程船，这些事故的救援工作均因复杂海况下的通信不畅而受到严重制约。此外，2021 年发生的苏伊士运河“长赐”轮搁塞事件，虽然并非直接源于通信问题，但也从侧面暴露了全球航运链条的脆弱性，警示我们必须将关键通信技术掌握在自己手中。因此，研制新型船载智能数字加密电台，突破国外技术垄断，实现该装备的国产化与数字化，已成为一项迫切的国家战略需求。此举旨在彻底解决我国船舶在远海通信覆盖、抗干扰传输与通信安全保密等方面的“卡脖子”难题，对于显著提升我国船舶的海上安全生产水平与在突发紧急事件中的快速处置能力，具有至关重要的意义。

2 STB-90V系统总体概述与加密体系架构

2.1 系统总体概述

STB-90V 终端定位为一款高性能、高安全的 150MHz VHF 频段船载数字加密电台。其设计遵循模块化、软件定义无线电的思想，硬件平台集成高性能射频前端、数字信号处理器与专用加密芯片，软件层面则实现通信协议栈与安全算法的灵活配置。终端全面兼容国际通用的 DMR 数字移动无线电标准，确保了与现有海事通信系统的互操作性，同时在安全性能上实现超越。其核心设计思想是在统一的硬件平台上，通过软件赋能，实现通信、组网与安全功能的深度集成。

2.2 加密体系架构

STB-90V 构建了一个层次化的端到端加密体系。该体系覆盖了从用户身份认证、密钥管理到业务数据加密的全过程。对于通信过程中的所有关键数据流，包括经 AMBE+2 声码器压缩后的数字语音、应用层产生的短消息以及各类船舶状态、传感器读数等用户数据，均纳入加密保护范围。为确保不同业务间的安全隔离，语音、短信及数据传输在加密时采用不同的根密钥种子进行派生，但所有最终用于 AES 加密的会话密钥长度均严格统一为 256 位，为系统提供了基准一致的高强度安全防护。

3 系统核心技术创新与设计

3.1 无线自组网扩覆盖技术

为彻底突破传统 VHF 通信的视距传输限制，STB-90V 集成了先进的无线自组网功能。该技术使每一部电台在海上均可作为一个智能节点，自动执行邻居发现、链路质量探测与网络路由维护。当船舶航行至岸基基站覆盖范围之外或卫星

信号微弱的海域时，电台能动态组建一个去中心化的 Mesh 网络。通过优化的 AODV 路由协议与分布式 TDMA 调度算法，通信数据可在多个节点间进行智能中继与多跳传输，从而将单点的通信能力有效延伸至整个网络可达的范围。此机制不仅能将通信覆盖半径扩展数倍，有效消除通信盲区，更能为渔船编队作业、海上搜救集群协作等应用场景提供一个弹性的、无需基础设施的专用通信网络，极大提升了通信系统的生存性与灵活性。

3.2 抗干扰物理层传输技术

海上无线信道以其高动态、多径衰落、多普勒频移及同频干扰严重而著称。为应对这一挑战，STB-90V 在物理层设计了多维度的抗干扰技术。首先，采用了自适应编码调制（AMC）技术。电台的基带处理器持续对接收信号强度、信噪比与误码率进行实时估计，生成信道质量指示。基于此，系统能在 QPSK、16QAM 等不同调制方式与 1/2、3/4 等不同编码速率之间动态选择最优组合。在信道条件恶劣时，自动切换至更稳健的低阶调制与低码率编码，优先保障通信的连通性与可靠性；在信道条件优良时，则切换至高阶调制与高码率编码，以最大化频谱利用率和数据吞吐量[1]。

其次，引入了混合自动重传请求（HARQ）机制。该机制结合了前向纠错与检错重传的优点。发送端在发送数据块的同时，会传输其冗余校验信息。接收端在解码失败时，并非简单丢弃数据，而是将错误数据块缓存，并请求发送端重传额外的冗余信息。接收端将初次接收的数据与重传的冗余信息进行合并解码，从而显著提高解码成功率，降低整体传输时延。AMC 与 HARQ 的协同工作，使电台能够智能地适应海上复杂多变的高动态信道环境，显著提升信号的稳定性与传输的可靠性。

4 高强度加密模块设计与实现

4.1 多层次动态密钥生成机制

密钥管理是加密系统的核心环节。STB-90V 终端采用创新的三因子混合密钥生成方案，每个数据包的最终加密密钥均由三个独立因子通过安全的密钥派生函数动态合成。半公开密钥在终端出厂时固化在程序内部，与设备制造商身份相关联，提供基础的设备标识与差异化。用户私密密钥由终端用户通过人机接口自行设定并安全保管的 32 字节长密钥，这是用户侧安全自主性的体现，也是整个密钥体系的最高权限因子。动态密钥在每次通信事件发生时，由系统随机数发生器实时产生短随机数，在语音通信中采用随机生成的颜色码，在短信或数据传输中使用与报文绑定的递增序列号[2]。

这种多层次密钥机制创造了显著的安全优势。即使攻击者通过某种方式获得了某一时刻的会话密钥，也无法据此推导出其他任何一次通信的密钥，因为动态因子每次都在变化。这从根本上实现了"一次一密"的密码学理想，极大地提高了系统对抗重放攻击、密码分析等攻击手段的能力。密钥派生过程采用基于 HMAC-SHA256 的密钥推导函数，将三个密钥因子进行混合运算，确保最终会话密钥的随机性和不可预测性。

4.2 AES-256 加密算法核心实现

STB-90V 终端选用 AES 作为核心加密算法，其实现包含完整的数据处理流程。算法采用分组密码体制，将明文按照 128 比特固定大小进行分组。对于 256 位密钥，算法需进行 14 轮加密变换，每轮加密包含字节代换、行移位、列混淆和轮密钥加四个关键操作。字节代换利用预先计算好的、具有高度非线性特性的 S 盒，对状态矩阵中的每一个字节进行查表替换，此操作是 AES 算法非线性的主要来源。行移位对状态矩阵的每一行进行循环左移操作，实现字节在行内的扩散[3]。

AES 加密算法中，加密和解密操作是相反的过程，因此需要使用相同的密钥作为加密和解密的关键参数。AES 算法支持三种密钥长度：128 比特、192 比特和 256 比特，对于不同长度的密钥，AES 算法采用不同的轮数进行加密。

AES 每一轮加密包含 4 个操作：字节代换（SubBytes，SB）、行移位（ShiftRows，SR）、列混淆（MixColumns，MC）和轮密钥加（AddRoundKey）。最后一轮同其它轮变换基本相同，唯一的不同是移除了列混淆变换。解密过程为对应的逆操作。由于每一步操作都是可逆的，按照相反的顺序进行解密即可恢复明文。加解密中每轮的密钥由初始密钥扩展得到。

AES 的一个特性是将称为状态（state）的密码中间结果

用一个具有四行四列的二维字节数组来表示。

4.3 DMR 标准下的加密数据封装

加密数据在 DMR 通信协议中的封装是实现安全通信的关键环节。DMR 标准采用双时隙 TDMA 技术，在 12.5 kHz 的信道带宽内，通过 4FSK 调制实现 9.6 kbps 的有效数据传输速率。系统基于 DMR 标准框架，对语音、短信和数据业务分别设计加密封装方案。常规的语音或数据突发结构包含两个各 108 比特的信息字段，用于承载加密后的用户数据；位于突发中央的 48 比特同步字段用于时隙同步与帧类型识别;以及必要的信令字段[4]。

对于语音业务，AMBE+2 声码器将 20ms 的语音帧压缩生成特定的比特流，加密模块使用动态生成的会话密钥，按照 AES-256 算法进行加密后，将密文比特流精确分割并映射到 DMR 语音突发的两个 108 比特的信息字段中。对于短信和用户数据，其封装流程与语音类似，但使用的 DMR 数据突发结构在中央字段承载数据同步模式[5]。每个数据/控制突发还包含 20 比特的时隙类型 PDU，用于指示其后 196 个信息比特的格式与含义。这种设计确保了加密数据与标准 DMR 协议的完全兼容。每个语音突发提供一个“声码器 socket”，该接口可以承载 2×108 比特的声码器负载（VP），即携带 60 毫秒的压缩语音。

4.4 全业务链加密处理流程

系统为不同业务类型提供细粒度的加密处理方案。语音加密流程使用内部存储的、与语音业务绑定的固定密钥作为基础，结合用户输入的私密密钥，再混入本次呼叫随机产生的色码，三者共同派生出唯一的会话密钥。由于色码在每次通话中都是随机且唯一的，实现了"一话一密"的安全目标。短信加密流程采用独立的固定密钥作为基础，结合用户私密密钥，再混入本条短信的发送序列号，派生出加密密钥。每条短信的序列号均不同，从而实现了"一信一密"。

数据加密流程其原理与短信加密相同，但使用专门的数据加密固定密钥参与运算。这种设计在逻辑上为不同业务域创建了独立的密钥空间，即使某一个业务的密钥理论上被破解，也不会波及其他业务的安全。系统还实现了完善的数据填充策略，当传输的原始数据不足一个完整 AES 分组时，采用 PKCS#7 填充方案，确保加密算法能正确处理任何长度的数据。接收端在解密后，根据最后一个字节的值移除填充内容，准确恢复原始数据。

5 结论

本文系统地阐述了一款新型船载智能数字加密电台 STB-90V 的完整设计方案与实现成果。该设计成功地将无线自组网技术、自适应抗干扰物理层传输技术与基于 AES-256 的高强度加密技术融为一体，构建了一个覆盖广、链路稳、安全强的综合性海上通信解决方案。

[参考文献]

[1]吴瑞芳.基于改进 AES 算法的计算机网络隐私数据安全加密方法[J].软件，2025，46（06）：175-177.DOI：CNKI：SUN：RJZZ.0.2025-06-051.

[2]李坤.数据加密技术在计算机中的应用研究[J].信息系统工程，2025，（04）：43-46.DOI：CNKI：SUN：XXXT.0.2025-04-011.

[3]薛晓铭.基于 AES 算法的数据安全传输加密与解密方法研究[J].电脑与电信，2025，（04）：43-46.DOI：10.15966/j.cnki.dnydx.2025.04.010.

[4]Abdalrahman M E A .A Cloud Database based on AES 256 GCM Encryption Through Devolving Web application of Accounting Information System[J].International Journal of Recent Technology and Engineering（IJRTE），2021，9（5）：216-221.

[5]Performance Analysis of Advanced Encryption Standard（AES）S-boxes[J].International Journal of Recent Technology and Engineering，2020，9（1）：2214-2218.DOI：10.35940/ijrte.f9712.059120.

作者简介：柯跃前（1966—），男，汉族，福建泉州人，高级工程师、教授，主要从事测控与海洋通导装备研究，

*泉州市科技局 2024“揭榜挂帅”项目（2024XQ018）