

基于 Hash 函数的轻量级 RFID 双向认证协议

龚海余¹, 李 飞¹, 赵国娟²

(1. 成都信息工程大学信息安全工程学院, 成都 610225; 2. 新疆大学电气工程学院, 乌鲁木齐 830046)

摘 要:通过对轻量级 RFID 系统中基于 Hash 函数认证协议安全性及计算成本等因素进行研究, 分析了目前该类协议存在的安全缺陷和计算成本。通过对协议的改进, 提出了一种轻量级 RFID 双向认证协议, 在满足同等安全性能的前提下, 减轻了标签的计算成本, 提高了标签的计算性能, 并通过 BAN 逻辑形式化证明了协议的安全认证过程。通过 51 单片机与天线模块仿制电子标签进行实验, 从安全性、隐私性、协议性能等因素与其他基于 Hash 函数的协议比较。实验表明, 本协议认证过程时间更短, 并当数据库标签数量越多, 改进协议的计算成本优越性较其他协议越突出, 具有一定的实用价值。

关键词:RFID; Hash 函数; BAN 逻辑; 认证协议; 标签

中图分类号:TP368

文献标志码:A

引 言

无线射频识别(Radio Frequency Identification, 简称 RFID)是一种非接触的自动识别技术, 是物联网核心技术之一。在最近几年, 物联网技术迅速发展, 已经在物流、交通运输、医疗、批发零售、设备资产管理、食品安全等方面取得了较好的应用。与此同时, RFID 的安全性问题也备受关注。由于 RFID 的计算能力跟存储能力有限, 这种硬件上的局限性决定了标签不可能实现复杂的运算^[1]。针对 Hash 函数的 RFID 认证协议, 从 Sarma 提出 Hash - Lock 协议至张捍东等前人对协议的不断改进, 协议从没有加密机制到可以抵制重放攻击与对标签的跟踪等攻击, 但受限于标签硬件因素, 还是存在计算成本大、安全性能差、大量标签认证时间长等缺点。通过对前人协议的分析, 提出了一种改进协议, 并通过实验验证结果。

1 RFID 系统简介

RFID 系统主要由三部分组成^[2], 包括后台数据库(Database, 简称 DB)、读写器(Reader)、标签(Tag)三部分, 如图 1 所示。

DB 一般是指数据处理服务器, 其具有强大的数据处理和存储能力。与 DB 连接的 Reader, 其功能是传递 DB 与 Tag 之间的数据, 一般不具有数据处理能力或者有较小的运算能力。而 Reader 与 Tag 之间的通信则是 RFID 系统的关键。Tag 一般是通过空中接口与 Reader 通信, 因空中接口的开放性及标签的低数据处理导致了通信信息的泄露, 且低成本 RFID 标签的最多只包含 10 000 个以内的逻辑门电路, 而用于安全机制的门电路基本在 3000 个左右^[3]。这些硬件上的局限性对 RFID 系统安全机制的设计要求提出了挑战。设计一种安全、低成本和高效的 RFID 认证协议引起了广大学者的探讨。

收稿日期:2015-06-26

作者简介:龚海余(1989-), 男, 湖南娄底人, 助教, 硕士, 主要从事物联网安全方面的研究, (E-mail)1243024108@qq.com;

李 飞(1966-), 男, 湖南常德人, 教授, 硕士, 主要从事物联网技术、网格计算方面的研究, (E-mail)512960520@qq.com

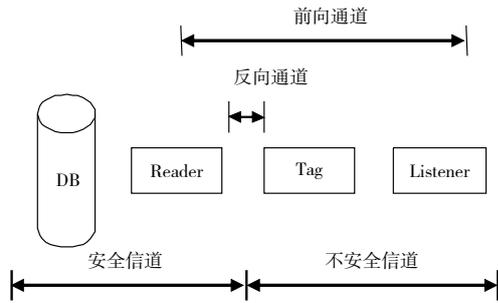


图1 RFID系统结构

2 RFID认证协议的安全问题

RFID系统在满足安全性条件下,需要考虑诸多因素。首先,协议必须能够对RFID系统的数据流提供有效的保护;而对于低成本、计算资源和存储受限的标签,协议所需要的通信量及计算量等性能指标也是必须考虑的因素^[4-6]。

3 基于Hash函数的RFID认证协议分析

3.1 基于Hash函数的安全通信协议的问题

Sarma等人^[7]提出的采用Hash函数的RFID认证协议,显然存在很多漏洞。其以明文方式传输不可取,标签易被跟踪、窃听,因此可以克隆标签进行重放攻击,还可进行中间人攻击、拒绝服务攻击;而Weis提出随机Hash-Lock协议,该协议在Hash-Lock协议的基础上增加了Hash函数与伪随机数发生器,通过增加标签成本换取标签不易被跟踪等问题,且阅读器需计算所有标签的Hash值,不但增加了阅读器的成本,同时也严重影响标签识别的效率;NTT实验室提出的基于Hash链的安全协议,很显然,当标签数量为 n 时,该协议要为每个标签计算 $2n$ 个Hash函数,计算和比较次数都比较大,不适合大量标签的情况;陈雁飞等^[8]提出的Reader_Tag安全协议,该协议将随机数移到后台,降低了标签的复杂性,且前向通道安全,相对于随机Hash-Lock协议,机器运算负载减少很多,效率明显提高,并且实现了身份的双向认证,有效实现了安全隐私保护。但每个标签保存两条记录,不利于标签数量过多的情形,且标签的计算量还是对标签的成本是个考验;张捍东等人^[9]提出的RFID安全协议,虽然协议设计的比较完善,但协议认证过程复杂,阅读器有计算和存储功能,通过阅读器的计算和存储能力换取安全性能。其次,对重放攻击抵抗能力不强。

本文在众多协议的基础上,提出基于Hash函数的改进型的安全认证协议。

3.2 改进后的安全通信协议

改进协议结构如图2所示。

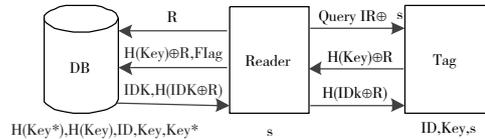


图2 改进之后的协议

前提假设:数据库与阅读器之间的有线信道为安全信道,而阅读器与标签之间的空中接口部分为不安全信道;协议中的Hash函数为安全函数;为了加快查询数据,根据文献^[10-11]中的建议,在 $H(Key)$ 上建立特殊索引。

Flag的定义:一般情况下, $Flag = 0$;当记录根据 $H(Key)$ 没有找到时, $Flag = 1$,根据 $H(Key^*)$ 查找,并将本次访问的时间等因素记录到日志文件,供今后的安全分析使用。

锁定标签:该协议DB中保存有:标签ID、更新之前的Key与 $H(Key)$ 、更新之后的 Key^* 与 $H(Key^*)$;标签中也同时写入标签ID、Key、s;阅读器中保存有s。

解锁标签:

(1) 阅读器发送随机数R给数据库DB,并把查询字段Query, $R \oplus s$ 发给标签Tag。

(2) 标签Tag把 $R \oplus s$ 与s异或得到R,计算 $H(Key) \oplus R$,并由阅读器转发给数据库。

(3) 数据库接口计算 $H(Key) \oplus R \oplus R$ 得到 $H(Key)$,根据 $H(Key)$ 查找数据库(Flag默认为0)。

① 如果能查找到一条记录,则把查找到的记录的IDk与R计算得到 $H(IDk \oplus R)$,并把IDk、 $H(IDk \oplus R)$ 发给阅读器Reader,同时数据库信息更新为: $H(Key^*) = H(H(Key \oplus R))$, $H(Key) = H(Key^*)$, $ID, Key = Key^*$, $Key^* = H(Key \oplus R)$ 。更新完成后进入步骤(4)。

② 若此次查询没有查找到数据,则标志位 $Flag = 1$,则根据 $H(Key^*)$ 查找,若查到一条记录,按前面的操作,并把相关数据记录并保存到日志文件中。若没有查到数据就中断通信。

(4) 阅读器Reader把 $H(IDk \oplus R)$ 发给标签Tag,然后标签根据自身存储的ID、R,计算 $H(ID \oplus R)$ 。如

果 $H(ID)$ 与传过来的 $H(IDk)$ 不相等,则结束通信;如果相等,更新 $Key = H(Key \oplus R)$; 如果迟迟没有接收到消息或者消息为不正确,则不更新 Key 。

此认证协议在数据库中的记录数减半,不但提高了查找的速度,而且标签计算也大大减小。

为了证明改进协议的先进性和安全性,下面采用 BAN 形式化语言分析与验证。

4 BAN 分析及改进协议的演示

4.1 BAN 分析

(1) 根据网络安全协议形式化分析与验证的基本方法,通过简化本协议,提炼出了本安全协议的基本模型:① $A \rightarrow B$: A 向 B 发送请求 Query; ② $B \rightarrow A$ 发送 $H(Key)$ 应答; ③ A : A 收到 $H(Key)$ 之后,查找数据库找到相同的记录,确定 B 的合法性; ④ $A \rightarrow B$: A 向 B 发送 $H(IDk)$; ⑤ B : B 根据自身的 ID , 通过计算得到 $H(ID)$, 比较 A 发来的 $H(ID)$, 确认 A 的合法性;

(2) 使用 BAN 形式证明理论,通过对协议过程省略和抽象,仅保留与安全分析有关的内容,协议形式化简化如下:

$$\textcircled{1} A \triangleleft \{Key, R\} k; \quad \textcircled{2} B \triangleleft \{ID, R\} k;$$

(3) 本安全认证协议的初始化假设:

$$\textcircled{1} A \equiv A \xleftarrow{k} B;$$

$$\textcircled{2} B \equiv B \xleftarrow{k} A;$$

$$\textcircled{3} A \equiv \#(R);$$

$$\textcircled{4} B \equiv \#(R);$$

$$\textcircled{5} A \equiv B \rightarrow Key;$$

$$\textcircled{6} B \equiv A \rightarrow ID.$$

(4) BAN 分析本改进协议的目标:

$$\textcircled{1} A \equiv Key;$$

$$\textcircled{2} B \equiv ID.$$

(5) 本协议推理过程:

① 当 $A \triangleleft \{Key, R\} k$ 时,由假设 $A \equiv A \xleftarrow{k} B$ 和消息含义规则

$$\frac{P \equiv \#(X), P \triangleleft \{x\}}{P \equiv Q \mid \sim X} \text{ 可以得出:}$$

$$A \equiv B \mid \sim (Key, R);$$

② 由已知假设 $A \equiv \#(R)$ 和新鲜规则 $\frac{P \equiv \#(X)}{P \equiv \#(X, Y)}$ 可以得出 $A \equiv \#(Key, R)$, 再由临时验

$$\text{证规则 } \frac{P \equiv \#(X), P \equiv Q \mid \sim X}{P \equiv Q \mid \sim X} \text{ 可以得出 } A \equiv B \equiv$$

$$(Key, R), \text{ 再由消息信念规则 } \frac{P \equiv Q \equiv (X, Y)}{P \equiv Q \mid \sim X} \text{ 可以得}$$

出 $A \equiv B \equiv Key$;

③ 由假设条件 $A \equiv B \rightarrow Key$ 和管辖权规则 $\frac{P \equiv Q \mid \Rightarrow X, P \equiv Q \mid \equiv X}{P \equiv X}$, 可以得出 $A \equiv Key$ 。

同理,可以推理得出 $B \equiv ID$ 。阅读器与 Tag 之间可以通过双向相互认证,从而能够信用对方。因此达到了认证的目的。

4.2 改进协议的演绎

假设数据库中存储一条记录,见表 1。

表 1 数据初始化

$H(Key^*)$	$H(Key)$	ID	Key	Key^*
$H(A)$	$H(A)$	1	A	A

解释:初始化时,标签的 ID 为 1, Key 与 Key^* 相等。 $H(Key^*)$ 与 $H(Key)$ 相等。同时,相应的标签初始化为 $ID = 1, Key = A, Flag = 0$ 。

阅读器给数据库 DB 发送随机数 R , 同时,阅读器加上认证查询 Query, 连同 $R \oplus s$ 一起发给标签 Tag。Tag 计算 $H(Key) = H(A)$, $H(A)$ 与随机数 R 异或得到 $H(A) \oplus R$, 由阅读器转发给数据库。数据库得到 $H(A) \oplus R$ 与 R 异或, 即: $H(A) \oplus R \oplus R = H(A)$, 再根据 $Flag = 0$ (默认), 通过 $H(A)$ 查找数据库表, 得到 $ID = 1, Key = A$, 能找到记录说明标签为合法标签, 标签认证过程结束。根据通过认证得到的记录 $(1, A)$ 和 r 计算 $H(1 \oplus r)$, 然后通过阅读器转发 $H(1 \oplus R)$ 给标签 Tag。如果找不到记录, 认证结束, 发送 EOF 由阅读器转发给标签。而此时, 数据库中的数据将发生变化, 见表 2。

表 2 数据库中数据变化后的结果

$H(Key^*)$	$H(Key)$	ID	Key	Key^*
$H(H(A \oplus R))$	$H(Key^*)$	1	A	$H(A)$

当标签 Tag 接收到 $H(1 \oplus R)$ 后, 标签 Tag 根据与自己计算的 $H(1)$ 是否相等。如果相等, 则阅读器通过验证, 更新标签 Tag 中的 $Key = H(A \oplus R)$, 标签解锁, 开放标签中数据段中的数据。如果接收到 EOF 或者根本没有接收到信号, 标签不更新 Key 。

特别说明: 当下次验证时, 如果是 $Flag = 0$, 则根据 $H(Key)$ 查找到 IDk, Key 。如果是 $Flag = 1$, 则根据 $H(Key^*)$ 查找 IDk, Key^* 。

5 改进协议验证及性能分析

5.1 实验验证

实验环境及过程:通过开发板上的 51 单片机加天线模块构成标签进行实验,当上位机程序接收到阅读器发送的随机数 R 进行定时开始,到阅读器正常认证后通过串口通知上位机作为一次认证过程。上位机累加时间差通过计算得到单个标签的平均认证时间(表 3),并通过标签进行多次认证分析得知:当数据库中存有标签数量越多(通过生成随机数的方式快速插入数据库导致数据记录条数增多),单个标签的查询性能提高越明显。

表 3 各种基于 Hash 函数的 RFID 安全协议的平均认证时间

基于 Hash 函数的 RFID 安全协议	认证时间/ms
Hash - Lock	28.7
随机 Hash - Lock	32.3
Reader - Tag 安全协议	36.9
基于 Hash 的 RFID 安全协议的研究	36.2
改进协议	33.1

从本实验数据中发现,Hash - Lock 协议认证简单,认证时间短,但有很大的安全问题。随机 Hash - Lock 把数据计算转移到阅读器,较 Hash - Lock 协议有一定的安全性。通过与 Reader - Tag 安全协议和基于 Hash 的 RFID 安全协议的研究中的方法进行比较发现,本协议的平均认证时间比这两种协议都短,且安全性能比两者都高,从而证明了本协议的优越性。从上面的认证过程发现,改进协议的电子标签计算成本也是有很大优越性的,几种协议的计算成本见表 4。

表 4 电子标签的计算成本与存储成本对比

基于 Hash 的 RFID 安全协议	Tag 的计算成本
Hash - Lock	1 + 0
随机 Hash - Lock	2 + 1
Reader - Tag 安全协议	4 + 0
改进协议	2 + 0

注:Tag 的计算成本包括 Hash 函数计算次数 + 随机数发生器产生次数

5.2 性能分析

5.2.1 安全性分析

改进协议是在陈雁飞等的基础上提出的,改进后的协议能抵抗假冒攻击、重放攻击、中间人攻击、通信数据流分析攻击,满足一定的安全需求。

5.2.2 隐私性分析

改进协议的数据流都采用 Hash 单向散列函数进行加密,且每次数据流的内容都会发生改变,不存在跟踪

标签,非法访问标签数据信息泄漏隐私等情况。

5.2.3 协议性能分析

改进协议最大的特点就是满足大量标签识别的情况。通过对协议的改进和后台数据库的重新设计,不仅大大提高了数据查询的速度,而且减少了标签存储成本。

6 结束语

本协议是在基于 RFID 系统的 Reader - Tag 安全协议上提出的改进协议,在此基础上不但重新设计了数据库,并且充分利用了两个性质:(1)每次验证绑定随机数使得每次通信的内容不同;(2)利用 $A \oplus B \oplus B = A$ 的性质达到安全通信的目的。改进协议具有运算成本低、标签负载小、认证效率高、安全性好等优点,是一种实用的算法。实验表明:随着数据库中标签数量的增多,它的优越性就更能表现出来。另外,本协议也有不足之处:(1)本认证协议因为在 Reader - Tag 协议的基础上改进的,实际应用过程中的诸多因素的干扰没有考虑,但不会影响本协议针对大量标签结果的趋势;(2)本协议如果 s 被内部人员利用,通过多次重放攻击,可以导致失步现象。以上不足之处在接下来的工作中重点解决。

参考文献:

- [1] 金永明,吴棋滢,石志强,等.基于 PRF 的 RFID 轻量级认证协议研究[J].计算机研究与发展,2014,51(7):1506-1514.
- [2] 于广威,何文才.基于 RFID 技术的身份识别系统的设计与实现[J].通信技术,2010,43(4):106-108.
- [3] 林贵彬,王永华,詹宜巨.一种基于随机序列的 RFID 安全协议[J].计算机工程,2008,34(20):151-156.
- [4] 伍新华,唐翠婷.一种基于 Hash 的 RFID 双向认证协议[J].武汉理工大学学报:交通科学与工程版,2011,35(3):571-574.
- [5] 丁振华,李锦涛,冯波.基于 Hash 函数的 RFID 安全认证协议研究[J].计算机研究与发展,2009,46(4):583-592.
- [6] 张兵,马新新,秦志光.轻量级 RFID 双向认证协议设计与分析[J].电子科技大学学报,2013,42(3):425-430.
- [7] 曾丽华,熊璋.Key 值更新随机 Hash 锁对 RFID 安全隐私的加强[J].计算机工程,2007,33(3):151-154.
- [8] 陈雁飞,马成勇,杨慧.基于 RFID 系统的 Reader-Tag

- 安全协议的设计及分析[J].计算机与数字工程, 2008,36(9):128-131.
- [9] 张捍东,丁磊,岑豫皖.基于 Hash 函数的 RFID 安全协议研究[J].计算机工程与设计,2013,34(11):3766-3769.
- [10] 赵海,欧阳元新,熊璋.用于 RFID 中间件的主存数据库索引结构[J].华中科技大学学报:自然科学版, 2012,40(S1):91-94.
- [11] Wang Wenchuang, Wang Keren. RFID Protocols Based on Data Buffer Mechanism [J]. Information and Electronic Engineering,2008,6(5):372-378.
- [12] Luo Zongwei,Zhou Shijie,Li Jenny.Enhancement of a Lightweight RFID Security Protocol[J].Journal of University of Electronic Science and Technology of China, 2007,36(6):1172-1178.

The Duplex Authentication Protocol of Lightweight RFID Based on Hash Function

GONG Haiyu¹, LI Fei¹, ZHAO Guojuan²

(1. School of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China;

2. College of Electrical Engineering, Xinjiang University, Urumchi 830046, China)

Abstract: Through the research on security and calculation cost and other factors of authentication protocol base on hash function in lightweight radio frequency identification(RFID) system, the security defects and computational cost of this kind of protocol are analyzed. Through the improvement of the protocol, a kind of lightweight RFID mutual authentication protocol is proposed. When it meets the condition of the same security property, the calculation cost of the tag is reduced, and the calculation performance of the tag is improved. And the safety certification process of the protocol is proved through the BAN logic formalization. Then through the experiment of the 51 ECU and antenna module to copy electronic tag, it was compared with other protocols which based on Hash function from the security, privacy, agreement and other factors. The experiments show, the authentication process time of this protocol is shorter, and the more tags in the database, the better superiority of the improved protocol's calculate cost. So, this protocol has a certain practical value.

Key words: RFID; hash function; BAN logic; authentication protocol; tag