文章编号:1000－2367(2019)01－0033－07 DOI:10.16366/j.cnki.1000－2367.2019.01.005

基于安全协议的智能灌溉系统设计

左黎明[a,b],周庆[a,b],陈兰兰[a,b],夏萍萍[a,b]

(华东交通大学 a.理学院;b.系统工程与密码学研究所,南昌 330013)

摘 要:针对现有智能灌溉系统中数据交互的安全问题,设计了一种基于安全协议的智能灌溉系统.智能灌溉系统以此安全协议为核心,并设计身份认证模块、签名模块、签名验证模块,实现了安全协议.最后对智能灌溉系统进行实验与仿真,实验结果表明基于安全协议的智能灌溉系统运行效率高,在智能灌溉装置计算能力和传输能力较弱的情况下具有良好的适用性和安全性.

关键词:精准灌溉;智能家居;SM2;大数据;安全协议

中图分类号:S275 **文献标志码**:A

随着物联网的快速发展,智能灌溉逐渐运用到农业灌溉与日常灌溉中,但其中所使用的智能控制系统存在诸多安全漏洞.在 2017 年 3 月 15 日的 315 晚会上现场演示对洗衣机、烤箱等智能家电入侵并控制其运行,智能控制系统少有考虑网络的安全.2017 年 10 月 17 日由新加坡媒体报道称 WiFi 网络协议存在安全漏洞,新加坡共有 1 100 万个使用 WiFi 连接的网点,包括住宅、公司、公共场所等均存在被黑客入侵的安全隐患,现有智能设备大多存在此类安全隐患,智能灌溉系统同样在入侵范围之内.

现有的智能灌溉系统大部分都使用无线网络进行数据传输,并且大多未考虑系统的安全性,很多国内外学者在智能灌溉方面发表了相关研究成果.2010 年高玉芹[1]提出基于 ZigBee 和模糊控制决策的自动灌溉系统设计,实现了基于 ZigBee 网络的精准灌溉,同年黎啟江等[2]提出了远程无线传感器技术在智能灌溉监控中的应用.2011 年戴菲菲等[3]提出基于 ZigBee 网络和 D-S 数据融合的灌溉系统设计,实现了灌溉自动化与精准灌溉,同年周振峰等[4]提出基于 WSN 与嵌入式组态软件的智能灌溉系统,使用 WSN 技术与嵌入式组态软件实现智能灌溉.2012 年杜云明等[5]提出基于单片机的温室灌溉控制系统设计,将单片机运用到灌溉系统实现自动灌溉,同年 Yu 等[6]提出用于喷灌和滴灌系统设计与优化的决策支持系统,使用决策支持系统实现精准灌溉.2013 年纪文义等[7]提出基于无线网络的农田灌溉智能监测系统,使用无线网络实现灌溉的自动化与智能监测,同年 Mohan[8]提出用于鲁棒性能的水平流域灌溉系统的设计,该设计采用数学仿真模型提高灌溉精度.2014 年王永涛等[9]提出基于无线数据传输的智能化节水灌溉控制系统研究方案,采用无线网络传输数据实现智能灌溉,同年邓晓栋等[10]提出基于 Android 平台的智能水肥灌溉系统设计,使用 Android 平台实现灌溉自动化,之后 Davis 等[11]提出智能灌溉控制器的成功实现方法,使用全新的灌溉方法实现智能灌溉,其他学者于 2014 年也发表了相关研究成果[12－14].2015 年贾艳玲等[15]提出了基于 ZigBee 技术的葡萄园智能灌溉系统设计,使用 ZigBee 技术实现葡萄园的智能灌溉,同年 Remini 等[16]提出干旱区的传统灌溉系统.2016 年 Eldeiry 等[17]提出遥感在灌溉和喷灌系统灌溉作物蒸散量估算中的应用,使用遥感技术实现智能灌溉.2017 年 Meysam[18]提出伊朗东北部中心枢纽喷灌系统的田间评价,通过系统评估对系统进行调整从而提高灌溉的精确性.2018 年索滢等[19]提出典型节水灌溉技术综合性能评价研究,采用文献调研与知识管理重构的方法提出了节水灌溉技术综合性能相关评价指标.同年陈际旭等[20]进行基于萤火虫算法的滴灌管网优化设计研究,利用萤火虫算法进行求解来优化不同管网布置形式下的各级管道的管径及投资,从而达到优化滴灌管网的目的.以上系统在数据交互的过程中大多涉及无线网络的使用,大多有被入侵的可能性,存在一定的安全隐患.针对这些问题,设计了一种基于安全协议的智能灌溉系统,基于 SM2 签名算法[21]的安全协议有效保护了智能灌溉系统中交互数据的完整性,解决了数据交互的安全问题.

收稿日期:2018-03-01;**修回日期**:2018-11-19.

基金项目:国家自然科学基金(11361024);江西省自然科学基金(20171BAB201009);江西省教育厅科技项目(GJJ161417);江西省研究生创新专项资金项目(YC2017-S257).

作者简介(通信作者):左黎明(1981－),男,江西鹰潭人,华东交通大学副教授,研究方向为信息安全、非线性系统,E-mail:limingzuo@126.com.

1 系统整体架构

智能灌溉系统由智能灌溉装置端、控制终端、App 客户端组成.智能灌溉装置端集成了树莓派(Raspberry Pi)与 DS18B20 温度传感器、AM2301 湿度传感器、TRSJ 型土壤 pH 传感器、U 盾,以及其他电子硬件.树莓派集成了调用 WiFi 网络模块、签名验证模块、信息处理模块的处理程序,传感器等电子硬件通过 GPIO 扩展板连接树莓派.控制终端集成了调用身份认证模块和植被数据预测模块的处理程序,并且控制终端嵌入 U 盾.App 客户端集成了信息处理模块与签名模块的处理程序,并且 App 客户端嵌入 TF 卡(含有 SM2 加密芯片的卡式 USBKEY).

智能灌溉系统的运行原理如下:智能灌溉装置端通过传感器收集数据,并由树莓派将数据发送给控制终端,通过 WiFi 网络模块进行数据传输.控制终端通过植被数据预测模块对数据进行处理,并将接收的数据发送给 App 客户端显示,同时预测下一阶段的数据.控制终端生成相关指令,由身份认证模块对指令进行编码.身份认证模块读取 U 盾中的私钥,通过 SM2 签名算法对指令进行签名,并将签名信息与指令组成数据包,将数据包发送给智能灌溉装置端.树莓派接收数据包,由签名验证模块读取 U 盾的私钥对数据包中的签名信息进行验证,验证通过后执行相关操作.

操作者可以通过 App 客户端显示的数据进行人为判断,发出指令.App 客户端中的签名模块对指令签名后进行编码,并读取 TF 卡中的私钥,通过 SM2 签名算法对指令进行签名.签名后通过信息处理模块将签名信息组成封包发送给控制终端,控制终端的身份认证模块对签名信息进行验证.验证成功后由身份认证模块再对指令进行签名,并将签名信息发送给智能灌溉装置端.智能灌溉装置端的签名验证模块对签名进行验证,验证成功后通过信息处理模块进行相关操作.系统整体架构如图 1 所示.

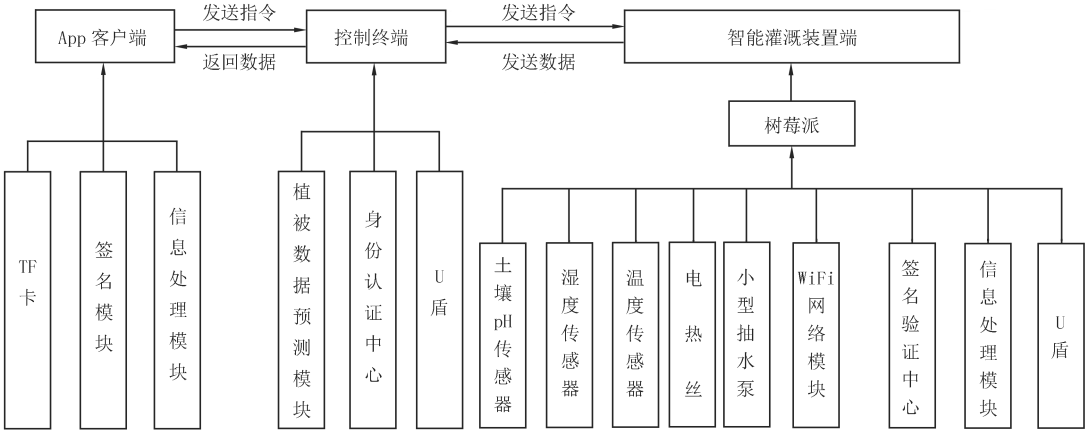

图 1 系统整体架构图

Fig.1 Overall architecture diagram of the system

2 SM2 签名算法

2.1 系统参数创建

系统参数是有限域 F_q 上的椭圆曲线,有限域的规模为 q,定义椭圆曲线方程 $E(F_q)$ 的两个元素 a、b,其中 $a,b \in F_q$;$E(F_q)$ 上的基点 $G=(x_G,y_G)(G \neq 0)$,其中 x_G 和 y_G 是 F_q 中的两个元素,G 的阶为 n.

2.2 建立密钥对

用户 A 由密钥生成算法[21] 生成密钥对(d_A,P_A),密钥对满足:$P_A=d_AG=(x_A,y_A)$.其中 d_A 作为用户私钥,P_A 作为用户公钥对外公开.

2.3 其他参数的建立

用户 A 具有长度为 len 比特的可辨识标识 ID_A,令 L_A 作为整数 len 转化而来的字符串.其签名者或验证者都需要使用密码杂凑算法[21] 计算得到自身需要的杂凑值 $Z_A=H_{256}(L_A \| ID_A \| a \| b \| x_A \| y_A)$,其中 $H_{256}()$ 为将给定信息生成长度为 256 位字符串的哈希函数.

2.4 签名生成

待签名消息为 m,为了获取消息 m 的签名 $\mathrm{sign}(m)=(r,s)$,具体实现如下:

步骤 1　设置 $\overline{m} = Z_C \parallel m$;

步骤 2　计算 $e = H_{256}(\overline{m})$;

步骤 3　随机选取 $k \in [1, n-1]$;

步骤 4　计算椭圆曲线上的点 $(x_C, y_C) = kG$;

步骤 5　计算 $r = (e + x_C) \bmod n$,若 $r = 0$ 或 $r + k = n$,则返回步骤 3;

步骤 6　计算 $s, s = ((1 + d_C)^{-1} \cdot (k - r \cdot d_C)) \bmod n$,若 $s = 0$,则返回步骤 3,得到消息 m 的签名为(r, s).

2.5　签名验证

对于签名信息 $\text{sign}(m) = (r', s')$ 进行签名验证,具体验证过程如下:

步骤 1　判断 $r' \in [1, n-1]$ 是否成立,若不成立,则签名验证失败,返回的验证结果为 false;

步骤 2　判断 $s' \in [1, n-1]$ 是否成立,若不成立,则签名验证失败,返回的验证结果为 false;

步骤 3　计算 $\overline{m}' = Z_C \parallel m'$;

步骤 4　计算 $e' = H_{256}(\overline{m}')$;

步骤 5　计算 $t = (r' + s') \bmod n$,如果 $t = 0$,则签名验证失败,返回的验证结果为 false;

步骤 6　计算椭圆曲线上的点 $(x'_C, y'_C) = s'G + tP_C$;

步骤 7　计算 $R = (e' + x'_C) \bmod n$,检验 $R = r'$ 是否成立,若成立则签名验证成功,返回的验证结果为 true,否则签名验证失败,返回的验证结果为 false.

3　智能灌溉系统设计

3.1　控制终端设计

控制终端集成了调用植被数据预测模块和身份认证模块的处理程序,并嵌入 U 盾,U 盾存储由基于椭圆曲线的密钥生成算法生成的密钥对.控制终端的具体设计如下.

(1)植被数据预测模块.植被数据预测模块部署在控制终端,其核心算法为时间序列模型中的三次指数平滑法,其作用为实现自动控制.已知在一天中土壤的温度、湿度、pH 值是呈二次曲线变化的,因此选择时间序列模型中的三次指数平滑法作为植被数据预测模块的核心算法.在此算法中设置每小时获取一次土壤的各项数据.三次指数平滑法的原理如下:设每小时获取的土壤湿度的值构成的时间序列为:$y_1, y_2, \cdots, y_t, \cdots, \alpha$ 为加权系数,并且 $0 < \alpha < 1$. 三次指数平滑法的计算公式为:

$$\begin{cases} S_t^{(1)} = \alpha y_t + (1-\alpha) S_{t-1}^{(1)}, \\ S_t^{(2)} = \alpha S_t^{(1)} + (1-\alpha) S_{t-1}^{(2)}, \\ S_t^{(3)} = \alpha S_t^{(2)} + (1-\alpha) S_{t-1}^{(3)}, \end{cases}$$

其中 $S_t^{(1)}$ 为一次指数平滑值,其中 $S_t^{(1)} = \alpha y_t + (1-\alpha) S_{t-1}^{(1)} = S_{T-1}^{(1)} + \alpha(y_t - S_{t-1}^{(1)})$.

同理 $S_t^{(2)}$ 为二次指数平滑值,$S_t^{(3)}$ 为三次指数平滑值,三次指数平滑法的预测模型为:

$$y'_{t+m} = a_t + b_t m + C_t m^2, m = 1, 2, \cdots,$$

$$\begin{cases} a_t = 3S_t^{(1)} - 3S_t^{(2)} + S_t^{(3)}, \\ b_t = \dfrac{\alpha}{2(1-\alpha)}[(6-5\alpha)]S_t^{(1)} - 2(5-4\alpha)S_t^{(2)} + (4-3\alpha)S_t^{(3)}, \\ c_t = \dfrac{\alpha^2}{2(1-\alpha)^2}[S_t^{(1)} - 2S_t^{(2)} + S_t^{(3)}], \end{cases}$$

其中 y'_{t+m} 为预测的下一时刻的土壤湿度,土壤 pH 值、温度的预测原理相同.

(2)身份认证模块设计.身份认证模块是有如下两个作用:1)对 App 客户端发送的签名通过 SM2 签名算法进行签名验证,并返回验证结果;2)对控制终端发出的指令通过 SM2 签名算法进行签名,并将生成的签名信息发送给信息处理模块,信息处理模块构造数据包发送给智能灌溉装置端.

3.2　App 客户端交互安全设计

App 客户端以信息处理模块、签名模块、TF 卡为核心,TF 卡具备读写能力,存储了基于椭圆曲线的密钥生成算法生成的密钥对.(1)签名模块.签名模块对 App 客户端生成的指令 m 进行签名,生成签名信息 $\text{sign}(m) = (r, s)$. 最后将生成的签名信息发送给信息处理模块.(2)信息处理模块.信息处理模块作用是将签名模块生成的签名信息构造成数据包发送给控制终端.

3.3　智能灌溉装置端设计

(1)硬件设计.智能灌溉装置端以树莓派、DS18B20 温度传感器、AM2301 湿度传感器、TRSJ 型土壤 pH 传感器、电热丝、灌溉机构为核心,电子硬件与灌溉机构通过 GPIO 扩展板连接树莓派.电热丝调节土壤温度,灌溉机构以灌溉喷头、抽水泵为核心.树莓派嵌入 U 盾,存储了基于椭圆曲线的密钥生成算法生成的密钥对.智能灌溉装置端如图 2 所示.

(2)签名验证模块.签名验证模块对控制终端发送的签名信息进行验证,并将签名验证结果 true/false 与指令发送给信息处理模块.

(3)信息处理模块.信息处理模块的作用是对签名验证模块发送的签名验证结果进行判断.如果签名验证结果为 true,根据指令执行浇水、施肥、升温、调节土壤 pH 的操作,否则不执行任何操作.

(4)WiFi 网络模块.WiFi 网络模块的作用是将树莓派连接到控制终端网络.

4 系统身份认证设计

4.1 认证参数设计

系统中指令统称为 (N,Z_L),Z_L 内容为如下参数中的任意一个:S_W,J_S,S_F 参数列表如表 1 所示.

4.2 智能灌溉装置端认证控制终端身份设计

智能灌溉装置端认证控制终端身份实现步骤如下.

(1)智能灌溉装置端收集数据并发送给控制终端.控制终端获取植被数据预测模块预测的数据与数据库中存储的植被基本信息数据,并将这两项数据进行对比,从而生成指令 (N,Z_L).身份认证模块读取控制终端嵌入的 U 盾中私钥,对指令进行签名.最后身份认证模块将签名信息编码成数据包 ADATA 发送给智能灌溉装置端.

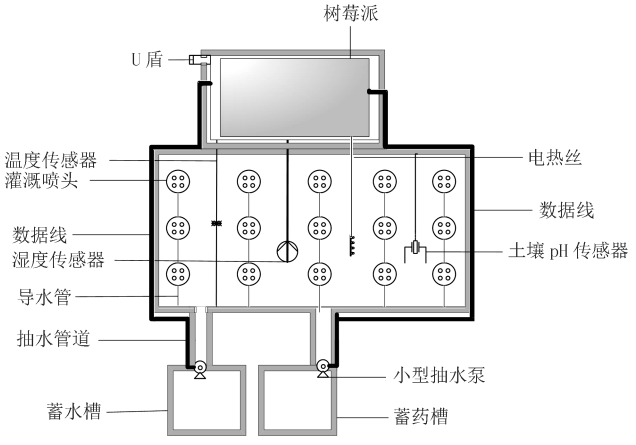

图 2 智能灌溉装置端示意图

Fig. 2 Schematic diagram of intelligent irrigation device

(2)智能灌溉装置端的签名验证模块读取 U 盾的公钥,并对数据包 ADATA 中的签名信息 sign(N,Z_L)进行签名验证,返回的验证结果为 true/false.智能灌溉装置端的信息处理模块对验证结果进行判断.若验证结果为 true,则根据指令执行相关操作,否则不进行任何操作,流程如图 3 所示.

表 1 参数列表

Tab. 1 Parameter list

参数名	含义
(N,S_W)	参数编码为 1111,S_W 含义为升温,N 为升温执行时间,树莓派的信息处理模块启动电热丝对土壤升温,升温时间 N.
(N,J_S)	参数编码为 1112,J_S 含义为浇水,N 为浇水执行时间,树莓派的信息处理模块启动小型抽水泵对植被进行灌溉,灌溉时间为 N.
(N,S_F)	参数编码为 1113,S_F 含义为施肥,N 为施肥执行时间,树莓派的信息处理模块启动小型抽水泵对土壤施肥,施肥时间为 N.
ADATA	参数内容为 2#111#1#signlen#$(N,Z_L,\text{sign}(N,Z_L))$,2 表示签名协议,111 表示签名类型,1 表示协议交互第一步,signlen 为最后一个“#”后的字符串长度,(N,Z_L)表示 App 客户端指令,(N,Z_L)表示指令签名信息.
FDATA	参数内容为 2#210#1#signlen#$(N,Z_L,\text{sign}(N,Z_L))$,第 1 个 2 表示签名协议,210 表示签名类型,第 2 个 2 表示交互第 2 步,(N,Z_L)表示控制终端指令,(N,Z_L)表示指令签名信息.

4.3 智能灌溉装置端认证 App 客户端身份设计

智能灌溉装置端认证 App 客户端身份实现步骤如下.

(1)操作者操作 App 客户端发出指令(N,Z_L).App 客户端的签名模块读取 TF 卡的私钥对指令进行签名,得到签名信息 sign(N,Z_L).由 App 客户端的信息处理模块将签名信息编码成数据包 ADATA 并发送给控制终端.

(2)控制终端的身份认证模块读取 U 盾中的公钥,并对 ADATA 中的签名 sign(N,Z_L)进行签名验证.若签名验证结果为

true,则身份认证模块读取 U 盾私钥,对 ADATA 中指令(N,Z_L)进行签名,得到签名 sign(N,Z_L).控制终端的信息处理模块将签名信息编码成数据包 FDATA 并发送给智能灌溉装置端.

(3)智能灌溉装置端的签名验证模块读取 U 盾的公钥,并对数据包 FDATA 中的签名 sign(N,Z_L)进行验证.若验证结果为 true,则进行相关操作,否则不进行任何操作.流程如图 4 所示.

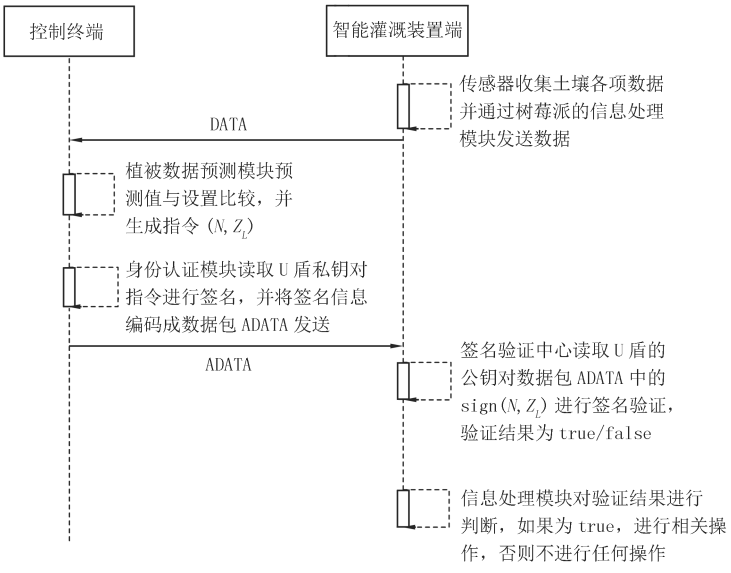

图 3　智能灌溉装置端认证控制终端身份流程图

Fig.3　Flow chart of intelligent irrigation device authenticating control terminal identity

5　实验与仿真

5.1　智能灌溉装置端认证控制终端身份的实验与仿真

实验与仿真结果如图 5 所示.控制终端的植被数据预测模块生成指令(N,Z_L),由身份认证模块对指令进行签名,签名核心代码如下.

```
sm2usbkey.TanSM2Sign(msgtxt, (uint)msgtxt.Length, signtext, out signlen);
string strsign = sm2usbkey.byteToHexStr(signtext);
string sendmessage = message + "," + ordercode + "," + strsign;
result = "2#210#2#" + sendmessage.Length + "#" + sendmessage;//生成数据包 FDATA
return result;
```

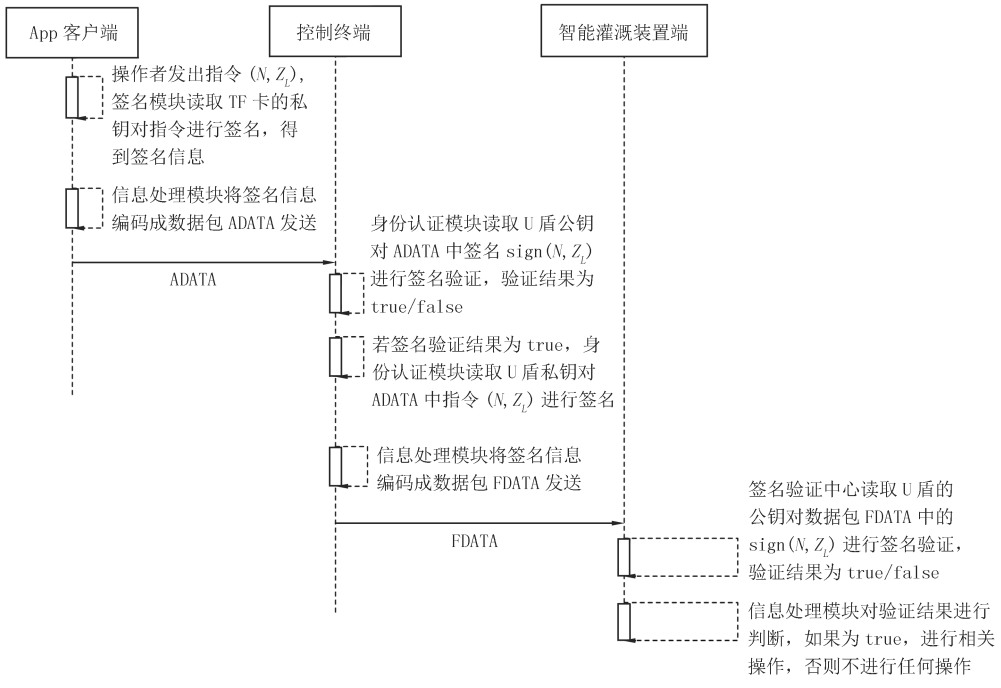

图 4　智能灌溉装置端认证 App 客户端身份流程图

Fig.4　Flow chart of intelligent irrigation device authenticating App client identity

身份认证模块将签名信息与指令生成数据包 FDATA 发送给智能灌溉装置端.智能灌溉装置端的签名验证模块对数据包中签名进行验证,签名验证核心代码如下.如果验证通过,则智能灌溉装置端进行升温、浇水、施肥等操作.

```
int signverifyflag = sm2usbkey.TanSM2Verify(ordercode, (uint)ordercode.
Length, bpkey,(uint)bpkey.Length, signmessage, (uint)signmessage.Length);
string flag = "false";
if (signverifyflag == 0)
flag = "true";
```

5.2 智能灌溉装置端认证 App 客户端身份的实现与仿真

实验与仿真结果如图 6 所示.操作者操作 App 客户端生成指令(N,Z_L),由 App 客户端的签名模块对指令进行签名,并编码成数据包 ADATA,签名核心代码如下.

```
sm2usbkey.TanSM2Sign(msgtxt, (uint)msgtxt.Length, signtext, out signlen);
string strsign = sm2usbkey.byteToHexStr(signtext);
string sendmessage = message + "," + ordercode+"," + strsign;
result = "2#111#1#" + sendmessage.Length + "#" + sendmessage;//生成数据包 ADATA
return result;
```

信息处理模块将数据包发送给控制终端,然后控制终端的身份认证模块对数据包中签名进行签名验证,签名验证代码如下.

```
//控制终端对从 App 客户端发送的签名信息进行签名验证
int signverifyflag = sm2usbkey.TanSM2Verify(ordercode,(uint)ordercode.
Length,bpkey,(uint)bpkey.Length,signmessage,(uint)signmessage.Length);
string flag="false";
if(signverifyflag==0)
flag="true";
```

如果验证通过,则由身份认证模块对指令(N,Z_L)签名,将签名信息与指令生成数据包 FDATA 发送给智能灌溉装置端.智能灌溉装置端的签名验证模块对数据包中签名进行验证.如果验证通过,由智能灌溉装置端进行升温、浇水、施肥等操作.

图 5 智能灌溉装置认证控制终端身份实验仿真结果

Fig.5 Simulation results of experiment on intelligent irrigation device authenticating control terminal identity

图 6 控制终端认证 App 客户端身份实验仿真结果

Fig.6 Simulation results of experiment on control terminal authenticating App client identity

6 总　结

本文设计了一种基于安全协议的智能灌溉系统，实现了智能精准灌溉，有效解决了基于安全协议的智能灌溉系统中数据交互的安全问题.本文详细叙述了 SM2 签名算法，说明了 SM2 签名算法在安全协议中如何进行运用，并对安全协议的交互过程进行了分析.本文对智能灌溉系统的运行原理进行了实验与仿真，从而论证了智能灌溉系统的可靠性与实用性.在今后，智能灌溉在农业灌溉与日常灌溉中的运用将日益广泛，对于智能灌溉系统中交互数据的安全性将会有更高的要求，基于安全协议的智能灌溉系统的研究将会继续进行.

参　考　文　献

[1] 高玉芹.基于 ZigBee 和模糊控制决策的自动灌溉系统的设计[J].节水灌溉，2010(8)：52-55.

[2] 黎啟江，王祥宁，张倩.远程无线传感器技术在智能灌溉监控中的应用[J].农机化研究，2010，32(3)：182-188.

[3] 戴菲菲，彭力.基于 ZigBee 网络和 D-S 数据融合的灌溉系统设计[J].计算机研究与发展，2011，48(S2)：350-354.

[4] 周振峰，张伟.基于 WSN 与嵌入式组态软件的智能灌溉系统[J].浙江农业科学，2011(2)：438-441.

[5] 杜云明，盖丽娜，颜兵兵.基于单片机的温室灌溉控制系统设计[J].农机化研究，2012，34(12)：88-91.

[6] Yu J M，Barradas M，Matula S，et al.A Decision Support System-FertIgat-Ion Simulator(DSS-FS) for designand optimization of sprinkler and dripirrigation systems[J].Computers and Electronics in Agriculture，2012，86：111-119.

[7] 纪文义，张继成，郑萍，等.基于无线网络的农田灌溉智能监测系统[J].农机化研究，2013，35(10)：171-173.

[8] Mohan J R.Design of Level Basin Irrigation Systems for Robust Performance[J].Journal of Irrigationand Drainage Engineering，2013，139(3)：254-260.

[9] 王永涛，陈思璇，李家春，等.基于无线数据传输的智能化节水灌溉控制系统研究[J].节水灌溉，2014(10)：92-96.

[10] 邓晓栋，翁绍捷.基于 Android 平台的智能水肥灌溉系统设计[J].广东农业科学，2014，41(9)：203-206.

[11] Davis S L，Dukes M D.Methodologies for Successful Implementation of Smart Irrigation Controllers[J].Journal of Irrigation and Drainage Engineering，2014，141(3)：1-9.

[12] 谢家兴，王卫星，陆华忠，等.基于 CC2530 的荔枝园智能灌溉系统设计[J].灌溉排水学报，2014，33(Z1)：189-194.

[13] 李合青，来智勇，张鑫.基于 ZigBee 的温室智能灌溉执行子系统的设计与实现[J].农机化研究，2014，36(1)：95-98＋107.

[14] 黄勇，张玉建，钱建峰，等.基于专家系统的南通地区稻田自动灌溉系统应用[J].中国农村水利水电，2014(8)：12-14.

[15] 贾艳玲，刘思远.基于 ZigBee 技术的葡萄园智能灌溉系统设计[J].江苏农业科学，2015，43(6)：383-385.

[16] Remini B，Achour B，Kechad R.The Foggara：A Traditional System of Irrigation In Arid Regions[J].GeoScience Engineering，2015，60(2)：30-37.

[17] Eldeiry A A，Waskom R M，Elhaddad A.Using Remote Sensing to Estimate E7apotranspiration of Irrigated Crops Under Flood and Sprinkler Irrigation Systems[J].Irrigation and Drainage，2016，65(1)：85-97.

[18] Meysam A.Field evaluation of centre pivot sprinkler irrigation system in the North-East of Iran[J].Journal of Water and Land Development，2017，34(1)：1-9.

[19] 索滢，王忠静.典型节水灌溉技术综合性能评价研究[J].灌溉排水学报，2018，37(11)：113-120.

[20] 陈际旭，徐淑琴，周豪.基于萤火虫算法的滴灌管网优化设计研究[J].灌溉排水学报，2018，37(9)：48-55.

[21] 汪朝晖，张振峰.SM2 椭圆曲线公钥密码算法综述[J].信息安全研究，2016，2(11)：972-982.

Design of intelligent irrigation system based on security protocol

Zuo Liming[a,b]，Zhou Qing[a,b]，Chen Lanlan[a,b]，Xia Pingping[a,b]

(a.School of Science；b.SEC Institute，East China Jiaotong University，Nanchang 330013，China)

Abstract：Aiming at the security problems of data interaction in current intelligent irrigation systems，a security protocol based on intelligent irrigation system is designed. Takeing the security protocol as the core，the intelligent irrigation system constructs a security protocol by designing the identity authentication module，the signature module and the signature verification module. Finally，the experiment and simulation of the intelligent irrigation system are carried out. The result shows that the intelligent irrigation system based on security protocol is efficient，and has good applicability and security in the case of weak computing and transmission capacity of intelligent irrigation devices.

Keywords：precision irrigation；smart home；SM2；big data；security protocol

[责任编校　陈留院]