

基于 Hash 函数的 RFID 安全认证协议研究

龚 晶, 石 会, 邓元庆, 刘 斌

(解放军理工大学 通信工程学院, 江苏 南京 210007)

摘 要: 近年来, 射频识别(RFID)技术发展非常迅速, 未来应用将无处不在. 针对 RFID 应用中存在的安全隐患, 分析了目前具有代表性的几个基于 Hash 函数的 RFID 安全认证协议的优缺点, 比较了各自的安全性, 提出了一个基于 Hash 函数的 RFID 安全认证协议. 该协议引入标签 ID 动态更新机制, 并设计了自同步解决方案, 该协议具有防跟踪、不可分辨性、抗重放攻击、哄骗攻击、去同步攻击和拒绝服务攻击, 较好地解决了 RFID 的安全隐患问题, 特别适合于低成本、低计算量、大规模的 RFID 系统.

关键词: RFID; 认证协议; Hash 函数; 安全性; 隐私

中图分类号: TP309.1

文献标识码: A

文章编号: 1000-7180(2014)09-0135-03

Research of the RFID Authentication Protocol Based on Hash Function

GONG Jing, SHI Hui, DENG Yuan-qing, LIU Bin

(College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China)

Abstract: In recently years, radio frequency identification (RFID) technology has been widely used. For security issues of RFID, this paper analyzes the advantages and disadvantages of several recently proposed protocols and gives some comparisons of the security properties. A new secure and efficient RFID mutual authentication protocol based on Hash function is proposed. The scheme established by the refreshed dynamically and self-synchronize of the tag's ID has the properties of untraceability, indistinguishability, resistant to the replay attack, spoofing attack, desynchronize attack and denial of service attack etc., so it can effectively solve the security issues of the RFID system. The scheme is especially applied in low cost, limited computation and large-scale RFID system.

Key words: RFID; authentication protocol; hash function; security; privacy

1 引言

与目前常用的识别方式(如条码、磁卡等)相比, RFID 标签^[1-3]具备一定计算能力和存储空间、可反复使用, RFID 技术具有快速读写、移动识别、可跟踪及随时定位等优点, 目前已应用在物流、储备及零售等领域, 随着技术的发展, 未来应用将无处不在. 然而, 由于 RFID 技术利用无线射频通道交换数据, 容易受到外部环境的干扰和攻击者的恶意攻击, RFID 标签中储存的个人信息、商业情报就可能被攻击者非法获取, 从而给使用者带来很大损失. 因

此, RFID 系统的安全性正日益受到研究者的关注.

随着 RFID 系统的广泛应用, 提出了很多的 RFID 认证协议, 主要分为三类: 基于对称加密算法或公钥加密算法的重量级安全认证协议; 基于 Hash 函数的安全认证协议; 基于简单逻辑运算的轻量级安全认证协议.

Sarma 等人提出了 Hash 锁协议^[4], 该协议要求标签具有一个 Hash 函数功能模块, 协议通过传输标签 key 的摘要值 metaID 来识别标签, 由于 Hash 函数的单向性, 攻击者不能获取标签的标识 ID, 但由于标识 ID 没有动态更新机制, Hash 锁协

收稿日期: 2013-11-12; 修回日期: 2014-01-09

基金项目: 国家自然科学基金项目(61271254)

议在安全上存在较大的隐患.

为了解除 Hash 锁协议^[5]中不安全因素,文献[3]中的标签回应阅读器的查询每次都是随机的,防止了攻击者根据特定输出的位置追踪攻击,但通过认证后的标签标识 ID 仍以明文的形式在不安全信道上传输,攻击者可以通过窃听来截获 ID,对标签及数据库实施有效的假冒和重放攻击.为了解决前向安全性问题,Hash 链协议^[6-7]中的标签内部集成了两个不同的 Hash 函数 G 和 H 模块,标签中储存其初始秘密值 $S_{k,1}$,它是可更新的,每个标签的 $S_{k,1}$ 都是唯一的,但它每次认证后通过 H 函数会自动更新.本协议采用了标识 ID 动态更新机制,确保了 RFID 系统的前向安全性和不可跟踪性,但标签内部需要有两个 Hash 函数模块,极大地增加了标签的成本.很多基于 Hash 函数的 RFID 认证协议^[8-9],但都或多或少地存在安全性隐患以及数据库计算量过大造成自动识别效率低的问题.

2 协议设计

本文提出一种安全的 RFID 双向认证协议,该协议采用挑战-应答机制,安全性高,具有防跟踪、抗重放攻击、欺骗攻击、去同步攻击和拒绝服务攻击,适合于标签数目较多的系统,且识别效率较高.

2.1 初始条件

从前面已获知:数据库与读写器都具有较强的

储存能力和计算能力,可以运行安全性很高的高级加密算法,因此相互之间的通信通常认为是安全的;两者彼此信任,即阅读器相对数据库是合法的,数据库相对阅读器是合法的;而标签与读写器之间的信息传输是不安全的.本协议主要讨论标签与阅读器之间的双向认证.

标签内部含有一个 Hash 函数(如 SHA-1, MD5 等,记为 H)的功能运算模块和一个伪随机数生成器功能模块,这在低成本标签中是可实现的,在初始状态下,数据库为标签分配标签的标识 ID 以及秘密值 key,标识 ID 是唯一的,此标识 ID 在后续认证过程中自动更新来防范恶意的追踪,而密钥 key 是固定不变的.后端数据库记录了每个标签的标识 ID 和密钥 key,除此之外,对每一个标签 Tag 还有两个字段,分别记录其标签 ID 的摘要值 $H(ID)$ 和更新前上一次标签 ID 的摘要值 $H(ID_{last})$,在首次认证前, $H(ID_{last})$ 为 0.引入 $H(ID_{last})$ 主要是当出现标签和数据库失去同步时,仍然能够实现双向认证且有相应的同步机制来恢复同步.所以数据库中每一个标签记录有 4 个字段信息,分别为 $(ID, key, H(ID), H(ID_{last}))$.

2.2 协议流程描述、

协议的认证过程如图 1 所示,其中 $H()$ 表示单向 Hash 函数, $\oplus$ 表示逻辑异或运算.

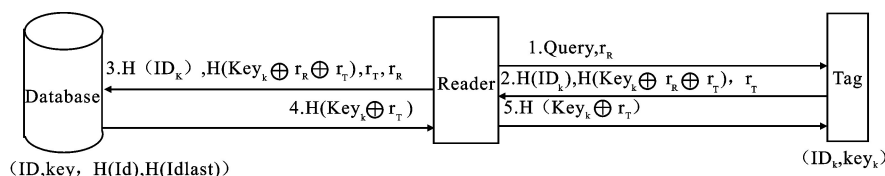


图 1 本文认证协议

本文协议的认证过程如下:

(1) 读写器生成一个随机数 r_R , 并和认证请求 Query 一起发给标签 k 作为认证请求.

(2) 标签收到该 Query 请求后,产生一随机数 r_T , 首先计算其标识 ID_k 的摘要值 $H(ID_k)$, 再计算其标签秘密值 key_k 与随机数 r_R, r_T 共同异或后的摘要值 $H(Key_k \oplus r_R \oplus r_T)$, 将两运算结果连同随机数 r_T, r_R 一起发送给阅读器.

(3) 阅读器将从标签发来的认证信息连同自身产生的随机数 r_R 一起组成四元组认证信息 $H(ID_k), H(Key_k \oplus r_R \oplus r_T), r_T, r_R$ 发送给数据库进行认证. 数据库根据收到的 $H(ID_k)$ 在数据库记录中 $H(ID)$ 字段进行查询, 这里分三种情况讨论.

A: 如果数据库中查询结果存在, 将该记录的标签秘密值 key 取出, 计算其与随机数 r_R, r_T 异或后的摘要值 $H(Key \oplus r_R \oplus r_T)$, 判断其与收到的 $H(Key_k \oplus r_R \oplus r_T)$ 是否一致? 若不一致, 认证失败, 该标签非法. 若一致, 标签通过认证. 同时更新数据库该记录的标签 ID, $ID \leftarrow ID_k \oplus H(ID_k)$; 再更新该记录 $H(ID)$ 字段, 计算已更新 ID 的摘要值: $H(ID_k)$ 替代老的 $H(ID)$.

B: 如果查询结果不存在, 则以此 $H(ID_k)$ 在数据库记录中 $H(ID_{last})$ 字段进行查询, 如果存在记录, 取出 key, 计算 $H(Key \oplus r_R \oplus r_T)$, 判断其与收到的 $H(Key_k \oplus r_R \oplus r_T)$ 是否一致? 若一致, 标签通过认证. 这种情况是由于当某种原因(如信道问题, 有

攻击发生等)数据库已经更新了标签的 ID,但标签还未更新,两者不同步造成的。

C:如果在数据库记录中字段 $H(ID)$ 和 $H(ID_{last})$ 中都找不到符合 $H(ID_k)$ 信息的记录,则说明标签不合法,不能通过认证,协议终止。

(4) A、B 两种情况中,当标签通过认证后,数据库将标签秘密信息 key 与标签发来的随机数 r_T 相异或后用 Hash 函数计算其摘要值 $H(Key \oplus r_T)$ 经阅读器转发给标签,表示标签合法。

(5) 标签收到经阅读器转发的数据库的认证信息,计算标签本身保存的 key_k 与先前发出的随机数异或后的摘要值 $H(Key_k \oplus r_T)$,再与收到的认证信息 $H(Key \oplus r_T)$ 相比较,若不一致,则阅读器是非法的。若一致,标签对阅读器的认证通过,此时标签 K 要对标签的标识 ID 进行更新, $ID \leftarrow ID_k \oplus H(ID_k)$ 。

3 协议安全性分析及比较

本协议是一个双向认证协议,前三步是阅读器对标签的认证,经过 $H(ID)$ 或 $H(ID_{last})$ 的检索及 $H(Key_k \oplus r_R \oplus r_T)$ 的计算比较,阅读器通过对标签的认证;后两步是标签对阅读器的认证,经过 $H(Key_k \oplus r_T)$ 的计算比较,标签通过对阅读器的认证。根据前述 RFID 系统的安全需求,对本文提出的安全协议进行如下分析:

(1) 机密性:本文协议中,阅读器与标签之间传输的认证信息都通过具有单向性的 Hash 函数加密,攻击者无法通过窃听的信息来解密得到原始信息。

(2) 完整性:在传递的认证信息中都引入了随机数 r_R 和 r_T 的参与,由于每次认证生成的随机数都不同,则摘要值就不同。即使被攻击者截获,进行假冒攻击或重放攻击,但由于随机数的不同,阅读器和标签都很容易分辨出来,不能通过认证。

(3) 不可分辨性:由于传递的认证信息中,标签的标识 ID 均通过单向函数加密,无法分辨出是哪一张标签的信息;同时由于本协议中每次认证后标识 ID 均自动更新,所以标识 ID 的摘要值 $H(ID)$ 也在变化,即使获得了同一标签的多次 $H(ID)$ 值,也无法确认是否是同一张标签发出的。

(4) 防追踪:在该协议中,标签在每次完成双向认证之后,均要更新标签的标识 ID,因此,摘要值 $H(ID)$ 也在更新;且每次计算 $H(Key_k \oplus r_R \oplus r_T)$ 都引入了随机值 r_T ,计算结果均不一样。当非法阅读器想要根据截获到的标签的响应信息 $H(ID)$ 及 H

$(Key_k \oplus r_R \oplus r_T)$ 意图跟踪以及用户位置隐私攻击难以实现。

(5) 前向安全性:当攻击者获得标签的秘密信息如 ID 和 key 后,利用了 Hash 的单向性来更新标签的密钥 ID 号 $ID \leftarrow ID_k \oplus H(ID_k)$,无法用更新后的 ID 来推算以前的标识 ID,保证了前向安全性。

(6) 抗异步攻击:当攻击者以某种方式建立一种不同步状态使数据库和标签的标识 ID 未同步更新,即阅读器已通过对标签的认证,数据库中已更新标签的 ID,此时,攻击者阻止标签收到阅读器发来的认证信息 $H(Key_k \oplus r_T)$ 或更改此认证信息,合法标签会认为此次阅读器未通过认证或通信失败,因此标识 ID 不会更新。但是本协议能保证此次 ID 的不同步不会影响标签的下次认证。在下次认证中,由于在数据库的每个记录中,还存在 $H(ID_{last})$ 字段,它保存有标签上一次 ID 的摘要值 $H(ID)$,能够对未更新 ID 的标签通过认证,使标签能够更新其 ID,再一次保持同步。由于有同步机制的保证,虽然标识 ID 在每次正确认证后都更新,该协议也能在分布式网络环境中使用。

将本协议与前述几个典型的基于 Hash 函数的认证协议进行安全性比较,如表 1 所示,其中 $\times$ 表示不安全, $\checkmark$ 表示安全。从表中可以看出,本文协议的安全性是符合 RFID 系统的安全性需求的。

表 1 协议安全性能比较

安全性能指标	Hash 锁	随机 Hash 锁	Hash 链	ID 变化协议	分布式 C-R	本文协议
机密性	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
完整性	$\times$	$\times$	$\times$	$\checkmark$	$\checkmark$	$\checkmark$
抗异步攻击	$\checkmark$	$\checkmark$	$\checkmark$	$\times$	$\checkmark$	$\checkmark$
双向认证	$\times$	$\times$	$\times$	$\checkmark$	$\checkmark$	$\checkmark$
前向安全	$\times$	$\times$	$\checkmark$	$\checkmark$	$\times$	$\checkmark$
防追踪	$\times$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$

4 结束语

本文提出了基于 Hash 函数的 RFID 双向认证协议,该协议能有效地解决目前 RFID 系统面临的安全问题,特别适合于低成本、大规模的电子标签系统,具有较高的实用价值。

参考文献:

- [1] 李晶晶,王德明,胡建国,等,RFID 标签芯片验证平台[J]. 微电子学与计算机,2012,29(10):144-147.

(下转第 142 页)

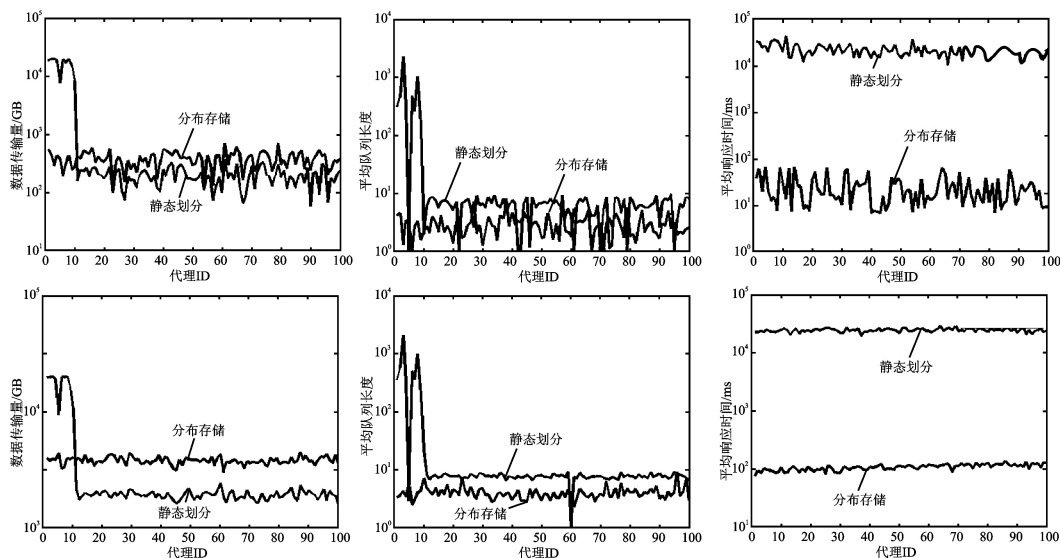


图 7 代理数为 100 和 1 000 情况下的对比结果

- on Software Engineering, 2003, 29(12): 1059-1071.
- [3] Li G, Cheung A, Hou S, et al. Historic data access in publish/subscribe[C]// Proceedings of ACM International Conference on Distributed Event-based Systems. [s. l.]:IEEE, 2007: 80-84.
- [4] Sourlas V, Paschos G S, Flegkas P, et al. Caching in content-based publish/subscribe systems [C]// Proceedings of GLOBECOM. Honolulu, HI:IEEE, 2009: 1-6.
- [5] Stoica I, Morris R, Karger D, et al. Chord: A scal-

able peer-to-peer lookup service for internet applications[J]. ACM SIGCOMM Computer Communication Review, 2001, 31(4): 149-160.

[6] Breslau L, Cao P, Fan L, et al. Web caching and Zipf-like distributions: Evidence and implications[J]. INFOCOM, 1999(1):126-134.

作者简介:

黄 强 男, (1977-), 博士, 高级工程师. 研究方向为雷达数据处理、多传感器数据融合、目标跟踪.

(上接第 137 页)

- [2] 齐爱琴, 申永军. 基于天线传感器网络的双因子认证协议的设计与研究[J]. 微电子学与计算机, 2012, 29(1): 121-123.
- [3] 张文丽. 基于 Hash 函数的 RFID 安全认证协议的设计[J]. 电脑与信息技术, 2012, 20(2): 56-59.
- [4] 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.
- [5] Rivest L, Weis A, Sarma E, et al. Security aspects of low-cost RFID systems [C] // Proc of the 1st Security in Computing. Berlin: Springer, 2003: 202-212.
- [6] OhKubo M, Suzuki K, Kinoshita S. Hash-chain based forward secure privacy protection scheme for low-cost RFID[C] // Proceedings of the 2004 Symposium on

Cryptography and Information Security. Sedai: IEEE, 2004: 719-724.

- [7] 王娟. 基于散列函数的 RFID 认证协议研究[D]. 南京: 南京邮电大学, 2011.
- [8] 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.
- [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: 自然科学版, 2012, 39(1): 173-178.

作者简介:

龚 晶 女, (1968-), 副教授. 研究方向为信息安全与电子技术