农业物联网与智慧园林中 RFID 信息的风险分析及对策研究

李永钧
(南京农业大学 园艺学院,江苏 南京 210095)

摘要:针对农业物联网与智慧园林中广泛应用的 RFID 系统存在的安全风险及现有 RFID 认证协议存在的缺陷,提出了一种将公钥加密算法与散列函数相结合的 RFID 信息认证方案,分析结果表明:该方案具有较高的安全性并且在实现上的资源消耗较小。

关键词:农业物联网;RFID;安全
中图分类号:TP391.44;TN929.5　**文献标识码**:A　**文章编号**:1002-2767(2016)05-0143-03　DOI:10.11942/j.issn1002-2767.2016.05.0143

目前,农业技术管理呈现出日益科学化、精细化与智能化的特点,在农作物种植养殖、农产品加工、农产品流通以及销售等环节中,开始广泛采用 RFID、传感器、无线通信等各种信息技术,通过构建物物相连、智能感知的物联网来提高农产品信息的采集速度,并以最快速度共享到供应链各系统,实现了对每个农业个体的追踪和溯源[1],为构建全方位的食品安全体系提供了保证。同时在目前正在兴起的智慧城市建设中,也广泛采用 RFID 等信息技术获取基础数据,通过构建智慧园林信息系统,实现园林和景区管理各部门信息的互联互通、聚合与协同,以提高园林景区的综合管理能力与管理水平。

射频识别技术 RFID 一般包括后台系统、阅读器及电子标签三部分,其基本原理见图 1。阅读器需要查询数据时,向电子标签发送指令,标签按照指令回传信息,完成对数据的操作。RFID 作为一种无线通信技术,主要通过无线信道进行阅读器和电子标签之间的通信,而无线信道的安全性使得信息的安全受到威胁。通常在 RFID 系统所使用的电子标签中,会存储有关农产品生产销售的相关信息甚至厂商的个人信息以及园林景区的重要基础数据,如果不能得到有效保护,有可能造成商业信息或重要信息的泄露,给经营者、管理者甚至消费者带来不必要的损失,因此,对于 RFID 系统的信息风险及其对策需要进行深入地分析和研究。

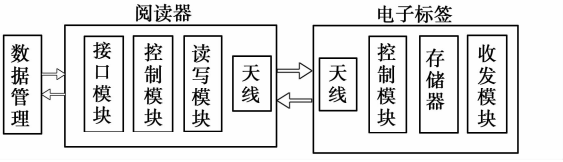

图 1　RFID 系统基本原理框图
Fig. 1　Basic principle block diagram of RFID system

1　RFID 存在的信息安全风险

1.1　信息泄露

在无线通信中,一般首先需要对通信双方的身份进行认证,以保证操作的合法性。其次需要对传输的信息采取某种加密手段以保证信息的安全。但在 RFID 系统中,电子标签和阅读器之间的通信一般未采取任何安全机制,不需要进行身份的验证,阅读器即可读取电子标签中存储的数据,从而导致商业信息或重要数据的泄漏[2]。

1.2　信息篡改

在 RFID 系统中,由于没有对通信双方的身份进行验证,也就没有办法对操作的权限进行限制,任何阅读器都可以读取电子标签中存储的数据,对于非法的访问者或攻击者,同样可以对所有开放的电子标签进行访问,或任意修改电子标签中的数据,对系统应用造成负面影响。

1.3　信息伪造

由于电子标签的开放性,可以采用不同的方法来伪造标签信息,以达到非法目的。一种方法是对合法的标签进行克隆,即非法用户对合法电子标签进行整体复制,克隆出与合法标签完全相同的电子标签。另一种方法是通过分析合法电子标签的数据存储结构,之后按照相同的数据格式

收稿日期:2016-03-31
作者简介:李永钧(1995-),女,山东省海阳市人,在读学士,从事风景园林与农业技术研究。E-mail:245380148@qq.com。

与结构，将数据写入一个空的电子标签中，来模仿合法标签[3]。

对阅读器与电子标签之间的无线通信进行攻击可以有多种方式，研究者对于各种攻击手段也进行了深入分析和研究，结合RFID的系统特点，设计提出了一些较为有效的方法。

2 目前使用的RFID安全协议

针对RFID系统可能遭遇的安全风险，有效的解决方案是采用安全认证协议，目前RFID认证协议主要分为三类：

2.1 通过简单的逻辑运算进行认证

这种方式主要通过逻辑运算来实现通信双方的身份认证或信息加密，一般使用某种函数对标签和阅读器之间的PASSWORD进行简单加密，并使用随机数与逻辑运算对收发的数据进行处理，使得通过无线信道传输的数据，既能进行相互的身份认证，也能保证信息的安全。这类认证协议对标签的计算能力要求较低，但是安全性也较低[4]。攻击者可以在很短的时间内进行反向运算，从而对数据进行解密。

2.2 基于高级加密算法的认证协议

这种方法是使用比较成熟的高级加密算法对阅读器和电子标签之间的数据传输进行加密，加密算法包括高级加密标准AES、基于离散对数问题的公钥密码体制EIGamal和ECC加密算法等。这类认证协议的共同特点是具有较高的安全性，但同时计算复杂性也高，对于阅读器的计算能力和电子标签的数据存储能力有很高要求[5]。

2.3 基于Hash函数的认证协议

目前，研究者已提出很多基于Hash函数的RFID认证协议，但都存在一定的安全隐患。例如实现成本较低的LCSS协议，通过在电子标签中设置标志位的方法，来避免对标签数据的穷举搜索，具有较高的安全性，但是LCSS协议不能防止攻击者主动发送查询命令获取标签响应对标签实施跟踪[6]。

3 HASH函数和公钥相结合的RFID认证方案设计

目前现有的RFID信息认证协议都存在一定的缺陷和不足。为此，在集成多种认证技术的基础上，提出了一种基于HASH函数与高级公钥加密算法相结合的RFID认证方案，以供分析探讨，进一步验证其安全性。

3.1 认证方案的设计与实现

本方案采用PKI(公钥基础设施)技术来设计和管理密钥，其中认证机构CA是PKI的重要组成部分，主要功能是通过数字证书来实现身份认证，保证信息安全。阅读器和电子标签都需要向CA申请数字证书，CA通过审核和身份验证，签发数字证书。阅读器和电子标签在进行数据通信时通过交换和验证对方的数字证书来保证身份的真实性。由于RFID电子标签的计算和存储能力较为有限，在设计CA生成数字证书所使用的加密算法上，并没有使用安全性较高但对计算能力同时有很高要求的RSA算法，而是采用了Rabin公钥体制。Rabin算法的安全性是建立在求解模数n的平方根这一数学难题之上，难度与RSA算法的大合数分解的数学难题大体相当，因此具有同等的安全性。但在验证电子标签或阅读器的数字证书时，只需进行一次模乘运算，相比RSA公钥算法更简单，验证效率更高[7]。同时在方案中结合了代理签名这一签名算法，也就是将传统数字签名中对计算能力要求较高的复杂运算剥离出来，由数字证书的验证方或可信的第三方来进行处理，既实现了电子标签对消息的数字签名，同时能够保持数字签名的安全性[8]。在此方案中采用代理签名技术将电子标签中的复杂计算交给阅读器来处理，有效解决了RFID电子标签难于计算签名的问题。基于此考虑，在认证过程中阅读器端采用了Rabin公钥算法，私钥为(m，n)，公钥 $p_r=m\times n$；电子标签采用代理签名，私钥为(a，b)，公钥 $(X=aG, Y=t^{-1}G)$。认证过程如下：

3.1.1 *系统初始化*　认证系统为每个阅读器和电子标签都分配一个具有唯一性的识别码IDp和IDq；随机数生成器RAND()由HASH链计算生成，也就是对前一次通信所使用的随机数进行HASH值的计算，作为本次通信选取的随机数。随机选取一个对称密钥E，HASH函数HASH()。然后将[n_{ca}，p_r，IDq，HASH()]保存到电子标签的存储器内存里面，同时将[n_{ca}，X，Y，IDp，HASH()]保存到后台系统或阅读器[9]。

3.1.2 *阅读器与电子标签的认证流程*　(1)阅读器端首先由RAND()函数随机生成一个随机数w，发送(Query，$Cert_r$，w)给电子标签，发起向电子标签的认证，其中Query为认证请求，$Cert_r$为阅读器的数字证书。

(2)电子标签使用认证中心 CA 的公钥 n_{ca} 对阅读器的数字证书 $Cert_r$ 进行验证,以确认该阅读器是否经过可信的第三方认证和授权。电子标签通过 RAND()函数生成随机数 o 作为随后通信的对话密钥,并利用公钥 p_r 对 o 进行 Rabin 加密处理,即计算 $a=o(o+w) \bmod p_r$,其中 w 也是由 RAND()函数生成的随机数。电子标签生成一个秘密的随机数 k,满足 $k\in[1,n-1]$,并计算 $u=k \bmod n$ 以及 $b=E_f(u,Cert_t)$,然后将 a 和 b 发送到阅读器端,其中 $Cert_t$ 是电子标签的数字证书。

(3)阅读器收到电子标签发来的 a 和 b 之后,使用私钥(m,n)对 a 进行解密得到 o,同时验证随机数 w 是否正确,之后用 o 对 b 进行解密得出$(u,Cert_t)$,对电子标签的数字证书进行验证,然后计算 $uY=(x_3,y_3)$,并转换 x_3 为整数,再计算模数 $r=x_3 \bmod n$。如果模数 r 为 0,则返回第一步,这时阅读器由 RAND()选择新的随机数 w;否则阅读器端将 o 的 HASH 函数值 HASH(o)′以及 Eo(r||HASH(r))发送到电子标签。

(4)电子标签收到函数值 HASH(o)′之后,验证 HASH(o)′与 HASH(o)是否相等。如果二者不相等就终止通信;相等则完成电子标签对阅读器的认证。电子标签进行解密运算 Eo(r||HASH(r))得到 r,之后计算模数 $s=k^{-1}(HASH(o)+rx) \bmod n$,计算结果(s,r)就是电子标签对于会话密钥 o 的数字签名,这时将数据(s,r)发送到阅读器端。

(5) 阅读器端接收到数据(s,r)以后,验证数字签名(s,r)的有效性,如果有效,则完成阅读器对电子标签的认证;否则就终止通信。

阅读器与标签的相互认证过程见图 2。

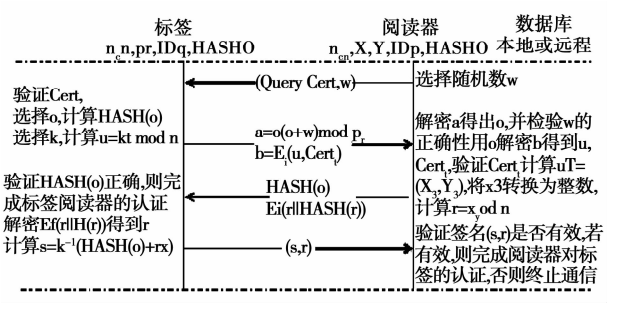

图 2　RFID 标签与阅读器相互认证过程

Fig. 2　RFID tag and reader mutual authentication process

3.2　认证方案的安全性分析

基于公钥算法和 HASH 函数的 RFID 安全认证方案,实现了阅读器和电子标签之间的身份认证,并对相互之间传送的数据进行了加密处理[10]。阅读器和电子标签在交换数据之前必须进行身份的认证,能够防范非授权的信息读取;同时在方案中使用的双方的数字证书都是由认证中心数字签名的,具有很高的安全性;之后的通信中,相互之间传送的是经过 HASH 函数处理过的加密信息,可以有效防止非法用户的窃取;而且在此方案中采用 HASH 链动态生成随机数,每次使用的随机数都与前一次不一样,也能够防范攻击者的前向攻击。

3.3　认证方案的性能分析

RFID 认证协议不仅要具有较高的安全性,还要充分考虑到电子标签在存储和运算能力方面的限制,采用更少的数据存储量和更为简便的认证与加密算法,以提高系统运行效率。整个认证过程中涉及到的计算量见表 1。总体上认证过程涉及的计算量不大,存储空间的资源消耗较小。

表 1　标签在公钥 RFID 认证方案中计算量

Table 1　Tag calculation in the public key RFID authentication scheme

认证过程 Certification process	Hash 运算 Hash operation	模乘运算 Modular multiplication	模加运算 Modular addition operation	求逆运算 Inverse operation	对称加/解密运算 Symmetric encryption/decryption operation
第(2)步	2	3	1	0	1
第(4)步	2	2	1	1	1

4　结论与讨论

在农业物联网和智慧园林中得到广泛应用的 RFID 作为一项先进的自动识别和数据采集技术,具有非视距、远距离、多标签识读等优点[11],但是由于 RFID 电子标签的工作原理以及成本方面的限制,电子标签和阅读器的信息安全风险在 RFID 系统中较为薄弱。本文针对现有 RFID 认证协议中存在的缺陷进行分析,提出了一个将公钥算法与散列函数相结合的 RFID 认证方案,并分析了方案的安全性与实现上的资源消耗,今后还需要通过软硬件实验和应用环境对其性能与安全性进行进一步分析和验证。

(下转第 156 页)

表 1　黔薯 6 号贵州省两年区试情况

年度	品种	产量/(kg·hm^{-2})	比 CK 增产/%
2013	黔薯 6 号	39918.00	-
	CK1 铜薯 2 号	33219.30	20.17
	CK2 福薯 16	28815.00	38.53
2014	黔薯 6 号	43104.60	-
	CK1 铜薯 2 号	38064.30	13.24
	CK2 福薯 16	30718.20	40.32
平均	黔薯 6 号	41511.30	-
	CK1 铜薯 2 号	35641.80	16.47
	CK2 福薯 16	29766.00	39.46

表 2　黔薯 6 号贵州省生产试验情况

地点	品种	产量/(kg·hm^{-2})	比 CK 增产/%
贵阳	黔薯 6 号	41238.45	-
	CK1 铜薯 2 号	41292.00	−0.13
	CK2 福薯 16	32505.60	26.87
凯里	黔薯 6 号	34781.40	-
	CK1 铜薯 2 号	29262.60	18.86
	CK2 福薯 16	28118.85	23.69
紫云	黔薯 6 号	32234.85	-
	CK1 铜薯 2 号	27469.95	17.23
	CK2 福薯 16	25569.00	26.07
平均	黔薯 6 号	36084.90	-
	CK1 铜薯 2 号	32674.95	10.44
	CK2 福薯 16	28731.15	25.60

4.2　培育壮苗

采取小拱棚育苗法，在 3 月上旬前后下种，种薯大小在 150～300 g 为宜。在下种后，每平方米苗床浇施稀粪水 30 kg，然后小拱棚覆盖。在齐苗前后，以保温催芽为主，超过 35 ℃时，揭膜降温。当薯苗高 25 cm 左右时，揭膜炼苗，控制浇水。经过 3～4 d 后，及时采苗插植。剪苗后苗床、培土和追施稀粪水。

4.3　合理密植

一般栽插 54 000～63 000 株·hm^{-2}。采用斜插法栽插，一般在 6 月中旬之前栽插结束。

4.4　科学施肥

施肥以有机肥为主，化肥为辅。一般施腐熟农家肥 22 500 kg·hm^{-2}，硫酸钾 225 kg·hm^{-2}。

4.5　病虫害防治

在整个生育期间较少有病害发生，在黑斑病发生较严重的地区可以用 50%多菌灵或 50%甲基托布津 500 倍液喷施防治。

4.6　适时收获

根据市场行情，分批收获上市，在下霜前收获结束。

4.7　种植区域

海拔 1 200 m 以下均可种植。

参考文献：

[1] 马代夫，刘庆昌. 中国甘薯育种与产业化[M]. 北京：中国农业大学出版社，2005：227-298.

[2] 郭其茂，杨立明，林子龙，等. “淀粉型”甘薯品种龙薯 28 号的选育[J]. 安徽农业科学，2015，43(14)：71-73.

[3] 李朝霞，陈正福，廖雪红，等. 高淀粉甘薯品种铜薯 1 号的选育及特征特性[J]. 种子，2012，31(12)：100-101.

[4] 郑光武，林世英，中奕，等. 高淀粉甘薯新品系“莆薯 1-6”选育研究初报[J]. 福建农林科技，2006(6)：9-10.

(上接第 145 页)

参考文献：

[1] 贾浩，沈岳，温佑杰. RFID 在农业物联网中的应用[J]. 湖南农业科学，2015(9)：122-125.

[2] 万晨妍，欧阳麒. RFID 系统中信息保密机制研究与设计[J]. 信息安全与通信保密，2011(9)：100-101.

[3] 王娟. 基于散列函数的 RFID 认证协议研究[D]. 南京：南京邮电大学，2012.

[4] 蒋皓石，张成，林嘉宇. 无线射频识别技术及其应用和发展趋势[J]. 电子技术应用，2005(5)：1-4.

[5] 吴叶科，宋如顺，陈波. 基于博弈论的综合赋权法的信息安全风险评估[J]. 计算机工程与科学，2011，33(5)：9-13.

[6] 邓淼磊，王玉磊，邱罡. 无需后端数据库的 RFID 认证协议[J]. 北京邮电大学学报，2009，32(4)：59-62，67.

[7] 高员. 基于公钥的 RFID 认证技术研究[D]. 西安：西安电子科技大学，2011.

[8] 尹淑娟. 基于 Hash 算法的 RFID 系统安全读写访问控制协议研究[J]. 科技信息，2012(36)：572.

[9] 高员，李琳，肖静，等. 代理计算签名及其在 RFID 认证中的应用[J]. 电子产品可靠性与环境试验，2015，33(1)：24-28.

[10] 董绍辉，西宝，田丽娜. 供应链信息共享中信息泄露的产生机理及防范措施研究[J]. 软科学，2009，23(5)：56-59.

[11] 梁晨. 基于物联网的 RFID 安全认证协议研究与设计[D]. 西安：西安电子科技大学，2011.

Risk Analysis and Countermeasures Research for RFID Information in Agricultural IOT and Intelligent Garden

LI Yong-jun

(Nanjing Agricultural University, Nanjing, Jiangsu 210095)

Abstract: As an advanced information recognition and data capture techniques, RFID are widely used in Agricultural IOT. However, due to the RFID tag works and cost constraints, information security through wireless channel is threatened. Through analyzing the security risks and existing defect of the RFID authentication protocol, an new RFID authentication scheme combined public key encryption algorithm and hash function was proposed, and it had higher security and the smaller resources consumption in achieving.

Keywords: agricultural IOT; RFID; authentication