doi:10.11959/j.issn.1000-436x.2017258

基于 ZigBee 的无线传感网可信溶液监测系统

王天舒，张功萱，杨曦晨
（南京理工大学计算机科学与工程学院，江苏 南京 210094）

摘 要：温室培养液中一些重要营养元素的浓度往往被忽视并且 ZigBee 监测系统的核心节点协调器容易遭受捕获攻击。设计可信溶液监测系统各节点硬件结构、外部电压测量过程和数据清洗过程。为协调器节点配备可信模块，设计针对协调器的可信 u-boot，对关键文件进行完整性检查，实现节点可信启动。实验结果表明，系统中每个节点可以自动地监测溶液浓度，并且协调器可信模块可以检测出被捕获的协调器并示警。因此该系统具有较强的功能性与安全性。
关键词：监测系统；ZigBee；无线传感网；可信
中图分类号：TN98, S126 **文献标识码**：A

Trusted solution monitoring system based on ZigBee wireless sensor network

WANG Tian-shu, ZHANG Gong-xuan, YANG Xi-chen
(School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract: In the greenhouse environment, the concentration of nutrient solution was always ignored. At the same time, the core node coordinator of the ZigBee wireless monitoring system was easily compromised. A trusted solution monitoring system based on ZigBee wireless sensor network was designed and implemented. Firstly the hardware structure of sensor, router and coordinator was introduced. Then the processes of external voltage measurement and data cleaning were illustrated. For realizing the trusted boot of the coordinator, trusted u-boot to measure the integrity of some key files was designed. Experimental results show that the solution concentration data could be sent from each node to the monitoring computer and the remote terminal. At the same time, the trusted module of the coordinator can detect the captured coordinator node and warning. Therefore, the designed system has strong function and security.
Key words: monitoring system, ZigBee, wireless sensor network, trusted computing

1 引言

目前中国温室、大棚面积占世界温室总面积 42.8%，中国已成为温室栽培规模第一大国。因此，温室环境控制水平是中国温室生产力关键指标。随着物联网[1]不断发展以及设施作物生产规模扩大，无线传感网技术[2]已被用于温室环境监控，从而使整个温室生产系统处于良好运行状态。胡瑾等[3]设计基于无线传感网温室光环境调控系统，通过调光节点控制 LED 亮度，实现光照强度监控。蒋毅琼等[4]利用 ZigBee 技术和 GPRS 技术，开发日光温室无线传感网 CO_2 监控系统，实现 CO_2 调控。Dan 等[5]设计智能农业温室环境监测系统，实现温度监控。Abdolhamid 等[6]基于 ZigBee 技术和 GSM 网络，设计并实现温室远程监控系统，监测温度、湿度以及光照。然而当前国内外研究者设计的基于无线传感网温室监测系统[3~14]主要关注温度、湿度、光照、土壤水分、土壤 PH 值、CO_2 浓度及营养液电导率。温室营养液中氮元素对作物生长也具有关键作用。然而目前尚未

收稿日期：2017-09-28
基金项目：国家自然科学基金资助项目（No.61272420, No.61472189）
Foundation Item: The National Natural Science Foundation of China (No.61272420, No.61472189)

有针对温室营养液氮元素的无线传感网监测系统具体实施方案。

另一方面，无线传感网要实现数据感知、采集与传输的基本功能，安全策略是最关键的技术之一[15]。对于基于 ZigBee 的无线传感器网络，敌手更倾向于向计算存储能力强的核心节点协调器发动捕获攻击。目前无线传感网安全策略[16~19]多数通过软件的方式实现一些加密、解密、散列等基本安全功能。这些安全策略并不能高效且准确地检测出被捕获的协调器节点。

根据研究现状，本文设计并实现基于无线传感网的可信溶液监测系统。一方面，该系统可以自动检测温室营养液氮浓度，并将实时数据发送至 PC 监测机与远程客户端。另一方面，根据可信计算理论，系统内的协调器节点配备有可信模块，周期性检测协调器节点可信性。可信计算理论的主要思路是从协调器软硬件的底层先建立一个可信根，再建立一条可信链，从可信根开始到引导文件，到操作系统，再到监测程序，一级度量认证一级，一级信任一级，把这种信任扩展到协调器，从而保证节点的完整性和安全性。功能性与安全性测试结果表明本文设计可信溶液监测系统具有实时性、准确性与可信性优点。

2 系统结构设计

ZigBee 技术作为一种无线传输技术，是温室生产系统中应用最广泛的无线传感网技术，具有功耗小、成本低和可靠性高优点。同时，ZigBee 协议栈 Z-Stack 支持 128 bit AES 加密算法，提供数据在无线传输过程中的加解密与完整性检查功能。本文设计的可信溶液监测系统采用 ZigBee 实现无线传输。系统由 6 个层次组成：传感器层、路由器层、协调器层、PC 监测机、云端、客户端，如图 1 所示。其中，传感器、路由器与协调器是 ZigBee 网络 3 种逻辑设备类型。一个 ZigBee 网络由一个协调器、多个路由器和多个传感器组成，可形成星型、树形与网型拓扑结构[10]。

实际应用时传感器节点分布于大范围无土栽培农田、测试溶液或培养基中，完成数据采集与发送任务。它们将采集的溶液氮浓度数据传输至路由器。在采集数据时环境或器件变化会影响数据质量，所以传感器还需要进行数据清洗工作。路由器负责寻找、建立以及修复网络报文的路由信息，并转发网络分组。协调器负责网络建立与相关配置，对收到的下层数据进行融合，并通过串口将数据发送至上层 PC 监测机。PC 监测机对数据进行实时监测，若发现溶液氮浓度不在标准范围内，则进行示警。同时，协调器还需将实时数据送入云端，并将数据分布式存储于云内。客户端设备包括 PC、平板电脑、便携电脑、智能手机、PDA 等各种可接入网络手持移动设备，工作人员可远程监控温室营养液氮浓度信息。

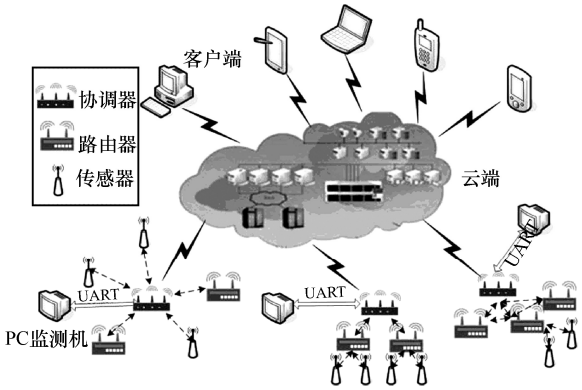


图 1 基于 ZigBee 的可信溶液监测系统的层次结构

3 系统硬件设计

3.1 传感器/路由器节点设计

考虑到传感器节点分布范围广、数量多的特点，需精简其组成部件以减少成本。如图 2 所示，传感器/路由器节点由传感模块、处理器 CC2530 两部分组成。路由器节点除了具有一般传感器节点的数据采集与无线传输功能，还具备路由功能，将上一跳节点数据发送至下一跳。此外，路由器还需具备一定数据融合能力，以减轻协调器负担。

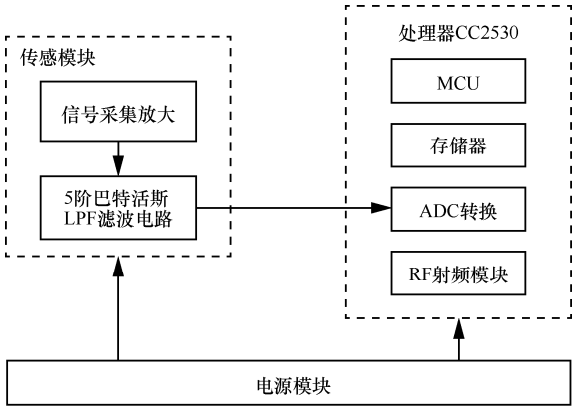


图 2 传感器/路由器节点结构

3.1.1　处理器 CC2530

处理器 CC2530 部分负责将传感模块采集的模拟信号转换成数字信号并进一步处理。CC2530 芯片主要由 MCU 微处理器、存储器、RF 射频模块、ADC 模拟数字转换器 4 个部分构成。其中，RF 射频模块具有 2.4 GHz IEEE 802.15.4 标准射频收发器、出色的接收器灵敏度和抗干扰能力。ADC 将滤波得到的模拟电压转换为数字电压，进而送入 MCU 进行处理。

3.1.2　传感模块

农作物（例如蔬菜）营养液的氮源主要以硝酸态氮为主。因此传感模块负责将营养液硝酸根浓度信号转换成 CC2530 处理的电压信号，它由信号采集放大电路与滤波电路组成。信号采集通过 403 型硝酸根电极与参比电极进行。403 型硝酸根电极属电压传感器，即测得的硝酸根溶液浓度信号为电压信号，其量级为毫伏级。而 CC2530 的 ADC 的分辨率为 12 位，所以 CC2530 无法检测毫伏级的电压变化。因此电压信号在发送到 CC2530 前需要对电压信号进行放大处理。本文采用 AD620AN 芯片对采集到的电压信号进行放大，其放大倍数 G 由 AD620AN 增益式(1)决定，其中，R_G 为芯片外接调整电阻阻值。

$$G = \frac{49.9}{R_G} \tag{1}$$

为避免环境或元器件对信号的干扰，需对采集放大的信号进行滤波处理，即尽可能减小脉动的直流电压中的交流成分，使输出电压纹波系数降低，波形变得较为平滑。本文采用如图 3 所示的 5 阶巴特沃斯 LPF 滤波电路对电压信号进行滤波，该电路需要包含三级放大器。由于 LM324 芯片具有 4 层放大器，且所需电源与 AD620AN 芯片相同，所以本文选用 LM324 芯片进行滤波处理。

3.1.3　电源模块

电源模块负责整个节点的电源供应，由两部分构成：3V 转 3.3V 为 CC2530 供电；3V 转±12V 为传感模块供电。由于传感器节点需要长期放置在野外，无法持续供电，所以本文采用两节五号电池串联供电，可支持 4~5 个月。在电量充足的情况下，两节 1.5V 干电池串联后输出电压为 3V。本文采用 TPS60211 芯片，将输入的 1.8~3.6V 电压转换成恒定 3.3V 电压；采用 MAX668 芯片作为升压型 DC 变换器，将 3.3V 电压转换成 12V 输出。此外，传感模块信号采集部分需±12V 双电源供电，故采用 TPS5430 芯片将+12V 输入电压转换为−12V 电压输出。

3.2　协调器节点设计

协调器除具有传感器/路由器节点数据采集与发送功能，还需负责网络建立、配置与管理，并将汇聚的数据传输至上层监测机。因此，协调器需要较高性能处理器与较大容量存储器以适应更强数据存储与实时计算需求。同时，协调器是整个无线传感网核心，最易遭受敌手捕获攻击，因此需要具备一定抗攻击能力。本文选用具有强大数据处理与存储能力的 ARM 架构 PandaBoard 开发板作为协调器核心载板，负责数据实时处理与传输。本文在核心板上增加可信模块与传感器模块，为协调器分别提供安全性增强与数据感知发送功能。如图 4 所示，

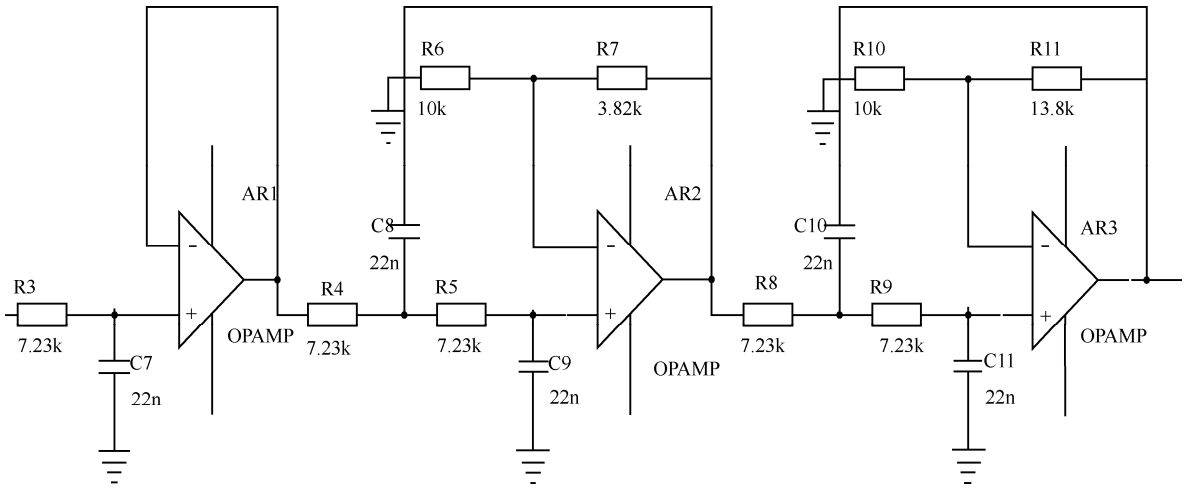


图 3　5 阶巴特沃斯 LPF 滤波电路

协调器硬件结构包括核心板 PandaBoard、可信模块与传感器模块。

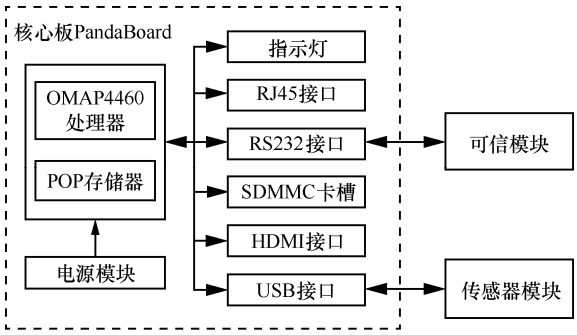


图 4 协调器节点结构

3.2.1 核心板 PandaBoard

PandaBoard 是以 OMAP4460 为处理器的开发平台，该平台可以在保持低功耗同时满足用户访问 OMAP4460 多媒体处理器的多种强大功能需求。由图 4 可知，该平台主要包括 OMAP4460、POP 存储器、电源模块以及多种接口及指示灯。OMAP4460 可以支持高级别操作系统，并提供最优视频与图形图像处理能力。电源模块采用 TI TWL6030 芯片进行电源管理，其内部包含 1 个电源管理系统、2 个 HS-I2C 接口、1 个 24 MHz 阻容振荡器等，并具有 MMC 卡检测机制。该芯片可以对整个 PandaBoard 的设备进行供电和电源管理。PandaBoard 具有丰富的指示灯与接口，接口包括 RJ45 接口、RS232 接口、SDMMC 卡槽、HDMI 接口以及 USB 接口等。在本文的溶液监测系统中，指示灯用来标识当前协调器可信状态。RJ45 接口用来与上位机实时通信，协调器可以通过网线将无线传感网中节点采集的数据传输至远程用户。RS232 接口与 USB 接口分别用来连接可信模块和传感器模块通信。协调器节点通过串口将待度量数据传输至可信模块，并通过 USB 接收传感器模块采集与接收数据。

3.2.2 传感器模块

协调器的传感器模块硬件结构与传感器/路由器节点相同，如图 2 所示。传感器模块负责采集本地溶液数据，接收下层节点消息，并通过 RS232 将这些信息发送至 PandaBoard。传感器模块的处理器计算能力有限，因此复杂的数据融合算法以及分簇算法仍然在 PandaBoard 中运行。

3.2.3 可信模块

一个无线传感器网络包含成百上千个传感器节点，这些传感器节点一般都采用简单且廉价的微处理器，具有有限的存储与计算能力。而传统的可信密码模块[20,21]（如 TCM、TPM）具有复杂的 TCG 软件协议栈与多种不同的密码机制，增加了计算复杂度。因此，传统的 TCM/TPM 并不适应于无线传感器网络。针对无线传感器网络的实际特点，本文利用可信计算技术设计一个具有轻量逻辑结构与优化功能的可信模块[22]。该模块内部的密码引擎可以集成符合《可信计算密码支撑平台功能与接口规范》的 SM3 密码杂凑算法和 SMS4 对称密码算法。

4 数据监测与处理

溶液监测系统通过测量外部电压实现对溶液氮浓度的度量。由于电压在测量的过程中容易受外界影响而发生突变，因此需要去除电压测量值中异常值。本章给出节点对外部电压的测量以及数据清洗的过程。

4.1 外部电压测量

本文使用单通道 AIN0 测量传感模块感知的外部电压，该测量流程如算法 1 所示。首先配置 P0DIR 寄存器，将 P0_0 引脚设置为输入与上拉模式；配置 ADCCFG 寄存器将 P0_0 引脚设置为模拟输入。然后配置 ADCCON3 寄存器，选择模拟电源电压为参考电压，分辨率为 14，信道 0；配置 ADCCON1 寄存器，设置 AD 转换启动方式为手动触发并且启动模数转换。最后进入 whlie 循环，若单次 ADC 采样结束则跳出循环，并将采样结果存于 *value* 中。

算法 1 电压测量过程

```
1) procedure value = Measure_voltage()
2)      set(P0_0)→up&&input;     //P0DIR
3)      set(P0_0)→Analog Input;   //ADCCFG
4)          refvol(AnaPower)&&  Resolution(14)
&&Channel(0); //ADCCON3
5)              AD_Change(Manual)&&Start(AD)
//ADCCON1
6)      while(1)
7)          if(testend())
8)          break;
9)              end if
10)     end while
11)     value = result;
12) end procedure
```

value 中存储的只是一个二进制数，还需进一步计算得到最终电压值。*value* 取值与电压 *Vol* 的关系

如式(2)所示。

$$value=\begin{cases}16\,383, & Vol=3.3\\ 0, & Vol=0\end{cases} \tag{2}$$

由于分辨率被设为 14 位，因此 *Vol*=3.3V（电压值为模拟电源电压）时，*value*=0X3FFF=$2^{14}-1$=16 383；*Vol*=0 时 *value*=0。*value* 与电压 *Vol* 关系为过零点二元一次方程，可以得到式（3）。但实时计算式(3)对计算能力有限的 CC2530 比较困难，而 16 383≈16 384=(2^{14})且移位操作更简单省电，故直接将 3*value* 的值右移 14 位。

$$Vol=\frac{3value}{16\,383} \tag{3}$$

4.2　数据清洗

外界环境、元器件等因素会导致测量的外部电压值突变，因此需要对这些测量值进行数据清洗。算法 2 给出数据清洗过程。

算法 2　数据清洗过程

1) procedureVol_clean =Data_clean (Vol_period)
2)　max_count = count(Vol_period);
3)　difference = absolute(Vol_period-max_count);
4)　difference = del_zero(difference);
5)　threshold = count(difference);
6)　*j* = 1;
7)　for *i* = 1 to size(Vol_period);
8)　if max_count-threshold≤Vol_period≤max_count+threshold
9)　Vol_clean[*j*] = Vol_period[*i*];
10)　else
11)　*j* = *j*+1;
12)　end if
13)　end for
14) return Vol_clean;
15) end procedure

假设在某个时间段内，采集溶液电压值均存储于数组 Vol_period。首先计算 Vol_period 数组出现频次最高值 max_count（第 2）行），再计算 Vol_period 数组内值与 max_count 差值的绝对值，并存入 difference 数组（第 3）行）。接下来，将 difference [0]值去掉（第 4）行），并计算 difference 数组出现频次最高值 threshold（第 5）行）。将 Vol_period 数组超出[max_count-threshold, max_ count+threshold]范围值删除，得到 Vol_clean 数组（第 6）~14）行）。Vol_clean 存储该段时间内经过数据清洗电压值。

4.3　通信数据分组

协调器节点通过串口与 PC 监测机进行通信，下层节点单次发送 15 B 数据给上层节点。因此，监测机单次接收 15 B 数据，每个字节的含义如表 1 所示。表 1 中节点的网络地址、氮浓度值与父节点网络地址是必需的。监测机对每次接收的数据进行截取，可以得到节点的网络地址与父节点网络地址。同时，监测机对溶液氮浓度值所在关键位置进行截取可以得到每个节点所测量的溶液中硝酸根离子的浓度。

表 1　协调器发送数据含义

字节	含义
01	CRC
02 03	父节点地址
04 05	溶液氮浓度值
06 07	子节点数据长
08 09	氮浓度分组标志
10 11	节点网络地址
12 13	回馈标志
14 15	总数据长度

5　协调器节点的可信增强

协调器节点在基于 ZigBee 的无线传感网中处于核心地位，容易遭受敌手的捕获攻击。本文对协调器节点进行可信增强，从而提高无线传感网的安全性。本节给出协调器节点的可信增强方案，包括协调器的可信 u-boot 设计与实现。

5.1　协调器的可信 u-boot 设计

攻击者在捕获协调器节点后，通过篡改协调器的内核代码或应用程序，获取节点的控制权，从而进一步控制整个网络，并恶意截取或篡改所有节点采集的数据。在本文的可信溶液监测系统中，协调器节点的可信模块可以周期性地对节点进行重启

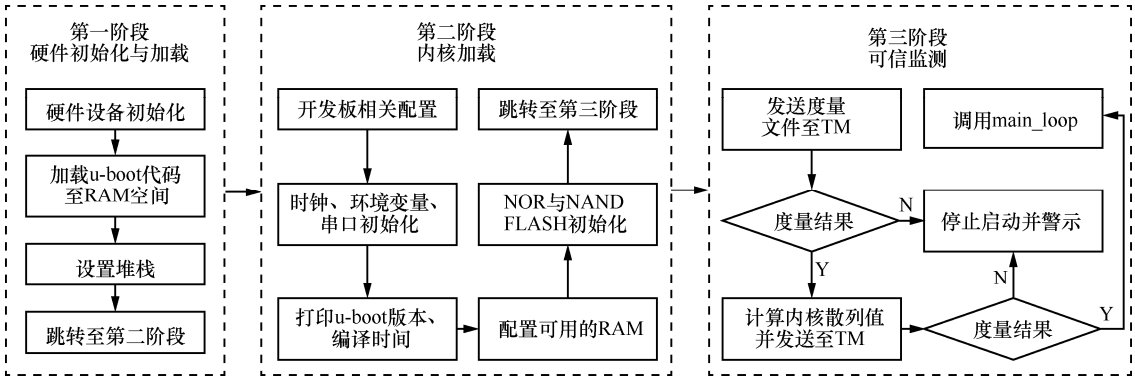


图 5 可信 u-boot 的流程

操作，定期检测协调器的安全性。重启的周期可以根据实际情况下协调器 LED 亮灯示警频率在可信模块中设置。在协调器节点进入操作系统之前，首先进入 u-boot。原有的 u-boot 只包括 2 个阶段：硬件的初始化与加载、内核加载。当时钟、环境变量、串口、Flash 等一系列初始化操作完成之后，u-boot 就开始调用主循环，进入操作系统阶段。本文在原有的 u-boot 基础之上，将可信监测作为第三阶段，在该阶段对协调器节点进行完整性度量。本文设计的可信 u-boot 的流程如图 5 所示。被攻击者捕获并被篡改内核代码的协调器节点不能通过可信模块的完整性检查而被检测出来。

第三阶段是可信 u-boot 的核心，经过前 2 个阶段硬件初始化工作，RS232 总线已可以进行数据传输。可信 u-boot 通过 RS232 首先发送待度量文件 u-boot.bin 至协调器可信模块。可信模块将成功接收的文件存放至自身的缓冲区，对文件进行完整性度量，并将得到的度量值 $ePCR1'$ 与标准度量值 $ePCR1'$ 进行比较。完整性度量的方法如式（4）所示，其中 *uboot* 表示当前待度量的 u-boot.bin 文件。标准度量值 $ePCR1'$ 预先存储于可信模块，通过 SM3 算法对安全的 u-boot.bin 文件进行散列并通过 SMS4 算法加密得到。

$$ePCR1' = SM4(SM3(uboot)) \tag{4}$$

若度量值 $ePCR1'$ 与标准度量值相同，判定 u-boot.bin 文件可信；否则，判定节点不可信。之后，可信模块将度量结果（可信：“Yes”；不可信：“No”）发送至可信 u-boot。若接收结果为“No”，可信 u-boot 停止操作系统启动，并长亮节点 LED 指示灯向客户提示操作系统不可信、启动失败；若接收结果为“Yes”，可信 u-boot 继续度量 uImage 文件。由于 uImage 文件体积较大，若通过 RS232 将整个文件传送至可信模块会损耗较长时间。因此，本文直接在可信 u-boot 本地计算内核散列值，计算方法如式(5)所示。

$$ePCR2' = SM3(u\,\mathrm{Im}age \,||\, SM3(uboot)) \tag{5}$$

可信 u-boot 将内核度量值 $ePCR2'$ 发送至可信模块。可信模块将收到的 $ePCR2'$ 与内部存储的标准内核度量值 $ePCR2'$ 进行比较。如果二者相同，判定协调器节点可信，回发“Yes”；否则，判定协调器已遭受攻击，回发“No”。可信 u-boot 接收可信模块的度量结果，若接收到“Yes”，将控制权转交给内核，开始启动操作系统内核，挂载文件系统，并执行溶液监测应用程序；否则，可信 u-boot 停止启动并进行亮灯警示。

5.2 协调器的可信 u-boot 实现

协调器节点上电后，直接进入 u-boot 的第一阶段，即执行 MLO 文件（x-loader）。随后，节点进入 u-boot 的第二阶段，从 SD 卡的第一个分区（FAT 格式，分区名 boot）中读取并加载 u-boot.bin 文件。为了制作可以被 PandaBoard 识别的 SD 卡，本文对 SD 卡进行分区。

如图 6 所示，本文将 SD 卡分成 2 个分区：“boot”和“rootfs”。“boot”分区体积较小，在系统中挂载为/dev/sdd1，是 FAT 格式的分区。“boot”分区存储 u-boot 第二阶段的可执行文件 uboot.bin 和操作系统内核文件 uImage。“rootfs”分区体积较大，在系统中挂载为/dev/sdd2，是 ext4 格式分区。“rootfs”分区存放文件系统。

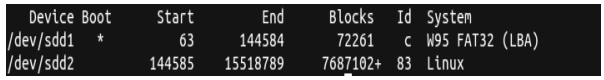


图 6 SD 卡分区结果

本文使用 git clone 命令从 Linaro 网站抓取最新版本 u-boot 源代码以对其进行二次开发。由图 5 可知，可信 u-boot 在源码基础上增加第三阶段，需将待度量的关键文件发送至可信模块。算法 3 给出可信 u-boot 文件读取函数。函数名为 Readfile，函数参数分别为文件名 filename、指定文件系统宏 FS_TYPE 及缓冲区地址 address。若文件读取成功，返回 1；否则，返回 0。首先 Readfile 函数判定需要读取的文件位于 SD 卡哪个分区：FS_TYPE 等于 FS_TYPE_FAT，目标文件位于“boot”分区；FS_TYPE 等于 FS_TYPE_EXT，目标文件位于“rootfs”分区。如目标文件位于“boot”分区，Readfile 函数首先调用 fs_set_blk_dev 函数来对块设备进行设置，其参数“mmc”“0”“FS_TYPE_FAT”分别表示读取目标为 SD 卡设备、boot 分区、FAT 格式。然后 Readfile 函数调用 file_fat_read 函数将指定文件读取至缓冲区。若目标文件位于“rootfs”分区，则 Readfile 函数先调用 fs_set_blk_dev 函数设置块设备，其参数“mmc”“0:2”“FS_TYPE_EXT”分别表示读取目标为 SD 卡设备、boot 分区、ext4 格式。ext4 格式目标文件需先用 ext4fs_open 函数打开文件，再使用 ext4fs_read 函数将文件读取至缓冲区。

算法 3　可信 u-boot 的文件读取

```
1) procedure Readfile(filename, FS_TYPE, address)
2)      if FS_TYPE == FS_TYPE_FAT
3) fs_set_blk_dev("mmc","0",FS_TYPE_FAT);
4)          file_fat_read(filename);
5)          return 1;
6)      else if FS_TYPE == FS_TYPE_EXT
7)fs_set_blk_dev("mmc","0)2",FS_TYPE_EXT);
8)          ext4fs_open(filename);
9)          ext4fs_read(filename);
10)         return 1;
11)     else
12)         return 0;
13)     end
14) end procedure
```

通过算法 3 可信 u-boot 可以将待度量的关键文件读取至缓冲区。缓冲区内关键文件通过 RS232 串口发送至可信模块。由于 RS232 串口的驱动程序没有直接提供文件发送功能，因此本文为 RS232 串口开发合适的文件发送功能函数，如算法 4 所示。首先定义一个串口结构体 test_serial，注册该串口设备并将其初始化。接下来，调用 Readfile 函数从“rootfs”分区中读取 u-boot.bin 文件并存储至缓冲区。随后，将 u-boot.bin 文件的长度和文件名存储到消息发送缓冲区的头部。最后调用 serial_putc 函数，通过串口将整个消息缓冲区中的内容（u-boot.bin 文件的名称、长度和具体内容）发送至可信模块。

算法 4　可信 u-boot 的文件发送

```
1) procedure sendfile(filename, FS_TYPE, address)
2)      structserial_devicetest_serial;
3)      serial_register(&test_serial);
4)      serial_initialize();
5) Readfile(uImage,FS_TYPE_EXT,0x93000000+16);
6)      sprintf(strflen,"%8d",lenread);
7)strcpy(strfname,"uImage");
8)      memcpy(0x93000000,strflen,8);
9)      memcpy(0x93000008,strfname,8);
10)     serial_putc();
11) end procedure
```

可信模块接收 u-boot.bin 文件后，对该文件进行度量，如果度量结果与内部存储的标准度量值相同，返回“Yes”；否则，返回“No”。可信 u-boot 通过调用 serial_getc 函数接收度量结果。如果度量结果为“No”，中断节点启动并进行亮灯示警；如果度量结果为“Yes”，通过式(5)计算 uImage 度量值 $ePCR2'$，并调用 puts 函数将该值发送至可信模块。接下来，可信 u-boot 调用 serial_getc 函数等待并接收可信模块的度量结果。若收到“Yes”，可信 u-boot 把控制权交给嵌入式操作系统，此时协调器为可信的；否则，中断启动并进行亮灯示警。

完成对可信 u-boot 的开发后，需要重新编译 u-boot。本文使用 Linaro 提供的交叉编译工具链 arm-linux-gnueabihf 对 u-boot 进行编译。图 7 所示为终端上的编译过程。u-boot 编译成功后会在根目录下生成 MLO 和 u-boot.bin 文件，本文将生成文件复制到 SD 卡的 boot 分区中。此时协调器节点上电后会按顺序运行第一、第二以及第三阶段的可信 u-boot 程序。

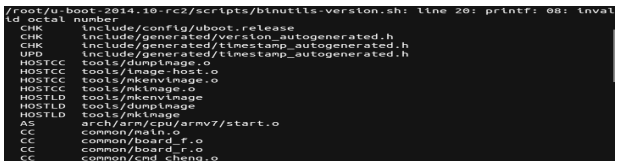


图 7 u-boot 的编译

6 系统测试与分析

本文对可信溶液监测系统进行两项测试以分析其性能：溶液浓度监测；协调器的可信启动。

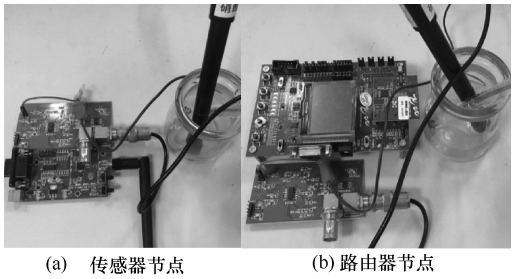
6.1 测试环境

测试环境的具体配置如下。

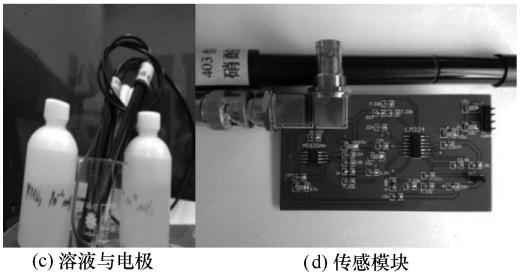
1) 上层监测机：CPU 为 Intel(R) Core i7-3770，内存大小 16 GB, 操作系统为 Windows 7，浏览器版本为 Google Chrome 58.0.3029.110。

本文通过宿主机观察可信模块与协调器节点的通信情况。宿主机环境：CPU 为 Intel(R) Core i7-3770，内存大小 16 GB，操作系统为 Windows 7，虚拟机软件为 VMware® Workstation 12 Pro，版本为 12.5.0，虚拟机操作系统为 Ubuntu 12.04，gcc 版本为 4.6.3，串口交互环境为 minicom。

传感器节点/路由器节点：CC2530-MDK 开发系统，自主开发传感模块。图 8（a）与图 8（b）分别为传感器节点与路由器节点实物图。图 8（c）给出实验中所用 KNO3 溶液、KNO3 电极以及参比电极。图 8（d）为节点传感模块，通过 BNC 接口与电极进行连接。



(a) 传感器节点 (b) 路由器节点



(c) 溶液与电极 (d) 传感模块

图 8 传感器节点与路由器节点实物图

2) 协调器节点：核心板为 Pandaboard-OMAP4460，开发板搭载裁剪后的 GentooLinux 系统，内核版本为 2.6；传感器模块与传感器节点/路由器节点相同；自主开发可信模块。图 9 给出了协调器节点的实物。

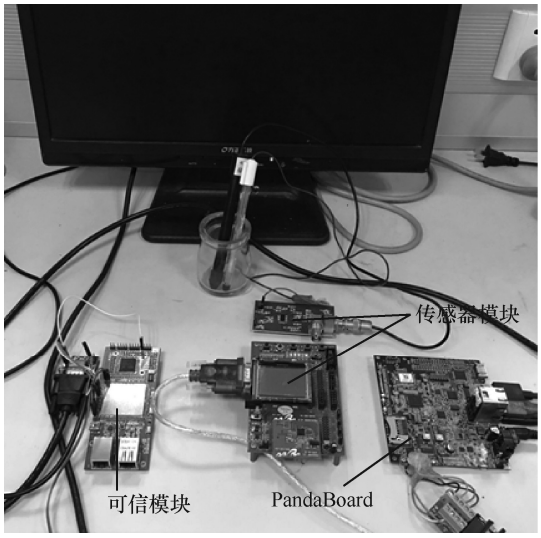


图 9 协调器节点实物

6.2 溶液标定

由于环境突变等因素会导致特定溶液浓度对应的电压值产生变化，因此需要周期性地对溶液进行标定。已知溶液浓度（C）与电压（Vol）之间的关系如式（6）所示。给定两份已知浓度的溶液，测试它们对应的电压值。将两份溶液的浓度以及电压值带入公式，可以得到常数 a 与 b。

$$Vol = aC + b \tag{6}$$

取样 3 份已知浓度的 KNO_3 溶液（10^{-2}mol/L、10^{-3}mol/L 与 10^{-4}mol/L），本文对 10^{-2}mol/L 与 10^{-4}mol/L 溶液进行测量，通过传感器节点测量对应的电压值。表 2 记录了两份溶液浓度与电压值。

表 2 电压与溶液测量值

溶液硝酸根浓度 C/(mol·L^{-1})	电压 Vol/V
10^{-2}	0.4
10^{-4}	2.3

将表 2 的数据代入式(6)得到 a=−191，b=2.31，那么式(6)可以表示为

$$C = \frac{191}{2.31 - V} \tag{7}$$

将式(7)写入程序并进行验证。使用传感器节点

对 10^{-3}mol/L 溶液进行测量，结果为 0.001，与 10^{-3}mol/L 完全吻合，验证测量结果精确性。

6.3　实时监测结果

协调器将实时数据发送至监测机或远程网络，用户可以实时监测温室营养液氮浓度，其界面如图 10 所示。左栏是所有节点网络地址，黑色与线灰色圆圈分别表示对应节点测量值为正常与异常。网页主体部分显示所有节点具体情况，包括节点网络地址、节点所属单位与部门、节点所在实验室、当前时间、节点所测对象、节点是否正常及节点状态。绿色圆圈代表节点状态为正常开启，空心代表节点处于关闭状态。

图 10　可信溶液监测系统界面

若用户需要查看具体节点氮浓度，点击左边节点，右边即出现对应氮浓度变化曲线。图 11 展示了网络地址为 0x214 节点所测量硝酸根离子浓度变化曲线。开始时，溶液浓度保持稳定不变，缓慢添加 KNO_3 后溶液浓度呈缓慢上升趋势，再缓慢添加蒸馏水后溶液中硝酸根离子浓度呈缓慢下降趋势。接着迅速添加蒸馏水后溶液浓度曲线呈剧烈下降趋势。最后，向溶液中迅速添加 KNO_3，溶液浓度曲线呈剧烈上升趋势。

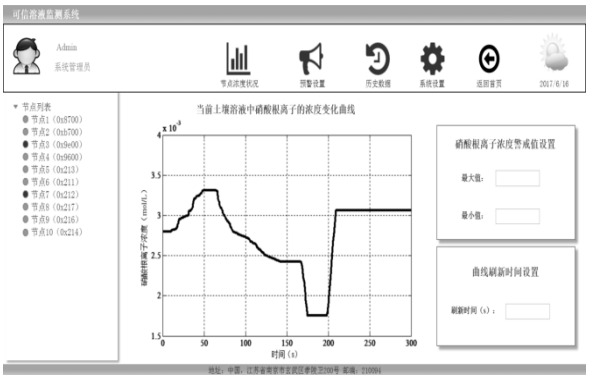


图 11　具体节点溶液中硝酸根离子浓度变化曲线

6.4　协调器节点的可信启动测试

协调器节点的可信模块一直处于监听状态，其串口保持打开。协调器节点核心板 PandaBoard 上电后，可信 u-boot 首先向可信模块发送 u-boot.bin 文件数据。当可信模块完成 u-boot.bin 文件的接收工作时，首先给出所解析文件的长度，并给出文件 SM3 散列值，如图 12 所示。

```
33494/33496 receiving data from pandaboard ES......   |*********  99%|
33495/33496 receiving data from pandaboard ES......   |*********  99%|
33496/33496 receiving data from pandaboard ES......   |********** 100%|

文件长度为:33496

SM3:
   5398b9b8 ea2ac15 a6d23f6e 53407244 fccd87c1 e45a1149 852911c bc7764a2
```

图 12　可信模块对 u-boot.bin 文件进行 SM3 散列

接下来，可信模块对 SM3 散列值进行 SMS4 加密，本文设置 SMS4 加密轮数为 100。图 13 给出了 SMS4 对散列值的加密结果以及 SM3 散列与 SMS4 加密总共需要消耗的时间（约 30 ms）。信息提示表明此时 u-boot.bin 文件未经过攻击篡改，协调器节点的启动到 u-boot 阶段是安全的。

```
executing SMS4 for 98 times......
executing SMS4 for 99 times......
SMS4:
  b45304a d0671603 34a38c50 2ca413e0 c881b191 7534dd0d 97b8c97d 8e27f9db
Used time is : 0.030794
SMS4 value is match with ePCR1
u-boot.bin is safe!
```

图 13　可信模块对散列值进行 SMS4 加密

随后协调器节点的可信模块将经过 SMS4 加密的 *ePCR*1′发送至协调器核心板 PandaBoard。可信 u-boot 收到度量值后，计算操作系统内核文件 uImage 的度量值 *ePCR*2′，并将结果发送回可信模块进行校验。可信模块将接收的 *ePCR*2′与内部存储的标准度量值 *ePCR*2 进行匹配。若两者相互匹配，可信模块发送“Yes”至可信 u-boot。从图 14 可以看出，此时内核文件是安全的，协调器节点可以正常启动。

```
received char is: 54
6
received char is: 52
4
received char is: 100
d
2b441479f3b8cebdf38097fcca9b964d

ready to print result...
 2b441479 f3b8cebd f38097fc ca9b964d
Hash value is match with ePCR2
Kernel image is safe!
Send Yes to Pandaboard ES
```

图 14　操作系统内核通过完整性度量

可信 u-boot 收到可信模块的判定结果后，选择是否正常启动系统。由于此时可信 u-boot 收到的结果为“Yes”，正常启动协调器节点，并进入操作系

统，如图 15 所示。

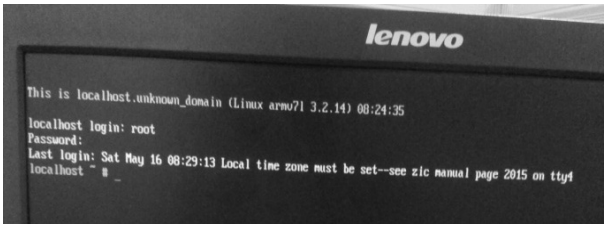


图 15 协调器节点正常启动进入操作系统

6.5 协调器节点抗攻击能力测试

实验模拟节点捕获攻击，对协调器节点的 u-boot.bin 文件进行篡改以测试所设计系统协调器节点的抗攻击能力。图 16 给出了可信模块对 u-boot.bin 文件的完整性度量结果。由图 16 可知，此时的度量值与标准的度量值 *ePCR2′*不匹配，可信模块判定协调器节点不安全，并向可信 u-boot 发送“No”，从而停止对协调器节点的启动。

```
executing SM4 for 95 times......
executing SM4 for 96 times......
executing SM4 for 97 times......
executing SM4 for 98 times......
executing SM4 for 99 times......
SM4:
 dfde35ed dd4aa1e6 9803b8fb f6aaf456 f11545e7 6edd9872 4f7c765c 7e79c5b1
Used time is : 0.056905
SM4 value is not match with ePCR1
u-boot.bin is not safe! abort booting
```

图 16 篡改 u-boot.bin 文件的实验结果

同样地，对操作系统内核文件 uImage 进行篡改以进行抗攻击测试。可信模块对 u-boot.bin 进行验证并将其度量值发送至可信 u-boot 后，可信 u-boot 计算得到 *ePCR2′*并将该值发送至可信模块。图 17 给了出对被攻击后的 uImage 文件的度量结果。由图 17 可知，可信模块判定协调器节点不安全，并向可信 u-boot 回复“No”指令。

```
7
received char is: 56
8
received char is: 53
5
received char is: 49
1
received char is: 50
2
ff5c26ed201f507a6db361e059678512

ready to print result...
 ff5c26ed 201f507a 6db361e0 59678512
Hash value is not match with ePCR2
Kernel image is not safe!
Send No to Pandaboard ES
```

图 17 操作系统内核未通过完整性度量

如图 18 所示，可信 u-boot 在收到“No”指令，判定 u-boot.bin 文件或 uImage 文件已遭受篡改，停止启动协调器节点，屏幕处于黑屏状态，通过长亮 LED 灯向用户示警。

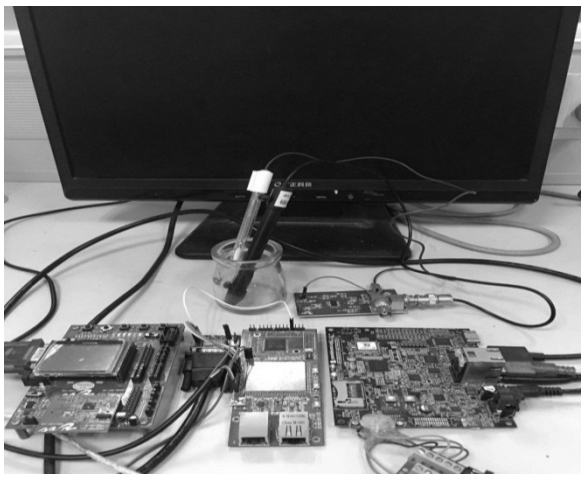


图 18 攻击协调器节点的实验结果

7 结束语

本文设计并实现了基于 ZigBee 的无线传感器网络可信溶液监测系统。系统内节点可以检测溶液中氮元素的浓度，并通过无线方式发送至上层节点。上位机与远程客户端可以对系统内所有节点所测的溶液进行监测与控制。设计的可信 u-boot 对协调器节点进行完整性检查，实现系统的可信增强，从而解决系统内的核心协调器节点容易遭受捕获攻击的问题。

参考文献：

[1] ATZORI L, IERA A, MORABITO G. The internet of things: a survey[J]. Computer Networks, 2010, 54(15): 2787-2805.

[2] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, et al. Wireless sensor networks: a survey[J]. Computer Networks, 2002, 38(4): 393-422.

[3] 胡瑾, 樊宏攀, 张海辉, 等. 基于无线传感器网络的温室光环境调控系统设计[J]. 农业工程学报, 2014, 30(4): 160-167.
HU J, FAN H P, ZHANG H, et al. Design of regulation system of light environment in greenhouse based on wireless sensor network[J]. Transactions of the Chinese Society of Agricultural Engineering, 2014, 30(4): 106-167.

[4] 蒋毅琼, 张漫, 李婷, 等. 基于 WSN 的日光温室 CO_2 浓度监控系统[J]. 中国农业大学学报, 2014, 19(4): 166-171.
JIANG Y Q, ZHANG M, LI T, et al. Development of a CO_2 concentration monitoring and controlling system in solar greenhouse based on WSN[J]. Journal of China Agricultural University, 2014, 19(4): 166-171.

[5] DAN L, XIN C, HUANG C, et al. Intelligent agriculture greenhouse environment monitoring system based on IOT technology[C]//International Conference on Intelligent Transportation, Big Data and Smart City. 2016: 487-490.

[6] TABATABAEIFAR A, SHAFIEIAN M A, BANIZAMAN H, et al. Design and implementation of a Web-based greenhouse remote moni-

toring system with Zigbee protocol and GSM network[J]. Journal of Intelligent Procedures in Electrical Technology, 2014, 5(19).

[7] WU R, XU Y, LI L, et al. Design and implementation of an intelligent monitoring system based on ZigBee for the agricultural greenhouse[M]. Springer Berlin Heidelberg, 2014: 195-203.

[8] HE G, WANG X, SUN G. Design of a greenhouse humiture monitoring system based on ZigBee wireless sensor networks[C]. Fifth International Conference on Frontier of Computer Science and Technology, 2010: 361-365.

[9] AZAZA M, TANOUGAST C, FABRIZIO E, et al. Smart greenhouse fuzzy logic based control system enhanced with wireless data monitoring[J]. Isa Transactions, 2016, (61): 297-307.

[10] AHAMED V S J, FAYAZ S. Smart wireless sensor network for automated greenhouse[J]. IETE Journal of Research, 2015, 61(2): 180-185.

[11] 于明月, 王立地, 栗庆吉, 等. 基于 ZigBee 的日光温室智能调控系统的研究与设计[J]. 浙江农业学报, 2017, 29(6): 1026-1036.
YU M Y, WANG L D, LI Q J, et al. Research and design of intelligent control system for solar greenhouse based on ZigBee[J]. Acta Agriculturae Zhejiangensis, 2017, 29(6): 1026-1036.

[12] 魏旭东, 史颖刚, 刘利付, 等. 基于 ZigBee 的温室环境检测系统设计[J]. 内蒙古农业大学学报(自然科学版), 2016, (4): 90-99.
WEI X D, SHI Y G, LIU L F, et al. Design of greenhouse environment detecting system based on ZigBee[J]. Journal of Inner Mongolia Agricultural University (Natural Science Edition), 2016, 37(4): 90-99.

[13] 毛鹏军, 姜水, 王俊, 等. 基于 ZigBee 技术的温室环境无线监测系统设计[J]. 中国农机化学报, 2015, 36(1): 102-106.
MAO P J, JIANG S, WANG J, et al. Design of wireless monitoring system for greenhouse environment based on ZigBee[J].Journal of Chinese Agricultural Mechanization, 2015, 36(1): 102-106.

[14] 郭文川, 程寒杰, 李瑞明, 等. 基于无线传感器网络的温室环境信息监测系统[J]. 农业机械学报, 2010, 41(7): 181-185.
GUO W C, CHEN H J, LI R M, et al. Greenhouse monitoring system based on wireless sensor networks[J]. Transactions of the Chinese Society for Agricultural Machinery, 2010, 41(7): 181-185.

[15] WANG Y, ATTEBURY G, RAMAMURTHY B. A survey of security issues in wireless sensor networks[J]. IEEE Communications Surveys & Tutorials, 2006, 8(2): 2-23.

[16] HE D, ZEADALLY S, WU L. Certificateless public auditing scheme for cloud-assisted wireless body area networks[J]. IEEE Systems Journal, 2015: 1-10.

[17] SHEN J, TAN H, MOH S, et al. Enhanced secure sensor association and key management in wireless body area networks[J]. Communications & Networks Journal of, 2015, 17(5): 453-462.

[18] LI J, LI Y, REN J, et al. Hop-by-hop message authentication and source privacy in wireless sensor networks[J]. IEEE Transactions on Parallel & Distributed Systems, 2014, 25(5): 1223-1232.

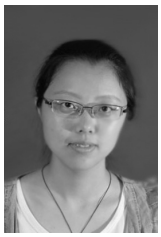
[19] CHANG C C, LE H D. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2016, 15(1): 357-366.

[20] WINTER J, DIETRICH K. A hijacker's guide to communication interfaces of the trusted platform module [J]. Computers & Mathematics with Applications, 2013, 65(5): 748-761.

[21] TPM Trusted Platform Module[M]. Springer US, 2011: 1310.

[22] WANG T, ZHANG G, YANG X, et al. A trusted and energy efficient approach for cluster-based wireless sensor networks[J]. International Journal of Distributed Sensor Networks, 2016: 1-13.

作者简介：



王天舒（1989-），女，江苏如东人，南京理工大学博士生，主要研究方向为无线传感网的分簇路由协议、可信计算。

张功萱（1961-），男，江西景德镇人，南京理工大学教授、博士生导师，主要研究方向为云计算、无线传感网、可信计算。

杨曦晨（1989-），男，江苏高邮人，南京理工大学博士生，主要研究方向为图像质量评价、无线传感网。