基于改进 Merkle 哈希树的仿生水声通信安全方案

Masoud KAVEH，Abolfazl FALAHATI
伊朗科技大学电气工程系，伊朗德黑兰市，13114-16846

摘要：近来，在传输系统中仿生信号已用于实现具有高信噪比的隐蔽水声通信。高信噪比使得攻击者能实行恶意计划，导致传输系统易受恶意攻击。提出一种基于改进Merkle哈希树的安全方案，能够抵御当前水下攻击，具体包含重放攻击、伪造消息攻击、消息篡改攻击和分析攻击。进行安全性分析，证明所提方案能够抵抗这些类型的攻击。性能评估表明，该方案在能量消耗、通信开销和计算开销方面的效率可满足水声通信的限制要求。

关键词：海豚哨音；改进Merkle哈希树；安全水声通信（UWAC）
https://doi.org/10.1631/FITEE.2000043