第 38 卷 第 2 期 计 算 机 工 程 2012 年 1 月
Vol.38 No.2 Computer Engineering January 2012

• 安全技术 • 文章编号：1000—3428(2012)02—0151—02 文献标识码：A 中图分类号：TP309

一个超轻量级的 RFID 认证协议

马巧梅[1,2]，王尚平[1]

(1. 西安理工大学计算机科学与工程学院，西安 710048；2. 宝鸡文理学院计算机科学系，陕西 宝鸡 721007)

摘 要：针对 UMA-RFID 协议的安全漏洞，提出一个改进的超轻量级的 RFID 认证协议。通过修改 UMA-RFID 协议的交互方式，避免泄露标签标识符，保证读写器应答消息的新鲜性。该协议仅使用异或操作和移位操作，降低了对标签计算能力和存储能力的要求。分析结果表明，该协议可有效抵抗假冒攻击和重传攻击，适合于较低成本的 RFID 系统。

关键词：无线射频识别；认证协议；超轻量级；安全性分析

Ultra-lightweight RFID Authentication Protocol

MA Qiao-mei[1,2], WANG Shang-ping[1]

(1. School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China;
2. Department of Computer Science, Baoji University of Arts and Sciences, Baoji 721007, China)

【Abstract】Aiming at the securing hole of UMA-RFID protocol, a ultra-lightweight RFID mutual authentication protocol is proposed. Through improving the interaction of UMA-RFID, the identifier of tag can be avoidably leaked and the freshness of message for tag answering can be realized each time. XOR operation and shift operation are merely utilized in the proposed protocol, and the demand for the capacity of calculation and storage of tag are reduced. The analysis of security and performance shows that this protocol can efficiently resist spoofing attack, which is suitable for much lower-cost RFID system.

【Key words】Radio Frequency Identification(RFID); authentication protocol; ultra-lightweight; security analysis

DOI: 10.3969/j.issn.1000-3428.2012.02.049

1 概述

无线射频识别(Radio Frequency Identification, RFID)系统作为一种非接触式自动识别技术，在带来成本节约和效率提高的同时，也带来了安全和隐私的风险。现有的大多数 RFID 交互认证协议都是基于 Hash 函数[1]，但是，RFID 系统中标签的计算能力和存储能力有限，Hash 函数要求 RFID 标签具有较高的计算能力和成本要求。对于较低成本的 RFID 标签而言，设计安全、成本较低的 RFID 交互认证协议成为具有挑战性的研究课题。为此，本文提出一个改进的超轻量级的 RFID 相互认证协议。

2 相关知识

文献[2-3]提出一个仅使用简单的按位逻辑运算的超轻量级 RFID 相互认证协议族(称为 UMAP)，包括 LMAP[2]和 EMAP[3]，该协议族在后来被发现一些恶意的攻击。文献[4]提出一个超轻量级且低成本的 RFID 认证协议(称为 SASI)。一些协议指出 SASI 存在安全漏洞，但它仍然是超轻量级协议设计中的一个里程碑。

根据 UMAP 协议族和 SASI 协议，提出 Gossamer 协议。作为 Gossamer 的发展，文献[5]提出了一个新的超轻量级 RFID 相互认证协议，称为 UMA-RFID，协议的执行过程如图 1 所示。文献[6]对 UMA-RFID 协议的安全性进行分析，指出了该协议容易受到另外一些恶意的攻击，如跟踪和去同步化。在 UMA-RFID 协议中，因为攻击者可以假装为合法的读写器向标签发送认证请求 Query，攻击者获取标签的响应 ID_{T0}，在下一次认证过程中，当真正合法的读写器发送认证请求时，攻击者响应刚才所得到的消息 ID_{T0}，这样使得真正合法的标签远离而去，并没有进行认证，于是该协议不能抵抗假冒攻击。另外，由于标签对于读写器的响应消息始终是消息 ID_{T0}，攻击者可以截取标签的响应信息 ID_{T0}，然后不停地向读写器发送截取的该信息 ID_{T0}，从而对系统造成威胁，甚至可能会使系统瘫痪，造成对后端数据库的重传攻击。上述分析表明，该协议不能抵抗假冒攻击和重传攻击。

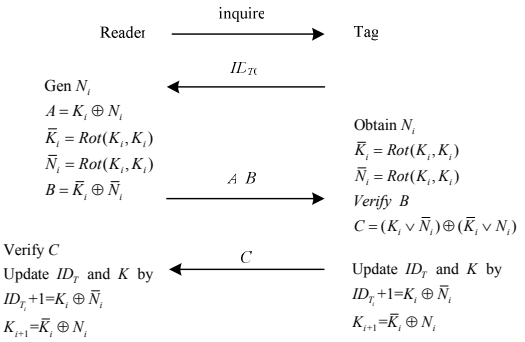

图 1 UMA-RFID 协议

综上所述，UMA-RFID 协议既不能抵抗跟踪和去同步化，也不能抵抗假冒攻击和重传攻击。造成上述安全隐患的主要原因是：

(1)读写器向标签发起询问请求时，没有产生随机数，不具有随机性。

基金项目：国家自然科学基金资助项目(60873268)；陕西省教育厅科学研究计划基金资助项目(09JK678, 09JK660)

作者简介：马巧梅(1983－)，女，硕士，主研方向：网络与信息安全；王尚平，教授、博士

收稿日期：2011-04-12 **E-mail：**mqm0707@163.com

(2)标签对于读写器的应答，每次应答都是不变的 ID_{T0}，也不具有随机性，同时泄露标签标识符 ID_{T0}。

本文以 UMA-RFID 协议的安全漏洞为目标，通过改进协议交互，避免泄露标签标识符 ID，实现每次标签对读写器应答消息的新鲜性，提出一个改进的超轻量级的 RFID 相互认证协议。

3 改进的超轻量级协议

初始化协议：假设读写器(Reader)和后端数据库(DB-Back)之间是安全信道，读写器和标签(Tag)之间是不安全信道，只考虑读写器和标签之间的通信。标签和读写器分别只需存储有一个静态的唯一的标签标识符 ID，ID 的长度为 128 bit。标签中有一个伪随机数发生器，且标签仅需进行位操作(例如 XOR、OR、AND)和移位操作。读写器有很大的计算能力。$Rot(A, B)$表示 A 向左旋转 n bit，n 是 B 中 1 的个数。新的协议如图 2 所示。

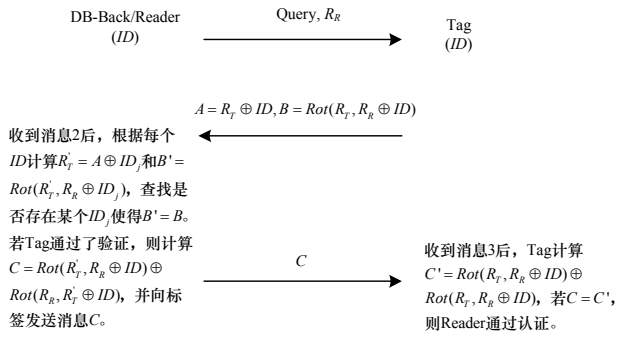

图 2 改进的超轻量级协议

按照消息传递的顺序对改进的协议执行过程描述如下：

Step1 RFID 读写器产生一个随机数 R_R，向标签发送一个 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。

当发生多个标签冲突时，会执行一次冲突仲裁过程，如二进制搜索算法[7]，这一过程完毕后会从中选取一个标签与读写器进行信息交互。

Step2 在 Step1 中被选中的标签产生一个伪随机数 R_T(ISO 和 EPC GEN2 标准都支持标签中伪随机数的产生)，并计算 $A = R_T \oplus ID$、$B = Rot(R_T, R_R \oplus ID)$，其中，$ID$ 是标签唯一的标识符。标签将 A、B 发送给读写器，读写器将 A、B 转发给后端数据库。

Step3 后端数据库收到消息 2 后，根据自己缓存中的每个 ID 计算 $R_T^{'} = A \oplus ID$ 和 $B' = Rot(R_T^{'}, R_R \oplus ID_j)$，然后查找是否存在某个 ID_j ($1 \leqslant j \leqslant m$，$m$ 为标签的最大个数)使 $B' = Rot \cdot (R_T^{'}, R_R \oplus ID_j)$ 与 $B = Rot(R_T, R_R \oplus ID)$ 相等，即 $B' = B$，如果有，则标签认证通过，认为该标签是合法的。并将 $C = Rot \cdot (R_T^{'}, R_R \oplus ID) \oplus Rot(R_R, R_T^{'} \oplus ID)$ 发送给标签；否则，返回给标签认证失败的消息，认为标签是非法的。

Step4 标签收到消息 3 后，标签根据存储器的 ID、R_T 及 R_R 计算 $C' = Rot(R_T, R_R \oplus ID) \oplus Rot(R_R, R_T \oplus ID)$，然后验证 C' 与收到的消息值 C 是否相等，若相等，则读写器认证通过，此时标签处于锁定状态。

4 安全性与性能分析

4.1 安全性分析

假冒攻击、重传攻击、追踪及去同步化是 RFID 协议面临的常见安全威胁，分析本文提出的协议针对这 4 种安全威胁的抵抗能力，说明协议的安全性。

(1)假冒攻击：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；攻击者获取标签的响应：$A = R_T \oplus ID$，$B = Rot(R_T, R_R \oplus ID)$；在下一次认证过程中，当真正合法的读写器发送 Query 和 $R_R^{'}$ 时，攻击者通过后向信道 $T \rightarrow R$ 响应刚才所得的信息 $A = R_T \oplus ID$，$B = Rot(R_T, R_R^{'} \oplus ID)$。

但是由于读写器在每一次认证会话过程中都会产生一个新的伪随机数，即 $R_R \neq R_R^{'}$，因此攻击者无法假冒合法读写器进行假冒攻击，即该协议可以抵抗假冒攻击。

(2)重传攻击：读写器与标签的交互过程中的数据即使被攻击者收集，在以后的协议执行过程中重放，也不能对协议构成威胁。

这是因为读写器与标签的交互过程中是利用随机数 R_R 和 R_T 保证数据的新鲜性的，因此用过去的数据进行欺骗，已经失去了时效性，标签或后端数据库能够很容易地检验出来是否是新鲜的消息，以防止重放攻击的发生，所以，该协议对重传攻击具有安全性。

(3)追踪：攻击者截获标签的响应：$A = R_T \oplus ID$，$B = Rot(R_T, R_R \oplus ID)$，然后通过认真分析该响应来跟踪发出该响应的标签。

由于在每一次的认证会话过程中，标签都产生新的伪随机数 R_T，因此攻击者也无法从该协议信息中判断是哪个标签做出的该响应。所以，该协议对追踪攻击具有安全性。

(4)去同步化：由于标签的 ID 是固定的，因此在协议的执行过程中，即使出现信息丢失或者是电源中断或与后端数据库失去连接，都不会影响后端数据库而造成协议执行障碍。

(5)隐私保护：标签对于读写器询问的应答消息：$A = R_T \oplus ID$，$B = Rot(R_T, R_R \oplus ID)$，即使攻击者获取消息 A、B，也无法得知标签的唯一标识 ID，同样对于消息 $C = Rot(R_T^{'}, R_R \oplus ID) \oplus Rot(R_R, R_T^{'} \oplus ID)$ 也是如此。因此，该协议保护了标签的隐私信息。

4.2 性能分析

RFID 协议的性能主要通过标签的存储空间、计算需求等方面的表征，设 L 为密钥的长度或者认证消息的长度。本文协议与 LMAP[2]、EMAP[3]、SASI[4]和 Lee 协议[5]的性能比较如表 1 所示。

表 1 超轻量级 RFID 协议的性能对比

性能指标	LMAP	EMAP	SASI	Lee 协议	本文协议
隐私保护	不安全	不安全	安全	安全	安全
相互认证性	不安全	不安全	安全	安全	安全
追踪性	不安全	不安全	安全	不安全	安全
去同步化	不安全	不安全	安全	不安全	安全
数据库中标签所需内存	6L	6L	4L	3L	1L
标签内存	6L	6L	7L	5L	3L
标签运算	∧，∨，+，⊕	∧，∨，⊕	∧，∨，+，⊕，Rot	⊕，Rot	⊕，Rot

(下转第 158 页)