第35卷 第24期 计 算 机 工 程 2009年12月
Vol.35 No.24 Computer Engineering December 2009
·安全技术· 文章编号：1000—3428(2009)24—0156—02 文献标识码：A 中图分类号：TP309

基于 Hash 函数的 RFID 挑战-应答认证协议

余恬恬，冯全源
(西南交通大学信息科学与技术学院，成都 610031)

摘 要：介绍几种典型的射频识别安全隐私保护协议的方法，针对这些协议和一些文献中提出的改进协议中的不足提出一种新的基于 Hash 函数的改进方案，该方案可以有效地抵御非法读取、位置跟踪、窃听、伪装哄骗和重放等不安全问题，并适用于标签数目和阅读器数目较多的情况，具有较好的安全性和高效性。

关键词：射频识别；安全隐私；Hash 函数

RFID Challenge-Response Authentication Protocol Based on Hash Function

YU Tian-tian, FENG Quan-yuan
(School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031)

【Abstract】 This paper introduces several typical methods to against security and privacy problems, and aim at the shortages in them and other improved ones which provided by some literatures, proposes a new improved scheme based on hash function. The modified scheme resists illegal access, tracking, eavesdropping, impersonation and replay attack, fits for the case which the tags and readers number is large and is security and efficiency.

【Key words】 Radio Frequency Identification(RFID); security and privacy; Hash function

1 概述

射频识别(Radio Frequency Identification, RFID)技术是一项利用射频信号通过空间耦合(交变磁场和电磁场)实现无接触信息传递并通过所传递的信息达到识别目的的技术，其最大优点在于非接触，可实现批量读取和远程读取，可识别高速运动物体，可工作在各种恶劣环境中，操作快捷方便。然而，正因为它是通过无线电波来传播信号的，所以会存在许多安全隐私问题，例如非法读取、位置跟踪、窃听、伪装哄骗和重放。

本文考虑的 RFID 系统由标签、阅读器和后台数据库组成。标签与阅读器之间的传输是无线通信方式，因此，标签与阅读器之间的通信是非常不安全的。在固定式 RFID 系统中，一般认为阅读器和后台数据库之间的传输是安全的，然而在很多移动式 RFID 系统中，阅读器与后台数据库之间的通信基本不能达到是安全的。文献[1-5]给出了解决标签与阅读器之间信息传输的问题。然而在许多方案中，有些都是基于阅读器和后台数据库之间的通道是安全的，或者是标签中存有大量的信息而使得计算速率低下。因此，本文针对许多文献中提出的方案的不足之处，在分析几种常用的 RFID 安全隐私保护方法的特点后，提出一种改进方案，该方法基于单向 Hash 函数，使标签与阅读器、阅读器与后台数据库之间的数据传输都是安全的，并且让后台数据库存有所有标签和阅读器的 *ID* 号而防止标签或阅读器存有太多的信息，标签和阅读器的合法性都由后台数据库来验证。GAI 方法不但能有效地抵御所存在的不安全性问题，而且能够适用于标签和阅读器数目较多的环境，具有较好的安全性和高效性。

2 3种典型的基于 hash 函数的认证方案

典型的加强 RFID 安全隐私保护的方法主要有 3 种：Hash 锁，随机 Hash 锁和 Hash 链协议[1-2]，它们都是基于单向 Hash 函数实现的。

2.1 Hash 锁协议

最初时，标签处于锁定状态，标签存储自身的 *ID* 值和经过 Hash 加密后的来代替真实标签 *ID* 号的值 *metaID*，即 *metaID*=Hash(*key*)；后台数据库存储每一个标签的密钥 *key*, *metaID*, *ID*。认证过程如图 1 所示。

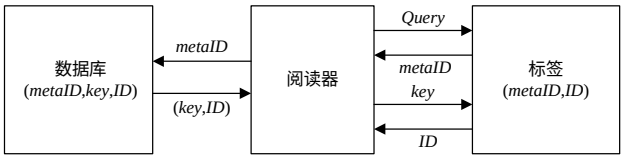

图 1 Hash 锁协议流程

首先阅读器为标识号为 *ID* 的标签产生一个密钥 key，并计算 *metaID*=Hash(key)，将 *metaID* 发送给标签；标签将 *metaID* 存储下来进入锁定状态。同时阅读器把(*metaID*, *key*, *ID*)储存到后台数据库中。在阅读器想询问标签信息时，阅读器向标签发送询问信息，标签回复 *metaID* 给阅读器，阅读器通过查询后台数据库，找到对应的(*metaID*, *key*, *ID*)记录，然

基金项目：国家自然科学基金资助项目(10876029)
作者简介：余恬恬(1986－)，女，硕士研究生，主研方向：RFID，网络信息安全；冯全源，教授、博士生导师
收稿日期：2009-07-10 **E-mail**：ytt10@sina.com

后将 *key* 值发给标签；标签收到 *key* 后就计算 Hash(*key*)，并对比计算的 Hash 值是否与收到的 Hash 值相等，若相等，则标签把自身的 *ID* 值发送给阅读器，此时标签处于解锁状态，并允许阅读器读取它的信息。

该协议利用 Hash 函数来加密传输中的信息，因为解密单向 Hash 函数是不太可能的，所以在一定程度上解决了访问控制的隐私保护。然而，因为每次标签回答的数据都是固定不变的，所以该协议不能防止位置跟踪攻击；并且 *ID* 也以明文的形式通过不安全信道，攻击者很容易得到标签的信息。

2.2 随机 Hash 锁协议

为了解决 Hash 锁协议中位置跟踪问题，将 Hash 锁方法加以改进，就得出了随机 Hash 锁方法，该方法中后台数据库存有所有的标签的 *ID* 号，设为 *ID*1, *ID*2, …, *IDn*。具体验证过程如图 2 所示。

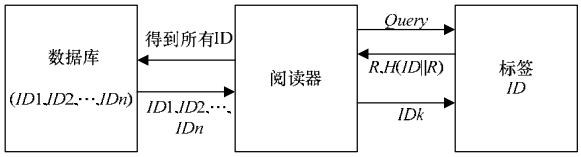

图 2 随机 Hash 锁协议流程

首先，阅读器向标签 *ID* 发送询问信息，标签产生一个随机数 *R*，计算 *H*(*ID*||*R*)，并将(*R*, *H*(*ID*||*R*))数据对发送给阅读器；阅读器收到数据后，从后台数据库中取到所有的标签 *ID* 值，分别计算各个(*R*,H(*ID*||*R*))值，并与收到的(*R*,H(*ID*||*R*))值比较，若有计算的值与收到的值相等，则向标签发送 *IDk*，标签比较收到的 *IDk* 是否与事先保留的 *IDk* 相等，相等则说明阅读器合法，标签就可向阅读器发送自身的信息。

在该方法中，标签每次回答都是随机的，因此，可以防止位置跟踪攻击。然而，此协议不适合有大量标签的情况，因为阅读器需要从所有的 *ID* 标识中查找对应的标签 *ID*，这大大增加了阅读器的计算量。

2.3 Hash 链协议

NTT 实验室提出了一个 Hash 链方法，该协议中的标签集成了 2 个不同的 Hash 函数 *H* 和 *G*。标签和后台数据库都存储了初始值 $S_{i,1}$，同时后台数据库还存储了所有标签的 *ID* 号。认证过程如图 3 所示。

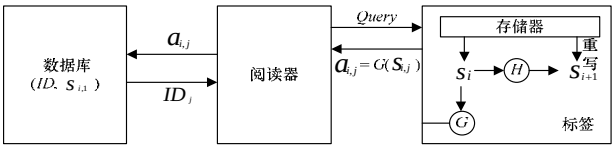

图 3 Hash 链协议流程

对于标签 *ID*，阅读器随机选取一个数 $S_{i,1}$ 发送给标签，并把(*ID*, $S_{i,1}$)存储到后台数据库中。在第 *i* 次数据交换中，阅读器向标签发出询问信息，标签回复 $a_{i,j}=G(S_{i,j})$，并更新 $S_{i+1}=H(S_i)$；阅读器收到 $a_{i,j}$ 后把 $a_{i,j}$ 传给后台数据库，后台数据库有所有的(*ID*, $S_{i,1}$)数据对，为每个标签计算 $a_{i,j}^*=G(H^j(S_{i,1}))$，并比较 $a_{i,j}^*$是否等于 $a_{i,j}$，若相等则返回相对应的 *ID*。

该协议满足了不可分辨性和前向安全性。因为 *G* 是单向函数，非法者无法通过 $a_{i,j}$ 推算出 $S_{i,j}$。*G* 是单向函数，即使非法者能观测到标签输出，也不能将 $a_{i,j}$ 和 $a_{i,j+1}$ 联系起来；因 *H* 也是单向函数，攻击者也无法从 S_{i+1} 推断出 S_i，但每次认证过程中，后台数据库都要对每个 *ID* 进行计算和比较，因此不适合存在大量标签的情况。

3 改进的认证协议

本文鉴于上述介绍的 3 种安全隐私保护方法和一些文献中给出的方案中存在的缺陷，结合几种方法的思想提出一种改进的方案，该方案同样是基于 Hash 函数的，在消息传递过程中，都使用 Hash 函数加密信息，而验证标签和阅读器的有效性都是由后台数据库执行，可以有效抵御非法读取、位置跟踪、窃听、伪装哄骗和重放等不安全问题，适合于标签数目和阅读器数目较多的情况，并且效率高效。

3.1 初始条件

在初始状态下，为了防止标签中存储的数据太多，标签中仅存放自己的 *ID* 号 *IDT*，而阅读器中也只存放自己的 *ID* 号 *IDR*，后台数据库中则存放所有的标签和阅读器的 *ID* 号 *IDT* 和 *IDR*，并且存有相对应的(*IDT*, *h*(*IDT*))数据对和(*IDR*, *h*(*IDR*))数据对，而 *h*(.)是指用 Hash 函数加密过的数据。

3.2 验证过程

基于 Hash 函数的改进的认证协议如图 4 所示。

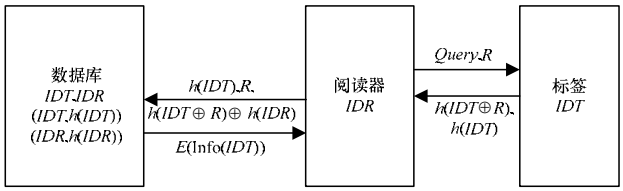

图 4 改进协议的认证过程

具体的验证过程如下：

(1)阅读器首先产生一个随机数 *R* 并向标签发送询问信息 *Query* 和随机数 *R*。

(2)标签利用接收到的 *R* 和自身的 *IDT* 号计算 $h(IDT\oplus R)$(⊕为异或运算)，并发送($h(IDT\oplus R)$，*h*(*IDT*))数据对给阅读器。

(3)阅读器从数据对中提取出 $h(IDT\oplus R)$，然后用 Hash 函数加密自身的 *IDR* 得出 *h*(*IDR*)，利用 $h(IDT\oplus R)$和 *h*(*IDR*)进行异或运算 $h(IDT\oplus R)\oplus h(IDR)$ 并发送 ($h(IDT)$，$R,h(IDT\oplus R)\oplus h(IDR)$)数据对给后台数据库。

(4)后台数据库通过从数据对中提出 *h*(*IDT*)并查找是否有相对应的 *h*(*IDT*)值，若有，则说明标签合法，否则，阅读器则忽略此消息，表明标签不合法；在后台数据库认证标签为合法之后，进行下面的步骤。

(5)后台数据库依据 *h*(*IDT*)得出对应的 *IDT*，然后通过 *IDT* 与收到的 *R* 计算 $h(IDT\oplus R)$，根据这些值从 $h(IDT\oplus R)\oplus h(IDR)$中解出 *h*(*IDR*)，查找是否有相应的 *h*(*IDR*)值，若有，则表明阅读器合法。因此，后台数据库可以通过前面计算出的标签值 *IDT* 查到标签对应的信息发送给阅读器。为了保护信息不外泄，把标签的信息 *Info*(*IDT*)发给阅读器前加密信息成 *E*(*Info*(*IDT*))后再发给阅读器。

4 改进方案的安全性和性能分析

(1)非法读取：只有通过数据库验证标签和阅读器为合法后，数据库才把合法标签的信息发送给阅读器，因此非法阅读器是无法获得标签信息的。

(2)窃听：所有有用的信息都是通过 Hash 函数加密后才传输的，而 Hash 函数是单向散列函数，因此，即使非法者截取信息，也无法解密 Hash 函数而得出信息的真正内容。

(下转第 161 页)