



研究与开发

一种基于散列函数的 RFID 安全认证方法

李川¹, 李学俊²

(1. 绵阳职业技术学院, 四川 绵阳 621000; 2. 西南科技大学, 四川 绵阳 621010)

摘 要: RFID 系统中有限的标签芯片资源, 导致数据与信息的安全成为 RFID 系统的重要问题之一, 散列函数的单向性为 RFID 的识别和认证提供了一种既可靠又有效的途径。在分析了现有几种典型散列认证协议的基础上, 提出了一种新的基于散列函数的安全认证协议。本协议旨在解决手持式、无线连接的 RFID 阅读器与标签、服务器间的识别, 利用散列函数实现服务器、阅读器以及电子标签三者之间的相互认证。经过安全性与性能的分析, 新协议在采用较小的存储空间和较低的运算开销的情况下, 可抵抗已知的大多数攻击, 有效地保证了 RFID 系统中数据和隐私的安全, 实现了终端与服务器间的双向认证和匿名认证, 非常适合于在大型分布式系统中使用。

关键词: RFID; 散列函数; 安全; 认证协议

中图分类号: TP393.01

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017108

A secure authentication method based on hash function for RFID system

LI Chuan¹, LI Xuejun²

1. Mianyang Polytechnic, Mianyang 621000, China

2. Southwest University of Science and Technology, Mianyang 621010, China

Abstract: Limited by the tag chip resource of a radio-frequency identification (RFID) system, the data and information security has been an important issue of an RFID system. The one-way Hash function provides an efficient and reliable approach for the identification and authentication of the RFID system. Based on the analysis of several typical Hash authentication protocols, a novel secure authentication protocol based on the Hash function was proposed. The protocol was intended to tackle the identification among the handheld RFID reader, tags and server. Specifically, the protocol utilizes the Hash function to achieve the mutual authentication between the above three objects. The performance analysis shows that the proposed protocol can resist the most known attacks with reduced storage capacity and lower computation overhead. Therefore, the proposed strategy effectively ensures the data and privacy security of the RFID system, achieving the bidirectional anonymous authentication between the terminal and server, which is very suitable for the distributed large-scale RFID system.

Key words: RFID, hash function, security, authentication protocol

收稿日期: 2016-12-22; 修回日期: 2017-04-10

基金项目: 四川省教育厅自然科学重点项目 (No.15ZA0369)

Foundation Item: Key Program of Nature Science of Sichuan Educational Committee (No.15ZA0369)



1 引言

射频识别 (radio frequency identification, RFID) 技术, 是一种非接触的自动识别技术, 利用射频信号或空间耦合识别特定目标并读写相关数据^[1]。通常 RFID 包括: 数据库、阅读器和标签 3 个部分, 一般情况下, 先由阅读器读取标签的 ID, 通过标签的 ID 在数据库中检索到对应信息, 再由数据库将查询结果返回给阅读器。然而, 由于 RFID 标签具有计算能力低、存储空间小、电源供给能力有限等限制, 对 RFID 系统设立的安全机制带来了新的要求^[2-5]。在 EPC-C1G2 标准 (Class-1 Generation-2) 中规定 RFID 标签成本应低于 0.05 欧元, 内部芯片的逻辑门电路为 5~10 k Ω , 其中负责安全保护的逻辑门电路只有 3 k Ω 左右, 一些基于传统加密技术, 如基于 DES 算法、基于公钥的加密算法等安全协议都不适应于低成本的 RFID 系统使用。因此, 设计一种安全、高效、低成本的 RFID 协议成为 RFID 技术发展中具有挑战性的课题。近年来, 基于散列函数算法的安全认证机制因为其安全性和计算量小等优点成为了研究解决 RFID 安全问题的研究重点, 到目前为止, 研究者已经提出许多种典型的基于散列函数的 RFID 安全协议, 例如: Sarma 等人^[6]提出的散列-lock 协议、Weis 等人^[7]提出随机散列-Lock 协议、Gao 等^[8]提出的用于供应链的 RFID 安全和隐私方案、Henrici 等人^[9]的基于散列函数的 ID 变化协议、Lee 等人^[10]的 LCAP 协议等。同时, 一些新的基于散列函数的认证协议也不断地被提出, 例如参考文献[11-14]。

随着 RFID 系统的不断深入发展, 电子标签在不久的将来势必会大面积取代条形码, 成为物体身份识别的唯一凭证^[15]。在大型分布式 RFID 系统中, 手持式、无线 RFID 阅读器为标签的识别与认证提供了方便性和灵活性, 然而由于阅读器与服务器间采用了不安全的无线连接, 使得服

务器在对标签识别的同时也需要认证阅读器的身份。现有的 RFID 认证协议都是建立在服务器与阅读器间为安全信道的基础上, 因此无法同时实现服务器、阅读器、标签三者之间, 既方便又快捷的认证服务。本文提出了一种基于散列函数的 RFID 认证方法, 通过使用标签伪 ID、标签认证值、读写器认证数值和随机数的散列运算, 完成标签、阅读器、认证服务器之间的认证, 其中标签伪 ID、标签认证数值和读写器认证数值可以动态更新, 并且更新后的伪 ID 具备防冲突和数据同步机制。

2 改进的认证协议

2.1 符号定义

表 1 所示为协议中所涉及的符号定义。

表 1 符号定义

符号	含义
DB	数据库服务器
AS	认证服务
R	阅读器
$E_k(M)$	密钥为 k 的对称加密算法
T	标签
TID	标签标识值
T_{num}	标签认证数值
R_{num}	阅读器认证数值
l	长度
r_i	随机数
h	$\{0, 1\}^* \rightarrow \{0, 1\}^l$ 散列函数
$TPID$	标签的伪标识值
M	标签物品的信息
$\parallel$	字符串连接、异或运算符号

2.2 协议应用场景及认证过程

2.2.1 协议应用场景

本协议中的 RFID 系统主要设备有阅读器(读写器)、电子标签、认证服务器和数据库。其中电子标签作为应答器附着在物体上标识目标对象,

用来存储目标对象的身份及其他信息；数据库作为存储器件，主要用来存储阅读器和标签的认证信息、数据信息以及其他数据；认证服务器作为数据库的访问控制端，主要用来识别和认证标签是否是其所属范围内的合法标签，同时认证阅读器是否合法，从而判断是否将所查询标签信息提供给阅读器；阅读器作为连接标签与认证服务器的中间器件，一方面可以从后台数据库中获得所盘存标签的数据信息，另一方面可为后台数据库更新和修改标签信息提供物理连接。

本协议系统中，数据库服务器和认证服务器之间的信息传输被认为是安全的，数据库非公开，由认证服务器上的应用软件保护数据库的安全，不被非法用户访问。标签和阅读器之间是非安全的无线信道，阅读器为移动式或手持式阅读器，也以无线连接的方式与认证服务器进行通信，且该 RFID 系统下的合法阅读器有若干个，分别拥有各自的身份标识值 (RID) 并保存于数据库中，由于阅读器为移动式且与认证服务器为无线方式连接，阅读器与认证服务器之间的信息传输同样被认为是不安全的。

2.2.2 协议流程

协议主要流程如图 1 所示，主要有 3 个阶段：初始阶段、查询与认证阶段 (A 阶段) 以及数据更新阶段 (B 阶段和 B' 阶段)，具体工作过程如下。

(1) 初始阶段

标签应存储的信息：TID、TPID、 T_{num} 。

阅读器应存储的信息：RID、 R_{num} 。

数据库应存储的信息：标签信息表、阅读器信息表、标签跟踪信息表。

标签信息表：TID、TPID、 T_{num} 、 $userinfo(M)$ ；阅读器信息表：RID、 R_{num} 、阅读器规格信息；标签跟踪信息表：车间、位置、RID、时间、TID。标签跟踪信息表参照企业管理信息系统要求设计。

(2) A 阶段：查询与认证阶段

A1: $R \rightarrow AS$: request. R 首先发送 request 请求

给 AS ，通知 AS 要发起对标签信息的读取操作。

A2: $AS \rightarrow R$: r_0 。 AS 收到 A1 的请求信息后，产生一个随机数 r_0 并返回给 R 。

A3: $R \rightarrow T$: r_0 、request. R 产生随机数 r_1 ，并将 r_1 、 r_0 以及 request 请求一起发送给 T 。

A4: $T \rightarrow R$: H_1 、 r_1 、TPID. T 收到 R 的请求命令后，产生随机数 r_2 ，然后结合标签自己的认证数值 T_{num} 以及接收到的随机数 r_1 和 r_0 计算 $H_1 = h(T_{num} || TPID || r_2 || r_1 || r_0)$ ，最后将自己的伪 ID (TPID) 连同 H_1 、 r_2 一并发给 R 。

A5: $R \rightarrow AS$: H_2 、RID、TPID、 r_2 、 r_1 。 R 接收到 A4 的请求信息后，从中提取 H_1 并结合自己的认证数值 R_{num} 计算出 $H_2 = h(R_{num} || H_1)$ ，最后将自身的 ID (RID) 连同 H_2 、TPID、 r_2 、 r_1 一并发给 AS 。

A6: $AS \rightarrow DB$: RID、TPID. AS 接收到 A5 的请求信息后，将 RID、TPID 转发给 DB。

A7: $DB \rightarrow AS$: T_{num} 、TID、 M 、 R_{num} 。 DB 根据 RID 和 TPID 的值在数据库中检索找到与之相对应的 T_{num} 、TID、 $userinfo(M)$ 和 R_{num} 值，然后将其一并发给 AS 。

A8: $AS \rightarrow R$: 认证失败或者 $userinfo(E_{R_{num}}(M, r_0))$ 。 AS 接收到 A7 后，利用 DB 返回的 T_{num} 、 R_{num} 计算 $H = h(R_{num} || h(T_{num} || TPID || r_2 || r_1 || r_0))$ ，并比较 H_2 和 H 值是否相等。若不相等或者数据库未检索到对应标签或阅读器，则认证失败，返回阅读器认证失败信息，查询结束；若相等则认证标签和阅读器合法， AS 发送标签信息 M 给 R ，然而由于 AS 与 R 之间为不安全的无线信道，因此标签信息 M 不是以明文的形式发送给 R ，而是通过一个对称加密算法 $E_k(M || r_1)$ 对 M 加密后再发送给 R ，加密密钥为阅读器的认证数值 R_{num} ，接下来由认证服务器决定是否转到 B 阶段或者结束认证协议。

其中 A1~A8 为认证服务器认证阅读器和标签阶段，供应链中用标签伪标识值可有效地防止

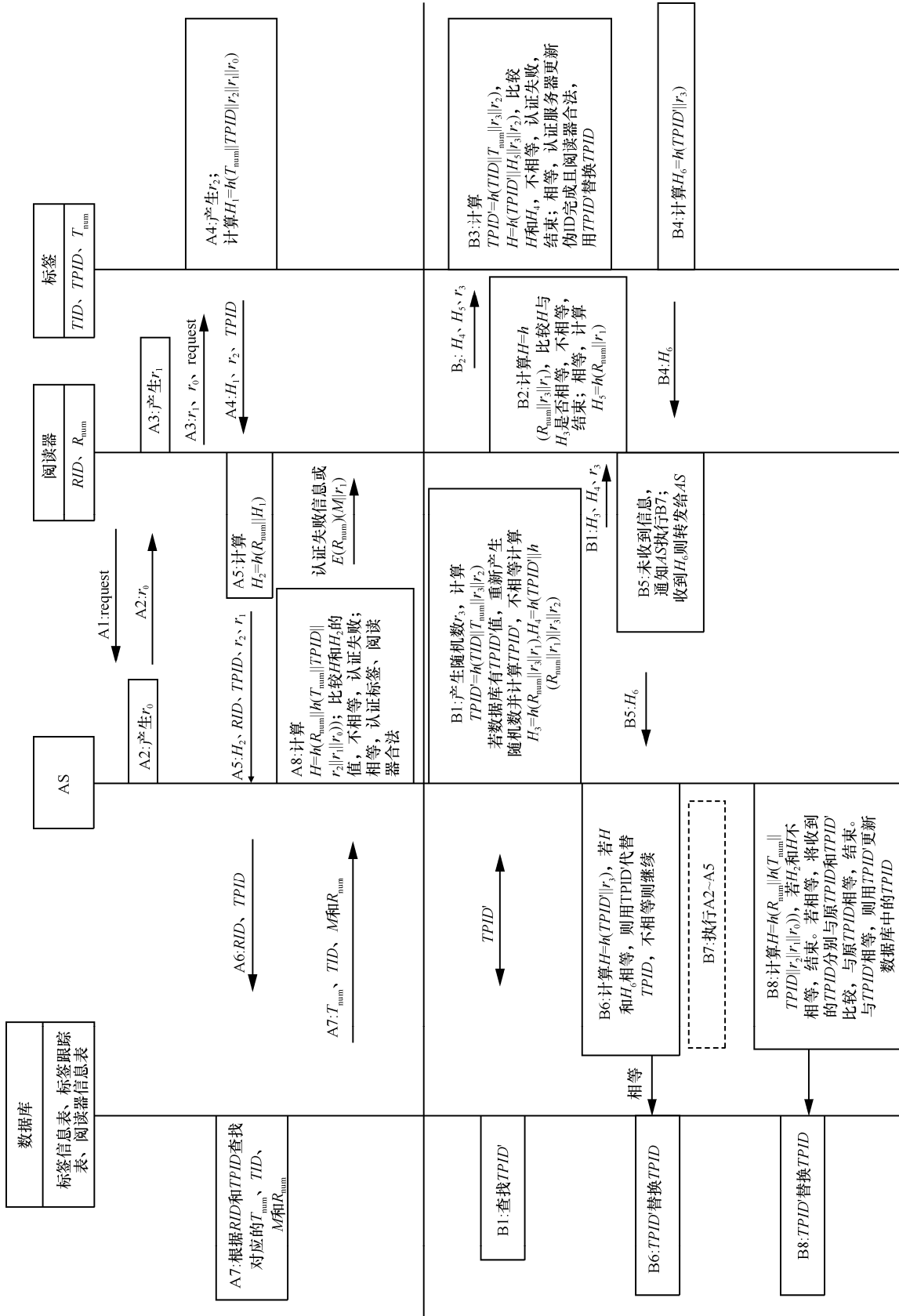


图 1 改进后的认证协议

跟踪, 认证服务器在每次成功识别标签后, 可添加一次阅读器读标签记录。

(3) 更新标签伪 ID 以及更新标签认证数值

①B 阶段: 更新数据库和标签中存储的伪 ID (TPID)

B1: $AS \rightarrow R: H_3, r_3$ 。AS 产生随机数 r_3 , 并利用 A 阶段 DB 的返回信息 A7 计算出新的标签伪 ID, 即 $TPID' = h(TID \| T_{num} \| r_3 \| r_2)$ 。然后 AS 将新产生的 TPID' 发送给 DB, DB 在其的 TPID 列表中检索是否有与 TPID' 相同的值, 若有, 则 AS 产生新的随机数 r_3 , 重新计算 TPID', 重复上述过程, 直至无相同的 TPID 值, 再利用选好的 r_3 计算 $H_3 = h(R_{num} \| r_3 \| r_1)$, $H_4 = h(TPID' \| h(R_{num} \| r_1) \| r_3 \| r_2)$ 。最后, AS 将选择好的 r_3 和 H_3, H_4 一起发送给 R。

B2: $R \rightarrow T: H_4, H_5, r_3$ 。R 接收到 B1 的请求信息后, 首先利用自己的认证数值 R_{num} 计算出 $H = h(R_{num} \| r_3 \| r_1)$, 然后对比 H 与 H_3 是否相等, 若 $H \neq H_3$, 则认证服务器认证失败, 协议结束; 若 $H = H_3$, 则计算 $H_5 = h(R_{num} \| r_1)$, 最后将 H_4, H_5 和 r_3 一起发送给 T。

B3: $T: H = h(T_{num} \| H_5 \| r_2)$ 。T 接收到 B2 的请求信息后, 首先利用自身的认证数值 T_{num} 和 TID 计算 $TPID' = h(TID \| T_{num} \| r_3 \| r_2)$, 然后用计算出的 TPID' 计算 $H = h(TPID' \| H_5 \| r_3 \| r_2)$, 然后判断 H 与接收到的 H_4 是否相等, 若 $H \neq H_4$, 通知阅读器认证失败, 协议结束; 若 $H = H_4$, 则认证阅读器合法并用新的 TPID' 代替旧的 TPID, 转入 B4 过程。

B4: $T \rightarrow R: H_6$ 。当标签认证阅读器合法后, 利用接收到的随机数 r_3 计算出 $H_6 = h(TPID' \| r_3)$, 最后发送 H_6 给 R, 表明 TPID 更新完成。

B5: $R \rightarrow AS: H_6$, 或者转至 B7 阶段, 执行步骤 A2~A5。若 R 收到 B4 的请求信息, 则说明标签更新 TPID 成功, 然后将 H_6 转发给 AS; 若 R 未收到任何信息, R 则通知 AS, 协议转至 B7。

B6: $AS: H = h(R_{num} \| h(TPID' \| r_3))$ 。AS 接收到 B5 的请求信息后, 利用 B1 阶段产生的 r_3 和 TPID' 计

算 $H = h(TPID' \| r_3)$, 然后比较 H 和 H_6 是否相等, 若相等说明标签更新 TPID 成功, 则用 TPID' 替代 DB 中的 TPID, 更新结束; 若不相等, 则转入 B7 阶段。

B7: 执行步骤 A2~A5。

B8: AS 接收到 A5 的请求信息后, 首先计算 $H = h(R_{num} \| h(T_{num} \| TPID \| r_2 \| r_1 \| r_0))$ 并与 H_2 做对比, 若 $H \neq H_2$, 协议失败并结束; 若 $H = H_2$, 则将接收的 TPID 与新、旧 TPID 进行对比, 若等于旧的 TPID, 则伪 ID 更新失败, 协议结束; 若等于更新的 TPID', 则用 TPID' 更替数据库中相应标签的 TPID, 标签伪 ID 更新成功。

其中 B7、B8 是为更新过程受到干扰, 为了防止标签中伪标识值 TPID 与数据库中对应的伪标识值 TPID 不同步而设置的; B7 和 B8 中的 r_0, r_1, r_2 是新产生的随机数, 与查询标签物品信息时的 r_0, r_1, r_2 数值上并不相同。

②B'阶段: 更新数据库与标签的认证数值 T_{num}

类似地, 在 A 阶段认证结束或在伪 ID 更新之后, 根据需要可以选择对标签认证数值进行更新, 更新流程如图 2 所示 (图 2 是在不需要验证阅读器身份时的方案, 若需验证读写器身份, 可参照 B 阶段方法相应修改), 具体步骤描述如下。

B1': $AS \Rightarrow R: H_7, r_4$ 。AS 产生随机数 r_4 , 利用 A 阶段中 T 产生的随机数 r_2 计算出 $H_7 = h(T_{num} \| r_4 \| r_2)$, 然后将 H_7, r_4 发送给 R 并发起更新标签认证数值更新请求。

B2': $R \rightarrow T: H_7, H_8, r_4$ 。R 接收到 B1' 的请求信息后, 将 H_7, r_4 一并转发发给 T。

B3': T 接收到 B2' 的请求信息后, 首先计算 $H = h(T_{num} \| r_4 \| r_2)$, 然后比较 H 与接收到的 H_7 是否相等, 若 $H \neq H_7$, 则认证失败, 协议结束; 若 $H = H_7$, 认证随机数 r_4 为服务器所发, 转入 B4' 阶段。

B4': $T \rightarrow R: H_9$ 。T 计算出新的标签认证数值 $T_{num}' = h(T_{num} \| r_4)$, 然后用新产生的 T_{num}' 计算出 $H_9 = h(T_{num}' \| r_4)$, 最后将 H_9 发送给 R, 并用 T_{num}' 替换 T_{num} 。

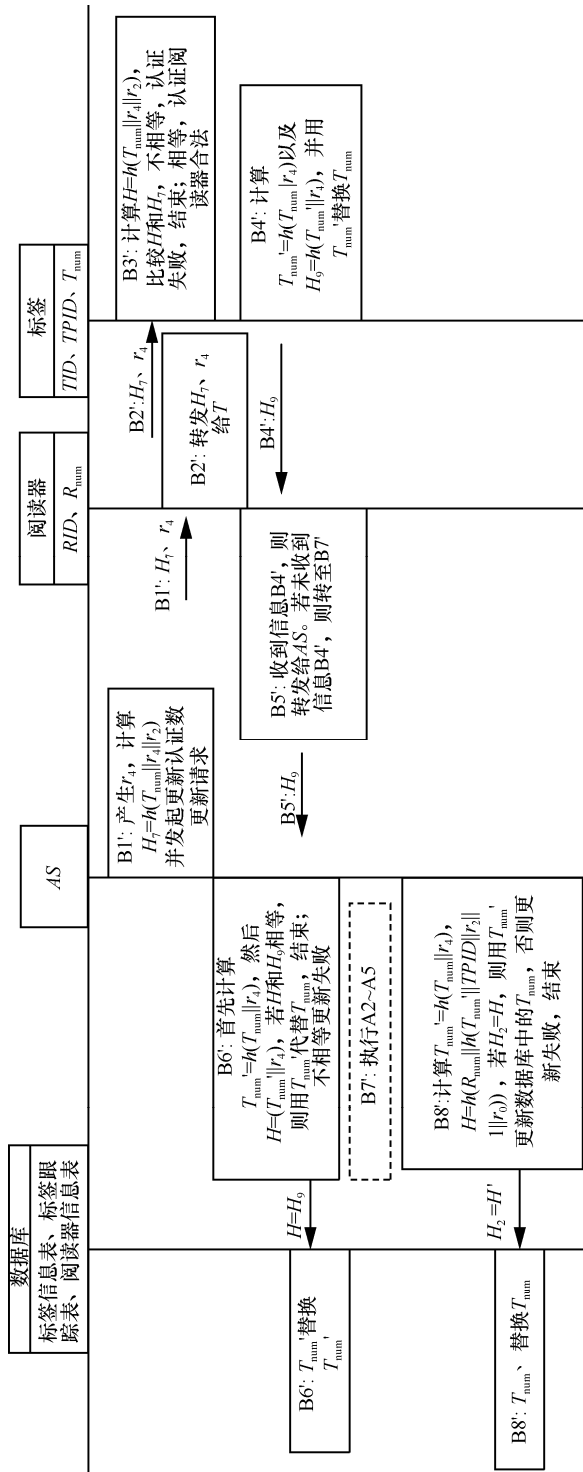


图2 更新标签认证数值

B5': $R \rightarrow AS: r_5, H_{10} = h(R_{num} || H_9)$ 。R 接收到 B4'后, 将 H_9 转发给 AS; 若没有接收到 B4', 则转至 B7'过程。

B6': AS 接收到 B5'后, 首先计算 $T_{num}' =$

$h(T_{num} || r_4)$, 然后利用新产生的 T_{num}' 计算 $H = h(T_{num}' || r_4)$ 并对比 H 与 H_9 , 若 $H = H_9$, 则说明标签更新认证数值成功, 通知数据库用新的 T_{num}' 替换旧的 T_{num} 值, 协议结束; 若 $H \neq H_9$, 标签认证数值更新失败, 协议结束。

B7': 执行 A 阶段的 A2~A5 步骤。

B8': AS 接收到 A5 后, 先计算 $T_{num}' = h(T_{num} || r_4)$, 然后用新产生的标签认证数 T_{num}' 计算 $H = h(R_{num} || h(T_{num}' || TPID || r_2 || r_1 || r_0))$ 并对比 H 与 H_2 是否相等, 若 $H = H_2$, 则说明标签认证数更新成功, 并通知数据库用 T_{num}' 替换相应标签的 T_{num} ; 否则更新失败。

同理, 也可以采用与更新标签认证数值同样的方法对阅读器认证数值进行更新, 但由于阅读器与认证服务器之间的通信不受资源等条件限制, 因此可以采用其他更便捷、有效的方式对读写器认证数值进行更新, 该内容不在本文研究范围之内, 故在此不赘述。

3 新认证协议的安全性

应用于 RFID 系统的安全认证协议主要解决三大基本问题, 分别为机密性、完整性以及可追踪安全性。针对这些要求对本文提出的安全协议分析如下。

3.1 双向认证

新的认证协议在阅读器与标签不知道相互秘密信息的情况下, 通过认证服务器 (这里将认证服务器与数据库看为一个整体) 实现了认证服务器、阅读器以及标签三方之间的相互认证以及信息更新。认证服务器 (AS) 通过计算 $H = h(R_{num} || h(T_{num} || r_2 || r_1 || r_0))$, 和阅读器发送的 $H_2 = h(R_{num} || H_1)$ 进行比较, 验证标签和阅读器是否合法, 其中 $H_1 = h(T_{num} || r_2 || r_1 || r_0)$ 由标签计算产生; 标签通过计算 $H = h(TPID || H_5 || r_3 || r_2)$ 与 $H_4 = h(TPID || h(R_{num} || r_1) || r_3 || r_2)$ 进行比较, 验证阅读器与认证服务器是否合法, 其中 H_4 和 $H_4 = h(R_{num} || r_1)$ 分别由认证服务器和阅读器计算产生。读写器通过计算 $H = h(R_{num} || r_3 || r_1)$

与 H_3 进行比较以及解码 $E_{R_{num}}(M||r_1)$ 的值, 验证认证服务器是否合法, 其中 B2 步骤读写器对 H_3 的判别不仅认证了服务器的合法性, 同时也认证了用于后续进行伪 ID 更新的随机数 r_3 的合法性。最后, 阅读器对标签身份的验证是基于认证服务器的。上述无论是标签对阅读器和认证服务器的认证, 还是认证服务器对阅读器和标签的认证, 只有拥有对应的秘密信息的合法终端才能计算并响应有效的认证消息, 最终通过相互验证。

3.2 重放攻击

本协议在 A 阶段, 用于认证标签身份和读写器身份的 H_1 和 H_2 都是分别包含标签认证数和读写器认证数以及随机数 r_0 、 r_1 、 r_2 的散列函数, 其中随机数 r_0 、 r_1 、 r_2 用来保证认证信息的新鲜性, 即使攻击者截获了以前的 H_1' 、 H_2' , 在新一轮的协议中也无法通过相应的认证; 其次, 认证服务器返回给阅读器的标签信息 $E_{R_{num}}(M||r_1)$ 也由 r_1 保证其新鲜性。在 B 阶段的伪 ID 更新中, 分别用于鉴别服务器身份和读写器身份的散列值 H_3 、 H_4 、 H_5 同样被随机数 r_1 、 r_2 、 r_3 保持其新鲜性, 即使截获之前对应的认证信息, 也无法用于本轮的验证。同理, B' 阶段也一样。

3.3 中间人攻击

整个协议中用于认证身份的信息都由各自产生的随机数和秘密信息的散列值构成, 攻击者无法在不知道对应秘密信息的情况下对认证信息进行修改而不让验证者察觉。即使在协议的初始阶段, 攻击者可以假冒成阅读器发起查询标签操作并发出 request 指令和随机数 r_0 、 r_1 , 从而进一步获得标签的返回值 H_1 、 r_1 、 $TPID$, 然而, 由于攻击者不知道阅读器的认证数 R_{num} , 攻击者同样无法得到接下来用于给服务器认证的信息 H_2 , 最终无法通过认证协议。

3.4 信息泄露

新认证协议中, 无论是标签的 ID (TID)、标签认证数 (T_{num})、阅读器的认证数 (R_{num}), 还是

标签的信息 (M) 都没有以明文的形式进行传输, 前者采用散列函数进行保护, 后者采用对称加密算法进行保护, 无论是散列函数还是对称加密算法, 在不知道对应秘密信息的情况下都无法从中获得其相应的保护信息。

3.5 前向安全

协议中用于相互认证以及信息更新的信息 H_1 至 H_9 , 都是基于秘密信息 (标签认证数和阅读器认证数) 与随机数的散列运算, 由于散列函数的单向性以及随机数的新鲜性, 即使攻击者获得了某个时刻的秘密信息 (T_{num} 、 R_{num}), 也无法推测出此时刻以前的秘密信息, 从而保证了数据的前向安全性。

3.6 标签的匿名性以及抵抗位置跟踪攻击

在对标签的认证及信息获取的过程中, 标签提供的身份标识都是伪 ID ($TPID$), 即使在更新 $TPID$ 的过程中用到了标签的 ID (TID), 但是在信息交互时都是将其与对应的秘密信息以及随机数进行散列运算后传输的, 由于散列函数的单向性, 攻击者无法从上述认证信息中获取标签的身份信息。其次, 在每次对标签进行读取及认证操作后, 服务器都可以选择对标签的 $TPID$ 进行更新, 因此, 攻击者通过获取标签 $TPID$ 来跟踪标签的操作, 将会在 $TPID$ 更新操作后失效。同时信息同步保护方案解决了标签伪 ID 更新不同步的问题, 更新过程中攻击者也无法通过监听标签和阅读器之间的信息来实施位置跟踪。

4 新方案的性能

根据第 3 节对本协议的安全性分析, 将本协议与现有几种典型的基于散列函数的认证协议的安全性进行比较, 比较结果见表 2。其中符号“×”表示协议不具备该安全特性, 符号“√”表示符合该安全特性。由表 2 中的对比结果可以看出, 本文提出的协议不仅可以满足认证服务器、读写器以及标签三方之间的相互认证需求, 而且整体的

表 2 协议安全性能分析^[7,10-14]

安全因子	散列-lock 协议	随机化散列-lock 协议	散列链协议	基于杂凑的 ID 变化协议	LCAP	本协议
ID 信息保护	×	×	√	√	√	√
重放攻击	×	×	×	√	√	√
抵抗假冒攻击	×	×	×	√	√	√
抵抗信息窃听	×	×	×	√	√	√
抵抗位置跟踪	×	×	√	√	√	√
前向安全性	×	×	√	×	√	√
信息更新	×	×	√	√	√	√
抵抗数据冲突	—	—	√	×	×	√
抵抗失同步攻击	—	—	×	×	×	√

安全性能也优于其他协议。

针对 RFID 安全协议性能的分析主要从标签与服务器所需的存储空间以及标签、阅读器、服务器的计算量等方面进行衡量,而就计算量而言,基于散列函数的认证协议计算量主要集中在对散列函数的运算上,因此本文采用统计各协议单次成功认证后,各部分(标签、阅读器、服务器)所需计算散列函数的次数进行粗略比较。其中 L 表示标签 ID 的长度, h 表示计数器的长度, H 表示一次散列运算, n 表示 RFID 系统中标签的数量, i 表示散列链的长度, E 表示一次对称加密或解密计算。

从表 3 中可以看出,本协议在标签与服务器所需的存储空间上与其他协议基本相等。在计算量方面,服务器的计算量除了 LCAP 协议以外,远小于其他协议;而标签和阅读器的计算量略大

于其他几个协议,造成这一结果的原因是,本协议不仅在标签、阅读器以及服务器三方之间互不信任的情况下实现了安全认证,同时保证了标签信息更新后与服务器之间的数据同步,在抵抗位置跟踪攻击的同时也防止了去同步攻击。

5 结束语

本文提出了一种基于散列函数的 RFID 系统安全认证协议,协议利用标签的伪 ID 实现了服务器、阅读器、电子标签三者之间的相互认证,并在对标签认证后进行认证信息的同步更新。通过对协议安全性与性能的综合分析,本协议在较低的资源消耗的情况下,很好地抵抗了如窃听、重放、篡改、跟踪、去同步等常见攻击,可为大型分布式 RFID 系统提供可靠的安全保障,具有较高的实用价值。

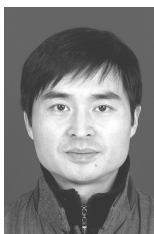
表 3 协议效率比较^[7,10-14]

性能指标	散列-lock 协议	随机化散列-lock 协议	散列链协议	基于杂凑的 ID 变化协议	LCAP	本协议
存储空间						
标签	$3L$	$3L$	$2L$	$2L+h$	$2L$	$3L$
认证服务器	$n \cdot 3L$	$n \cdot 3L$	$n \cdot 2L$	$n \cdot (2L+2h)$	$n \cdot L$	$n \cdot 3L$
计算量						
标签	$1H$	$1H$	$2H$	$3H$	$1H$	$4H$
阅读器	—	$n \cdot H$	—	—	—	$3H+E$
认证服务器	$n \cdot H$	—	$n \cdot i \cdot H$	$(n+2) \cdot H$	$1H$	$5H+E$

参考文献:

- [1] 黄玉兰. 物联网射频识别(RFID)核心技术详解:第2版[M]. 北京: 人民邮电出版社, 2012: 1-14.
HUANG Y L. Radio frequency identification development internals: 2nd edition[M]. Beijing: Posts and Telecom Press, 2012: 1-14.
- [2] GAO L, MA M, SHU Y, et al. An ultralight weight RFID authentication protocol with CRC and permutation[J]. Journal of Network and Computer Applications, 2014(41): 37-46.
- [3] 肖锋, 周亚建, 周景贤, 等. 标准模型下可证明安全的 RFID 双向认证协议[J]. 通信学报, 2013, 34(4): 82-87.
XIAO F, ZHOU Y J, ZHOU J X, et al. Provable secure mutual authentication protocol for RFID in the standard model[J]. Journal on Communications, 2013, 34(4): 82-87.
- [4] 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): 133-146.
- [5] 张敏. 基于物联网技术下的图书管理系统构建[J]. 河南理工大学学报(自然科学版), 2012, 31(3): 326-329.
ZHANG M. Research on system library management based on technology of internet of things[J]. Journal of Henan Polytechnic University (Natural Science), 2012, 31(3): 326-329.
- [6] SARMA S, WEIS S, ENGELS D. RFID systems and security and privacy implications[C]//The 4th International Workshop on Cryptographic Hardware and Embedded Systems, August 13-15, 2002, Redwood Shores, CA, USA. Berlin: Springer, 2002: 454-469.
- [7] WEIS S A, SARMA S E, RIVEST R L, et al. Security and privacy aspects of low-cost radio frequency identification systems[C]//The 1st Security in Pervasive Computing, March 12-14, 2003, Bop-pard, Germany. Berlin: Springer, 2003: 201-212.
- [8] GAO X, XIANG Z, WANG H, et al. An approach to security and privacy of RFID system for supply chain[C]//2004 IEEE International Conference on E-Commerce Technology for Dynamic E-Business, September 13-15, 2004, Beijing, China. New Jersey: IEEE Press, 2004: 164-168.
- [9] HENRICI D, MAULLER P. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers[C]//The 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops, March 14-17, 2004, Los Alamitos, CA, USA. New Jersey: IEEE Press, 2004.
- [10] LEE S M, HWANG Y J, LEE D H, et al. Efficient authentication for low-cost RFID systems[C]//The 2005 International Conference on Computational Science and its Applications, May 9-12, 2005, Singapore. Berlin: Springer, 2005: 619-627.
- [11] 陶源, 周喜, 马玉鹏, 等. 基于散列函数的移动双向认证协议[J]. 计算机应用, 2016, 36(3): 657-660.
TAO Y, ZHOU X, MA Y P, et al. Mobile mutual authentication protocol based on Hash function[J]. Journal of Computer Applications, 2016, 36(3): 657-660.
- [12] 王明斐, 魏勇, 孙挺. 基于散列函数和排列的轻量级RFID安全认证协议[J]. 湘潭大学自然科学学报, 2016(1): 115-119.
WANG M F, WEI Y, SUN T. A lightweight RFID security authentication protocol based on Hash function and arrangement[J]. Natural Science Journal of Xiangtan University, 2016(1): 115-119.
- [13] 朱洪岩, 谢晓尧, 吴景春. 基于散列函数的RFID安全认证协议改进[J]. 长江大学学报(自然科学版), 2016, 13(13): 39-43.
ZHU H Y, XIE X Y, WU J C. RFID authentication protocol development based on Hash function[J]. Journal of Yangtze University (Natural Science Edition), 2016, 13(13): 39-43.
- [14] 赵太飞, 邹波, 尹航. 基于散列链的RFID认证协议[J]. 微型机与应用, 2016, 35(19): 60-63.
ZHAO T F, ZOU B, YIN H. RFID authentication protocol based on Hash chain[J]. Microcomputer and its Applications, 2016, 35(19): 60-63.
- [15] 贝毅君, 干红华, 程学林, 等. RFID技术在物联网中的应用[M]. 北京: 人民邮电出版社, 2013.
BEI Y J, GAN H H, CHENG X L, et al. RFID technology applications in internet of things[M]. Beijing: Posts & Telecom Press, 2013.

[作者简介]



李川 (1972-), 男, 绵阳职业技术学院副教授, 主要研究方向为信号处理与传输。



李学俊 (1975-), 男, 博士, 西南科技大学计算机学院副教授, CCF 会员, 主要研究方向为数据库应用、多源图像数据融合及处理。