海洋观测通信组网安全及其硬件加速研究

徐天亮[1], 王晨旭[1, 2, 3], 王新胜[1, 2, 3], 罗清华[1, 2, 3], 刘志勇[1, 2, 3], 周志权[1, 2, 3]

(1. 哈尔滨工业大学(威海)信息与电气工程学院, 山东 威海 264209; 2. 山东船舶技术研究院, 山东 威海 264209; 3. 海洋通信与组网观测技术威海市重点实验室, 山东 威海 264209)

摘要: 从我国海洋信息观测需求入手, 分析海上临时无线组网安全通信基本需要, 提出一种基于 AES 和 RSA 算法与消息认证码(MAC)组合的一次性双向口令认证协议, 并对 RSA 算法硬件加速评估, 优化算法设计, 减少资源消耗, 解决海上信息采集临时组网通信安全问题。

关键词: 海洋组网; 加密算法; Hash 函数; 双向认证; 硬件加速

中图分类号: TP212 **文献标识码**: A **文章编号**: 1000-3096(2018)01-0015-06

DOI: 10.11759/hykx20171011020

随着物联网的迅速发展, 越来越多的领域开始涉及物联网通信技术, 物联网必然成为未来网络通信的主流技术, 在海洋观测领域通信组网也将会有广阔的应用空间[1-2]。另一方面, 海洋的观测数据属于国家机密, 应予以保护。我国在党的十八大报告中对海洋安全提出的一系列要求, 包括海洋资源开发、海洋环境保护、海洋经济发展和海洋权益维护等[3], 为了实现我国建设海洋强国的目标, 国家制定了一整套海洋战略规划和实施计划, 其中涉及政治、军事、文化、经济、外交、管理、法律、科技、安全、社会、教育等相关战略领域。这些海洋战略的实施依赖于完整且安全的海洋信息系统。

2016 年颁布的《中华人民共和国网络安全法》对于关键信息基础设施的信息安全有明确的要求, 为了防止信息的篡改、窃取和泄露等威胁。本文主要针对海上组网通信的安全性进行研究, 分析海洋观测临时通信组网的可能性。

1 海洋观测通信组网

1.1 海洋信息安全与海洋观测分析

海洋信息系统为各项海洋工作提供完整的信息支撑与安全畅通的信息通信渠道, 最大限度地发挥海洋信息资源的价值[4]。因此, 海洋信息系统发展是国家海洋战略的重要组成部分。采集海洋的信息数据包括温度、密度、潮汐、水深等敏感信息, 这些信息在海面作业、海上航行和海洋军事领域起着尤为重要的作用。比如在军事领域方面, 风向和海浪会影响重武器的发射精度; 水文参数和地形信息影响作战计划的制定, 如果敌方获取了对应的参数, 则会针对地形信息制定反策略计划, 严重危害我国海上领土安全。可见, 保障海洋信息的安全尤为重要。

在海洋观测网中, 如何确保信息在传输过程中不被他人篡改, 如何鉴别信息的完整性。对于完整性鉴别技术, 我们可以通过对身份、口令、密钥以及信息数据等项实施鉴别, 在通过加密技术实现对数据的保护。我国的海洋观测数据对于国防、国家安全、国民经济具有重要的作用, 因此海洋观测数据传输的安全性也是必须要考虑研究的内容, 包括基于硬件认证协议的身份鉴别技术; 基于硬件加速的大数据加解密技术。

1.2 海上临时无线组网通信

海洋信息向陆上数据中心的传输及各终端的协同观测, 需组网完成。但与陆上网络不同, 海洋信息的观测设备位于海上及水下, 传输环境复杂。特别是

收稿日期: 2017-10-11; 修回日期: 2017-12-23

基金项目: 山东省自然科学基金项目(ZR2014FM023); 山东省重大科技创新工程项目(2017CXGC0921); 哈尔滨工业大学创新基金项目(HIT.NSRIF.2016108); 哈尔滨工业大学(威海)学科建设引导基金(WH20160103, WH20160207)

[Foundation: NSF project of Shandong province (ZR2014FM023), Major Scientific and Technological Innovation Project of Shandong Province of China (2017CXGC0921), Research and Innovation Fund Project of Harbin Institute of Technology (HIT.NSRIF.2016108), Discipline Construction Guiding Foundation in Harbin Institute of Technology at Weihai (WH20160103, WH20160207)]

作者简介: 徐天亮(1995-), 黑龙江双鸭山人, 男, 硕士研究生, 从事芯片安全及其可靠性, E-mail: tianlianghit@163.com; 王晨旭(1977-), 通信作者, 河南周口人, 男, 副教授, 硕士生导师, E-mail: wangchenxu@hit.edu.cn.

水下，传输环境更为复杂多变，需要有针对性的研究相关技术。面对实际的应用需求，采集对应的海洋数据信息，此时需要在海上建立临时的无线网络进行互相传输和信息通信，如图 1 所示的海上组网通信结构图。

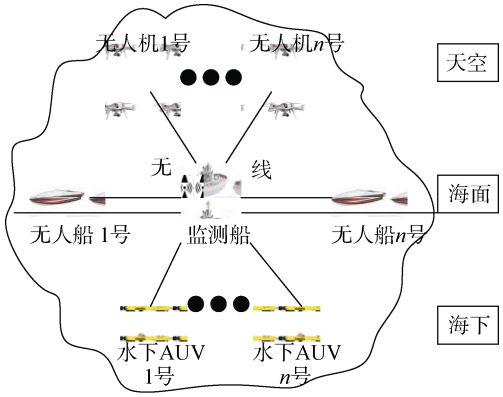

图 1　海上组网通信结构图

Fig. 1　Communication structure of marine networking

从图 1 可以看出，整个结构实现监测船与空中、海上、海下等移动设备之间的相互通信。值得的注意的是海洋信息传输的基础是海洋通信技术，没有通信基础设施的支持，海洋信息不可能传输到陆上。但海洋通信环境存在特殊性，如海面通信节点的稀疏性，水天通信距离远(卫星)，水下传输环境的复杂多变性，给水下、水面、水天通信链路的可靠性带来了很大的挑战，需要考虑解决。这就要求我们设计一种双向认证协议，保障海上监测船终端与无人机、无人船、水下探测机器人(AUV)等移动设备的通信安全。

2　面向海上临时组网的双向认证技术研究

在物联网的信息通信过程中，监测服务器和移动设备的数据交互安全尤为重要。哈希函数有两个优点，一是具有较小的计算消；二是具有良好的安全性，而口令认证是一种常用的用户认证协议。因此，使用哈希函数来保护口令安全是最典型、应用最广泛的协议算法。

哈希函数函数，也叫 Hash 或单向散列函数，它通过 Hash 算法把任意 n 位长度的输入数据压缩成固定长度的输出，表达式为 h=H(n)，h 是固定长度散列值，H(M)是单向散列函数，也就是一种反映输入数据与存放地址的映射关系，值得注意的是构造的 Hash 表中散列值尽可能均匀分布。

在目前已有的双向认证协议中，林扬武提出一种基于 Hash 函数和消息认证码(MAC)的双向口令认证协议[5]，尽管作者分析能够抵抗所有已知攻击，但存在密钥窃取泄露的危险。通过喻丽春提出的基于 AES 和 RSA 算法的一次性口令认证[6]思想。结合两种方案的优点，提出一种新的基于 AES、RSA 和消息认证码的一次性双向口令认证协议。该协议使用 AES 对称加密和 RSA 非对称加密算法保护数据的传输安全，使用 Hash 函数和消息认证码(MAC)完成双向口令认证过程。

完整的协议包括注册阶段和认证与密钥协商阶段两部分。约定以 ME 表示移动设备，这里的移动设备包括无人机、无人船、水下探测机器人(AUV)等无线设备，MS 表示监测服务器，PW_{ME} 表示对应 ID_{ME} 的口令信息，RSA 算法生成的公钥和私钥分别以(e, N)和(d, N)表示，KP 表示 AES 对称算法生成的密钥，H(x)表示 x 的哈希值，$Ee(x)$表示(e, N)加密 x，$E_{KP}(x)$ 表示使用 KP 加密 x，MAC 值是通过 KP 加密的一组数据信息，“: ”表示连接符号。

2.1　注册阶段

当移动设备 ME 要与监测服务器 MS 进行通信时，首先需要通过注册阶段，具体请求和密钥产生过程如图 2 所示。

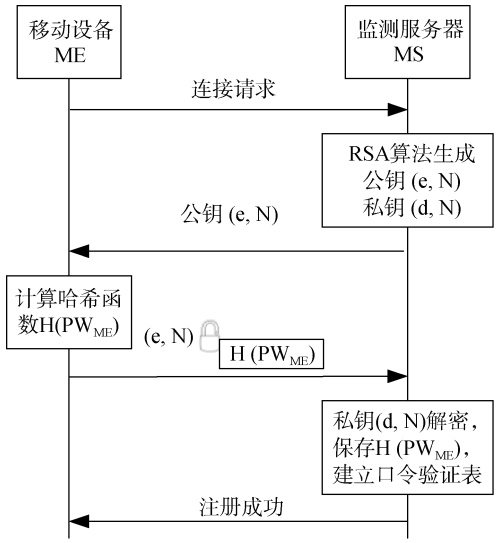

图 2　设备注册阶段流程

Fig. 2　Process of equipment registration

具体工作流程如下:

第 1 步: ME 向 MS 发送连接请求。

第 2 步: MS 通过 RSA 加密算法中密钥生成阶段,

生成公钥(e, N)和私钥(d, N)，发送公钥(e, N)到 ME 端。

第 3 步: ME 利用 MD5 算法计算口令信息 PW_{ME} 的 Hash 值 $H(PW_{ME})$，在使用 MS 的公钥(e, N)加密 $H(PW_{ME})$，发送 $Ee(H(PW_{ME}))$到 MS 端。

第 4 步: MS 使用私钥(d, N)解密得到 $H(PW_{ME})$，判断移动设备是否重复，如果不重复，保存该数据 $H(PW_{ME})$，同时 MS 建立口令验证表，表中含有每个用户的 ID 信息以及通过该 ID 计算的 Hash 散列值。如果重复，则提示移动设备已经被使用，同时告知 ME 修改注册 ID。服务端返回注册成功。

2.2 认证与密钥协商阶段

认证与密钥协商阶段的前两步为密钥协商，后 4 步为双向认证过程，完整流程图如图 3 所示。

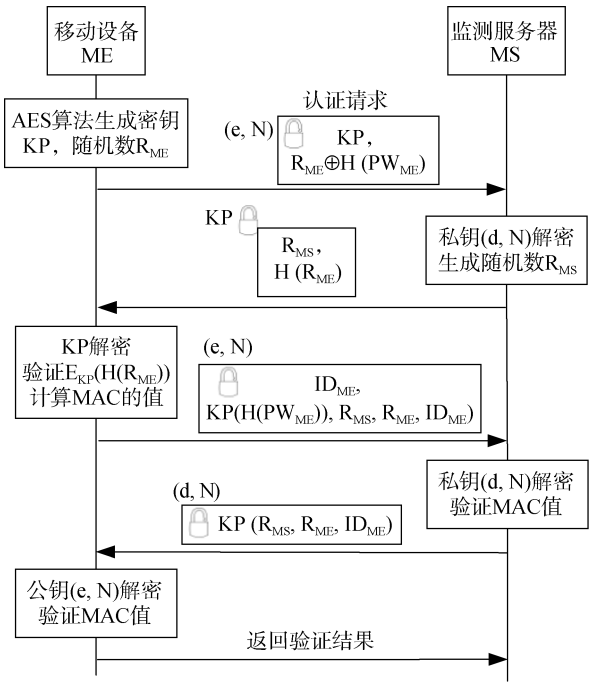

图 3 完整认证阶段流程

Fig. 3 Complete authentication phase flow chart

具体工作流程如下:

第 1 步: 移动设备 ME 向监测服务器 MS 提交认证请求，同时 ME 使用 AES 加密算法生成加密密钥 KP，并且生成一个随机数 R_{ME}，使用公钥(e, N)加密 KP，发送 Ee(KP)和 $Ee(R_{ME} \oplus H(PW_{ME}))$到 MS 端。

第 2 步: MS 使用私钥(d, N)进行解密，得到密钥 KP，计算得到 R_{ME}，生成随机数 R_{MS}，使用 KP 加密 R_{MS}, R_{ME}，发送 $E_{KP}(R_{MS})$和 $E_{KP}(H(R_{ME}))$到 ME 端。

第 3 步: ME 使用 KP 解密得到 R_{MS}，并验证 $E_{KP}(H(R_{ME}))$。此时 ME 调用密钥 KP 计算 MAC 的值 $KP(H(PW_{ME}), R_{MS}, R_{ME}, ID_{ME})$，然后将 ID_{ME} 与计算出来的 MAC 值使用 MS 的公钥(e, N)加密后，发送到 MS 端。

第 4 步: MS 使用私钥(d, N)解密得到 $KP(H(PW_{ME}), R_{MS}, R_{ME}, ID_{ME})$，根据 ID_{ME} 查口令验证表得到 $H(PW_{ME})$，调用密钥 KP 计算 $H(PW_{ME}), R_{MS}, R_{ME}, ID_{ME}$ 的 MAC 值，并检验该值与移动设备 ME 传过来 MAC 值是否一致。如果一致，则监测服务器 MS 认证移动设备 ME 成功，协议继续；若不一致，则验证失败，拒绝移动设备 ME 的认证请求。

第 5 步: MS 调用密钥 KP 计算 R_{MS}, R_{ME}, ID_{ME} 的 MAC 值，并将该值 $KP(R_{MS}, R_{ME}, ID_{ME})$使用 MS 的私钥(d, N)加密后，发送给移动设备 ME 端。

第 6 步: ME 使用公钥(e, N)解密得到 $KP(R_{MS}, R_{ME}, ID_{ME})$，并调用密钥 KP 计算 R_{MS}, R_{ME}, ID_{ME} 的 MAC 值，并检验该值与收到的 MAC 值是否一致。如果一致，则移动设备 ME 认证监测服务器 MS 成功，协议完成；否则拒绝监测服务器 MS 的认证请求。

3 协议的安全性分析

本协议可抵抗如下攻击。

3.1 DOS 攻击

拒绝服务攻击简称 DOS 攻击，当攻击方对监测服务器 MS 进行 DOS 攻击时, MS 会在认证与密钥协商阶段的第 4 步检测出移动设备 ME 的非法性，在此之前，移动设备不需要多次迭代哈希运算，减少了移动设备部分计算量。而对于验证过程只需要查找口令表中 $H(PW_{ME})$信息一次，通过调用密钥 KP 计算 MAC 值一次。由于监测服务器生成的随机数 R_{MS} 可以重复使用，因此在 DOS 攻击下，生成随机数时的资源消耗可以忽略不计。即本协议可以抵抗 DOS 攻击。

3.2 抗重放攻击

由于在每次验证 MAC 值交互时加入验证者自己选取的随机数，即使传输的数据被窃取泄露，或者监测服务端系统瘫痪，在选取的随机数不重复的情况下, MAC 值的永远不会重复。因此，本协议可以抵抗重放攻击。

3.3 抗口令猜测攻击

通过减少移动设备 ME 的连接次数来防止在线口令猜测攻击。由于 Hash 函数和生成消息认证码(MAC)的过程所产生的碰撞概率等价于离线口令猜测，而对应的概率值比较低，通过分析确定本文协

议可以防止离线口令猜测攻击。

3.4 抗盗取验证表攻击

在本协议中，监测服务器 MS 的口令查找表中只包含移动设备的 ID_{ME} 和口令信息的 Hash 值，并未存储用于 MAC 算法的对称密钥 KP，所以攻击方即使通过其他信息泄漏通道获得口令验证表，也不能在密钥未知的条件下生成正确的 MAC 值，即无法获取任何的有用数据。同时本协议使用 AES 对称和 RSA 非对称组合技术生成加密密钥，并在双方的密钥协商阶段每次只传递一个加密数据或加密密钥，即使部分数据被窃取泄露，攻击方也无法获取全部的随机数和密钥或者是明文数据，能够保障数据的安全性。

3.5 抗假冒监测服务器攻击

如果攻击者想要假冒监测服务器 MS，他必须能够使用密钥 KP 计算 R_{MS}，R_{ME}，ID_{ME} 的 MAC 值，但是移动设备和监测服务器都生成一次性的随机数，通过 RSA 与 AES 加密实现了移动设备和监测服务器的双向认证，并且攻击者不能同时获得密钥 KP，(e, N)和(d, N)。因此，攻击者不可能通过假冒监测服务器 MS 实现与移动设备 ME 之间的通信。

3.6 抗假冒移动设备攻击

如果攻击者想假冒移动设备 ME，他必须通过密钥 KP 计算 $H(PW_{ME})$, R_{MS}, R_{ME}, ID_{ME} 的 MAC 值来实现假冒，但这些计算所使用的数据被全部泄漏的可能性极低，即便他能够窃取口令验证表，通过查表获得 $H(PW_{ME})$信息，也无法在密钥未知或其他随机数未知的情况下生成正确的 MAC 值。因此假冒移动设备 ME 也是不现实的。

4 硬件加速

本文提出的协议使用 RSA 与 AES 两种加密算法结合加密数据的思想，非对称的 RSA 算法弥补对称 AES 算法单个密钥保存不安全性问题；反之，AES 算法解决 RSA 算法运算速度较慢的问题[7]，两者之间相互弥补不足，结合加密方案对于实际应用更加安全。由于协议中 RSA 算法消耗的资源相对较多[8]，这里则主要介绍 RSA 算法的硬件实现，采用 Verilog 硬件描述语言对 RSA 加密算法进行设计描述与仿真，且下载到 DE2 开发板中进行 FPGA 硬件加速优化，同时，将 RSA 算法的核心模幂运算转化成多个模乘运算，使用从高位到低位扫描方式的蒙哥马利优化算法进行 RSA 算法的模乘运算，即在硬件实现中不使用传统的除法操作，而采用移位操作来实现模乘运算，使算法效率得到提高。

4.1 RSA 模块设计

通过对信息加密的硬件应用需求分析，本协议中 RSA 算法的 Verilog 描述的顶层模块设计命名为 RSA_1024，也就是说，该算法能实现 1024 位数据的加密和解密，具体管脚设计如图 4 所示。

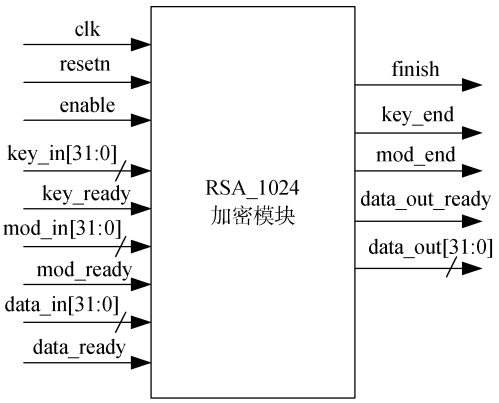

图 4 RSA_1024 模块外部管脚示意

Fig. 4 Schematic diagram of the outer foot of the RSA_1024 module

RSA_1024 顶层模块输入信号分别为：clk 输入时钟、resetn 复位信号、enable 使能信号、key_in 加解密密钥 e/d 输入、mod_in 模 n 输入、data_in 明文 M(密文 C)数据输入、key_ready 准备输入密钥数据信号、mod_ready 准备输入模数据信号、data_ready 准备输入明密文数据信号。加密模块的输出信号有：finish 模块结束信号、data_out 数据输出的结果信号、key_end 密钥数据输入结束信号、mod_end 模输入结束信号、data_out_ready 明密文输出信号。

RSA 加密模块采用的是并行数据输入的方式，最高可支持 1024 位数据运算。为了优化结构减少资源的浪费，在设计中将所用到的输入数据以 32bit 为一组，以周期为单位连续 32 次输入，也就是采用分组输入数据的方式把 1024bit 数据拆解成 32×32 的数据进行输入。只有当对应的加密密钥 e、模 n、明密文数据的准备信号拉高时，才可以输入对应数据。加密运算结束后准备输出信号拉高，输出对应加密的数据。只要模块结束信号为低，那么整个 RSA 模块就会停止工作。

4.2 RSA 加密系统功能划分

所设计的 RSA_1024 加密系统的整体结构包括控制功能实现模块、数据处理模块和数据存储模块

三个部分组成，如图 5 所示。对应不同部分功能的实现还调用了相关模块。

在图 5 中，RSA_1024 加密模块整体可分为三大部分，RSA 控制功能实现模块、实现类似 Q=Z+C+XY 功能的数据处理模块、分别作为明文或密文数据输入和模 n 输入的分组采集模块 RAM_0 和 RAM_1。其中 RSA 控制功能实现模块主要作用是对加解密钥 e/d 输入进行分组采集，通过密钥移位进行分支语句的判断，来执行数据模幂运算和蒙哥马利模乘运算。而通过 RAM 地址选择控制和循环计数控制来分别对数据存储模块进行选择 RAM_0、RAM_1 和存储运算过程中间的数据值。控制状态转换开关在 RSA 整体功能实现的过程中起到联系各个模块的作用，共同实现 RSA 加密算法。

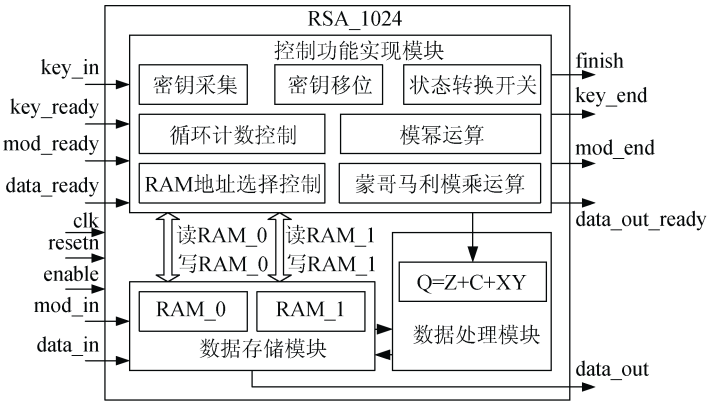

图 5　RSA_1024 加密系统功能划分

Fig. 5　Functional division of RSA_1024 encryption system

4.3　仿真验证与面积评估

为验证 RSA 加密算法的功能，采用仿真工具 ModelSim 对 RSA 加密算法的 Verilog 设计进行功能仿真，验证的功能结果正确。再利用 Quartus II 软件将代码下载到 DE2 开发板中进行 FPGA 验证，其中主芯片采用 Cyclone II 的典型芯片 EP2C35F672C6，验证的结果同样正确。对 RSA 加密算法硬件加速评估，优化算法设计，减少资源消耗。使用的工艺库为 SMIC 65nm CMOS 工艺库，在 Linux 系统下使用 synopsys 公司的 Design Compiler(DC)进行逻辑综合。逻辑综合是将 RTL 级描述的算法，转变为由逻辑门组成的逻辑电路。DC 首先对 RTL 模块进行加载读取，然后根据约束脚本中的时间、面积、输入输出延时等约束信息，使用代工厂(Foundry)提供的 SMIC 65nm 工艺库通过对应的逻辑门组成逻辑电路，并对逻辑电路进行优化。本文所使用的 RSA 加密算法综合后得到 2691 个有效门，均衡考虑满足使用条件，对本文提出的协议实现进一步资源优化。

5　结束语

本文的协议在注册过程中使用 RSA 非对称加密，不依赖于安全通道也可以确保注册数据信息的安全性，这在海上临时无线组网观测系统身份双向认证过程中尤为重要。认证过程中使用对称 AES 生成密钥 KP 可以在本次通信结束后，继续使用，持续保障无线数据传输的安全。本文协议使用的哈希次数相对较少，但数据的传输次数和加解密次数相对增多。这使系统安全性明显增强，但系统在认证过程中耗时增大。这些问题可通过硬件加速和提升硬件配置解决。在注册和认证过程中不依赖安全通道，所有数据采用加密传输，移动设备不需要存储元件，只需记住 ID 和口令就能够进行双向身份认证，这对海上临时无线组网观测系统的双向通信提供保障。

参考文献:

[1] 李磊. 物联网对计算机通信网络的影响[J]. 电子技术与软件工程, 2017, (12): 34-40.
Li Lei. The impact of internet of things on computer communication networks[J]. Electronic Technology & Software Engineering, 2017, 12: 34-40.

[2] 王景中, 凌晨. 基于节点认证的物联网感知层信息安全传输机制的研究[J]. 技术研究, 2014, 2: 53-57.
Wang Jingzhong, Ling Chen. Reliable information transmission mechanism research of the internet of things Sensing layer based on the Node Authentication[J]. Net Info Security, 2014, 2: 53-57.

[3] 梅莉蓉. 海洋信息系统安全体系研究[J]. 通信技术, 2017, 50(8): 1822-1825.

Mei Lirong. Security architecture of marine information system[J]. Communications Technology, 2017, 50(8): 1822-1825.

[4] Xu W, Yan S F, Ji F, et al. Marine information gathering, transmission, processing, and fusion: Current status and future trends[J]. Science China(Information Science), 2016, 46(8): 1053-1085.

[5] 林扬武. 物联网的安全认证技术研究[J]. 无线互联科技, 2012, 10: 8-9.
Lin Yangwu. Research on internet of things security certification technology[J]. Wireless Internet Technology, 2012, 10: 8-9.

[6] 喻丽春. 基于 AES 和 RSA 算法的一次性口令认证[J]. 西安邮电大学学报, 2017, 22(1): 38-43.
Yu Lichun. One-time password authentication based on AES and RSA algorithm[J]. Journal of Xi'an University of Posts and Telecommunications, 2017, 22(1): 38-43.

[7] Liu Z, Huang X Y, Hu Z, et al. On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(3): 237-248.

[8] Liu Z, Großschädl J, Hu Z, et al. Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things[J]. IEEE Transactions on Computers, 2017, 66(5): 773-785.

Research on safety and hardware acceleration of ocean observing communication networks

XU Tian-liang[1], WANG Chen-xu[1, 2, 3], WANG Xin-sheng[1, 2, 3], LUO Qing-hua[1, 2, 3], LIU Zhi-yong[1, 2, 3], ZHOU Zhi-quan[1, 2, 3]

(1. Information and Electrical School, Harbin Institute of Technology, Weihai 264209, China; 2. Shandong Institute of Shipbuilding Technology, Weihai 264209, China; 3. Weihai City Key Laboratory of Ocean Communication and Networking Observation Technology, Weihai 264209, China)

Received: Oct. 11, 2017
Key words: Ocean Networking; Encryption algorithm; Message Authentication code; Two-way Authentication; Hardware Acceleration

Abstract: Given the demand for gathering ocean information in our country, this paper analyzes the basic requirements for the security of temporary wireless networks that are used for communication in a maritime environment. In this context, this study presents a one-time two-way password authentication protocol based on the AES, RSA encryption algorithm and message authentication code (MAC) combination. This paper also evaluates hardware acceleration for the RSA algorithm, presents an optimization algorithm design, reduces resource consumption, and solves the security issues concerning temporary ocean networks used for information collection purposes.

(本文编辑: 梁德海)