

集成国密算法安全芯片的电力无线传感器研究

随着传感技术的发展,电力无线传感器在智能电网中得到大量应用,但同时也带来了信息安全问题。电力无线传感器通信过程无安全防护,传感数据易被截取、伪造和篡改等,从而影响电网安全稳定运行。提出在无线传感器、无线接收基站中集成基于国密算法的安全芯片,开发基于国密算法的电力传感数据安全接入系统,无线传感器与基站通过双向认证后方可相互通信,传感数据加密传输,避免因篡改、伪造控制指令控制传感设备,保障电网运行的安全。

李良^{1,2} 丁岳^{1,2} 王峰^{1,2} / 1.北京智芯微电子科技有限公司(北京市电力高可靠性集成电路设计工程技术研究中心) 2.北京智芯微电子科技有限公司(国家电网公司重点实验室、电力芯片设计分析实验室)

0 引言

随着我国智能电网建设,越来越多的无线传感设备被应用于电力系统在线监测中,通过传感器构成的感知层来达到智能控制的目的。感知层是智能电网的基础设施,它利用感知设备、智能终端等对电网环境、电力设备以及基础设施等进行感知,如部署在电气设备、线路和电力环境等的传感器、智能表计等。感知设备获取的传感数据可通过无线或有线方式进行传输,并由汇聚节点进行统一汇聚、分析、处理和上报,最终结果用于服务端的相关决策。智能电网不仅面临传统信息和网络模式的安全问题,还存在感知层中智能终端等带来的新安全问题:①感知设备易受攻击。感知设备由于功能简单、数量巨大及部署地偏远,很容易被攻击者实施直接的物理攻击;②无线通信易受攻击。感知设备通常通过无线方式进行信息采集,无线通信的开放性使攻击者很容易通过窃听、伪造和重放等方式实施攻击。

根据《国家电网公司智能电网信息安全防护总体方案》要求:信息采集处理类的系统,包括输变电设备在线监测系统,在接入内网时应采用终端身份认证和访问控制措施,建立加密通道来进行信息采集,保证业务数据的保密性和完整性。

1 基于国密算法的电力传感数据安全接入系统设计

现有变电站中的传感器等收集到的传感数据大部分使用无线传输,且不具备安全机制,无法满足电力传感数据传输安全方面的要求。本文方法保证传感数据的合法性和安全性,保障传感器数据安全接入到主站系统中。加密算法是防止非法设备侵入和通信信息泄密的主要技术手段。具有信息加密的功能,还具有数字签名、身份验证等功能。使用密码技术不仅可以保证信息的机密性,而且可以保证信息的完整性,防止信息被篡改、伪造和假冒。为保障无线接入的数据安全,项目根据传感器的处理能力、功耗等指标,采用集成SM1、SM7加密算法的安全芯片。

1.1 适用于电力物联网感知层的安全机制、安全芯片及密钥算法

无线传感器的数据传送给综合监测单元(CMU),再利用CMU的上行通道接入到变电设备状态接入控制器(CAC),之后通过专线接入变电站的状态接入网关机(CAG)。无线传感



李良/高级工程师

关键词/Keywords

无线传感器·
无线基站·
国密算法·
安全芯片·

器、无线综合监测单元等无线通信设备中将集成安全芯片，进行设备的身份认证，同时对通信数据进行加密保护，从而实现电力传感数据从过程层到间隔层的安全接入，如图1所示。

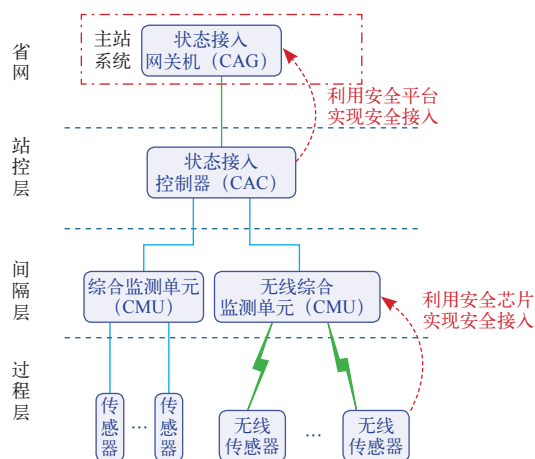


图1 电力传感数据安全接入系统

1.2 基于国密算法的传感数据安全接入技术

基于国密算法的传感数据安全接入方案中，设备身份认证是保护系统安全的一个重要机制，无线监测装置要保证数据来源的可靠性，综合监测单元也需确保数据传向正确的对象，双方均有权要求验证对方身份以维护自身利益。本文设计为双向认证，即传感器要验证CMU的身份，CMU也需验证传感器的身份。为避免无线传输的数据被非法者窃听，需对传输线路上数据进行加密处理，使非法窃听器即使获得了信息也无法知晓信息的真实内容。为避免无线传输的数据被干扰或破坏，需对传输线路上的数据进行完整性验证，使数据接收者能够甄别数据的有效性。无线传感装置和无线CMU集成国密算法安全芯片，其中SM1算法模块为传感器和CMU之间的数据接入提供安全保障措施，如图2所示。

2 基于国密算法的电力传感数据安全接入系统实现

2.1 集成国密算法的无线温湿度传感器设计实现

2.1.1 集成国密算法的无线温湿度传感器原理

无线温湿度传感器采用高准确度数字式温

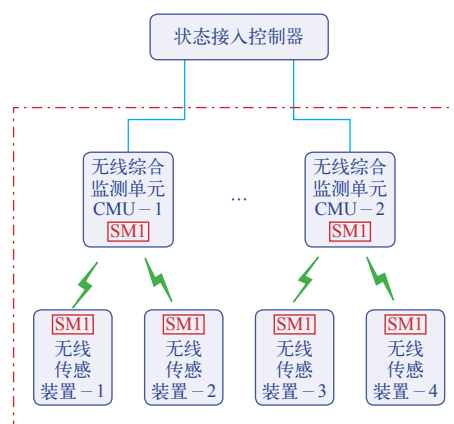


图2 无线传感器安全防护示意图

湿度传感器芯片，具有自动校准、测量准确度高及响应速度快的特点。湿度的测量主要依靠一个电容性聚合体湿敏感元件，它具有吸湿性与胀缩性，高分子聚合物吸收水分后其介电常数明显改变，随着环境湿度的提高，高分子聚合物吸附的水分子增多，温湿度传感器的电容量增加，所以根据电容量的变化可测得相对湿度，这种方法的优点是响应时间快、温度特性好。测温度时主要依靠一个能隙材料制成的测温元件，测量时先由温度传感器产生温度信号，经过放大，送至A-D转换进行转换、校准和纠错，最后将数据传给微处理器。

电池给整个无线传感器系统提供电源，单片机通过I²C总线访问传感器，传感器出来为数字信号，如温湿度数字信号。nRF5188单片机通过SPI控制2.4 G通信模块，功耗1 mA，通过SPI控制安全芯片，原理图如图3所示。

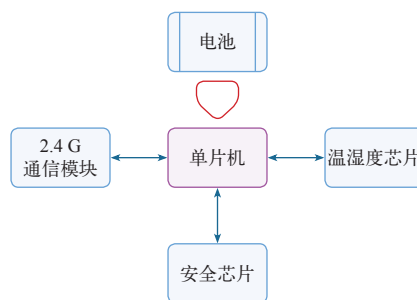


图3 无线温湿度传感器详细设计原理图

2.1.2 传感单元

SHT21温湿度集成传感器。采用CMOS过程

微加工专利技术 (CMOSens technology)，确保产品具有极高的可靠性和出色的长期稳定性。该传感器由1个电容式聚合体测温元件和1个能隙式测温元件组成，并与1个14位A-D转换器以及1个2-wire数字接口在单芯片中无缝结合，使得该产品具有功耗低、反应快和抗干扰能力强等优点。

SHT21的特点具有以下功能：相对湿度和温度的测量兼有露点输出；全部校准，数字输出；接口简单（2-wire），响应速度快；超低功耗，自动休眠；出色的长期稳定性；测温准确度 $\pm 45\%RH$ ，测温准确度 $\pm 0.5\text{ }^{\circ}\text{C}$ （ $25\text{ }^{\circ}\text{C}$ ）。

2.1.3 主控单元设计

nRF5188单片机稳定性极好，可以在十分恶劣的环境下稳定工作，IC功能包括：256 KB片上闪存和16 KB RAM；数字和混合信号周边，包括SPI、2-wire和ADC以及正交解码器；16PPI通道；搭配片上LDO时电源范围为1.8~3.6 V，LDO旁路模式为1.75~1.95 V；完整的蓝牙协议堆栈（到配置文件的链接层）。

对于专有应用程序，nRF51822提供全新改进型Gazell™ 2.4 GHz RF协议堆栈，与nRF24L系列Gazell应用程序达至互操作性。与上一代的nRF24LE1相比，nRF51822与全新Gazell协议堆栈的组合能削减高达30%的功耗。

2.1.4 安全芯片

安全芯片嵌入到监测装置或传感器的主板中，安全芯片和监测装置/传感器之间通过SPI接口相连，并向监测装置/传感器提供控制指令以访问安全芯片资源。安全芯片将一张具有操作系统（COS）的CPU封装成SOP8模块。将其嵌入传感器中，完成数据的加密解密、双向身份认证、访问权限控制、通信线路保护、临时密钥导出和数据文件存储等多种功能。安全芯片的基本操作方式为：从接口设备接收一条命令，然后经过处理返回应答信息给接口设备。其具体运行过程如图4所示。

在命令的处理过程中，如果在其中的任意一层模块处理中发现错误，芯片返回出错信息。防

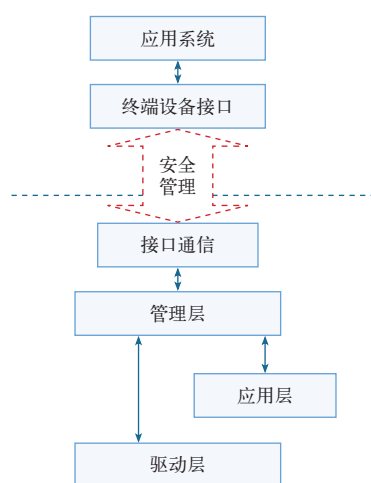


图4 芯片运行过程图

止恶意攻击，从而保证了安全芯片的安全性。

安全芯片在做好COS后，可以根据使用的需要采用不同的封装形式，可以封装成接触式卡片，也可以封装成SOP8的模块；接触式卡片封装的芯片可以与卡基一起封装成接触式CPU卡，SOP8封装的模块可以作为一个安全存取单元，将其嵌入到无线传感器中，完成数据的加密解密、双向身份认证、访问权限控制、通信线路保护和数据文件存储等多种功能。

2.2 集成国密算法的无线基站设计实现

外接电源给无线传输基站提供电源，Freescale公司Kinetis K60系列MCU通过SPI总线访问2.4 G无线传输模块，接收无线传感器信号。K60主控芯片通过SPI控制安全芯片。无线基站通过公网GPRS模块与计算机端相连，也可以通过网口、串口与计算机进行通信，基站通信原理图如图5所示。

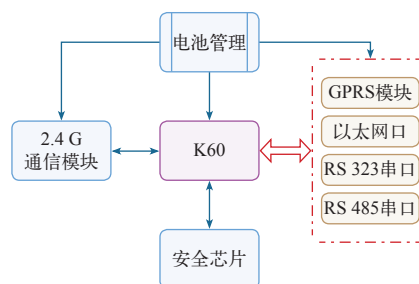


图5 基站通信原理图

K60工作电压为1.71~3.6 V，闪存的写电压为

1.71~3.6 V, 采用ARM Cortex-M4内核, 其性能可达到1.25Dhrystone MIPS/MHz。该系列提供高达180 MHz 的性能和IEEE 1588以太网MAC, 用于工业自动化环境中准确、实时的时间控制。硬件加密支持多个算法, 以最小的CPU负载提供快速、安全的数据传输和存储。系统安全模块包括安全密钥存储和硬件篡改检测, 提供用于电压、频率、温度和外部传感(用于物理攻击检测)的传感器。Kinetis K60 MCU适用于设计基站。

3 基于国密算法的电力传感数据安全接入系统实验验证

3.1 基于国密算法的电力传感数据安全接入系统数据加解密验证

为了验证基于国密算法的电力传感数据安全接入系统数据经过加密传输, 在无线基站内部将明文数据和密文数据通过RS 232总线打印出来, 以验证数据的加密通信, 基于国密算法的电力传感数据安全接入系统验证测试拓扑图如图6所示。

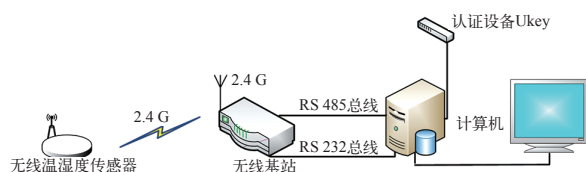


图6 测试拓扑图

主要设备列表如下表所示。

表 主要设备列表

序号	设备名称	测试拓扑图中的设备名称	数量/台
1	无线基站	无线基站	1
2	便携式计算机	计算机	1
3	集成国密算法无线温湿度传感器	无线温湿度传感器	1
4	智能密码钥匙Ukey	认证设备Ukey	1

SJK1704智能密码钥匙用于验证无线传感数据经过SM1加密, 插入便携式笔记本USB口。

打开SMart Card Program V1.2 Beta版软件, 将数据整理为智能密码钥匙识别的指令。通过软件连接智能密码钥匙, 将指令流如下发送给智能密码钥匙用于验证数据的正确性。

根据系统拓扑图组建系统, 将无线基站的232串口、485串口及智能密码钥匙Ukey连接到便携式计算机, 无线基站上电, 打开_Px326.11SetupPackage V3, SSCOM3.2软件。

从SSCOM3.2软件, 获取三组无线传感器原始明文密文数据。

获取的原始数据如下:

集成国密算法无线温湿度传感器地址为: 8001, 数据如下所述。

System[5]密文:

60, ae, 8b, 3b, 1f, df, d, ad, f9, 85, 99, c9, 42, 9d, d4, ba,

System[5]明文:

5, 71, 80, 1, b5, 5, f, 7, f8, 15, 7, eb, 48, 20, 3c, 0,

System[5]密文:

b8, d1, bd, 2, 73, 72, 0, 88, 1c, 5d, e0, 4, 15, f3, af, 4,

System[5]明文:

5, 71, 80, 1, b5, 40, f, 8, ff, 96, 0, 6a, 48, 20, ed, 0,

SJK1704智能密码钥匙用于验证无线传感数据经过SM1加密, 插入便携式笔记本USB口。打开SMart Card Program V1.2 Beta版软件, 将数据整理为智能密码钥匙识别的指令。通过软件连接智能密码钥匙, 将指令流如下发送给智能密码钥匙用于验证数据的正确性。

正常情况下密钥是不可知的, 为验证加密的正确性, 故将密钥设置为一个固定值, 设置SM1加解密密钥指令如下: 77777777777777777777777777777777。

集成国密算法无线温湿度传感器地址为: 8001, 数据如下所述。

(1) 温度数据

System[5]密文:

60, ae, 8b, 3b, 1f, df, d, ad, f9, 85, 99, c9, 42, 9d, d4, ba,

System[5]明文:

5, 71, 80, 1, b5, 5, f, 7, f8, 15, 7, eb,

48, 20, 3c, 0,

解密密文: 8072010010 60AE8B3B1FDF0DADF98
599C9429DD4BA

SW: 9000 Response: 05718001B5050F07F81507E
B48203C00

加密明文: 8072000010 05718001b5050f07f81507e
b48203c00

SW: 9000 Response: 60AE8B3B1FDF0DADF985
99C9429DD4BA

(2) 湿度数据

System[5]密文: b8, d1, bd, 2, 73, 72, 0,
88, 1c, 5d, e0, 4, 15, f3, af, 4,

System[5]明文: 5, 71, 80, 1, b5, 40, f, 8,
ff, 96, 0, 6a, 48, 20, ed, 0,

解密密文: 8072010010 B8D1BD02737200881C5D
E00415F3AF04

SW: 9000 Response: 05718001B5400F08FF96006
A4820ED00

加密明文: 8072000010 05718001B5400F08FF9600
6A4820ED00

SW: 9000 Response: B8D1BD02737200881C5DE
00415F3AF04

通过上述数据的对比, 基于国密算法的电力
传感数据安全接入系统数据均经过加密传输, 可
实现数据的保密传输。

3.2 基于国密算法的温湿度传感器测量参数验证

为验证集成国密算法的无线温湿度传感器测
量的准确度及范围, 本文通过第三方检测机构对
本文所述的样品进行了温湿度测量值的验证。

试验箱显示 $(25.4 \pm 2) ^\circ\text{C}$ 、 $(20 \pm 3) \%$
温湿度工作2 h测试样品显示 $27 ^\circ\text{C}$ 、 20.5% ; 试
验箱显示 $(50 \pm 1) ^\circ\text{C}$ 、 $(90 \pm 3) \%$ 温湿度工
作2 h测试样品显示 $50 ^\circ\text{C}$ 、 86.5% ; 试验箱显
示 $(-40 \pm 1) ^\circ\text{C}$ 温度工作2 h测试样品显示
 $-39.45 ^\circ\text{C}$; 试验箱显示 $(-20 \pm 1) ^\circ\text{C}$ 温度工作2 h
测试样品显示 $-20 ^\circ\text{C}$; 试验箱显示 $(-0 \pm 1) ^\circ\text{C}$
温度工作2 h测试样品显示 $0 ^\circ\text{C}$ 。试验箱显示
 $(20 \pm 1) ^\circ\text{C}$ 温度工作2 h测试样品显示 $20 ^\circ\text{C}$ 。试

验箱显示 $(40 \pm 1) ^\circ\text{C}$ 温度工作2 h测试样品显示
 $40.5 ^\circ\text{C}$; 试验箱显示 $(60 \pm 1) ^\circ\text{C}$ 温度工作2 h测试
样品显示 $60.5 ^\circ\text{C}$; 试验箱显示 $(85 \pm 1) ^\circ\text{C}$ 温度工
作2 h测试样品显示 $84.5 ^\circ\text{C}$ 。

通过上述第三方检测机构的温湿度试验, 基
于国密算法的电力传感数据安全接入系统可准确
有效地测量温湿度信息。

4 结束语

本文创新性地提出一种由国密算法实现的适用
于电力物联网感知层的双向认证安全机制, 该安全
机制由两次独立的单向身份认证构成, 认证因子
16 B数据经SM1加密后得到16 B的认证码, 两次认
证码对比相同才视为认证通过, 保证无线电力传感
数据的安全性。研制一种集成国密算法安全芯片
的无线电力温湿度传感器, 保证无线电力传感器传
输的数据均为国密算法SM1加密的密文数据。

本文完成电力传感数据安全接入, 避免了
通过篡改或伪造控制指令控制感知设备或智能终
端, 使得终端进行非正当操作从而实施攻击, 造
成质量事故引起的停电问题, 生产、生活用电得
到保障; 电力公司能够更加有效、持续的调配电
力资源, 使得电网资源利用率最大化。电力传感
数据的安全接入, 可提升变电站日常运维工作效
率, 运维成本得到降低。

参考文献

- [1] 刘勇, 黄茂云, 张东升. 电缆接头无线测温装置
设计[J]. 科技创新与应用, 2017(5): 38-39.
- [2] 崔丽, 周宇浩, 张益, 等. 电力电缆智能温度巡检
系统设计[J]. 实验室研究与探索, 2016, 35(4):
78-81.
- [3] 高强, 王洪礼, 刘歆, 等. 高压变电站无线测温
预警系统设计[J]. 仪表技术与传感器, 2009(1):
105-107.
- [4] 杨明欣, 王建波, 于志强, 等. 基于TI单片机低
功耗无线测温装置的设计[J]. 电子制作, 2013
(15): 87-91.

(收稿日期: 2018-01-20) EA