基于动态共享密钥的移动 RFID 双向认证协议

王国伟,贾宗璞,彭维平
(河南理工大学计算机科学与技术学院,河南焦作 454000)

摘 要: 针对移动无线射频识别认证协议面临的身份认证和隐私保护、动态密钥安全更新和去同步化攻击问题,提出一种可动态更新共享密钥的移动 RFID 双向认证协议. 协议基于 Hash 密码机制,利用随机数同时进行密钥安全更新和身份认证,并采用对分表存储的当前和历史共享密钥进行动态添加和删除的方法,保留最后一次合法认证后的一致共享密钥. 安全性能分析与效率分析表明,该协议能够实现动态密钥安全更新和身份认证、能够在遭受去同步化攻击后保证密钥同步,且具有较强的计算和存储性能. 通过和同类 RFID 认证协议比较,协议弥补了同类 RFID 协议存在的不足,适用于被动式标签数量庞大的 RFID 系统.

关键词: 无线射频识别; 移动; 认证协议; 动态共享密钥
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2017)03-0612-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.03.016

A Mutual Authentication Protocol of Mobile RFID Based on Dynamic Shared-Key

WANG Guo-wei, JIA Zong-pu, PENG Wei-ping
(*School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, Henan* 454000, *China*)

Abstract: In order to solve the problems about identity authentication, privacy protection, dynamic shared-key updating and de-synchronization that emerged in mobile radio frequency identification (RFID) authentication protocols, the paper proposes a mutual authentication protocol of mobile RFID whose shared-key can be updated dynamically. Based on Hash cryptography, the proposed protocol uses pseudo-random number to perform simultaneous operations on secure shared-key updating and identity authenticating, then uses a method of dynamic deletion and addition of shared-key that respectively stored in current data table and historic data table to reserve the coherency of shared-key among backend server, reader and tag after the latest legal authentication. The securities and efficiencies analysis show that the protocol can achieve secure updates of dynamic shared-key, identity authentication and shared-key synchronization after being attacked, and in addition, the proposed protocol has strong computation and storage abilities. Compared with other similar mobile RFID protocols, the proposed protocol can make up for the deficiency of these protocols, which is suitable for RFID systems with a large number of passive tags.

Key words: radio frequency identification (RFID); mobile; authentication protocol; dynamic shared-key

1 引言

由于无线射频识别(Radio Frequency Identification, RFID)系统中标签的计算能力和存储空间有限,使得身份认证和隐私保护成为 RFID 系统面临的严重安全威胁[1~3]. 传统的 RFID 系统中,固定式阅读器和后台数据库以有线的方式进行安全通信,而在移动 RFID 系统中,可移动阅读器、后台数据库和标签之间均以无线方式进行不安全通信[4]. 因此,移动 RFID 系统面临的安全风险更加严重和多样化. 解决 RFID 系统安全问题常用的方法是设计安全有效的 RFID 认证协议. 然而,国内外学者提出的认证协议大多是针对传统 RFID 系统,不能适用于移动 RFID 系统. 而在移动 RFID 认证协议中,动态更新共享密钥的机制存在数据同步问题[5]. 此外,如果更新共享密钥的参数不具备机密性,则会带来密钥泄漏的风险. 基于上述问题,本文基于 Hash 密码机

收稿日期:2015-05-29 修回日期:2015-11-09;责任编辑:梅志强
基金项目:河南省科技攻关项目(No. 132102210123);河南省教育厅重大科技攻关项目(No. 13A520321)

制,提出一种可动态更新共享密钥的移动 RFID 双向认证协议.

2　相关研究工作

2004 年,Ohkubo M 等人[6]提出的 Hash 链协议采用动态更新标签 ID 的机制,本质上属于动态共享秘密的认证协议. 但文献[7]认为,Hash 链协议是单向认证协议,只能对标签进行认证,不能对阅读器进行认证,敌手可通过伪装阅读器进行合法认证,也不能防范重放攻击. 此外,由于标签收到阅读器的认证请求后立即更新密钥,当出现通信异常或者遭受攻击时,则会造成后台数据库不更新密钥,因此易遭受去同步化攻击.

2011 年,Cho 等人[8]提出了基于匹配算法的动态密钥 RFID 认证协议、Yeh 等人[9]提出了基于二次剩余定理的动态密钥 RFID 认证协议. 这两种协议均采用同样的方式防范去同步化攻击,其核心思想为:发生去同步化攻击后,下一次认证则比较标签的当前密钥和后台数据库存储的前一次认证成功时的密钥,如果二者相等,则标签通过认证. 然而,当出现连续 2 次或者 2 次以上去同步化攻击时,这种方式会造成共享密钥不一致从而使标签无法通过认证. 此外,文献[10]认为这两种协议无法保障阅读器的匿名性.

2011 年,Sandhya 等人[11]提出了单向认证的动态密钥移动 RFID 认证协议. 在协议的步骤 3 中,阅读器发送的由 Hash 函数加密的阅读器标识信息 $H(\mathrm{ID}_R)$ 在每次认证过程中均保持不变,且在步骤 4 中,阅读器没有对后台数据库进行认证,而是直接解密数据并将其回传标签. 因此,截获 $H(\mathrm{ID}_R)$ 后,敌手可伪造阅读器并通过认证,后台数据库则更新共享密钥为 $K_{i+1}=\mathrm{PRNG}(K_i)$,然而在标签认证阅读器时,由于伪造阅读器无法通过认证,标签将不更新密钥并结束协议. 因此协议存在中间人攻击和重放攻击威胁.

2013 年,Lee 等人[12]提出了基于 Hash 锁的动态密钥移动 RFID 认证协议. 协议中,敌手可在 step2 中截获标签和后台数据库存储的随机挑战 α^i. 截获 α^i 后,敌手可伪造标签使合法阅读器获得上次认证时合法标签的密码 PWD 和身份标识 $\mathrm{ID}_{\mathrm{tag}}$,其中 PWD 用于解锁合法标签,$\mathrm{ID}_{\mathrm{tag}}$ 用于读取和显示标签的数据信息. 当伪造标签和相应的合法标签在阅读器信号范围内时,敌手可通过伪造的第三方标签欺骗合法阅读器解锁并显示合法标签的信息,因此协议不能防范标签伪造且存在中间人攻击和重放攻击威胁. 此外,在协议的 step3 中,如果发生去同步化攻击将会造成后台数据库和标签中存储的 α^{i+1} 不一致,因此协议还存在去同步化攻击漏洞.

2014 年,刘鹏等人[13]提出了阅读器、标签和后台数据库相互认证的移动 RFID 认证协议. 协议中,后台数据库需对认证信息进行逐一计算和比较才能确认标签和阅读器的合法性. 当标签认证信息非法时,后台数据库需要对全部的标签进行 Hash 计算和比较才能确认其非法. 当敌手通过噪音阅读器向后台数据库持续发送虚假认证信息时,后台数据库将一直处于大负荷工作状态进而影响正常标签的认证,因此协议易遭受拒绝服务攻击.

3　本文协议

3.1　初始条件及符号说明

本文提出的认证协议基于以下假设:

(1)标签只有有限的计算能力和存储空间,后台数据库和阅读器具有较强的计算和存储性能.

(2)阅读器与后台数据库之间、阅读器与标签之间的通信信道均不安全.

(3)协议中所使用的单向 Hash 函数和伪随机数是安全的.

系统初始化时,每个标签和阅读器中分别存储与后台数据库的共享密钥,并包含相同单向 Hash 函数和伪随机数生成器;后台数据库中的当前信息表和历史信息表中均初始化与标签和阅读器相一致的首次共享密钥.

系统初始化时,后台数据库设置四张数据表分别用于存储标签\阅读器与后台数据库的当前和历史共享密钥以及身份标识等信息,其数据表结构和字段及说明如表 1 所示.

表 1　后台数据库数据表结构

表名	字段名	说明
Tag_c_au	Tag_id	标签 ID,主键
Tag_c_au	Tag_c_key	标签当前共享密钥
Tag_c_au	H_id_key	标签 ID 的密钥 Hash 码
Tag_h_au	Tag_id	标签 ID
Tag_h_au	Tag_h_key	标签历史共享密钥
Tag_h_au	H_id_key	标签 ID 的密钥 Hash 码
Reader_c_au	Reader_id	阅读器 ID,主键
Reader_c_au	Reader_c_key	阅读器当前共享密钥
Reader_h_au	Reader_id	阅读器 ID
Reader_h_au	Reader_h_key	阅读器历史共享密钥

认证协议所使用的符号定义及说明如表 2 所示.

表 2 符号定义及说明

符号	说明
$H_k(\ )$	单向哈希函数
$\mathrm{PRNG}_k(\ )$	伪随机数
$E_k(\ )$	对称加密算法
ID_t	标签的 ID 标识
ID_r	阅读器的 ID 标识
S_t	标签产生的随机数
S_r	阅读器产生的随机数
K_t^i	标签与后台数据库的当前共享密钥
K_t^{i+1}	标签与后台数据库更新后的共享密钥
K_r^i	阅读器与后台数据库的当前共享密钥
K_r^{i+1}	阅读器与后台数据库更新后的共享密钥
$\parallel$	连接运算
$\oplus$	异或运算
Query	认证请求

3.2 认证流程

协议认证流程如图 1 所示：

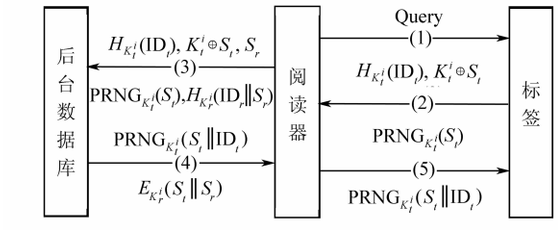


图1 认证基本流程

步骤 1 阅读器向标签发送认证请求 Query.

步骤 2 标签产生随机数 S_t 并计算 $H_{K_t^i}(\mathrm{ID}_t)$、$K_t^i\oplus S_t$ 和 $\mathrm{PRNG}_{K_t^i}(S_t)$，然后将 $H_{K_t^i}(\mathrm{ID}_t)$、$K_t^i\oplus S_t$ 和 $\mathrm{PRNG}_{K_t^i}(S_t)$ 发送给阅读器.

步骤 3 阅读器生成随机数 S_r，计算 $H_{K_t^i}(\mathrm{ID}_r\parallel S_r)$，然后将 $H_{K_t^i}(\mathrm{ID}_t)$、$K_t^i\oplus S_t$、$\mathrm{PRNG}_{K_t^i}(S_t)$ 和 S_r 以及 $H_{K_t^i}(\mathrm{ID}_r\parallel S_r)$ 发送给后台数据库.

步骤 4 后台数据库分别对阅读器和标签进行身份认证和密钥更新.

(1)认证阅读器：后台数据库遍历 Reader_c_au 表，计算每个 $H_{K_t^i}(\mathrm{ID}_r\parallel S_r)$ 并和接收到的 $H_{K_t^i}(\mathrm{ID}_r\parallel S_r)$ 进行比对，若存在某一条记录使比对成立，则阅读器合法；若没有记录使对比成立，则遍历 Reader_h_au 数据表，计算每个 $H_{K_t^i}(\mathrm{ID}_r\parallel S_r)$ 并和接收到的 $H_{K_t^i}(\mathrm{ID}_r\parallel S_r)$ 进行比对，若存在某一条记录使对比成立，则阅读器合法；若没有任何记录使对比成立，则阅读器非法，认证失败.

(2)认证标签：阅读器通过认证后，①后台数据库根据 $H_{K_t^i}(\mathrm{ID}_t)$ 查询 Tag_c_au 表，若检索到结果，则取出 K_t^i，计算 $S_t=K_t^i\oplus S_t\oplus K_t^i$，然后进行 $\mathrm{PRNG}_{K_t^i}(S_t)$ 运算，并和接收到的 $\mathrm{PRNG}_{K_t^i}(S_t)$ 进行比较，若二者相等，则标签合法；若不相等，则标签非法，认证结束；②若在 Tag_c_au 表检索不到结果，则查询 Tag_h_au 表，若检索到结果，则取出 K_t^i，计算 $S_t=K_t^i\oplus S_t\oplus K_t^i$ 和 $\mathrm{PRNG}_{K_t^i}(S_t)$，最后将运算结果和接收到的 $\mathrm{PRNG}_{K_t^i}(S_t)$ 进行比较，若二者相等，则标签合法，否则标签非法，认证结束；③如果在 Tag_h_au 表中检索不到结果，说明标签非法，认证失败.

(3)更新密钥：在阅读器和标签均通过认证的情况下，后台数据库分别进行标签和阅读器的共享密钥更新：①更新阅读器密钥：计算 $K_r^{i+1}=\mathrm{PRNG}_{S_t}(K_r^i)$，并将 Reader_c_au 中 ID_r 对应的当前共享密钥更新为 K_r^{i+1}；根据步骤 4 进行一致性比较的数据表进行判断和操作：如果是 Reader_c_au 表，则删除该表中和阅读器对应的数据，并将 K_r^i 和 ID_r 添加到表中. ②更新标签密钥：计算 $K_t^{i+1}=\mathrm{PRNG}_{S_t}(K_t^i)$，并将 Tag_c_au 中 ID_t 对应的当前共享密钥更新为 K_t^{i+1}、标签 ID 的 Hash 码更新为 $H_{K_t^{i+1}}(\mathrm{ID}_t)$；根据步骤 4 查询 ID_t 的来源数据表进行判断和计算：如果是 Tag_c_au 表，则删除表中该标签对应的数据，然后将 K_t^i、ID_t 和 $H_{K_t^i}(\mathrm{ID}_t)$ 添加到该表中.

(4)后台数据库使用 K_r^i 加密 $E_{K_r^i}(S_t\parallel S_r)$，并将 $E_{K_t^i}(S_t\parallel S_r)$ 和 $\mathrm{PRNG}_{K_t^i}(S_t\parallel\mathrm{ID}_t)$ 转发给阅读器.

步骤 5 阅读器使用 K_r^i 得到 $S_t\parallel S_r=E_{K_r^i}^{-1}(S_t\parallel S_r)$，然后和原来的随机数 S_r 进行比较，若二者相等，则后台数据库通过认证，阅读器使用 S_t 更新共享密钥为 $K_r^{i+1}=\mathrm{PRNG}_{S_t}(K_r^i)$，并发送 $\mathrm{PRNG}_{K_t^i}(S_t\parallel\mathrm{ID}_t)$ 给标签；若二者不相等，则认证失败.

标签接收到数据后，计算 $\mathrm{PRNG}_{K_t^i}(S_t\parallel\mathrm{ID}_t)$ 并和接收到的 $\mathrm{PRNG}_{K_t^i}(S_t\parallel\mathrm{ID}_t)$ 进行比较，若二者相等，则阅读器合法，标签更新共享密钥为 $K_t^{i+1}=\mathrm{PRNG}_{S_t}(K_t^i)$；若二者不等，则认证失败. 至此认证结束.

4 协议安全性能和效率分析

4.1 安全性能分析

(1)机密性. 认证过程中，标签的 ID_t 和 K_t^i 以及阅读器的 ID_r 和 K_r^i 均通过加密形式传输，由于单向 Hash 函数和伪随机数的安全性，敌手即便截获这些信息的密文，也无从得知阅读器和标签的标识信息 ID_t 和 ID_r 以及密钥信息 K_t^i 和 K_r^i. 此外，标签产生的随机数 S_t 也以密文形式进行传输，因此标签产生的随机数 S_t 具有机密性，当后台数据库、阅读器和标签使用 S_t 更新共享密钥时，可以保证更新后的密钥具有机密性和随机性

且不能通过截获的数据计算得出.

(2)位置追踪. 认证过程中传输的数据均由随机数 S_t 和 S_r 直接或间接参与,且后台数据库与标签/阅读器的共享密钥由上一次认证的随机数生成,因此所有传输数据均有随机性. 由于随机数的相异性使得标签响应的数据在每次认证过程中均不相同,敌手即便截获了传输的数据也无法判断是哪个标签在哪次认证过程中产生,因此协议可以有效防止因标签固定输出带来的位置追踪问题.

(3)前向安全性. 认证过程中传输的认证数据由随机数 S_t 和 S_r 直接参与,因此敌手不可能通过本次认证的数据计算得出上一次的认证数据. 此外,在标签响应的 $H_{K_t^i}(\mathrm{ID}_t)$ 中,虽然 ID_t 是固定的,但 S_t 的保密性和随机性使得 K_t^i 也是一个随机的保密值,因此,敌手无法通过本次认证的数据推导出上次认证时的数据,协议具有前向安全性.

(4)重放攻击. 在认证过程中,后台数据库分别存储了与阅读器/标签的共享密钥. 以标签为例,假设敌手截获当前认证过程中的数据后构造数据进行重放攻击:敌手可使用 $H_{K_t^i}(\mathrm{ID}_t)$、构造 M_1 和 M_2 后向阅读器进行响应,阅读器将这些信息转发给后台数据库后通过 Tag_h_au 表存储的历史记录可以检索出 K_t^i,之后取出 K_t^i 进行 $\mathrm{PRNG}_{K_t^i}(K_t^i \oplus M_1)$ 运算并比较 $\mathrm{PRNG}_{K_t^i}(K_t^i \oplus M_1)$ 和 M_2 是否一致. 由于上次认证时 K_t^i 保密且是随机数,同时随机数运算 PRNG( )是安全的,因此敌手不可能构造出使比较成立的 M_1 和 M_2,此时协议因比较不成立而结束. 因此,协议可以防范重放攻击.

(5)去同步化攻击. 在认证过程中,如果是从当前数据表 Tag_c_au\Reader_c_au 中得出结果,说明标签\阅读器和后台数据库的共享密钥一致,即上一次认证过程没有发生去同步化攻击,此时后台数据库将删除历史记录表中的相关密钥,然后将上次认证过程中和标签\阅读器一致的密钥添加到历史记录表中;如果是从历史记录表 Tag_h_au\Reader_h_au 中得出结果,说明标签\阅读器和后台数据库的共享密钥不一致,即上一次认证过程发生了去同步化攻击,此时,后台数据库不对历史数据表进行操作,表中仍保存着和标签\阅读器相一致的共享密钥. 在以后的认证过程中,不管发生多少次连续或者不连续的去同步化攻击,后台数据库均可以保证历史记录表的数据中存在最后一次和该标签或阅读器相一致的历史密钥数据,在后续的认证过程中,使用该密钥即可彻底防范去同步化攻击.

(6)中间人攻击(Man in the middle attack,MITM). 假设敌手截获正常认证过程中传输的数据并使用第三方阅读器或者标签进行中间人攻击:由于协议采用了后台数据库认证阅读器以及标签、阅读器认证后台数据库和标签认证阅读器的方法,所有的数据传输均在接收方对发送方的身份进行认证后才能进行,此外阅读器和标签的标识信息均在加密后匿名传输,使得第三方的阅读器或标签在协议中无法通过认证,因此协议可以有效避免中间人攻击.

(7)拒绝服务攻击(Denial of Service,DoS). RFID 系统中,向后台数据库持续发送大量数据请求会造成后台数据库负载过大甚至瘫痪,从而达到拒绝认证合法标签的目的[14]. 假设 RFID 系统中标签数量为 n,阅读器数量为 m,且 $n \gg m$,则向后台数据库发送 y 轮 k 个非法请求时,文献[13]需要进行 $y \times k \times (m+n)$ 次 Hash 运算和比较才能确认标签非法,本文协议采用了先查询后认证的方法,因此不需要任何计算;认证阅读器时,由于阅读器数量较小,所进行的 $k \times (m+2)$ 次异或和随机数运算量也很小,因此本文协议能更好地防范拒绝服务攻击.

(8)标签和阅读器伪造. 本文协议采用了后台数据库、阅读器和标签之间按流程相互认证的方法,关键的认证信息在接收时必须对发送方的身份进行认证后再进行处理,由于阅读器和标签的标识和密钥信息具有机密性且关键的认证信息均进行加密和随机化,使得敌手无法获得阅读器和标签的身份标识或者密钥信息从而伪造阅读器和标签,因此协议可以防范阅读器和标签伪造.

4.2　效率分析

RFID 认证协议的效率主要从存储量、计算量、通信量和会话次数方面衡量[15]. 设共享密钥、Hash 码以及随机数的长度均为 l;h 代表 Hash 运算;x 代表异或运算;s 代表随机数运算;d 代表取余运算;n 表示标签的数量;m 表示阅读器的数量;存储量为标签完成 1 次认证所需的存储容量;计算量为完成 1 次认证时标签、阅读器和后台数据库所进行的运算;通信量为完成 1 次认证需要传输的最大数据长度;会话次数为完成 1 次认证所需要的交互次数.

(1)存储量:RFID 系统中,后台数据库和阅读器具有较大的存储容量,对协议的效率影响不大,本文只讨论标签的存储容量. 本文协议中,标签需存储密钥 K_t^i 以及标签 ID,即 $2l$.

(2)计算量:由于异或运算的计算开销很小,在分析时予以忽略. 在一次认证过程中,标签响应阅读器需要进行 1 次 Hash 计算和 2 次随机数计算;认证阅读器需要进行 1 次随机数计算,因此标签计算量为 $h+3s$. 阅读器向后台数据库发送数据时需要 1 次 Hash 计算和 1 次随机数计算;在认证后台数据库和更新密钥时需进行 2 次随机数计算,因此阅读器计算量为 $h+3s$. 后台数据库认证阅读器时平均需要 $mh/2$ 次 Hash 计算;认证

标签时需要 1 次随机数计算;更新密钥时需要 2 次随机数计算,因此后台数据库计算量为 $mh/2+3s$.

(3)通信量:在一次认证过程中,阅读器转发数据到后台数据库时通信量最大,通信量为 $5l$.

(4)会话次数:在一次认证中,后台数据库、阅读器和标签之间需要进行 5 次会话.

4.3 和同类协议的比较分析

根据以上分析,将本文提出的 RFID 认证协议与部分采用动态密钥机制的 RFID 认证协议进行比较,结果如表 3 所示.

表 3 协议比较

	安全性能								效率						
									标签开销		阅读器计算量	数据库计算量		通信量	会话次数
	机密	追踪	前向	重放	去同步化	MITM	DoS	伪造	计算量	计算量		认证阅读器	认证标签		
文献[6]	×	√	√	×	×	×	√	×	$2l$	$2h$	0	0	$nh\times i$	$1l$	n
文献[8]	×	√	√	√	◿	√	√	√	$2l$	$2h+2d+s$	s	0	$2h+s+nx/2+x$	$3l$	5
文献[9]	×	√	√	√	◿	√	√	√	$4l$	$4h+3d+2s$	s	0	$16h+2d+s$	$5l$	5
文献[11]	√	√	√	×	√	×	√	√	$3l$	h	$h+s$	mh	$(n+1)h+2s$	$2l$	5
文献[12]	√	√	√	×	×	×	√	×	$3l$	0	$2h+s$	0	$2h+s$	$3l$	5
文献[13]	√	√	√	√	@	√	×	√	$2l$	$2h$	$2h+s$	$(m+1)h$	$(n+1)h$	$3l$	5
本文协议	√	√	√	√	√	√	√	√	$2l$	$h+3s$	$h+3s$	$mh/2+s$	$2s$	$5l$	5

√代表具备该项安全性能;×代表不具备该项安全性能;◿代表一定程度上具备该项安全性能;@代表不存在该项安全性能

4.3.1 安全性能比较

根据表 3,安全性能方面,本文协议具备较全面的安全性,可以弥补同类 RFID 认证协议存在的不足.

4.3.2 效率比较与分析

(1)标签的存储量和计算量

RFID 系统中,标签只有有限的资源,易成为 RFID 认证协议效率方面的瓶颈,因此标签的存储量和计算量是衡量 RFID 认证协议效率的关键. 以 160 位 SHA-1 Hash 函数和流密码 Grain 实现伪随机数为例,Hash 函数的计算开销为 1274 时钟周期,伪随机数的计算开销为 104 时钟周期[16~18]. 以标签存储容量与计算量的基本单位之和作为标签的总体开销来衡量本文与同类 RFID 认证协议,其结果如图 2 所示.

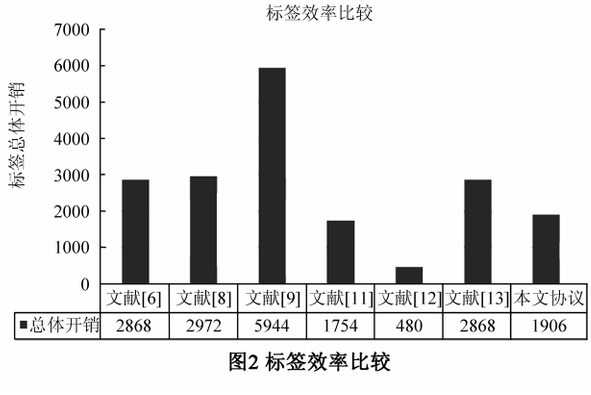


图2 标签效率比较

从图 2 可以看出,本文协议标签的总体开销小于文献[6,8,9,13],大于文献[11,12],但文献[11,12]存在多项安全漏洞,其低开销是以牺牲安全性能为代价的.

(2)阅读器计算量

本文协议中,阅读器计算量大于文献[6,8,9,11],小于文献[12,13]. 但文献[6,8,9]中阅读器没有进行认证的预备计算,使得后台数据库不能对阅读器进行认证,其较小的运算无法保证阅读器的匿名性;此外,相对于阅读器较高的计算能力,本文多出的计算量并不影响协议效率.

(3)后台数据库计算量

①认证标签计算量. 本文协议中,后台数据库避免了针对大规模标签的逐一遍历和计算,因此,后台数据库针对标签进行认证的计算量均小于表 3 中的其他文献.

②认证阅读器计算量. 本文协议大于文献[6,8,9,12],小于文献[11,13]. 但在文献[6,8,9]中,后台数据库没有对阅读器进行任何认证计算,因此无法保证阅读器的匿名性;而文献[12]中,后台数据库根据阅读器固定标识进行查询以认证阅读器,无法防范第三方阅读器的中间人攻击. 这些协议虽然降低了认证阅读器的计算量却相应地增加了遭受攻击的风险.

(4)通信量

本文协议通信量和文献[9]相等,虽大于其他协

议,但属于同一数量级.

(5)会话次数

本文协议会话次数低于 Hash 链协议,和其他协议会话次数相同.

总之,本文协议整体效率优于同类采用动态密钥机制的移动 RFID 认证协议. 和同类采用动态密钥机制的传统 RFID 认证协议相比,在关键的标签效率方面具有优势,虽然增加了阅读器和后台数据库的计算量,但使得协议的计算开销更加均衡,弥补了同类协议中后台数据没有对阅读器进行认证计算以及阅读器只进行信息转发而不进行计算所带来的安全风险. 此外,本文协议的应用范围更为广泛,不仅适用于传统的 RFID 系统,也适用于移动 RFID 系统.

5　结论与展望

安全和效率分析表明,本文提出的基于动态共享密钥的移动 RFID 双向认证协议能够防范位置追踪、重放攻击、去同步化攻击、中间人攻击等多项安全威胁,可以弥补同类 RFID 认证协议存在的安全缺陷;协议中关键的标签效率具有更好的性能,适用于被动式标签数量庞大的移动和传统的 RFID 系统. 下一步的工作将对协议流程进行优化,合理降低后台数据库和阅读器的计算量,在保证安全的基础上使协议具有更好的性能.

参考文献

[1] Liao Y P, Hsiao C M. A secure ECC-based RFId authentication scheme integrated with ID-verifier transfer protocol [J]. Ad Hoc Networks, 2014, 18(7): 133 – 146.

[2] 张学军,王玉,王锁萍,等. 基于循环移位的轻量型相互认证协议研究[J]. 电子学报, 2012, 40(11): 2270 – 2275.
ZHANG Xue-jun, WANG Yu, WANG Suo-ping, et al. Research on the cyclic shift lightweight mutual authentication protocol[J]. Acta Electronica Sinica, 2012, 40(11): 2270 – 2275. (in Chinese)

[3] 钱志鸿,王义君. 物联网技术与应用研究[J]. 电子学报, 2012, 40(5): 1023 – 1029.
QIAN Zhi-hong, WANG Yi-jun. IoT technology and application[J]. Acta Electronica Sinica, 2012, 40(5): 1023 – 1029. (in Chinese)

[4] Doss R, Sundaresan S, Zhou W. A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems[J]. Ad Hoc Networks, 2013, 11(1): 383 – 396.

[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, 29(4): 581 – 589.
ZHOU Yong-Bin, FENG Deng-Guo. Design and analysis of cryptographic protocols for RFID[J]. Chinese Journal of Computers, 2006, 29(4): 581 – 589. (in Chinese)

[6] Ohkubo M, Suzuki K, Kingships S. Hash-Chain based forward-secure privacy protection scheme for low-cost RFID [A]. Proc of Symposium on Cryptography and Information Security[C]. Sendai, Japan: SCIS, 2004. 719 – 724.

[7] 李辉,侯义斌,黄樟钦,等. 一种智能攻击模型在 RFID 防伪协议中的研究[J]. 电子学报, 2009, 37 (11): 2565 – 2573.
LI Hui, HOU Yi-bin, HUANG Zhang-qin, et al. Research on the attack model for RFID anti-counterfeit protocol[J]. Acta Electronica Sinica, 2009, 37 (11): 2565 – 2573. (in Chinese)

[8] Cho J S, Yeo S S, Kim S K. Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value[J]. Computer Communications, 2011, 34(3): 391 – 397.

[9] Yeh T C, Wu C H, Tseng Y M. Improvement of the RFID authentication scheme based on quadratic residues [J]. Computer Communications, 2011, 34(3): 337 – 341.

[10] Niu B, Zhu X, Chi H, et al. Privacy and authentication protocol for mobile RFID systems[J]. Wireless Personal Communications, 2014, 77(3): 1713 – 1731.

[11] Sandhya M, Rangaswamy T R. A secure and efficient authentication protocol for mobile RFID systems[J]. Journal of Digital Information Management, 2011, 9 (3): 99 – 105.

[12] Lee H C, Eom T Y, Yi J H. Secure and lightweight authentication protocol for mobile RFID privacy[J]. Applied Mathematics & Information Sciences, 2013, 7(1): 421 – 426.

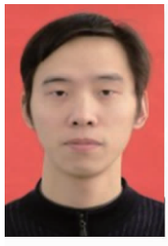
[13] 刘鹏,张昌宏,欧庆于. 基于 Hash 函数的移动射频识别互认证安全协议设计[J]. 计算机应用, 2013, 33(5): 1350 – 1352.
LIU Peng, ZHANG Changhong, OU Qingyu. Authentication protocol of mobile RFID based on hash function[J]. Journal of Computer Applications, 2013, 33(5): 1350 – 1352. (in Chinese)

[14] Duc D N, Kim K. Defending RFID authentication protocols against DoS attacks[J]. Computer Communications, 2011, 34(3): 384 – 390.

[15] 郭奕旻,李顺东,陈振华,等. 一种轻量级隐私保护的 RFID 群组证明协议[J]. 电子学报, 2015, 43(2): 289 – 292.
GUO Yi-min, LI Shun-dong, CHEN Zhen-hua, et al. A lightweight privacy-preserving grouping proof protocol for RFID systems[J]. Acta Electronica Sinica, 2015, 43(2): 289 – 292. (in Chinese)

[16] 王晨旭,韩良,喻明艳,等. 一种适用于 RFID 标签的安全化密码算法实现[J]. 电子学报,2014,42(8):1465-1473.
WANG Chen-xu, HAN Liang, YU Ming-yan, et al. A secure cipher implementation suitable for RFID-tags[J]. Acta Electronica Sinica, 2014, 42(8): 1465-1473. (in Chinese)
[17] 马昌社. 前向隐私安全的低成本 RFID 认证协议[J]. 计算机学报,2011,34(8):1387-1398.
MA Chang-She. Low cost RFID authentication protocol with forward privacy[J]. Chinese Journal of Computers, 2011,34(8):1387-1398. (in Chinese)
[18] Doss R, Zhou W, Sundaresan S, et al. A minimum disclosure approach to authentication and privacy in RFID systems[J]. Computer Networks, 2012, 56(15): 3401-3416.

作者简介



王国伟 男,1979 年生,河南省平顶山人,河南理工大学在读博士研究生. 主要从事物联网安全认证协议方面的研究.
E-mail:wangguowei@hpu.edu.cn

贾宗璞(通信作者) 男,1963 年生,河南邓州人,工学博士,现为河南理工大学教授,博士生导师. 主要从事计算机测控技术、物联网安全等方面的研究.
E-mail:jiazp@hpu.edu.cn

彭维平 男,1979 年生,湖北天门人,工学博士,河南理工大学副教授. 主要从事信息安全、物联网安全用等方面的研究.
E-mail:pwp999@hpu.edu.cn