计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
46(4):583-592,2009

基于 Hash 函数的 RFID 安全认证协议研究

丁振华[1,2]　李锦涛[1]　冯　波[1,2]
[1](中国科学院计算技术研究所　北京　100190)
[2](中国科学院研究生院　北京　100049)
(zhding@ict.ac.cn)

Research on Hash-Based RFID Security Authentication Protocol

Ding Zhenhua[1,2], Li Jintao[1], and Feng Bo[1,2]
[1](*Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100190)
[2](*Graduate University of Chinese Academy of Sciences, Beijing* 100049)

Abstract　Radio frequency identification (RFID) is a technique using radio frequency for object identification. It is regarded as one of the ten most important technologies of this century due to its celerity, real-time, veracity in collecting and processing information through unique identification. RFID can be widely used in manufacture, retail, logistics, transportation, medical treatment, national defence, etc. However, wireless transmission, broadcast of signals, resource-constraint, etc. bring some potential risks, which disturb the reliability of RFID system and block the deployment progress of RFID techniques. To prevent the security threats, based on the analysis of the security problem, two concepts of operation mode, the single session mode and the successive session mode, are proposed; and a Hash-based Security Authentication Protocol (HSAP) between tags and the back-end server for low-cost RFID system is designed. This protocol can prevent many security problems including spoofing attack, replay attack, tracking, as well as the problem of desynchronization. The formal proof of correctness of the proposed authentication protocol is given based on GNY logic. As only hash function and bitwise OR operation are required to be computed by tags, so the proposed strategy is very suitable for low-cost RFID system compared with previous works.

Key words　RFID; HSAP; tag; reader; hash; back-end server; security; authentication protocol

摘　要　无线传输、信号广播、资源受限等特点使 RFID 技术存在潜在安全隐患.在对 RFID 技术所面临的安全问题进行了详细地描述和分析后,提出了认证识别的单一会话模式和连续会话模式的概念,基于 Hash 函数设计了一个介于 RFID 标签和后端服务器之间的安全认证协议 HSAP,以解决假冒攻击、重传攻击、追踪、去同步化等安全问题,并基于 GNY 逻辑给出了形式化的证明.由于在 RFID 标签中仅仅使用了 Hash 函数和或操作,因此 HSAP 协议跟先前的工作相比更适合于低成本 RFID 系统.

关键词　RFID; HSAP; 标签; 读写器; Hash; 后端服务器; 安全; 认证协议

中图法分类号　TP309

1　概　　述

射频识别(radio frequency identification, RFID)是应用无线电波(频率为 50 kHz～5.8 GHz)来自动识别单个物体对象技术的总称.作为一种快速、实时、准确地采集与处理信息的高新技术,通过对实体对象的唯一有效标识,RFID 可广泛应用于生产、零

收稿日期:2007-12-29;**修回日期**:2008-09-11
基金项目:广东省重点科技攻关基金项目(2005B80406004);粤港关键领域重点突破基金项目(200649813001)

售、物流、交通、国防等各个行业,被列为本世纪十大重要技术之一.

RFID 的历史非常悠久,美国人 Harry Stockman 于 1948 年 10 月首次详细描述了 RFID 的理论和实现方法[1].到今天,它已经走过了 50 多年的发展历程.目前 RFID 使用的频率主要有 6 种:135 kHz 以下,13.56 MHz,433.92 MHz,860～960 MHz,2.45 GHz以及 5.8 GHz.其中,860～960 MHz 频段的相关技术是目前的研究热点.

1.1 RFID 系统组成

RFID 系统一般由三大部分组成:RFID 标签(tag or transponder)、RFID 读写器(reader or transceiver)和后端数据库(后端服务器)[2],如图 1 所示:

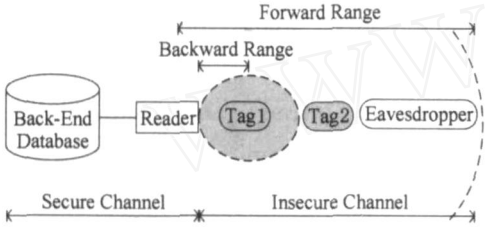

Fig. 1 Components of RFID system.

图 1 RFID 系统基本构成

RFID 标签:由芯片和耦合元件(天线)构成,芯片用于计算,天线用于无线通信,芯片的计算和存储能力十分有限.每个标签具有唯一的电子编码.RFID 读写器:由射频接口(radio frequency interface)和控制单元(control unit)组成[3],其计算能力和存储能力都比较大.RFID 读写器通过射频接口来获取标签中的数据(主要是 ID),并将其传递给后端数据库:从 RFID 读写器到标签的信道,称为前向信道(forward channel),信号的距离可达百米,是不安全信道;从标签到读写器的信道,称为后向信道(backward channel),强度相对较弱,范围几米,也是不安全信道.后端数据库:接收来自 RFID 读写器的数据,通常假设其计算和存储能力强大,存储有标签的信息或关联信息,RFID 读写器和后端数据库之间是安全信道.

1.2 RFID 系统通信模型

ISO/IEC 18000 标准定义了 RFID 的系统通信模型[4-5],如图 2 所示.共有 3 层组成:应用层、通信层和物理层.

1) 应用层.用于解决和最上层应用直接相关的内容,包括认证、识别以及应用层数据的表示、处理逻辑等.通常情况下,我们所说的 RFID 安全协议指的就是应用层协议,本文所讨论的所有 RFID 安全协议都属于这个范畴.

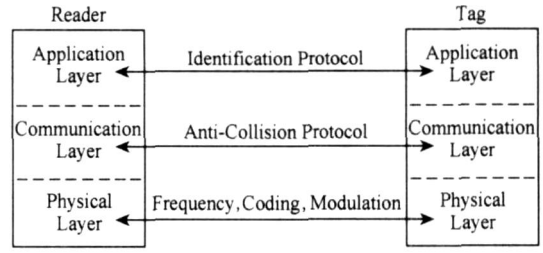

Fig. 2 Communication model of RFID system.

图 2 RFID 系统通信模型

2) 通信层.定义了 RFID 读写器和标签之间的通信方式.防冲突协议就属于该层,主要解决多个标签同时和一个读写器通信的冲突问题.

3) 物理层.定义了物理的空中接口,包括频率、物理载波、数据编码、分时等问题.

RFID 技术的不接触、无须可视、信号广播等特点给攻击者带来了巨大的活动空间.此外,RFID 设备(主要是标签)低成本的要求使得它们具有十分有限的计算资源(通常来讲,低成本 RFID 标签包含 5000～10000 个门电路[6],可用于安全机制的是 400～4000 个门电路[7]).所有这些特点和局限性都对 RFID 系统安全机制的设计提出了特殊的要求,因此设计安全、高效、低成本的 RFID 协议也就成为了一个新的具有挑战性的课题.

在这篇文章中,我们在对 RFID 技术所面临的安全问题进行了详细的描述和分析后,提出了认证识别的单一会话模式和连续会话模式的概念,设计了一个介于 RFID 标签和后端服务器之间的双向安全认证协议 HSAP,并基于 GNY 逻辑给出了正确性证明.该协议能够成功地解决假冒攻击、重传攻击、追踪、去同步化等安全问题.由于在 RFID 标签中仅仅使用了 Hash 函数和或操作,在性能上跟先前的工作相比更适合于低成本 RFID 系统.

2 RFID 安全问题分析

要设计好 RFID 安全协议的一个困难就是定义敌人和攻击,这对于确立设计的原则、假定、目标非常重要.下面就对 RFID 系统所面临的安全问题(攻击)进行分析.

2.1 RFID 安全问题分析

首先,我们要定义 RFID 概念下的两个术语:“安全”和“隐私”.在 RFID 研究领域,安全是指下面

的一个或者多个元素:1) 机密性.即消息内容的安全.2) 完整性.3) 发送方和接收方的身份认证.4) 有效性(可用性).这 4 个元素主要来自安全需求的角度[7-8].相对于安全的概念来讲,隐私则是一个包含了政策、法律等多领域的多元概念.对隐私的详细定义可以参见文献[7].评价 RFID 系统隐私的一个标准是看其是否提供了匿名性和不可连接性,也有研究者认为这两者是同一个概念[9];这两个元素主要来自隐私保护需求的角度.通常来讲,隐私是安全问题的一种[10].

一个 RFID 系统所面临的具体的安全问题主要包括如下几种:

1) 假冒攻击(spoofing attack).攻击者假冒读写器来记录标签的响应,之后,攻击者用该响应去响应合法的读写器使得该合法的读写器仍然以为真正的标签还在,而实际上标签已经离去.通常来讲,解决假冒攻击问题的主要途径是执行认证协议和数据加密.

2) 重传攻击(replay attack).攻击者通过中途截取读写器和标签之间通信的有效信号,之后将该有效信号在 RFID 系统中进行重传从而对系统进行的一种攻击.通常来讲,解决重传攻击问题需要用到挑战-响应机制,计时和计数的机制也经常用来抵御重传攻击.

3) 追踪(tracking).不同于前面的两种攻击,追踪是一种对人有威胁的安全问题,攻击者通过标签的响应信息来追踪标签.因此,一个 RFID 系统应该满足:不可分辨性(indistinguishability)和前向安全(forward security).不可分辨性是包含在 ID 匿名(anonymity)[11]中的一个概念,意味着一个标签所发出的信息与其他标签所发出的信息具有不可分辨性,即与 ID 无关;前向安全则是指,如果一个攻击者获取了该标签先前发出的信息,那么攻击者用该先前获取的信息不能够确定该标签.通常来讲,Hash 函数的随机特性和随机数被用来解决该类问题.

4) 去同步化.去同步化(desynchronization)主要是指通过使标签和后台数据库所存储的信息不一致导致标签失效的一种威胁[12].读写器对标签有读和写两种操作,在现实的 RFID 应用中,写操作的内容主要是标签 ID,攻击者通过对写操作(如升级 ID)的攻击而带来去同步化问题.

5) 其他.偷听(eavesdropping).由于读写器和标签之间是无线通信,攻击者可以中途读取读写器和标签之间通信的有效信号,从而执行加强的攻击,如重传或假冒攻击;会话劫持(session hijacking/interception)该攻击是中间人攻击(man-in-the-middle attack)[13]的一种具体体现形式,它所带来的主要威胁是应用层的去同步化问题;RFID 病毒(virus)[14-15]可以通过 RFID 中间件的过滤功能来去除.电磁干扰(jamming)、能量分析[16]、克隆(clone)和篡改标签(tampering)等 RFID 安全问题发生在物理层,不在本文研究范围之内,更多信息可参见文献[17].

所以能否抵御假冒攻击、重传攻击、追踪和去同步化等安全威胁通常被用来作为评价一个应用层安全协议的指标[2,6,18-20].在本文的第 4 节,我们将主要针对如上这几个方面进行安全性分析.

2.2 相关工作

目前,针对以上安全问题实现 RFID 安全性机制所采用的方法主要有物理机制和密码机制两种[5].物理机制包括法拉第笼(Faraday cage)、阻塞器标签(blocker tag)[10]、主动干扰(active jamming)、按钮式标签、裁剪标签技术(clipped tag)、消除标签数据(kill tag)、跳频通信技术(frequency hopping spread spectrum)等等,但是这些物理方法增加了额外的物理设备或元件,既不方便,还增加了成本.鉴于物理安全机制存在的种种缺点,在最近的 RFID 安全机制研究中,提出了许多基于密码技术的安全机制.

在诸多的基于密码技术的安全机制中,基于 Hash 函数的 RFID 安全协议的设计备受关注,因为,无论是从安全需求来讲,还是从低成本的 RFID 标签的硬件执行上来讲(块大小 64 b 的 Hash 函数单元只需大约 1700 个门电路即可实现[21]),Hash 函数都是最适合于 RFID 认证协议的.这类协议又大致可以分为两类:静态 ID 机制和动态 ID 机制.所谓"静态 ID 机制"是指标签的标识在认证识别过程中保持不变,而"动态 ID 机制"是指标签的标识在每一次的认证识别会话中变化.采用动态 ID 机制时的一个非常重要的问题就是数据同步问题,也就是说,后端数据库中所保存的标签的标识和存储在标签中的标识必须同步刷新,否则,在下一次认证识别会话中就会出现合法 RFID 标签无法通过认证和识别的系统异常[5].目前,基于 Hash 函数的静态 ID 机制安全协议包括:Sarma 等人的 Hash-Lock 协议[22]、Weis 等人的随机化 Hash-Lock 协议[23]、Rhee 等人的分布式 RFID 询问-响应认证协议[2]等,此外还包

括 Ha 等人[18]和 Choi 等人[20]的工作;动态 ID 机制包括:Ohkubo 等人的 Hash-链协议[11]、Lee 等人的 LCAP 协议[19]、Henrici 等人的基于杂凑 ID 变化协议[24]、Dimitriou 等人的防追踪和克隆的轻量级协议[25]、Avoine 等人的可伸缩安全协议[26]等等. 其中,静态 ID 机制主要存在的问题是后端服务器的计算量太大;动态 ID 机制主要存在的问题是 ID 的刷新会带来去同步化问题.

除了基于 Hash 函数的安全机制外,到目前为止提出的安全机制还包括 Molnar 等人的基于共享密钥的伪随机函数而设计的数字图书馆协议[27]、Juels 等人的再次加密机制[28]、Feldhofer 等人的低成本 AES[29]、Vajda 和 Buttyán 的基于轻量级块密码的认证机制[30]等等.

以上所述的这些协议大多是 3 轮协议,如图 3 所示[31]:

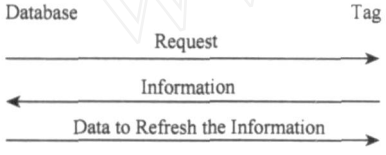

Fig. 3 3-round protocol model.

图 3 三轮协议模型

3 协议设计

在这一部分,我们首先分析了认证识别的执行过程,提出了单一会话模式和连续会话模式的概念;然后,采用挑战-响应机制、基于 Hash 函数、兼顾有效利用读写器的计算能力设计了一个能成功解决假冒攻击、重传攻击、追踪、去同步化等安全问题的 RFID 安全认证协议 HSAP;接着,利用 GNY 逻辑对协议的正确性进行了形式化证明.

3.1 操作模式和执行考虑

从协议的执行角度考虑,加之 RFID 标签识别过程的复杂性,我们可以将认证识别的执行过程分为两种操作模式,即标签认证识别的单一会话模式(single session mode)和连续会话模式(successive session mode).

定义 1. 单一会话模式. 它是指从读写器发出 *Query* 命令到后端服务器对标签实现认证,再到标签对读写器的返回实现认证的一次完整执行过程.

定义 2. 连续会话模式. 它是指为读取磁场内的全部标签,读写器不断地发送 *Query* 请求,从而执行的连续认证识别过程.

一次认证识别会话就是图 3 所示 3 轮协议模型的一次执行过程,在 EPC GEN2[32]中称为"Inventory round". 连续会话模式则需要考虑当前会话与前后会话的关系. 在先前的协议[2,20,22-23]设计中,都是只考虑了单一会话模式;虽然在协议[11,18-19,24-25]的设计中,考虑了先前会话,但此时对先前会话的考虑只为解决协议设计中因标签 ID 升级而带来的去同步化问题.

其次,在协议的执行过程中,在文献[2,11,18-20,22,24-25]等的协议设计中,不需要 RFID 读写器执行任何计算,读写器的作用仅仅是进行后端数据库和标签之间的信息传输的通道,忽略了 RFID 读写器本身具有的相对强大的计算和存储能力(以符合 EPC GEN2 标准的 Alien-9800 读写器为例,其主频为 400 MHz,内存 128 MB);而我们在协议的设计过程中则结合了连续会话的操作模式,有效地利用了 RFID 读写器的计算和存储能力.

3.2 HSAP 协议描述

1) 初始条件及符号

在 HSAP 协议里面,后端服务器的数据库存储着标签的 ID 及与之关联的信息,并且能够执行 Hash 计算;RFID 读写器具有一个伪随机数发生器,并能执行 Hash 计算,能够存储和传输后端服务器和标签之间所传输的数据;RFID 标签具有一个伪随机数发生器,并能执行 Hash 计算和或(OR)操作. 有关 HSAP 协议中的参数如表 1 所示,协议的执行过程如图 4 所示.

Table 1 List of Symbols

表 1 本文定义的一些记号和术语

Symbol	Definition
T	RFID Tag
R	RFID Reader
B	Back-End Database
Query	Request generated by Reader
ID	Identification of Tag
ID'	Identification of Tag in previous session
$H()$	One-way hash function, $H:\{0,1\}^* \rightarrow \{0,1\}^l$
$H_L()$	Left half of $H()$
$H_R()$	Right half of $H()$
r_R	Random number generated by reader
r_T	Random number generated by tag
$\|$	Bitwise OR operation

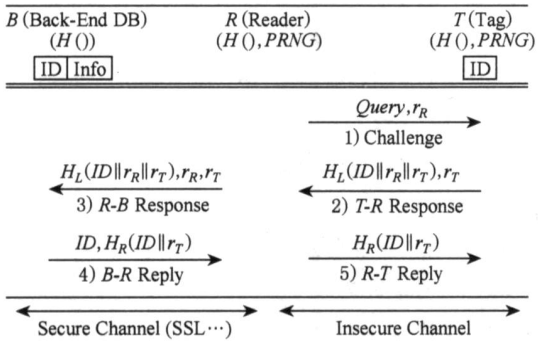

Fig. 4 Proposed protocol.

图 4 HSAP 协议

2) 执行过程

我们按照消息传递的顺序对所设计的协议进行描述:

步骤 1. challenge.

RFID 读写器生成一个伪随机数 r_R,向标签发送 *Query* 认证请求,同时将 r_R 发送给标签. 此时可能会发生 3 种情况: ①没有标签响应; ②一个标签响应; ③多个标签同时响应[32]. 当发生多标签冲突的时候,会执行一次冲突仲裁(collision arbitration)过程,如帧-时隙 Aloha 算法[33],如图 5 所示. 这一过程完毕后会从中选取出一个标签与读写器进行信息交互.

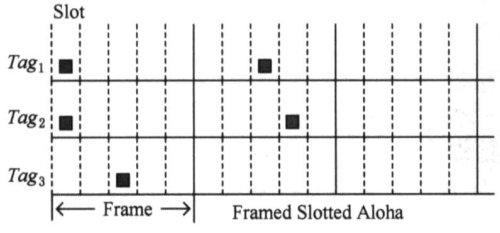

Fig. 5 Aloha collision arbitration.

图 5 Aloha 冲突仲裁

步骤 2. *T*-*R* Response.

在步骤 1 中被选中的标签 *T* 生成一个伪随机数 r_T(ISO 和 EPC GEN2 标准都支持标签中伪随机数的产生),计算 $H_L(ID\|r_R\|r_T)$,其中 *ID* 为标签之标识. 标签将 $H_L(ID\|r_R\|r_T)$ 和 r_T 发送给 RFID 读写器.

步骤 3. *R*-*B* Response.

在 RFID 读写器收到来自标签 *T* 的 $H_L(ID\|r_R\|r_T)$ 和 r_T 以后,它要完成一个过滤的操作:读写器根据上一次所缓存的 *ID* 计算 $H_L(ID'\|r_R\|r_T)$,如果 $H_L(ID'\|r_R\|r_T)=H_L(ID\|r_R\|r_T)$,则过滤掉该标签. 这时如果该标签 *T* 是前一次会话中认定的合法标签时,该过滤可以降低后端服务器的计算负载;如果该标签 *T* 是上一次认证会话中认定的非法标签时,该过滤可以避免攻击者对后端服务器的重传攻击.

如果以上两种情况都不是,即 $H_L(ID'\|r_R\|r_T)\neq H_L(ID\|r_R\|r_T)$,则 RFID 读写器将 $H_L(ID\|r_R\|r_T)$, r_R, r_T 发送给后端数据库.

步骤 4. *B*-*R* Reply.

后端数据库查找是否有某个 ID_j $(1\leq j\leq n)$,使得 $H_L(ID_j\|r_R\|r_T)=H_L(ID\|r_R\|r_T)$ 成立;如果有,则认证通过,并将 $H_R(ID\|r_T)$ 和该 *ID* 发送给 RFID 读写器;否则,返回给读写器认证失败信息,并将该 ID 返回给读写器.

步骤 5. *R*-*T* Reply.

RFID 读写器存储该 *ID*,并将 $H_R(ID\|r_T)$ 发送给标签 *T*,标签验证 $H_R(ID_j\|r_T)=H_R(ID\|r_T)$ 是否成立,如成立,则认证通过,此时标签可以转为安静状态[33];否则,认证失败.

3.3 协议证明

到目前为止,已经有很多的 RFID 安全协议被提出,但是大都缺乏严格的形式化分析和证明,接下来,我们就采用经典的安全协议分析方法 GNY 逻辑[34]对上面所提出的 HSAP 协议进行形式化的分析和证明.

1) 协议的形式化

对消息标识"不是由此首发"标记 *,并对消息作出逻辑性可以理解的解释,如图 6 所示:

Protocol Generic Type:

Msg. 1 $R\rightarrow T: r_R$

Msg. 2 $T\rightarrow R: H_L(ID\|r_R\|r_T), r_T$

Msg. 3 $R\rightarrow B: H_L(ID\|r_R\|r_T), r_R, r_T$

Msg. 4 $B\rightarrow R: ID, H_R(ID\|r_T)$

Msg. 5 $R\rightarrow T: H_R(ID\|r_T)$

Formalized Protocol:

Msg. 1 $T<*r_R$

Msg. 2 $R<*H_L(ID\|r_R\|r_T), *r_T :>T\mid\equiv\phi(H(X))$

Msg. 3 $B<*H_L(ID\|r_R\|r_T), *r_R, *r_T$

Msg. 4 $R<*ID, *H_R(ID\|r_T) :>B\mid\equiv\phi(H(X))$

Msg. 5 $T<*H_R(ID\|r_T) :>T\ni ID\|r_T$

Fig. 6 Generic type of protocol.

图 6 协议的形式化

2) 证明目标和初始化假设

正确性的证明目标如图 7 所示,主要有两个,即交互实体之间对交互信息新鲜性的相信.

$$\begin{array}{l}\textcircled{1}\ B\mid\equiv T\mid\ :\#\ (H_L(ID\ \|r_R\ \|r_T))\\ \textcircled{2}\ T\mid\equiv B\mid\ :\#\ (H_R(ID\ \|r_T))\end{array}$$

Fig. 7 Goals of the correctness proof.

图 7 正确性证明目标

初始化假设如图 8 所示. 假设 ①～④是标签 T、读写器 R、后端数据库 B 的拥有(possess);假设 ⑤～⑧是标签 T、读写器 R、后端数据库 B 对拥有的新鲜性的相信;假设 ⑨⑩则建立在读写器 R 是标签 T 和后端数据库 B 之间的一个可信任第三方(trusted third party, TTP)的基础上.

$$\begin{array}{ll}\textcircled{1}\ T\ni(r_T, ID) & \textcircled{2}\ T\ni H(X)\\ \textcircled{3}\ R\ni r_R & \textcircled{4}\ B\ni H(X)\\ \textcircled{5}\ T\mid\equiv\#\ (r_R) & \textcircled{6}\ R\mid\equiv\#\ (r_T)\\ \textcircled{7}\ B\mid\equiv\#\ (r_R, r_T) & \textcircled{8}\ T\mid\equiv\#\ (r_T)\\ \textcircled{9}\ T\mid\equiv T\xleftrightarrow{r_T}B & \textcircled{10}\ B\mid\equiv B\xleftrightarrow{r_T, r_R}T\end{array}$$

Fig. 8 Initial assumptions for proof.

图 8 初始化假设

3) 证明过程

该部分基于 GNY 逻辑的证明是在图 8 的初始化假设基础上进行的. 我们严格遵循文献[34]中所述的逻辑推理规则来进行证明. 其中, A_n 表示图 8 中的第 n 条初始化假设;而像 $T1$, $P1$, $F1$ 等符号则遵循了文献[34]中 GNY 逻辑推理规则的书写形式.

Message 1

① $T<r_R$/By $T1$/

② $T\ni r_R$/By $P1$/

Message 2

③ $R<H_L(ID\ \|r_R\ \|r_T), r_T$/By $T1$/

④ $R\ni H_L(ID\ \|r_R\ \|r_T), r_T$/By $P1$/

Message 3

⑤ $B<H_L(ID\ \|r_R\ \|r_T), r_R, r_T$/By $T1$/

⑥ $B\ni H_L(ID\ \|r_R\ \|r_T), r_R, r_T$/By $P1$/

⑦ $B\mid\equiv\#\ (ID\ \|r_R\ \|r_T)$/$A7$, By $F1$/

⑧ $B\mid\equiv\#\ H_L((ID\ \|r_R\ \|r_T))$/7, By $F10$/

⑨ $B\mid\equiv T\mid\ :H_L((ID\ \|r_R\ \|r_T))$/5, 6, $A10$, By $I3$/

⑩ $B\mid\equiv T\mid\ :\#\ H_L((ID\ \|r_R\ \|r_T))$/8, 9, By $F1$/

Message 4

⑪ $R<ID, H_R(ID\ \|r_T)$/By $T1$/

⑫ $R\ni ID, H_R(ID\ \|r_T)$/By $P1$/

Message 5

⑬ $T<H_R(ID\ \|r_T)$/By $T1$/

⑭ $T\ni H_R(ID\ \|r_T)$/By $P1$/

⑮ $T\mid\equiv\#\ (ID\ \|r_T)$/$A8$, $F1$/

⑯ $T\mid\equiv\#\ H_R((ID\ \|r_T))$/15, By $F10$/

⑰ $T\mid\equiv B\mid\ :H_R((ID\ \|r_T))$/13, $A1$, $A9$, By $I3$/

⑱ $T\mid\equiv B\mid\ :\#\ (H_R(ID\ \|r_T))$/16, 17, By $F1$/

如上所述,图 7 中的正确性证明目标在该证明过程中的步骤 10(目标 1)和步骤 18(目标 2)完成.

4 分 析

4.1 安全性能分析

在本文的第 2.1 节,我们分析了 RFID 系统所面临的各种问题,并结合 RFID 系统信道模型(如图 9 所示)针对假冒攻击、重传攻击、追踪、去同步化等问题对 HSAP 协议进行了安全性分析.

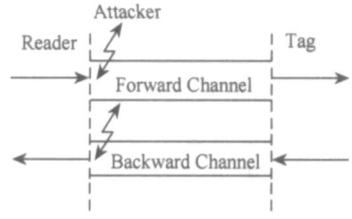

Fig. 9 Channel model of RFID system.

图 9 RFID 系统信道模型

1) 假冒攻击

①攻击者(attacker)伪装成合法的读写器通过前向信道 $R\rightarrow T$ 向标签发送 $Query$ 和 r_R;

②攻击者获取标签的响应: $H_L(ID\ \|r_R\ \|r_T), r_T$;

③在下一次认证会话中,当真正合法的读写器发送 $Query$ 和 r_R'的时候,攻击者通过后向信道 $T\rightarrow R$ 响应 $H_L(ID\ \|r_R\ \|r_T), r_T$;

由于读写器在每一次认证会话中都产生一个新的伪随机数,即 $r_R\neq r_R'$,所以攻击者就无法假冒合法标签进行假冒攻击. 所以,该协议对假冒攻击具有安全性.

2) 重传攻击

①在读写器通过前向信道向标签发送 $Query$ 和 r_R 之后,攻击者获取标签的响应: $H_L(ID\ \|r_R\ \|r_T), r_T$;

②在以后的认证会话中,攻击者通过后向信道响应 $H_L(ID\ \|r_R\ \|r_T), r_T$,从而对后端服务器发动重传攻击.

通过前一次对"标签"(实为攻击者)的认证和该协议中 RFID 读写器的过滤功能,RFID 读写器可以成功地将攻击者的重传攻击屏蔽掉.所以,该协议对重传攻击具有安全性.

3) 追踪

在伪装成合法的读写器通过前向信道向标签发送 $Query$ 和 r_R 之后,攻击者获取标签的响应: $H_L(ID \| r_R \| r_T), r_T$;并通过分析该响应来追踪发出该响应的标签.

由于在每一次认证会话中,标签都产生新的随机数 r_T,加之 Hash 操作是单向安全的,所以,攻击者也就无从得知所收到的是哪个标签的响应 $H_L(ID \| r_R \| r_T), r_T$.所以,该协议对追踪具有安全性.

4) 去同步化

在该协议的执行过程中,如果发生信息的丢失或中断,如与后端服务器连接断掉,手持 RFID 读写器断电等情况,由于标签的 ID 是固定的,所以对后端数据库服务器没有影响,而不像先前的协议中的标签 ID 升级的情况出现异步问题,重启一次会话即可恢复.

表 2 针对假冒攻击、重传攻击、追踪、去同步化等问题,对 HSAP 协议与先前的 RFID 认证协议进行了安全性分析和比较.为了更全面、更清晰地分析 HSAP 协议的安全性,我们同时对"静态 ID 机制"和"动态 ID 机制"的协议进行了分析和比较.

Table 2 Analysis of Security

表 2 安全性分析

	Threats	Dynamic ID Scheme				Static ID Scheme			
		Ohkubo	Henrici	Lee	Dimitriou	Sarma	Weis	Rhee	HSAP
1	Spoofing attack	×	×	○	○	×	×	○	○
2	Replay attack	×	○	○	○	×	×	○	○
3	Tracking	○	○	○	○	×	×	○	○
4	Desynchronization	—	×	×	×	—	—	—	—

○:Security; ×:Insecurity; —:No such problem

4.2 性能分析

对 RFID 安全协议的计算性能分析主要是从存储(tag)、计算需求(tag 和 database)、通信(tag 和 reader 之间)、连续会话(m 次) 4 个方面进行分析[35],如表 3 所示:

Table 3 Analysis of Performance

表 3 性能分析

Performance		Dynamic ID Scheme				Static ID Scheme			
		Ohkubo	Henrici	Lee	Dimitriou	Sarma	Weis	Rhee	HSAP
Storage	Tag	$1l$	$3l$	$2l$	$1l$	$2l$	$1l$	$1l$	$1l$
Compute	Tag	$2h$	$3h$	$2h$	$3h+r$	$1h$	$1h+r$	$2h+r$	$2h+r$
	Database	$nh/2 \times i$	$3h+r$	$2h$	$4h$	$0h$	$0h$	$(n/2+1) \times h$	$(n/2+1) \times h$
Comm.	Tag-Reader	$1l$	$2l$	$1.5l$	$2l$	$2l$	$1l$	$1l$	$0.5l$
	Reader-Tag	$0l$	$1l$	$0.5l$	$1l$	$1l$	$1l$	$1l$	$0.5l$
	Sum	$1l$	$3l$	$2l$	$3l$	$3l$	$2l$	$2l$	$1l$
Successive Session Mode	Database	$O(m \times n)$	$O(m)$	$O(m)$	$O(m)$	$0h$	$0h$	$O(m \times n)$	$O(n)$

l: ID 的长度或 Hash 输出的长度(详见文献[36]); h: Hash 操作; r:产生随机数操作;(随机数的长度与 ID 相比较小,不予考虑); n:标签的数量; i: Hash 链的长度; m:连续会话的次数.

由表 2 和表 3 可以看出,"静态 ID 机制"中的 Sarma, Weis 的协议虽然在数据库端不需要进行 Hash 计算,但是由于其完全没有达到安全目标,而且 Weis 的协议中数据库和读写器之间的数据通信

量过大,而且完全目标也没有达到,所以不可行,Rhee 的协议后端服务器的计算负载仍然较大;而"动态 ID 机制"中 4 个协议的后端数据库的计算量相对比较小,但是由于存在明显的数据去同步化问题,亦没有达到安全目标,所以可行性亦较小. 安全协议的设计,首先应该满足安全需求,然后再考虑降低(计算、存储、通信)性能的消耗.

从表 2 可以看出,我们所设计的安全认证协议 HSAP 能够成功地解决假冒攻击(spoofing attack)、重传攻击(replay attack)、追踪(tracking)、去同步化(desynchronization)问题. 从表 3 可以看出,在同类型的静态 ID 机制中,HSAP 协议标签存储是 $1\ l$,标签所需的计算量是 $2h + r$,标签与读写器之间的通信量是 $1\ l$;而后端服务器的数据库在连续会话模式中的时间复杂度是 $O(n)$,远低于同等安全水平的 Rhee 的协议.

5 总结与展望

RFID 技术是普适计算理念最好的体现之一. 它有着传统技术不可比拟的优势,同时也正在开辟着不少新颖而有价值的商业应用. 但是 RFID 标签有限的计算和存储资源会带来各种各样的安全问题,这也是 RFID 技术能否被广泛部署所面临的关键问题之一. 基于密码技术的 RFID 安全协议是一种实现和保护 RFID 系统安全性的重要方法,也是当前该领域研究的热点问题. 本文在对 RFID 技术所面临的安全问题进行了详细地描述和分析的基础上,提出了单一会话模式和连续会话模式的概念,设计了一个低成本 RFID 系统中介于 RFID 标签和后端服务器之间的具有鲁棒性的双向认证协议,用于保护数据安全和隐私. 并从理论证明、性能比较、安全性分析 3 个角度对 RFID 安全协议进行了阐述.

随着电路制造工艺的不断提升,RFID 的生产成本将会越来越低,也就使得 RFID 标签上将会有越来越多的计算资源可用于安全方面,因此我们相信这个领域的研究会有更多的突破. 值得说明的是,安全和隐私的级数需要依赖于具体的应用,并不存在普遍适用的解决方案.

致谢 在此,我们向对本文的工作给予支持和建议的同行,尤其是信息安全国家重点实验室的周永彬老师、Arizona State University 的孙亮和中国科学院计算技术研究所的黄倩表示感谢.

参 考 文 献

[1] Landt J, Catlin B. Shrouds of Time—The history of RFID, Ver. 1.0 [R]. Pittsburgh: AIM Inc., 2001

[2] Rhee K, Kwak J, Kim S, et al. Challenge-response based RFID authentication protocol for distributed database environment [C] //Proc of the 2nd Int Conf on Security in Pervasive Computing. Berlin: Springer, 2005: 70-84

[3] Finkenzeller K. RFID Handbook: Radio-Frequency Identification Fundamentals and Applications [M]. Second edition. New York: John Wiley and Sons Ltd, 2003

[4] Avoine G, Oechslin P. RFID traceability: A multilayer problem [C] //Proc of the 9th Int Conf on Financial Cryptography. Berlin: Springer, 2005: 125-140

[5] Zhou Yongbin, Feng Dengguo. Design and analysis of cryptographic protocols for RFID [J]. Chinese Journal of Computers, 2006, 29(4): 581-589 (in Chinese)
(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)

[6] Peris-Lopez P, César Hernández Castro J, Estévez-Tapiador J M, et al. RFID systems: A survey on security threats and proposed solutions [C] //Proc of the IFIP-TC6 11th Int Conf on Personal Wireless Communications. Berlin: Springer, 2006: 159-170

[7] Ranasinghe D, Engels D, Cole P. Low-cost RFID systems: Confronting security and privacy [C] //Proc of the Auto-ID Labs Research Workshop. Cambridge, MA: Auto-ID Labs, 2004

[8] Stajano F, Anderson R. The resurrecting duckling: Security issues for ad-hoc wireless networks [C] //Proc of the 7th Int Workshop on Security Protocols. Berlin: Springer, 1999: 172-194

[9] Kwak J, Rhee K, Oh S, et al. RFID system with fairness within the framework of security and privacy [C] //Proc of the European Workshop on Security and Privacy in Ad Hoc and Sensor Networks. Berlin: Springer, 2005: 142-152

[10] Juels A, Rivest R, Szydlo M. The blocker tag: Selective blocking of RFID tags for consumer privacy [C] //Proc of the 8th ACM Conf on Computer and Comm Security. New York: ACM, 2003: 103-111

[11] Ohkubo M, Suzuki K, Kinoshita S. Cryptographic approach to "Privacy-Friendly" tags [OL]. [2007-10-07]. http://www.rfidprivacy.us/2003/papers/ohkubo.pdf

[12] Lee S. Mutual authentication of RFID system using synchronized secret information [D]. Daejeon, Korea: School of Engineering, Information and Communications University, 2005

[13] Welch D, Lathrop S. Wireless security threat taxonomy [C] //Proc of the 2003 IEEE Systems, Man and Cybernetics Society Information Assurance Workshop. Los Alamitos, CA: IEEE Computer Society, 2003: 76-83

[14] Rieback M, Crispo B, Tanenbaum A S. Is your cat infected with a computer virus? [C] //Proc of the 4th Annual IEEE Int Conf on Pervasive Computing and Communications. Los Alamitos, CA: IEEE Computer Society, 2006: 169-~179

[15] Rieback M R, Simpson P N D, Crispo B, et al. RFID malware: Design principles and examples [J]. Pervasive and Mobile Computing, 2006, 2(4): 405-426

[16] Merritt R. Cellphone could crack RFID tags, says cryptographer [OL]. (2006-02-14) http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=180201688

[17] Xiao Q, Boulet C, Gibbons T. RFID security issues in military supply chains [C] //Proc of 2nd Int Conf on Availability, Reliability and Security. Los Alamitos, CA: IEEE Computer Society, 2007: 599-605

[18] Ha J C, Ha J H, Moon S J, et al. LRMAP: Lightweight and resynchronous mutual authentication protocol for RFID system [C] //Proc of the Int Conf on Ubiquitous Convergence Technology. Berlin: Springer, 2007: 80-89

[19] Lee S M, Hwang Y J, Lee D H, et al. Efficient authentication for low-cost RFID systems [C] //Proc of the Int Conf on Computational Science and Its Applications. Berlin: Springer, 2005: 619-627

[20] Choi E Y, Lee S M, Lee D H. Efficient RFID authentication protocol for ubiquitous computing environment [C] //Proc of the Int Workshop on Security in Ubiquitous Computing Systems. Berlin: Springer, 2005: 945-954

[21] YÄuksel K. Universal hashing for ultra-low-power cryptographic hardware applications [D]. Worcester, MA: Department of Electronical Engineering, Worcester Polytechnic Institute, 2004

[22] Sarma S, Weis S, Engels D. RFID systems and security and privacy implications [C] //Proc of the 4th Int Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2002: 454-469

[23] Weis S A, Sarma S E, Rivest R L, et al. Security and privacy aspects of low-cost radio frequency identification systems [C] //Proc of the 1st Security in Pervasive Computing. Berlin: Springer, 2003: 201-212

[24] Henrici D, P Mäuller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers [C] //Proc of the 2nd IEEE Annual Conf on Pervasive Computing and Communications Workshops. Los Alamitos, CA: IEEE Computer Society, 2004

[25] Dimitriou T. A lightweight RFID protocol to protect against traceability and cloning attacks [C] //Proc of the 1st Int Conf on Security and Privacy for Emerging Areas in Communications Networks. Los Alamitos, CA: IEEE Computer Society, 2005: 59-66

[26] voine G, Oechslin P. A scalable and provably secure hash-based RFID protocol [C] //Proc of the 2nd IEEE Int Workshop on Pervasive Computing and Communications Security. Los Alamitos, CA: IEEE Computer Society, 2005

[27] Molnar D, Wagner D. Privacy and security in library RFID: Issues, practices, and architectures [C] //Proc of the 11th ACM Conf on Computer and Communications Security. Los Alamitos, CA: IEEE Computer Society, 2004: 210-219

[28] Juels A, Pappu R. Squealing euros: Privacy-protection in RFID-enabled banknotes [C] //Proc of the Financial Cryptography. Berlin: Springer, 2003: 103-121

[29] Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm [C] //Proc of the Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2004: 357-370

[30] Vajda I, Buttyán L. Lightweight authentication protocols for low-cost RFID tags [C] //Proc of the 2nd Workshop on Security in Ubiquitous Computing. Budapest, Hungary: Budapest University of Technology and Economics, 2003

[31] Avoine G. Adversarial model for radio frequency identification, 2005/049 [R/OL]. [2005-02-21]. http://eprint.iacr.org/, 2005

[32] EPCglobal. EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz~960MHz, Version 1.0.9[S]. Cambridge, MA: EPCglobal Inc., 2004

[33] International Organization for Standardization (ISO). ISO 18000-6, RFID for Item Management—Air Interface, Part 6: Parameters for Air Interface Communications at 860MHz to 960MHz [S]. 2004

[34] Gong L, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols [C] //Proc of the 1990 IEEE Computer Society Symp on Research in Security and Privacy. Los Alamitos, CA: IEEE Computer Society, 1990: 234-248

[35] Tsudik G. YA-TRAP, yet another trivial RFID authentication protocol [C] //Proc of the 4th Annual IEEE Int Conf on Pervasive Computing and Communications Workshops. Los Alamitos, CA: IEEE Computer Society, 2006: 640-643

[36] Kaps J P, Gaubatz G, Sunar B. Cryptography on a speck of dust [J]. IEEE Computer Magazine, 2007, 40(2): 38-44

Ding Zhenhua, born in 1980. Ph. D. candidate in the Institute of Computing Technology, the Chinese Academy of Sciences. Member of China Computer Federation. His main research interests include RFID security protocol and RFID middleware.

丁振华,1980 年生,博士研究生,中国计算机学会会员,主要研究方向为 RFID 安全协议、RFID 中间件技术.

Li Jintao, born in 1962. Ph. D., professor and Ph. D. supervisor in the Institute of Computing Technology, the Chinese Academy of Sciences. His main research interests include pervasive computing, multimedia computing and virtual reality.

李锦涛,1962 年生,博士,研究员,博士生导师,主要研究方向为普适计算、多媒体技术、虚拟现实技术.

Feng Bo, born in 1975. Ph. D. candidate in the Institute of Computing Technology, the Chinese Academy of Sciences. His main research interests include RFID anti-collision algorithm and RFID middleware.

冯 波,1975 年生,博士研究生,主要研究方向为 RFID 防冲突技术、RFID 中间件技术.

Research Background

Radio frequency identification (RFID) is the latest technology to play an important role for object identification as a ubiquitous infrastructure. However, current low-cost RFID tags are highly resource-constrained and cannot support its long-term security, so they have potential risks and may violate privacy for their bearers. To remove security vulnerabilities, based on the analysis of the security problem, we propose two concepts of operation mode, the single session mode and the successive session mode; design a robust mutual authentication protocol between a tag and a back-end server for low-cost RFID system that guarantees data privacy and location privacy of tag bearers. Our protocol can prevent the following security problems. Spoofing attack, replay attack, tracking and synchronization. As tags only have hash function and exclusive-or operation, our proposed protocol is very feasible for low-cost RFID system compared with the previous works. The formal proof of correctness of the proposed authentication protocol is given based on GNY logic. Our work is supported by the Key Science-Technology Project of the Guangdong Province (2005B80406004) and the Guangdong-Hong Kong Technology Cooperation Funding Scheme (200649813001).