异构网络中安全数据传输机制的研究与设计

石玲玲　　1　，李敬兆　　2

(1 安徽理工大学 现代教育技术中心，安徽 淮南 232001；2 安徽理工大学 电气与信息工程学院，安徽 淮南 232001)

摘　要：为保证无线和有线异构网络环境中数据安全传输，采用一种基于优化的 AES-GCM 认证加密算法和基于 SHA 的数字签名算法相结合的安全数据传输机制.该机制包括密钥的生成与管理、通信方的双向身份认证及高效安全的数据传输三部分，采用与随机数和时间戳相关的参数生成密钥，并使用改进的 ECDH 算法实现通信实体间的密钥共享来防止重放攻击，保证密钥安全；通过减少传统 AES 算法加密轮数保证消息传输高效性，为保证消息传输安全性，提出采用 CTR 分组加密结构，并将通信方的物理地址、随机数和计数器值作为初始化值用于生成优化的 AES-GCM 认证加密算法的密钥流.异构网络下的通信实验表明，本文提出的安全数据传输机制明显缩短了加密传输时间，保证了安全性和高效性.

关键词：异构网络；AES-GCM；椭圆曲线密码体制 ECC；数字签名；密钥管理

Research and design of secure data transmission mechanism in heterogeneous network

SHI Ling-ling　　1　，LI Jing-zhao　　2

(1 Modern Educational Technology Center, Anhui University of Science and Technology，Huainan 232001，China;

2 College of Electrical and Information Engineering，Anhui University of Science and Technology，Huainan 232001，China)

Abstract：In order to ensure the security of data transmission in wireless and wired heterogeneous networks, a secure data transmission mechanism based on optimized AES-GCM authentication encryption algorithm and SHA-based digital signature algorithm is adopted. This mechanism includes three parts: key generation and management, two-way identity authentication of communicators and efficient and secure data transmission. The key is generated by parameters related to random number and timestamp, and the key sharing among communication entities is realized by using improved ECDH algorithm to prevent replay attacks and ensure key security. It reduces the number of encryption rounds of traditional AES algorithm to ensure the efficiency of message transmission, in order to ensure the security of message transmission, CTR block encryption structure is proposed, and uses the physical address, random number and counter value of communicators as the initialized value to generate the key stream of the optimized AES-GCM authentication encryption algorithm. The communication experiment in heterogeneous networks shows that the secure data transmission mechanism proposed in this paper significantly shortens the encrypted transmission time and guarantees the security and efficiency.

Key words：heterogeneous network; AES-GCM; ECC; digital signature; key management

作者简介：

石玲玲　女，(1990-)，硕士，工程师.研究方向为计算机网络、信息安全.E-mail:15855401823@163.com.

李敬兆　男，(1964-)，教授，博士生导师.研究方向为嵌入式技术、物联网和云计算.