# 面向物联网的RFID安全策略研究

胡 婕,宗 平
(南京邮电大学 物联网学院,江苏 南京 210003)

**摘 要**:RFID是一种非接触式的自动识别技术,尤其在物联网中具有广泛的应用。但是,在实际应用环境中,RFID尚存在诸多安全隐患。增强RFID的安全性能够进一步扩大其使用范围,在讨论目前RFID的安全问题以及物理安全机制和加密机制的基础上,重点研究了基于加密机制的几种安全协议的特点,并对这些协议进行了比较分析,提出了新的RFID安全策略,设计了一种混合方式的安全模型—Hybrid-Encryption。经证明,该模型能够有效解决物联网应用环境中的RFID应用系统的安全问题。

**关键词**:加密机制;RFID系统;安全策略
**中图分类号**:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)05-0151-04

# Study of RFID Security Strategy Based on IOT

HU Jie, ZONG Ping
(College of Internet of Things, Nanjing University of Post and Telecommunications, Nanjing 210003, China)

**Abstract**: RFID is a non-contact automatic identification technology. It has a wide range of applications, especially in IOT. However, in the application environment, there are still many security risks. To enhance the security of RFID can expand its use further. Based on discussing the current problems of RFID security, its physical security mechanism and encryption mechanism, study the features of several security protocols with encryption mechanism and compare these security protocols. Then propose a new RFID security strategy and design a mixed security model as Hybrid-Encryption. The testification shows that this model can solve the security problem of RFID application system in IOT effectively.

**Key words**: encryption mechanism; RFID system; security policy

## 0 引 言

自国际电信联盟(ITU)在突尼斯举行的信息社会世界峰会上发布了《Internet Reports 2005: The Internet of Things》,提出了"物联网"概念以来,物联网及相关技术受到人们的广泛关注。

无线射频识别(Radio Frequency Identification, RFID)技术是物联网应用中实施感知的一种重要手段。RFID系统使用无线射频技术在开放系统环境中进行对象识别[1],是集编码、载体、识别与通信等多种技术于一体的综合技术,它通过射频信号自动识别目标对象并获取相关数据,识别无须人工干预,相当于无线的条形码。在实际应用环境中,RFID标签、网络和数据等环节都存在安全隐患[2]。RFID系统安全问题主要反映在两个方面:第一是RFID标签和后端系统之间的通信是非接触和无线的,它们的通信内容很容易泄露;第二是标签的成本会直接影响标签本身性能,很难实现对安全威胁的高效防护。没有可靠的信息安全机制,就无法有效地保护射频标签中的数据信息。另外,不具有可靠信息安全机制的射频标签还存在着易向邻近的读写器泄漏敏感信息、易被干扰和易被跟踪等安全隐患[3]。

为此,文中针对RFID系统中存在的安全问题,在分析和比较现有一般解决策略的基础上,给出了一种混合方式的安全模型—Hybrid-Encryption,并对相关的技术方法做出了说明。

## 1 RFID系统及其安全问题

### 1.1 RFID系统

RFID是一种非接触式的自动识别技术,它通过射频信号自动识别目标对象并获取相关数据,可工作于各种环境之下。最基本的RFID系统包括标签、读写器和天线三部分[4]。RFID标签(Tag)具有唯一的RFID编码,附着在所要标识的对象上。Tag可以分为有源和无源,也可分为只读和读写。RFID读写器(Reader)是一个带有天线的无线发射与接收设备,它

**收稿日期**:2010-10-13;**修回日期**:2011-01-16
**基金项目**:江苏省科技支撑项目(BE2009157)
**作者简介**:胡 婕(1988-),女,硕士研究生,主要研究方向为信息安全;宗 平,博士,教授,主要研究方向为计算机网络、信息安全等。

的处理能力、存储空间都比较大[5]，它是 RFID 系统中最重要的基础设施。天线(antenna)是 RFID 标签和读写器之间实现射频信号空间传播和建立无线通讯连接的设备。图 1 给出了 RFID 应用系统的组成结构。

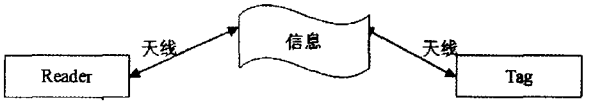


图 1 RFID 应用系统组成结构

### 1.2 RFID 安全问题

目前，由于 RFID 主要应用于企业供应链中，对私密性要求不高，很多用户对于 RFID 的安全问题并不重视。但是，随着应用的扩展，如果不能有效地解决基于物联网的 RFID 系统的安全问题，未来遍布全球的 RFID 应用系统安全可能会向人们提出许多难题。虽然与计算机和网络的安全问题类似，但 RFID 的安全问题要严峻的多[6]，主要表现在以下几个方面：

(1)各组件的安全脆弱性。在 RFID 系统中，数据随时会受到攻击，不管是在传输中或者是已经保存在标签、阅读器或在后端系统中。

(2)数据的脆弱性。一般每个标签拥有一个 IC，即是一个带存储器的微芯片，攻击者可以通过阅读器或其它手段读取标签中的数据；在读写标签的情况下，甚至可能改写或删除标签中的内容。另一方面，阅读器中数据的脆弱性。阅读器在收到数据以后，要进行一些相关的处理，在处理过程中，数据安全可能会受到类似计算机安全脆弱性的问题。

(3)通信的脆弱性。标签和阅读器互相传送数据是通过无线电波进行的，在这种交换中，攻击者可能截取数据或者阻塞、欺骗数据通信，甚至采用非法标签发送数据。

文中主要研究针对 RFID 攻击的防范策略与技术方法。对 RFID 的攻击方式主要有两种：主动攻击和被动攻击。截获信息的攻击称为被动攻击，如试图非法获取应答器中重要数据信息等。更改、伪造信息和拒绝用户使用资源的攻击为主动攻击。在实际应用中，RFID 系统的安全隐私问题主要集中在 RFID 标签与读写器之间[7]。

## 2 RFID 安全策略分析

现在针对 RFID 的安全攻击，可以采用的解决策略主要有三大类：物理安全机制、加密机制以及二者相结合的机制。

### 2.1 物理安全机制

物理安全机制是使用物理方法来保护标签安全性的机制[8]，主要有以下几种：

(1)Kill 指令。一旦对标签实施了 Kill 毁坏命令，标签便不能再被使用。杀死标签的口令只有 8 位，因此恶意攻击者仅以 $2^8$ 计算代价就可以获得标签的访问权。因此，简单的 Kill 指令并不是一个有效的安全策略。

(2)静电屏蔽。从电磁场的观念，无线电波可以被由传导材料构成的容器屏蔽。但是，这需要一个外部设备，既造成了不便也增加了成本。

(3)主动干扰。主动干扰机制是另一种屏蔽标签的方法。标签用户可以通过一个设备主动广播无线电信号以阻止或破坏附近的物联网阅读器的操作。此方法也需要一个外部设备，同时也可能带来法律问题。

(4)阻止标签。通过采用一个特殊的阻止标签使得阅读器的读取命令得到的总是相同的应答数据，从而保护标签。但是此方法需要有阻止标签，使得成本偏高，也可能导致拒绝服务攻击，同时，超出保护区域的标签将得不到保护。

### 2.2 加密机制

由于物理安全机制尚存在着不足之处，人们继而提出了许多基于密码技术的软件安全机制。

(1)Hash-Lock 协议。Hash-Lock 协议不使用真实的标签 ID，而用 metaID 来代替。它是基于单向散列函数的，可以防止未经授权的读者阅读标签的内容，发现欺骗的企图。但是其 metaID 是不变的，并以明文的形式传送[9]。然而 Hash-Lock 协议很容易受到假冒攻击和重传攻击。

(2) Randomized Hash - Lock 协议。Randomized Hash-Lock 协议采用了随机数的询问-应答模式，其协议执行过程和 Hash-lock 基本一致。这个协议中，标签中不直接存放标签的 ID，而是存放标签 ID 的 Hash 值，这种机制使标签 ID 不直接暴露，有一定的机密性，但是它不能抵御重放攻击和目标跟踪[10]。同时，Reader 需要计算所有 ID 的哈希值，使得认证时间加长[11]。显然该协议并不十分有效。

(3)Hash 链协议。Hash 链协议本质上也是基于共享密钥的询问-应答协议。与上述两个协议不同，在 Hash 协议中 tag 和 reader 有一个约定的初始密钥值，并且 tag 具有自主更新 ID 的能力，这就要求该协议中的 tag 是读写 tag。同时，由于需要两个不同的散列函数，使得 tag 的成本增加。另外，Hash 链是一个单向认证协议，只能认证 tag 的身份，它同样容易受到重放和假冒攻击。

(4)基于杂凑的 ID 变化协议。该协议的执行过程与 Hash 链协议相似，但是每次会话的 ID 都不一样，该协议可以抵抗重放攻击。因为在认证之后，tag 会根据 reader 的返回消息更新自己的 ID。因此该协议中的 tag 也应该是读写 tag。但是如果攻击者的攻击是在

数据库更改ID而tag还没更改ID时发生,将导致数据不同步,合法的tag在以后的会话中将无法认证。所以该协议不适用于分布式数据库的计算环境。

(5)LCAP协议。LCAP协议也是询问-应答协议,但是与前面的协议不同,它每次执行之后都要动态刷新tag的ID。在该协议中,tag也是在消息接收验证通过之后才更新其ID的[12]。因此它与杂凑的ID变化协议一样不适用于分布式数据库。

(6)分布式RFID询问-应答认证协议。它是典型的询问-应答型双向认证协议。在协议执行过程中,reader和tag分别生成一个随机数,只有当reader和tag都通过认证才可以进行访问。目前尚未发现该协议有明显的安全漏洞,但是执行一次认证需要tag进行两次杂凑运算,因此它的认证时间相对较长,并且tag的制造成本很高。

显然,各种加密机制都有各自的特点。表1给出了上述加密机制的比较说明。

表1　加密机制的比较说明

| | Tag类型(只读/读写) | Tag的ID是否更新 | Tag的制造成本 | 易受何种攻击 | 适用场合 |
|---|---|---|---|---|---|
| Hash-lock协议 | 只读 | 否 | 低 | 假冒攻击、重传攻击 | 安全要求不高的场合 |
| Randomized Hash-Lock协议 | 只读 | 否 | 低 | 假冒攻击、重传攻击 | 安全要求不高的场合 |
| Hash链协议 | 读写 | 是 | 高 | 假冒攻击、重传攻击 | 安全要求不高的场合 |
| 基于杂凑的ID变化协议 | 读写 | 是 | 高 | 攻击使数据不同步 | 不适用于分布式数据库 |
| LCAP协议 | 读写 | 是 | 高 | 攻击使数据不同步 | 不适用于分布式数据库 |
| 分布式RFID询问-应答认证协议 | 只读 | 否 | 很高 | 尚未发现安全漏洞 | 可以用于隐私保护上 |

通过分析和比较,可以看出在Hash-Lock协议和Randomized Hash-Lock协议中,尽管tag的造价低廉,但是这两种机制的安全性也很低。而改进的Hash链协议在安全方面也没有很大的提高,甚至由于使用读写式tag使得tag的造价增加。基于杂凑的ID变化协议和LACP协议在安全方面较之前3种都有了一定程度上的提高,但是因为tag的ID需要更新,这就使得该协议存在安全隐患,同时也提高了tag的造价。分布式RFID询问-应答认证协议是以上协议中最为安全的,但是一方面它的运算时间很长,另一方面它的tag制造成本也较高,并且在该协议中,tag的ID是不会动态更新的。为此,在物联网应用环境中,RFID使用十分广泛,必须设计出一种有效的安全机制,在确保其安全性的同时,又不增加额外的计算开销,tag等相关设备的制作成本也较低。

上述协议中消息都是以明文的形式传送的,为了增强其安全性,考虑将消息加密后以密文的形式来传送。

## 3　Hybrid-Encryption安全模型设计

对称密码体制是一种传统密码体制。在加密系统中加密和解密采用相同的密钥。对称密码体制具有很高的保密强度,同时计算开销小、加密速度快。但是它存在着通信双方之间确保密钥安全传递的问题。另外,对称加密体制仅能用于提供数据的机密性,不能用于数字签名。

非对称密码体制也叫公钥加密技术,在该加密系统中,加密和解密是相对独立的,使用不同的密钥,加密密钥公开,解密密钥私有,并且不能互相推导。非对称密码体制算法复杂、加密数据的速率较低,然而它能方便、安全地实现数字签名和认证。

在物联网应用环境中,存在着众多的用户群体,且不同的用户群体之间有着不同的安全要求。因此,采用对称密码与非对称密码相结合的机制,提出一种混合型的安全模型—Hybrid-Encryption模型。既保证高效的安全性,又提供较好的开放性,以适应物联网的应用环境。Hybrid-Encryption模型的安全处理机制如图2所示。

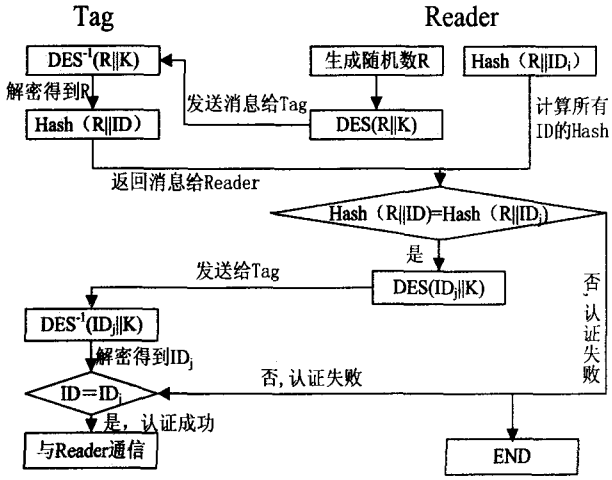


图2　Hybrid-Encryption模型的安全处理机制

在实际应用时,reader和tag之间有一个事先约定好的密钥K。

(1)reader生成一个随机数$R$,利用对称加密算法DES(或者AES),生成$D(R||K)$,发送$D(R||K)$给tag进行询问;

(2)tag收到$D(R||K)$后解密,得到$R$,采用非对称机密算法Hash,计算Hash($R||ID$),将Hash($R||ID$)返还给reader;

(3)reader将自己知道的$ID$都进行Hash($R||ID_i$)找到$ID_j$,使得Hash($R||ID_j$)=Hash($R||ID$),计算$D(ID_j||K)$发送给tag;

(4)tag收到$D(ID_j||K)$后解密得到$ID_j$,与自己的$ID$进行比较。如果相同,通过认证。

在Hybrid-Encryption模型中,所传送的数据都是

加密后的。DES 为对称加密算法，Hash 为非对称加密算法。对称加密算法 AES 比 DES 具有更好的保密性，但是运算量也更大。如果希望进一步提高安全性，也可以使用读写 tag。在第 3 步中，reader 随机生成一个新的 $ID^{'}$，并计算 $D(ID^{'} \| K)$ 发送给 tag。第 4 步 tag 通过认证后，将 $ID$ 同步更新为 $ID^{'}$。

Hybrid-Encryption 模型的优势主要在于传送的信息是通过对称加密算法进行加密的，这样可以增强其安全性，减小被破译的风险。由于应用了非对称加密思想，可以适应物联网应用环境的开放性。

Hybrid-Encryption 模型的处理算法复杂度分析如下：首先是 tag 方，tag 收到 $D(R \| K)$ 后解密，DES 算法是一个分组加密算法，它以 64 位为分组对数据加密，一共进行 16 轮完全相同的运算。DES 算法加密解密的时间复杂度均为 $O(n)$，空间复杂度也为 $O(n)$。接着 tag 要计算 Hash( $R \| ID$ )，Hash 算法中的 Hash 函数是一个单向函数，因此 Hash 算法的复杂度就取决与该函数的复杂度，而这个函数可以是不固定的，例如可以利用 DES 来构造 Hash 函数，也可以利用 IDEA 来构造 Hash 函数，所以 Hash 算法的复杂度需要具体情况具体分析。认证过程的最后，tag 还会收到 $D(ID_j \| K)$，解密仍然是 DES 算法。所以 tag 的时间复杂度是：$O(n)$ +Hash 函数的时间复杂度，空间复杂度是：$O(n)$ +Hash 函数的空间复杂度。现在再考虑 reader 的复杂度。Reader 首先用 DES 加密随机数，在收到 tag 返回的 Hash 值后也要计算 Hash 并和返回的 Hash 匹配，之后同样是用 DES 对 $ID_j$ 进行加密。Hash 的匹配一般是通过 Hashtable 进行，其复杂度为 $O(\log 2n)$。因此，reader 的复杂度为：$O(n)$ +Hash 函数的时间复杂度+ $O(\log 2n)$。通过分析，可以看到，该算法在功能上有较好的改进，但是对性能的影响却是有限的。不过由于 tag 上要同时集成 DES 算法和 Hash 算法，所以 tag 的制造成本会有所提高。

## 4 结束语

随着 RFID 系统的应用范围不断扩大，RFID 系统的安全性和保密性显得愈加重要。尽管在 RFID 的安全问题上已经做了不少研究，RFID 系统仍然具有各种各样的安全问题。文中分析了对 RFID 的安全问题，在研讨目前主要安全协议的基础上，给出了一种混合方式的安全模型，并对该模型的有效性和算法复杂度做出了说明。随着科技的不断进步，相信在不久的将来，RFID 的安全问题将得到进一步的提高。

**参考文献：**


[1] 王昭顺，张晓锋. RFID 安全隐患及其解决方案[C]// 2008 国际 RFID 技术高峰论坛论文集. 北京：出版者不详，2008：107-111.

[2] 杨海东，杨 春. RFID 安全问题研究[J]. 微计算机信息，2008(8)：238-240.

[3] 郎为民，刘德敏，李建军. RFID 安全机制研究[J]. 技术前沿，2007(9)：55-58.

[4] 落红卫，程 伟. RFID 安全威胁和防护措施[J]. 电信网技术，2010(4)：38-40.

[5] 周永彬，冯登国. RFID 安全协议的设计与分析[J]. 计算机学报，2006(4)：581-589.

[6] 李 莉，刘建伟. RFID 安全保密技术研究进展[J]. 信息安全与通信保密，2007(8)：165-167.

[7] 彭 昭，刘 威，马选斌，等. RFID 系统安全与隐私问题研究[J]. 微电子学与计算机，2007(8)：129-131.

[8] 祝胜林，杨 波，张明武. RFID 协议及其安全性研究[J]. 信息安全与通信保密，2007(8)：168-170.

[9] Weis S A. Security and Privacy in Radio-Frequency Identification Devices[D]. Massachusetts: Massachusetts Institute of Technology, 2003.

[10] 欧阳麒，蒋兴浩，孙锬锋. 一种基于相互认证的安全 RFID 系统[J]. 信息安全与通信保密，2006(12)：142-144.

[11] Weis S A, Sarma S E, Rivest R L, et al. Security and privacy aspects of low-cost frequency identification systems[C]// Proceedings of the 1st International Conference on Security in Pervasive Computing. Berlin: [s. n.], 2004: 201-212.

[12] Lee S M, Hwang Y J, Lee D H, et al. Efficient authentication for low-cost RFID systems[C]//Proceedings of the International Conference on Computational Science and Its Applications. Berlin: [s. n.], 2005: 619-627.


(上接第 146 页)


2010.

[10] 刘 敏，吕先竞，宋玉忠. 基于 OpenID 的分布式认证系统的设计与实现[J]. 现代情报，2008(6)：90-92.

[11] 张志明，徐建桥，严承华. 基于图像数字水印的身份认证研究[J]. 计算机与数字工程，2006，38(3)：95-97.

[12] 许 峰，林果园，黄 皓. Web Service 的访问控制研究综述[J]. 计算科学，2005，32(2)：1-4.


(上接第 150 页)


程与应用，2010(3)：4-8.

[11] Bayer B. An optimum method for two-level rendition of continuous-tone pictures[C]//IEEE International Conference on Communications. [s. l.]: IEEE, 1973: 11-15.

[12] 廖小涛，张晓林，刘荣科. SPIHT 算法容错性能的分析及改进[J]. 遥测遥控，2003(5)：44-48.