DOI:10.19695/j.cnki.cn12-1369.2015.11.152

基于混沌加密的RFID认证协议设计

王海春 李均 邓珊
(成都信息工程大学 四川成都 610000)

摘要: 本文描述了一种基于混沌加密的RFID认证协议设计。主要研究了混沌加密技术在RFID系统应用中的安全隐私保护问题,在对国内外已有的RFID安全认证协议研究进行研究基础上,应用基于混沌哈希的安全技术、隐私保护技术,提出了一种基于混沌加密算法的安全性较高的RFID安全认证协议,对其安全性能进行了对比分析,并进行了BAN逻辑验证,结果表明改进的认证协议满足安全性的目标。总结了实验数据,提出了相关理论模型,对今后RFID认证协议的实际应用,提供了坚实的理论基础。相关项目已投入实际使用。

关键词: RFID认证协议 混沌周期性 隐私保护 身份认证
中图分类号: TP391.45 **文献标识码:** A **文章编号:** 1007-9416(2015)11-0206-02

1 引言

RFID技术,也称无线射频识别技术,它是一种无需人为干预、无需通信双方直接接触便可达到信息的传递、识别、操作的目的。它作为物联网范畴内的重要技术之一,随着物联网技术的快速兴起,RFID技术也越来越多的得到人们的关注,从居民的身份证、超市管理,到金融、国防等领域。然而,随着RFID技术的快速兴起,RFID技术中所存在的一些问题也日益凸显出来,其中最引发人们关注的是RFID技术的安全隐私保护问题,因为RFID技术已经深入到人们的日常工作、学习、生活中,安全隐私问题不容小觑。

考虑到RFID标签固有的内部资源有限、能量有限和快速读取的要求,在设计基于加密方案的安全协议时,所采用的加密算法既要简单方便,又不能占用较多的系统存储资源,因此传统的加密算法不太适合于RFID标签中,必须寻求一种既简单又具有高安全性的加密算法。

混沌是一种非线性动力学规律控制的行为,表现为对初始值和系统参数的敏感性、白噪声的统计特性和混沌序列的遍历特性,其吸引子的维数,有十分复杂的分形结构,具有不可预测性,可用于随机密钥的计算。混沌信号的隐蔽性、不可预测性、高复杂度和易于实现等特性都特别适用于保密通信,因此可以考虑将混沌加密应用于RFID安全机制中。

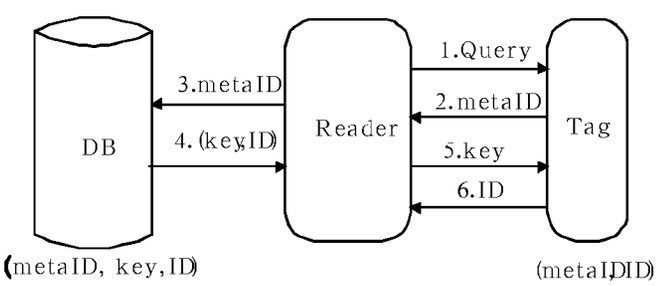

图1 Hash-Lock协议工作过程图

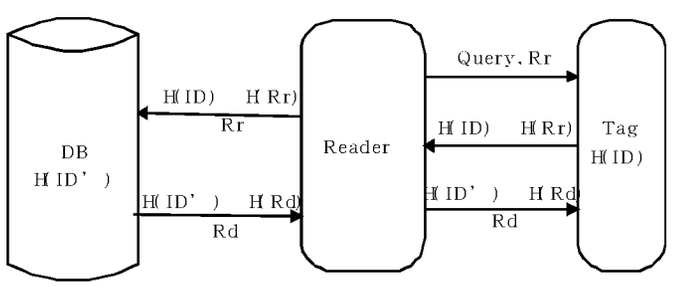

图2 基于混沌加密的RFID认证方案工作过程图

本文主要研究了混沌加密技术在RFID系统应用中的安全隐私保护问题,所做的工作有:

(1)对国内外已有的RFID安全认证协议研究进行了研究,提出了两种基于混沌加密算法的安全性较高的RFID安全认证协议,主要特点是,应用了基于混沌哈希的安全技术、隐私保护技术,提出了具有混沌特点的RFID动态密钥协议。对其安全性能进行了对比分析,并进行了BAN逻辑验证,结果表明改进的认证协议满足安全性的目标。

(2)为了强化基于混沌的RFID认证协议本身的安全性能,对混沌序列的周期性进行了大量实验研究。总结了实验数据,提出了相关理论模型,对今后RFID认证协议的实际应用,提供了坚实的理论基础。

(3)为了强化RFID安全认证协议的实际应用,提出了双混沌实验模型,对推进基于混沌加密技术的RFID的安全认证协议的应用,提供了一个更为具体的方法,并对构造的双混沌性能和安全性进行了实验分析,结果表明,该加密算法具有大周期性、随机性良好、安全性高的特性。

(4)分析了现有的RFID身份认证中的隐私安全隐患,引入了零知识证明协议,提出了一种基于零知识的身份动态认证机制,并进行了数据验证和安全性分析,结果表明混沌加密算法可应用于该零知识身份认证协议,且具有很好的安全性。

2 国内外研究现状

RFID技术最早在国外应用,Harry Stockman可以称为RFID技术发展的奠基人,他的"利用反射功率的通讯"为RFID技术的发展提供了理论支撑[1],此后,越来越多的科学家们开始投入了对RFID技术的研究[2]。

在80年代之前,由于RFID技术发展水平低,而且研发成本比较昂贵,导致它的应用范围较局限,大都应用于军事领域,而随着科技的发展,RFID技术也得到了迅猛的发展,其应用也越发广泛。就美国来说,美国政府一直把对RFID技术的发展应用作为重中之重的研究[3],US国防部规定,零五年以后国内的军用物资全部要贴上射频标签,美国FDA也推荐2006年起在药品上使用射频标签,用以防

收稿日期:2015-10-23

作者简介:王海春(1957-),男,四川成都人,教授,学位:硕士,研究方向:计算机应用、信息安全、教育教学改革;李均(1989-),男,四川成都人,研究生,研究方向:计算机应用、信息系统;邓珊(1989-),女,河南新乡人,研究生,研究方向:计算机应用、数据库系统。

止假药的流通。在政府大力推动下，已经形成了一整套的独特特色的射频识别体系，建立了RFID标准，在硬件和软件研发方面均走在行业前列。欧洲大部分国家对RFID应用的研究也比较早，比如Nokia、PHILIPS、SAP等在电子标签芯片上都研制了具有各自特色的成品。中国在对RFID技术的研究起步较晚，主要在80年代后逐渐兴起，最典型的运用是我国居民二代身份证在身份认证方面对RFID技术的利用。目前，RFID技术主要应用在物流管理系统、停车场管理系统、高速公路收费系统、超市货物跟踪系统等领域中[3]。

RFID技术应用的普及性也让人们越发关注系统的安全隐私保护的问题，至今为止，已有相当多的安全策略被提出，有些专家提出了在物理层面上对其进行保护，比如Auto-ID组织设计的"杀死"标签机制，若是内嵌RFID标签的商品被售出，就启动该命令，这样就可以防止非法用户对物品的恶意跟踪，但一旦启动了该命令，标签便不能够再次利用，浪费了资源；利用静电屏蔽原理，把标签放置于一个封闭的金属容器中，阻挡外界信号的进入，但这也阻挡了合法读写器对其进行读写，实用性不强。考虑到物理方法所隐含的缺陷，专家学者们又提出了基于密码加密机制的通信协议，比如Sarma、Engels等人提出的Hash-Lock协议[9]，Weis等人提出的随机化Hash-Lock协议，Henrici等提出的哈希ID变化协议，薛佳楣等人设计的RFID反追踪安全机制等等，其他的关于加密机制的认证方案可查询文献。以上这些安全协议数量众多，但却存在各种各样的安全缺陷，不能满足RFID系统的安全性和实用性要求[4]。

3 现有的RFID安全认证协议分析

Sarma等人于2003年设计提出了基于哈希函数的Hash-Lock认证机制，在起始状态，对每个标签生成一随机数Key，得到metaID=Hash(Key)，标签中存放自身ID和相应的metaID，利用metaID取代标签ID 进行通信，防止了标识信息被非法窃取，后台数据库中存放相应的metaID，Key，ID。该协议的具体过程如图1所示。

协议工作步骤如下：

(1)标签Reader向Tag发Query查询请求。

(2)Tag收到请求后，把自身metaID发送至Reader。

(3)Reader接收metaID，并将其发送至后台数据库。

(4)后台将收到的metaID与数据库中数据进行查找对比，若找到与metaID相同的数据，则把与该数据相配套的(key，ID)传送至Reader；若不存在，则认证失败。

(5)Reader将得到的key数据传送至Tag。

(6)Tag把收到的key进行哈希运算，对比H(key)与metaID是否相等，若相等，则发送自身ID至Reader，Reader将其与步骤4中得到的ID对比，若相同，则双方认证完成；否则，Tag不合法。

该认证机制将通信中的数据用哈希函数进行隐藏，由于哈希函数的单向性，该协议在保护数据隐私方面起到一定作用，而且整个通信过程只需要进行一次哈希运算，计算量也较小。但是，该协议也有较多的安全漏洞，步骤2中Tag每次响应Reader时都是固定的metaID，很难抵挡位置跟踪；步骤6中ID以明文方式在无线信道中传送，易于被非法用户窃取，难以抵抗假冒和重传攻击；Tag的ID固定不变，很有可能被别人克隆。因此，Hash-Lock协议并不能满足系统安全性要求。

4 基于混沌加密的RFID认证方案

通过前述对射频识别技术面临的隐私问题分析，以及对攻击者常用的攻击手段的介绍，可以看出RFID技术存在的安全威胁不可忽视，亟需需求相应对策来保证系统的安全。我们对现有的几种RFID认证协议进行的分析、对比，看出这些协议各有各的优势和不足，本文借鉴它们的思想，在哈希锁协议的基础上提出了改进方案。

考虑到RFID标签固有的内部资源有限、能量有限和快速读取的要求，在设计基于加密方案的安全协议时，所采用的密码算法在保证安全的情况下应该是越简单越好。复杂度高的算法在计算时间和计算量上都比较耗费，不适合应用于低成本的电子标签中，因此很少采用公钥加密算法。现有的认证协议大都是基于哈希函数加密技术实现的。

一般情况下，我们假定标签是被动式标签，也即是无源标签，它的低成本使得它的存储容量非常小，只能存储少量的数据信息，而且它计算能力很低。所以，在初始化时，标签Tag中只限于存储自己的唯一的标识符ID经过运算后的哈希值H(ID)，本方案采用的是第三章构造的双混沌加密算法产生的哈希值。后台数据库系统中存储的是与Tag的ID相对应的H(ID')，这样做的目的是防止后台数据库被非法入侵者入侵后造成标签ID泄露。协议流程图如下图2所示。

4.1 协议的描述

协议认证过程如下：

(1)RFID读写器生成一随机数Rr，然后把Rr和请求Query一起发送给标签。

(2)标签接收读写器发送过来的Rr，对Rr进行Hash运算，然后把加密后的结果进行异或H1=H(ID)⊕H(Rr)，发送给读写器。

(3)读写器接收标签发送过来的H1数据后，将H1和Rr发送至后台系统中。

(4)后台系统接收H1和Rr后，运算得到如图示数据。随后在数据库中查找是否存在。若存在，则证明该标签是合法的，否则是不合法。

(5)后台数据库生成一随机数Rd，然后把H2=H(ID')⊕H(Rd)和Rd一起发送到阅读器，阅读器接收数据后，再发送至标签。

(6)标签接收数据H2和Rd后，首先进行验证，看是否存在ID使得H(ID)=H2⊕H(Rd)，若存在，则证明读写器合法，否则，则证明读写器不合法。至此，双方认证结束。

4.2 对协议的安全性分析

(1)隐私保护。

在本方案中，标签与数据库中存放的都是经过Hash运算后的128位的比特值，这样，标签在没有提供任何能够危及自己的信息的前提下即可完成读写器对自身合法性的认证。而且即使数据信息遭到泄露，攻击者得到的只是Hash值，由Hash的单向性不可能推导出ID。

(2)有效抵挡位置跟踪。

每次标签传送到H(ID)⊕H(Rr)动态变化，攻击者不能根据固定输出对标签进行跟踪。

(3)数据安全。

本方案采用的是混沌Hash，一般的Hash算法，比如MD5，SHA-1等算法已被王小云等人成功破解，它们的安全性面临严重威胁，攻击者可以对其进行破解，而在混沌Hash中，Hash值和具体采用的混沌映射、迭代次数、参数、初始值等等都有很大关系，其序列轨迹极其复杂，对其进行破解比较困难。

(4)存在的隐患。

目前该协议仍缺乏ID动态刷新机制，存在不能抵挡标签复制的隐患。

5 结论

……下转第209页

关重要,它能保证网络系统安全,可靠,持续地运行。安全的物理环境和相关的基础设施主要有如下:①机房相关场地要保证安全,它将影响到网络系统的安全性和可靠性,所以得选择一个合适的安装场所。②对于虫害、腐蚀度、湿度、温度、空气洁净度、振动这些方面都必须要有严格的标准并按照这个要求执行,从而保证计算机系统的安全。③机房要防止没有经过授权的个人或其它团体进入,更改,破坏网络设备。要求机房设备所在的建筑物应能具有抵御各种如水灾,火灾等各种自然灾害,从而保证机房的安全防护。机房要建立安全管理制度。提高包管理员的职业道德修养和技术素质。(2)防病毒措施。防病毒就是要将病毒危害程度降到最低,采用有效的手段对病毒进行预防、检查和清除,保证网络安全可靠的运行,防病毒可以做到下面几条:①安装防火墙软件和杀毒软件,时不时对计算机进行检测;②对于来历不明的外存储器如光盘,U盘一定要事先对它进行查毒处理;③备份各种文件;④对来历不明的邮件不要轻易打开,对电子邮件提高警惕;⑤避免浏览假冒见面及非法网页。(3)进行身份认证。处于网络系统中,将服务者根据其在网络中声称的身份,对其进行鉴别与判断。进行身份认证是网络系统中判断它是否是真人本身的一个经过。(4)信息的备份与恢复措施。数据库管理员为了维护数据最经常做的一件事就是备份数据了,它是数据丢失时为了能恢复数据的一个重要操作,它保证了数据的安全性和完整性。只有通过备份才能恢复因意外而导致的数据丢失,它是数据能进行恢复的前提,是一个重要的方法。目前有三种备份方案,它们分别是:增量备份,只备份数据库、备份数据库和事务日志。备份保护了数据,它是在意外发生以后使用备份的数据来恢复数据的一种手段。访问控制它能保证计算机网络系统中的资源不被未经授权的人访问和盗用。访问控制是保护计算机网络和安全预防的一个重要措施。访问控制还是维护保护计算机网络系统安全和网络资源的一个重要操作。计算机网络管理员要限制和控制用户的账号使用还有访问网络的时长和方式。计算机网络系统中最基本的方式就是用户名或是用户的帐号了,它必须只有系统管理员才可以创建。各种安全策略必须互相配合才能起到真正的保护套路。(5)建立信息的加密措施。信息处理是计算机最广泛的一个应用了,利用信息处理,我们可以提高工作的效率,可在信息处理的过程中,如数据的采集、处理、传输的时候也增加了泄密的可能性。保密性主要是利用密码信息对加密数据进行处理,防止数据非法泄漏,它是计算机网络安全的一个重要方面。所以对存储在各种介质上的信息和要传输的数据进行加密措施是非常有必要的,它保护了传输中的数据。(6)保护应用层措施。应用层的保护,主要是保护Web服务器应用安全,保护网络支付平台上的软件,对其建立相应的保护设备,应用层的保护不同于其它网络保护。它涉及到的业务有访问控制、认证、不可抵赖性、Web安全性、机密性、数据安全性等等。对于在应用层上,对网络支付结算数据包的加密,Web浏览器和Web服务器主要是通过对IP层的加密,甚至很多其它应用还会有限定的安全加密要求。(7)防火墙。防火墙是一种保护计算机网络安全的技术性措施,防火墙本身是一种隔离技术,在两个网络之间隔着一道墙壁,这道墙它就是防火墙。防火墙用来限制和阻碍非法用户和未授权的用户使用他人的内部网络系统数据,它能防止偷窃和起到破坏作用的恶意攻击,通过一道监控系统去隔离内和外不同的网络。防火墙系统的一个重要目标就是能辨认用户,对网络里面进出的所有信息进行排查,防止产确定的信息进入防火墙所要保护的系统。总之防火墙对计算机网络安全起得了一个很关键的作用。(8)建立网络智能型日志系统措施。日志是记录从某个用户开始登录,到它退出系统结束,包含错误的登录信息,系统的使用情况和对数据库相关操作等,所有执行的一切操作都在之内。日志所记录的内容包含有用户、操作对象、操作执行时间和操作类型,操作上的IP地址等等,以防后面的核查审计所用。日志系统具有自动分类检索能力和综合性数据记录功能。

6 结语

计算机网络安全已经影响到人们的生活了,计算机网络安全急需我们对它的重视,计算机网络系统面临着重要的挑战,需要来自不同方面的配合。我们应该做好网络安全防范措施,确保计算机网络安全可靠有效地持续进行。

参考文献

[1]李冰.网络攻击的六大趋势[J].科技广场,2002.
[2]杨波.网络安全理论与应用[M].北京:电子工业出版社,2003.

……上接第207页

综上所述,基于Hash的认证协议在计算量和存储空间上相比方案1有一定的优势,但它没有动态更新ID的机制,在一些安全性要求较高的应用环境中,比如军事和金融领域内,会出现标签被复制的危险,而且标签内存储的是经过Hash加密后的密文,由于Hash函数的单向性,不能反向推出其标识,在一些要求认证合法后进行数据修改的应用中,比如一卡通系统,不能对其中的余额进行更新操作。因此在一些安全性要求不太高的环境,例如一些门禁系统中,就可以采取基于Hash的认证方案,而对于安全性要求比较高的应用中,虽然在计算速度和存储容量上花了一些代价,但最主要的还是其在安全方面的优势,因为衡量一个好的安全认证协议不仅仅要看其在计算量和存储方面的优势,更主要的是能够有效抵挡各种攻击。本节在对传统的Hash-Lock认证协议的不足的基础上进行研究、改进,提出了独具特色的两种安全性较高的RFID安全认证协议,主要特色是,应用了基于混沌哈希的安全技术、数据保护技术,提出了具有混沌特点的RFID动态密钥协议,并对其性能进行了分析、对比。简要介绍了BAN逻辑的概念,阐述了如何利用BAN逻辑对协议的安全性进行证明,并给出了对改进协议安全性进行证明的过程,结果表明,协议满足安全性目标的要求。

参考文献

[1]雷吉成.物联网安全技术[M].电子工业出版社,2012.6:66-67.
[2]RFID世界网,RFID技术的发展历程及应用现状,http://www.rfidworld.com.cn,2005.
[3]ISO/IEC 18000-3. Information Technology AIDC Techniques-RFID for Item Management-Air Interface, part 1:Generic parameters for air interface communication for globally accepted frequencies. International Organization for standardization, 2003.
[4]蒋皓百,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,2005,31(5):51-56.