DOI:10.3969/j.issn.1006-6403.2017.11.005

农业物联网的轻量级安全架构

[黄泽龙 叶惠卿 张文安]

摘要

随着物联网技术、农业规模化生产的蓬勃发展，依托物联网系统提供的自动化、智能化服务，农业生产逐步实现降险增产节能。与此同时，农业物联网系统安全显得尤其重要。本文针对农业物联网的安全需求，结合物联网设备处理能力有限的特性，提出轻量的安全架构，关键技术，为农业生产保驾护航。

关键词： 物联网 安全 农业

黄泽龙

中国电信股份有限公司广州研究院，工程师，主要研究方向物联网安全、移动安全认证、移动支付和智能卡应用。

叶惠卿

广东环境保护工程职业学院讲师，主要研究方向为信息安全。

张文安

中国电信股份有限公司广州研究院高级工程师，多年来主要从事电信增值业务研发，负责过中国电信语音增值业务、移动支付、移动安全认证及物联网相关产品的研发工作。

1 概述

现如今，我国正大力发展智慧农业，应用基于物联网技术的智慧监测系统，提高农业生产规模化、集约化的管理水平和应对异常能力。比如，[1,2,3] 提出的基于物联网技术的水产养殖系统，系统实时监测养殖水质参数，远程控制设备（如增氧机、水泵、消毒机等）实时调控水质，提供视频监控、生产管理、疫病远程问诊、水产品食品溯源等功能；[4,5,6] 提出的基于物联网技术的种植监测系统，系统实时监测温室（大棚）、果园种植环境，远程控制设备（如水泵、排气扇等）执行灌溉、通风、采光。这些系统一般划分为三个逻辑层：设备层、网络层和应用层，如图1所示。

设备层由传感器、控制设备以及采集（控制）节点组成，传感器负责采集养殖水质、种植环境和气象等参数，控制设备负责调控生长环境。网络层一般采用无线网络，包括 WIFI、2/3/4G、NB-Iot 等传输技术，负责将监测参数、控制结果等信息上传到平台，以及将操作命令下发到采集（控制）节点。应用层包括处理平台、手机 App 等，负责存储、处理和应用信息，并为用户提供操作界面。

农业物联网系统为农业生产提供高效、自动化和远程的管理服务，减少人工开销、增加产量、降低风险、提高监管水平。但是，多数系统没有深入考虑安全问题，存在安全隐患，一旦出现问题，后果不堪设想，例如：

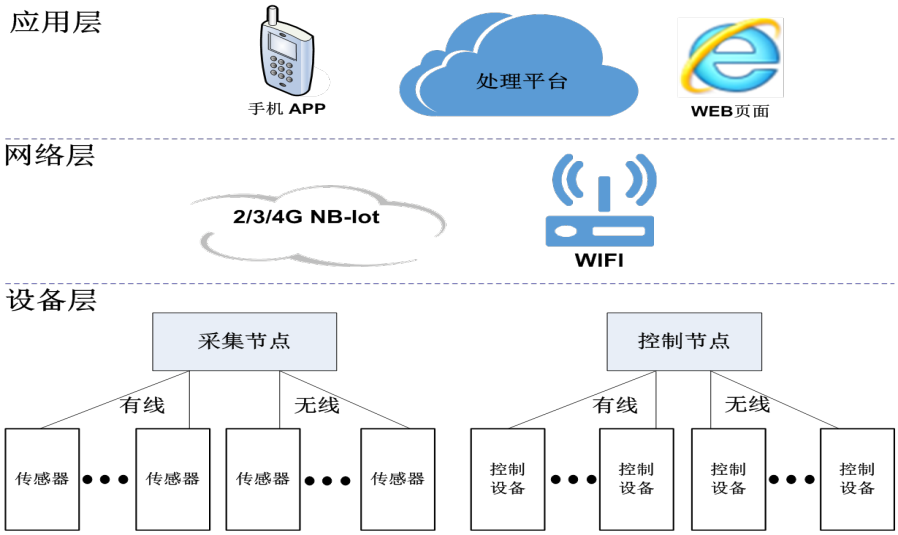

图 1 农业物联网系统架构

① 水质参数篡改，如溶解氧参数被非法篡改，造成无法监测到养殖水缺氧；

② 设备非法启停，如水泵无故排水，消毒机无故开启以及增氧机无故停止；

③ 传感器被冒充，上报无效的监测数据。

此外，考虑到成本，农业物联网系统的节点、设备一般采用计算能力有限、存储容量较小的芯片（比如，STM32），造成节点和设备难以或无法使用复杂的安全方案。

因此，本文结合农业物联网设备处理能力有限的特性，提出一种轻量级的安全架构，介绍架构采用的关键安全技术，以满足农业物联网的安全要求。

2 轻量级的物联网安全架构

轻量级的物联网安全架构如图 2 所示，包括设备层、网络层和应用层三层的安全。由于网络层采用无线网络传输信息，且无线网络已经存在许多安全保护技术、安全标准，故不作为研究重点 7，架构着重考虑设备层、应用层的安全。设备层安全包括物理安全、身份认证和数据安全；应用层安全包括数据隐私、异常监测、访问控制，身份认证以及告警。

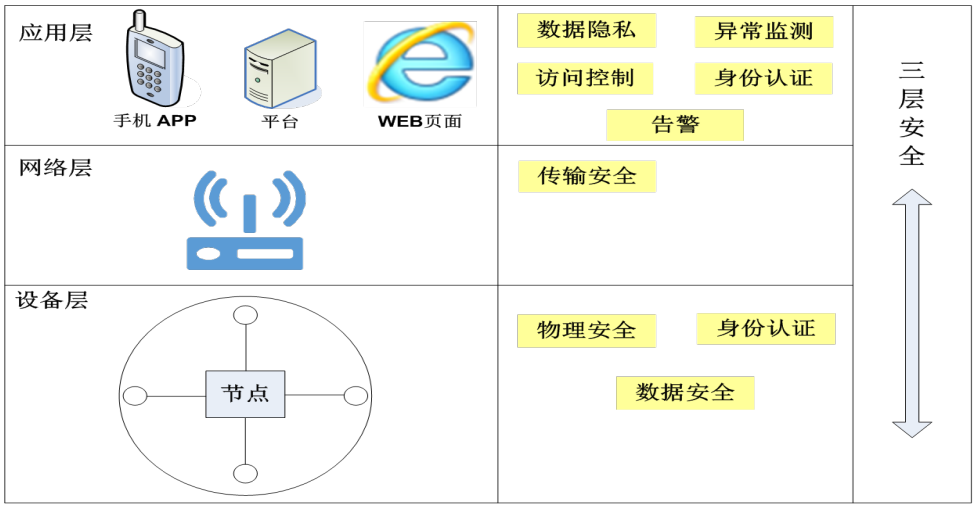

图 2 轻量级的物联网安全架构

2.1 设备层安全

设备层的物理安全，主要保证设备不被轻易破坏、恶

意移动位置，以及非法读取内部输出信息。安全措施包括：为设备加上保护外箱；在设备中增加定位芯片；禁用设备的芯片调试接口，或授权后才能访问调试接口。

设备层的身份认证，验证平台身份，确保数据上传到合法处理平台，以及控制指令来自合法处理平台，认证方法见3.2。设备层中，传感器、控制设备和节点间不使用身份认证。

设备层的数据安全，通过对设备和节点间的通信数据加密和计算 MAC，确保数据合法。

2.2 应用层安全

应用层通过如下方式保证设备、用户的身份合法性，操作合法性，以及数据存储安全：

① 数据隐私——敏感数据加密存放（密码改为存放 HASH 值，位置信息改为存放密文等）和传输（平台和节点间的消息采用敏感数据加密以及计算消息 MAC）；

② 异常监测——监测设备、设备访问是否出现异常行为，包括：设备同时通过不同 IP 或多个连接发送数据，设备访问太频繁、访问 IP 频繁变化，设备连续发送无效报文，设备位置偏移设定值，用户操作太频繁或连续请求非授权访问；出现异常行为时，平台暂停或禁止设备和用户访问；

③ 访问控制——包括资源访问控制和操作访问控制；资源访问控制限制用户可以访问的监测参数、传感器和控制设备等系统资源，操作访问控制限制用户可以对资源执行的操作，比如启停控制设备，修改传感器配置等；

④ 身份认证——认证设备和用户的身份合法性；设备的身份认证方法见 3.2；用户的身份认证方法采用密码校验 + 短信验证码二次校验的方式。

⑤ 告警——当设备和用户的访问，以及环境参数出现异常时，通过短信、App 短消息等通知用户。

3 关键安全技术

3.1 密钥体系

安全架构包含两种密钥：设备和节点间的共享密钥，节点和平台间的共享密钥。密钥在生产时固化到节点、设备中，省去密钥分发的机制 8。密钥采用 3 级分层结构，如图 3 所示。节点内存放身份认证密钥、消息加密钥、消息 MAC 密钥和设备密钥四种密钥，设备内只存放设备密钥，具体如下：

①身份认证密钥——用于平台和节点间的双向身份认证；

②消息加密密钥——用于平台和节点间敏感数据加密；

③ 消息 MAC 密钥——用于平台和节点间报文的 MAC 值计算；

④设备密钥——用于节点和设备间的数据加密、MAC 计算。

其中，每个节点的身份认证密钥、消息加密钥、消息 MAC 密钥和设备密钥各不相同，每个传感网络内使用不同的设备密钥，但传感网络内部的节点和设备使用同一个设备密钥。

密钥的生成和分散方法采用 [9] 中提供的方法。

3.2 身份认证换协议

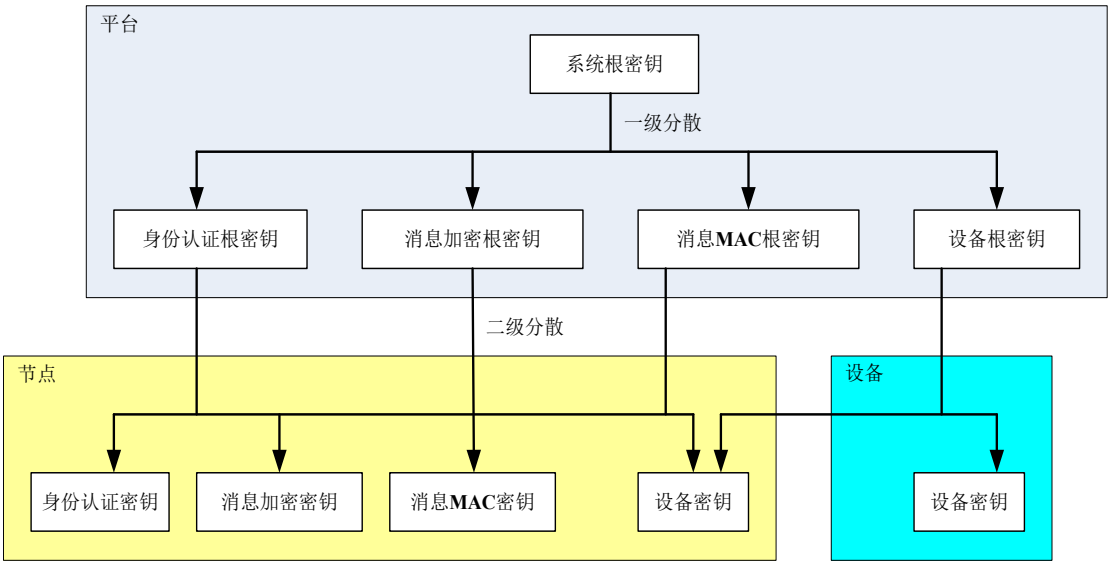

图 3 密钥体系

由于节点、设备的计算能力、资源有限（一般采用STM32 芯片），若平台和节点间身份认证采用 [10] 提出的基于公钥体制的认证协议，会出现计算耗时过长等问题，难以实现。因此，认证方式采用对称加密算法 3DES 和哈希算法 HMAC_SHA1，具体为：假设 P 表示平台，N 表示节点，KEY 表示平台和节点间的身份认证密钥，Ri 表示参与方 i 产生的随机数，可表示为：

1、N --> P:Nid, RN

2、P-->N: RP, HMAC_SHA1(KEY, RN)

3、N-->P: Nid, HMAC_SHA1 (KEY, RP)

步骤 1、节点向平台发起认证请求，请求参数包括节点 ID Nid、长度为 8 字节的 16 进制随机数 RN；

步骤 2、平台使用 KEY，RN 计算 MAC 值，并将 MAC 值和长度为 8 字节的 16 进制随机数 RP 发送给节点；

步骤 3、节点验证平台提供的 MAC 值通过后，使用 KEY，Rp 计算 MAC 值，并请求平台验证 MAC 值，平台验证节点提供的 MAC 值通过后，完成双方身份认证。

3.3 会话密钥

双向身份认证通过后，平台和节点采用如下方法生成会话密钥：假设 KEYs 表示会话密钥，XOR 表示异或运算，KEY 表示平台和节点间的消息加密或消息 MAC 密钥，可表示为：

KEYs=3DES(KEY, RN XOR RP)

为加强安全性，设置会话密钥具有时效性。超过时效，或节点重新建立连接时，平台强制要求节点再次执行双向认证，重新生成会话密钥。

3.4 加密与计算 MAC

平台和节点间采用会话密钥对消息进行加密和计算 MAC。

节点和设备间采用设备密钥对消息进行加密和计算 MAC。

加密采用 3DES 算法，计算 MAC 采用 HMAC_SHA1 算法。

4 结束语

本文提出的安全架构，重点关注设备层、应用层的安全，包括设备的物理安全，平台与节点间的身份认证、消息加密、消息 MAC，平台数据安全存放，设备和用户的异常监测以及用户的访问控制，提供多方面安全保护：

① 身份安全，平台和节点的双向身份认证，防止设备、平台被冒充；

② 信息安全，敏感数据的加密传输与存放，确保信息的机密性；信息的 MAC 验证，确保信息完整和防篡改；

③ 位置安全，内置位置芯片，防止设备被移动到非指定地点，提供无效监测数据；

④ 访问安全，监测设备和用户的异常访问行为，异常发生时，中断或禁止访问，防止恶意访问系统资源和非授权操作；

⑤信息告警，系统、设备、生产环境参数异常时，及时通知。

综上，本文提出的安全架构采用轻量级的认证、加密算法，能在计算能力、资源有限的物联网设备上实现，能多方面保证农业物联网系统安全，易实现又不失安全性。

参考文献

1 曾宝国，刘美岑 . 基于物联网的水产养殖水质实时监测系统 [J]. 计算机系统应用 , 2013, 22(6):53-56

2 徐晓姗 . 基于物联网和 3G 技术的智能水产养殖环境监测系统的设计与应用 [J]. 网络安全技术与应用 , 2014(9):235-236

3 黄建清，王卫星，姜晟，等 . 基于无线传感器网络的水产养殖水质监测系统开发与试验 [J]. 农业工程学报 , 2013, 29(4):183-190

4 朱娟 . 基于无线传感网络的智慧农业监测系统研究 [J]. 湖南农机 , 2014(3):77-79

5 盛平，郭洋洋，李萍萍 . 基于 ZigBee 和 3G 技术的设施农业智能测控系统 [J]. 农业机械学报 , 2012, 43(12):229-233

6 夏雪，丘耘，胡林，等 . 基于 3G 和 DDNS 的果园环境远程监控系统 [J]. 自动化与仪表 , 2013, 28(8):23-26

7 武传坤 . 物联网安全关键技术与挑战 [J]. 密码学报 , 2015, 2(1):40-53

8 孙玉砚，刘卓华，李强，等 . 一种面向 3G 接入的物联网安全架构 [J]. 计算机研究与发展 , 2010, 47(s2):327-332

9 黄泽龙，张文安，谢云 . 移动支付密钥体系研究 [J]. 电信科学 , 2011, 27(6):21-27

10 马文杰 . 物联网安全技术的研究与应用 [D]. 山东大学 , 2011

（收稿日期：2017-10-24）