文章编号:2095-476X(2015)02-0052-04

轻量级RFID标签所有权匿名安全转换协议的研究

甘勇, 李天豹, 许允倩

(郑州轻工业学院 计算机与通信工程学院,河南 郑州 450001)

摘要: 基于RFID系统工作原理和低成本标签存储计算能力有限的特性,提出一种新的RFID标签所有权转换协议. 协议通信过程采用轻量型运算,标签以假名经伪随机加密函数处理后在无线信道传输,采用共享密钥恢复机制进行标签与所有者之间的认证、授权,保证了协议的健壮性;密钥由通信双方协商动态更新,提高了标签在所有权转换过程中信息数据的安全性. 与其他协议比较分析结果表明,该协议低复杂度的算法可以抵抗多类攻击,且具有较低的通信量和较高的计算效率.

关键词: 射频识别标签;所有权转换;双向认证;轻量型运算;安全性;隐私性

中图分类号: TP309 **文献标志码:** A **DOI:** 10.3969/j.issn.2095-476X.2015.02.012

Research on lightweight anonymous secure ownership transfer protocol of RFID tag

GAN Yong, LI Tian-bao, XU Yun-qian

(*College of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450001, *China*)

Abstract: Based on the mechanism of RFID system and limitation of low-cost tags which storage capacity and computing ability, a new RFID tag ownership transfer protocol was presented. In communication process of protocol, lightweight operations were adopted, tag anonym was transmitted in wireless channel which was processed by Pseudo-random Encryption Function. Shared-key recovery mechanism was used to excute authentication and authorization between tags and owners, which could ensure the robusthess of the protocol. At the same time, the shared-key dynamically negotiated and updated by both communication sides. It improved the security of information data in the process of ownership transfer. The analysis results compared with other protocols showed that the protocol could resist various attacks by low-complexity algorithms, and had lower traffic and higher computation efficiency.

Key words: RFID tag; ownership transfer; mutual authentication; lightweight operations; security; privacy

0 引言

射频识别RFID(radio frequency identification)技术是以计算机和通信技术为基础的综合性技术,它利用无线射频对目标进行非接触式自动识别. 作为一种能够使数据信息自动识读、自动采集到计算

收稿日期:2014-11-10

基金项目:国家自然科学基金项目(61340059)

作者简介:甘勇(1965—),男,湖南省株洲市人,郑州轻工业学院教授,博士,主要研究方向为分布式计算机系统、计算机网络、信息安全.

机的重要方法和手段,RFID 标签被广泛运用于物流、防伪、医药、金融等各个行业. 随着 RFID 技术进入越来越多的应用领域,以及应用环境日益复杂,系统的安全与隐私问题成为严重制约 RFID 技术进一步推广的瓶颈.

目前,RFID 系统主要存在隐私和认证两个方面的安全隐患: 在隐私方面,主要是防止攻击者对 RFID 标签进行任何形式的非法跟踪; 在认证方面,主要是要确保标签只能与合法的读写器进行通信. 攻击者易干扰、篡改或窃听两者之间的通信,并跟踪标签持有者的位置和行为,它还有可能伪装合法的标签和阅读器. 因此,一个有效安全的 RFID 协议应保证标签与合法读写器之间认证、授权、所有权转换的安全进行,还应满足通信系统拥有更低的计算量和更高的通信效率,并满足系统通信健壮性等要求[1].

目前国内外对 RFID 系统安全问题的研究主要通过完善逻辑方法和认证协议机制,以增加标签所有者的隐私和安全[2-11].

2007 年 K. Osaka 等[2] 提出了一个基于哈希函数和对称密码体制的 RFID 安全协议,在进行所有权转换时,该协议通过改变对称密钥来保护新旧所有者的隐私. 但如果攻击者用相同的随机数对读写器发起请求,读写器会给出同样的响应,因此该协议中读写器存在被跟踪的危险. 同年 S. Fouladgar 等[3] 设计了一个具有后向隐私的所有权转移协议,原所有者发送给新所有者数据库中标签的所有相关信息,然后新所有者的读写器向其后端数据库发送所有权转移请求,若认证成功,新所有者的数据库通过读写器向标签发送密钥更新信息,然而标签的密钥不是每次都更新,所以仍有被跟踪的机会和危险. 2009 年邵婧等[4] 提出了一个先授权后更新的转换协议,该协议由新、旧所有者双方进行密钥协商,然后原所有者向新所有者发送经私钥加密的标签所有相关信息,完成授权,读写器接收信息后进行双向认证,接着更新标签私钥. 该协议能保护标签的位置信息,提供前向安全,并能抵御重放攻击,但无法抵御去同步化攻击. 2011 年金永明等[5] 提出了一种基于 SQUASH 方案的轻量级所有权转移协议 LOTP,该协议经过优化后可以保证所有者前向隐私和后向隐私安全,但该协议并不能抵抗重放攻击. 张辉等[6] 提出了一种基于部分 ID 的认证协议,如果攻击者在解剖标签后进行复制,然后用伪造的标签发动攻击,则该协议无法抵御.

鉴于此,本文拟提出一种轻量级 RFID 标签所有权匿名安全转换协议,以期以较低的通信量和较高的计算效率解决标签与读写器无线信道间信息传输的安全与隐私问题.

1　协议描述

本协议的设计基于以下安全需求分析.

由 RFID 系统的安全性分析可知,制约 RFID 安全的瓶颈主要来自读写器与标签之间不安全的无线信道,因而协议要能够防止对交互数据的外部攻击和恶意篡改,有效应对重放攻击、DoS 攻击及攻击者对标签的跟踪等,以此保护 RFID 标签免受物理和协议的攻击.

除此之外,协议在低成本的被动标签上要能够挫败外来攻击对标签的静态克隆. 对于低成本 RFID 标签来说,协议还需有合适的通信量,同时降低标签的存储量和计算量,尽可能把计算和存储转移到后端数据库中,并能够有效地保护 RFID 系统的安全性和隐私性.

目前大多数标签认证协议是基于对称密码体制[8],本文提出的协议认证过程在采用单钥密码体制的基础上,只使用简单的比特异或、移位等运算,符合轻量级协议的标准. 协议分为两个阶段,一是认证与授权阶段,二是所有权转换阶段. 在通信双方进行保密通信时,需有一个共享的密钥,为防止攻击者截获密钥,必须时常对密钥进行更新. 以此为基础,基于询问 - 应答模式,本文提出 RFID 匿名双向认证协议的设计思路,从而实现标签与后台数据库之间的相互认证,并提供读写器与标签的认证.

本协议符合一般性,并基于如下假设: 读写器与后端数据库之间的通信信道是安全的,且后端数据库属于安全数据库; 标签与读写器之间的无线信道是不安全的; 标签具有伪随机数发生器,能够生成伪随机数,并且可以进行简单的比特异或、移位运算; 标签的物理内存是安全可靠的.

1.1　初始化过程

整个 RFID 系统{T,R,DB} 需要进行以下初始化: 系统用户(制造商、应用程序等) 为标签 T 和读写器 R 之间的物理安全生成初始共享密钥 k,该密钥会在随后的每次认证会话中进行动态协商更新; 为每个标签 T_i 分配各自唯一的标识符 ID_i,标签状态 S(2 b) 初始化为 00,连同标签的相关信息都存储

于标签中;在后端数据库 DB 中为每个标签存储一条记录 $[IS, k_{old}, k_{new}]$ 以及相应的认证数据,其中 $IS_i = h(ID_i)$ 作为标签的假名,k_{new} 为读写器与标签最新协商的密钥,k_{old} 为上一轮成功认证后标签与读写器的共享密钥. 由于低成本标签多为无源标签,故协议由读写器开始发起对话请求.

1.2 标签所有权转换过程

1.2.1 认证与授权阶段 认证与授权步骤如下.

步骤 1 标签初始状态置为"00"(待通信),读写器产生随机数 r 并发起访问请求 request,同时将 r 发送给标签.

步骤 2 标签 T_i 收到请求后状态置为"01"(待认证),通过伪随机数发生器产生随机数 m,计算 $L_1 = h(h(ID_i) \oplus r) \gg l/2$($l$ 为密钥长度),$L_2 = (h(ID_i) \oplus m \oplus L_1) \gg r$,$L_3 = E_{ki}(m)$,并将 $L_1 \| L_2 \| L_3$ 发送给读写器.

步骤 3 读写器接收 $L_1 \| L_2 \| L_3$ 后传向后端数据库,数据库计算 $P = L_1 \ll l/2$,在数据库中检索所有的 $[IS, k_{old}, k_{new}]$ 组,验证是否存在 $h(IS_j \oplus r) = P$. 若无匹配项,则该标签为非法标签,结束认证过程;若检索到匹配项,则计算 $m' = (L_2 \ll r) \oplus h(ID_i) \oplus L_1$,然后用 k_{new} 加密 m' 得到 $E_{knew}(m')$. 若 $L_3 = E_{knew}(m')$,则继续步骤 4;若 $L_3 \neq E_{knew}(m')$,用 k_{old} 加密 m' 得到 $E_{kold}(m')$. 若 $L_3 = E_{kold}(m')$,则继续步骤 4;若 $L_3 \neq E_{kold}(m')$,则认证失败.

步骤 4 数据库计算 $M_1 = f(m' \oplus r) \oplus IS_j$,$M_2 = h(k'_i \gg m/2) \oplus IS_j$,更新数据库中 $[IS_j, k_{old}, k_{new}]$ 三元组,使 $k_{old} = k_{new}$,$k_{new} = f(k'_i \gg m/2)$,将 $M_1 \| M_2$ 发送给标签.

步骤 5 标签收到 $M_1 \| M_2$ 后,计算 $IS'_j = f(m \oplus r) \oplus M_1$,$h(k'_i \gg m/2)' = M_2 \oplus h(ID_i)$,若 $IS'_j = h(ID_i)$ 且 $h(k'_i \gg m/2)' = h(k_i \gg m/2)$,则标签对读写器认证成功,标签状态置为"10"(已认证),标签计算并更新内部存储的密钥 $k_i = f(k_i \gg m/2)$,同时向读写器返回认证成功消息,否则返回认证失败消息.

1.2.2 所有权转换阶段 所有权转换步骤如下.

步骤 1 新所有者 NO(new owner)向当前所有者 CO(current owner)发送自己的身份标识 ID_N 和标签所有权转移请求 $reqt$,待转移所有权标签内部状态 S 置为"11"(待转换).

步骤 2 CO 接收 ID_N 和 $reqt$ 并判断所有者提出的授权请求是否合法,若为合法请求,CO 生成随机数 r_1,计算 $P_1 = h(k \oplus r_1)$,$P_2 = E_k(IS \oplus r_1)$,然后将 P_1,P_2 连同 r_1 一起发送给 NO.

步骤 3 NO 生成随机数 r_2,将 P_1,P_2,r_2 和 S 传送给 T,同时计算并设置自己与标签的共享密钥为 $k_{tp} = h(P_2 \oplus r_2)$.

步骤 4 T 接收到 NO 的消息后验证状态位,确认要进行所有权转换,用 k 解密 P_2,得到 r_1,计算 $P'_1 = h(k \oplus r_1)$,并验证 P'_1 与 P_1 是否相等. 若相等,则标签更新与新所有者的共享密钥 $k = h(P_1 \oplus r_2)$,标签内部状态位置为"00";若不相等,则不操作. 然后计算并向新所有者发送 $P_3 = (k \oplus r_2) \gg S$.

步骤 5 NO 接收标签的消息 P_3 后计算 $P'_3 = k_{tp} \oplus r_2$,验证 P'_3 与 P_3 是否相等. 若相等,则所有权转换成功;若不相等,则 NO 重复步骤 3,直到所有权转换成功.

2 协议安全性、隐私性分析

与目前存在的可选模式协议[11]相比较,新协议在标签认证授权中减少了第三方可信中心(TC)的参与,因此标签的当前所有权节点不需要向可信任中心发起获取标签密钥的请求,从而有效降低了复杂度标签的管理成本,减少了标签的通信与计算开销. 采用伪随机数发生器结合标签假名进行认证,克服了静态标识机制的标签认证过程带来的缺点,在尽量减少标签计算存储消耗的同时,实现了标签的不可跟踪性. 新协议采用 Timestamp 机制为标签设置状态位,能够在认证、授权、所有权转换的不同阶段,对读写器发出的响应和请求进行有效识别,解决在多标签应用环境下产生的时钟同步问题.

双向认证:在协议会话中,读写器与后端数据库之间的信道是安全可靠的,可看作一个整体,只有合法的标签和读写器才能正确接收来自对方的响应,由此通信双方的合法性得以验证,从而实现了标签与读写器之间的双向认证.

匿名性:协议中通信过程对请求的响应不包含标签的标识符 ID,而是采用了经过哈希函数计算的假名 IS,因此攻击者并不能得到标签 ID,也就不能对标签进行跟踪,从而有效保护了标签所有者的隐私,实现了认证的匿名性.

假冒攻击:当攻击者伪装成合法的读写器时,需要计算出 $M_1 \| M_2$ 作为对标签的响应,而在无法获得标签的密钥与标签上一轮对话所产生随机数的前提下,攻击者无法计算出有效的 $M_1 \| M_2$,同时

标签在不同阶段通过状态位变化来识别接收到的读写器响应是否合法,因此攻击者伪装为合法读写器是行不通的.

重放攻击: 协议中用标签与读写器产生的随机数来抵抗重放攻击. 消息 $L_1 \parallel L_2 \parallel L_3$,$M_1 \parallel M_2$ 依赖 R 与 T 产生的随机数 r 和 m,因此 $L_1 \parallel L_2 \parallel L_3$,$M_1 \parallel M_2$ 也具有随机性,攻击者从之前会话中得到的响应结果在后续的安全通信中是无效的.

DoS 攻击: 如果攻击者截断或篡改消息 $M_1 \parallel M_2$,由于数据库在此之前已经更新了标签 T_i 对应的密钥 k_{new},而标签 T_i 却因为认证失败而保留上轮成功认证后的密钥,因此会造成读写器与标签之间共享密钥的不同步,本协议中后端数据库为每个合法标签存储一组 $[S, k_{old}, k_{new}]$ 值,在受到 DoS 攻击的时候能够用上轮的共享密钥进行认证.

前向安全: 本文协议中,当标签所有权移交给当前所有者后,DB 和 Tag 都会对共享密钥进行更新,且更新过程是不可逆的,因此当前所有者不能获取上一节点与标签之间的通信隐私,即使标签被攻击者破解,标签与之前所有者的通信隐私仍然是安全的.

后向安全: 在当前所有者把标签所有权转交给新所有者的过程中,当前所有者无法参与新所有者与标签的密钥协商会话,因此标签所有权转移后,之前的所有者不能再由标签通信获得标签的秘密信息.

本文协议与其他几种协议方案的安全性和隐私性对比结果见表 1.

表 1　本文协议与其他协议安全性和隐私性比较

方案	双向认证	匿名性	假冒攻击	重放攻击	DoS 攻击	前向安全	后向安全
文献 [2]	√	×	√	×	×	×	√
文献 [4]	√	×	√	√	√	√	√
文献 [6]	√	√	√	√	√	×	√
文献 [7]	√	×	√	√	√	√	√
文献 [9]	√	√	×	√	√	√	√
文献 [10]	×	√	√	×	√	√	√
本文协议	√	√	√	√	√	√	√

3　结语

本文提出了一种轻量级 RFID 标签所有权匿名安全转换协议,协议通信过程采用轻量型运算,标签以假名经伪随机加密函数处理后在无线信道传输,采用共享密钥恢复机制进行标签与所有者之间的认证、授权,保证了协议的健壮性; 本协议的设计满足了 RFID 标签所有权转移过程中的隐私性与安全性需求,且通信量和计算量适中,对于低成本标签是可行的,在实际应用中具有重要意义. 如何在动态机制下保护标签信息安全性,抵御去同步化等攻击,同时减少标签的计算量和标签存储空间的占用,是下一步研究工作要解决的问题.

参考文献:

[1] Song B, Mitchell C J. Scalable RFID security protocols supporting tag ownership transfer [J]. Computer Communications, 2011, 34(4): 556.

[2] Osaka K, Takagi T, Yamazaki K, et al. An efficient and secure RFID security method with ownership transfer [J]. Lecture Notes in Computer Science, 2007, 4456: 778.

[3] Fouladgar S, Afifi H. An Efficient Delegation and Transfer of Ownership Protocol for RFID Tags [M]. Austria: First International EURASIP Workshop on RFID Technology, 2007.

[4] 邵婧,陈越,甄鸿鹄. 供应链环境下的 RFID 标签所有权转换方案 [J]. 计算机工程与设计, 2009, 30(24): 5618.

[5] 金永明,孙惠平,关志,等. RFID 标签所有权转移协议研究 [J]. 计算机研究与发展, 2011, 48(8): 1400.

[6] 张辉,侯朝焕,王东辉. 一种基于部分 ID 的新型 RFID 安全隐私相互认证协议 [J]. 电子与信息学报, 2009, 31(4): 853.

[7] Zhou X L, Wang A L, Xi T. A new optional ownership transfer mode of RFID tags [J]. Journal of Information & Computational Science, 2013, 10(8): 2471.

[8] 贺蕾,尹毅峰,金松河,等. 一种支持密钥协商的标签所有权转换协议 [J]. 科学技术与工程, 2013, 13(28): 8339.

[9] 李慧贤. 轻量级 RFID 双向认证协议设计与分析 [J]. 西安电子科技大学学报, 2012, 39(1): 172.

[10] 邓淼磊,马建峰,周利华. RFID 匿名认证协议的设计 [J]. 通信学报, 2009, 30(7): 20.

[11] 甘勇,杨佳佳,李天豹. 一种可选模式的 RFID 标签所有权转移协议 [J]. 郑州轻工业学院学报: 自然科学版, 2014, 29(5): 52.