第38卷 第18期
Vol.38 No.18

计 算 机 工 程
Computer Engineering

2012年9月
September 2012

• 安全技术 •

文章编号：1000—3428(2012)18—0126—04 文献标识码：A 中图分类号：TP391

基于流密码的RFID安全认证协议

龚洁中，陈恭亮，李林森，李建华

(上海交通大学信息安全工程学院，上海 200240)

摘 要：针对无线射频识别(RFID)认证协议安全性较差的问题，在分布式RFID询问-应答认证协议的基础上，设计一个基于流密码算法的RFID安全认证协议。理论分析结果表明，该协议能够抗假冒攻击、重传攻击、追踪，解决去同步化问题，并使后台数据库的响应速度更快，实用性更强。

关键词：无线射频识别；流密码；安全认证协议；假冒攻击；重传攻击；追踪；去同步化

RFID Secure Authentication Protocol Based on Stream Cipher

GONG Jie-zhong, CHEN Gong-liang, LI Lin-sen, LI Jian-hua

(School of Information Security Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

【Abstract】 Aiming at the security problem of Radio Frequency Identification(RFID) authentication protocol, this paper designs a secure RFID authentication protocol based on stream cipher, inspired from the challenge-response-based RFID authentication protocol for distributed database environment. Theory analysis proves that the proposed protocol can prevent several attacks including spoofing attack, replay attack, tracking and desynchronization. And it improves the efficiency of searching on the back-up database which makes the protocol more applicable.

【Key words】 Radio Frequency Identification(RFID); stream cipher; secure authentication protocol; spoofing attack; replay attack; tracking; desynchronization

DOI: 10.3969/j.issn.1000-3428.2012.18.034

1 概述

无线射频识别(Radio Frequency Identification, RFID)技术通过利用射频通信，能够对单个物体对象进行机器的自动识别，并可以在各种恶劣的环境中工作，极大地方便了人们对各类物体(包括人)的辨识和管理。目前该项技术已经广泛应用于各种生产活动以及日常生活，例如物流管理、零售结算、门禁系统、公交卡、校园卡等，作为物联网的关键技术，其在未来十年的发展必然是不可限量。

一个典型RFID系统的硬件组成包括RFID电子标签(Tag)、RFID读写器(Reader)和后台数据库(Database)3个部分；而在软件组成方面，除了必要的数据管理软件外，最重要的就是用于读取标签对应数据信息的认证协议。但一直以来，由于缺乏安全可靠的标签数据保护机制，RFID系统的安全性不断被质疑。

总体来说，RFID的安全问题包括隐私和认证2个方面[1]。由于读写器无需经过身份认证即可读取任意标签信息，因此引发了隐私权的问题，此外还牵涉到定位追踪的问题；而认证问题是由于电子标签在被读取时无需被认证，从而存在电子标签被克隆、篡改等威胁。因此，亟需设计出能够有效解决这些问题的安全协议。

本文认为一个安全且实用的RFID认证协议应该满足以下要求：(1)双向认证；(2)不可追踪；(3)抗假冒和重传攻击；(4)通信数据量不太大；(5)所用的算法硬件实现成本低；(6)后台数据库计算负荷不能过大；(7)适用于分布式数据库环境。根据上述要求，再结合流密码算法的一些特性，本文提出一个更为实用的RFID安全认证协议。

2 相关研究

目前，基于密码技术设计的安全协议已经有很多，其中以Hash函数为基础的安全协议设计备受关注，比较著名的有Hash-Lock协议[2]、随机Hash-Lock协议[3]、Hash-Chain协议[4]、分布式RFID询问-应答认证协议[5]、基于杂凑ID变化协议[6]、LCAP协议[7]等，此外还有其他一些非Hash函数的安全机制，例如重加密协议、轻量级块密码认证机制。以上这些协议都还存在缺陷，安全性有待进一步的提高。例如：Hash-Lock协议使用metaID来替代真实的ID号作为查询信息，但由于metaID是保持不变

基金项目：国家自然科学基金资助项目(61071078)

作者简介：龚洁中(1983－)，男，博士研究生，主研方向：密码分析，RFID协议，网络安全；陈恭亮，教授、博士、博士生导师；李林森，副教授、博士；李建华，教授、博士生导师

收稿日期：2011-09-29 **修回日期**：2011-12-30 **E-mail**：gongjiezhong@sjtu.edu.cn

的，并且 ID 是以明文方式在不安全信道中传递的，因此能够被跟踪，也容易受到假冒和重传攻击，完全不符合安全要求。Hash-Chain 协议需要使用 2 个不同的 Hash 函数，标签 ID 需要不断地自主更新，其实际上是一个只能对标签进行认证的单向认证协议，非常容易受到重传和假冒攻击，后台数据库的计算负荷会很大，并且实现成本很高。分布式 RFID 询问-应答认证协议是一种适用于分布式数据库环境的双向认证协议，本身没有明显的安全漏洞，但由于需要进行 2 次 Hash 运算，并且电路中还需要集成随机数发生器模块，不适用于低成本 RFID 电子标签，另外后台数据库的遍历 Hash 运算查找也将造成很大的计算负担。文献[8]的结论也表明，单纯地利用逻辑与、或、异或和模加运算很难设计出一个安全的轻量级认证协议。

3　基于流密码的认证协议

当前，流密码算法的发展达到了一个较高的水平，欧洲 ECRYPT 项目中提出了很多优秀而又安全的流密码方案，不但速度快，而且构造简单，硬件实现所需门数少。例如，Grain v1 大概需要 1 700 门，Trivium[9]大概需要 3 000 门[10]。同时，一个安全的流密码算法必然会是一个很好的随机数发生器，并且也可以作为 hash 函数使用。本文对 Trivium 算法作为 hash 函数的表现做了测试：在短输入明文的环境中，每改变输入序列 1 个比特位，测试输出结果的比特位改变比例。为此，在实验中采用 160 bit 输入来分别测试 30 bit、50 bit 以及 80 bit 输出状态下的比特位变化率，实验结果如表 1 所示，完全满足 hash 函数所需要的雪崩特性。由于流密码的输出具有可变长特性，因此在不同规模的 RFID 系统中，可以复用同样的协议设计，只需对输出参数做出调整，就能实现不同的安全级别。

表 1　Trivium 算法的雪崩效应

输出/bit	最大比特位变化率/(%)	最小比特位变化率/(%)	平均比特位变化率/(%)
30	73.3	26.7	50.6
50	70.0	32.0	51.2
80	62.5	40.0	49.7

目前的协议大多采用一种 3 轮协议模式，本文的协议设计中仍沿用这一模式，同时对分布式 RFID 询问-应答认证协议做了很多改进。在描述协议之前，先对初始条件做一些必要的设定：

(1)RFID 电子标签包含唯一的不变 ID 号(记为 *IDs*)，同时具有一个可变 ID 号(记为 *IDv* ，可看作一个可更新的随机数)，能够执行流密码算法(假如输入密钥和初始值分别为 K、IV ，则输出密钥流记为 $G(K,IV)$ ，并且输出结果按照一定的长度要求可划分为 3 个部分，分别记为 G_1、G_2、G_3 ，并能记录被非正常访问次数 c (一次常规访问后清 0)。

(2)RFID 读写器还具有生成伪随机数的能力。

(3)后台数据库存储着电子标签的 *IDs* 及其对应的一些相关信息，其所在服务器具有大规模运算能力。

整个协议的执行过程如图 1 所示。

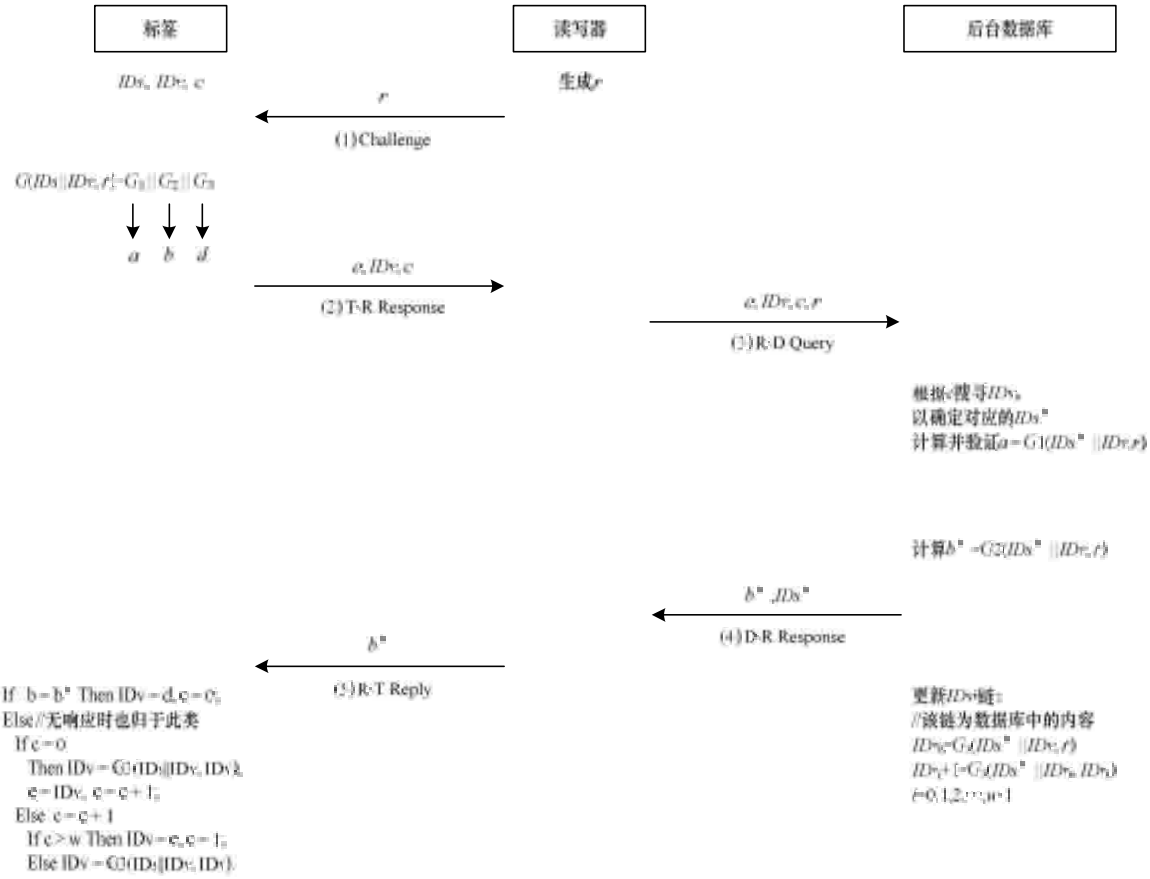

图 1　协议过程

下面根据消息传递的次序对设计方案做具体描述:

(1)Challenge

RFID 读写器生成伪随机数 r，并将其发送给目标 RFID 电子标签，提出认证请求。

(2)T-R Response

标签计算 $G(IDs \| IDv, r) = G_1 \| G_2 \| G_3 = a \| b \| d$，并将 a、IDv、c 发送给读写器。为方便叙述，将整个输出序列分成的三部分分别记为 a、b、d，并将其分别对应于虚拟划分的运算输出 G_1、G_2、G_3。

(3)R-D Query

RFID 读写器收到来自标签的响应后，将 a、IDv、c 连同 r 发送给后台数据库请求查询。

(4)D-R Response

后台数据库收到查询请求后，先根据其中的 c 确定查询 IDv 的数据域，这与 IDv_i 在后台数据库中的存储结构有关，如图 2 所示。

IDs	…	IDv_0	IDv_1	IDv_2	…	IDv_W

图 2 数据库中的 IDv_i 链

查询规则如下:

1)若 $c=0$，则在 IDv_0 域中可查询到 IDv；若 $c \neq 0$，则在对应的 IDv_c 域中查询，当 $c > w$ 时，$c = c \bmod w$，这里的 w 表示存储的 IDv_i 链的最大长度。这样的查询能够实现，与 IDv_i 的更新方式相关:

由 IDv_i 的更新规则可以得出，每次更新后，在 IDv_0 中保存的是 $b = b'$ 时，标签中更新的 $IDv = d$，而在 IDv_1 中保存的是 $b \neq b'$ 时，标签中更新的 $IDv = G_3(IDs \| IDv, IDv)$，其后的 $IDv_2, IDv_3, \cdots, IDv_w$ 依次为下一次非正常访问后标签中的状态，而标签连续非正常访问的次数由参数 c 来记录。这样在查询 IDv 时，通过参数 c 即可实现快速定位。而参数 w 表示标签最大连续非法访问的次数，超过这个数量时标签的 IDv 值将做一次回归，其大小的选取与系统响应速度以及标签使用环境相关。

2)查询到相应的 IDs' 后，计算:

$G(IDs' \| IDv_i, r) = G_1' \| G_2' \| G_3' = a' \| b' \| d'$

3)验证 $a = a'$ 后，将 IDs' 的对应信息 $Inf(IDs')$ 和 b' 一起发送给读写器，同时进行 IDv_i 链的更新。

(5)R-T Reply

读写器将 b' 反馈给标签，标签比较 b 和 b'，若没有收到反馈，亦视为不相等，然后根据规则更新 IDv 和 c，协议执行完毕。

4 协议的安全性分析

RFID 系统面临的安全问题主要有假冒攻击、重传攻击、追踪以及去同步化问题，下面将针对这几个方面对本文协议进行安全性分析。

4.1 假冒攻击

攻击者首先假扮成合法读写器向标签发送认证请求 r，标签反馈信息 a、IDv、c。在下一次认证会话中，合法的读取器发送认证请求 $r*$ 时，攻击者假扮合法标签响应 a、IDv、c。

但由于读写器每次认证会话都会产生新的伪 随机数，即 $r \neq r*$，因此攻击者不能假冒合法标签进行假冒攻击，即本文协议可以抗假冒攻击。

4.2 重传攻击

在合法的读取器发送认证请求 r 后，攻击者截获了标签的响应 a、IDv、c，在下一次读取器发送认证请求 $r*$ 时，攻击者假扮合法标签响应 a、IDv、c。

由于 $r \neq r*$，而且 IDv 也已经更新为 $IDv*$，因此攻击者要想假扮合法标签需要产生 $a*$、$IDv*$、$c*$，而在不知道 IDs、$IDv*$ 的情况下是无法伪造出的，即本文协议可以抵抗重传攻击。

4.3 追踪

攻击者假扮成合法读写器向标签发送认证请求 r 后，获取标签的反馈信息 a、IDv、c，并通过该响应来追踪发出该响应的标签。

由于标签在每次认证会话后(无论是否合法)都会更新 IDv，加上流密码算法的不可逆性，因此攻击者无法得知收到的是哪个标签的响应，从而可以降低依赖于 a、IDv、c 组合的追踪威胁。这里需要注意的是参数 c，由于在步骤(2)中是以明文形式出现的，而若是连续非正常访问，其大小变化仅仅持续加 1，这可能会导致短时期内的锁定，造成一定的安全隐患，但长期跟踪是无法进行的，任意一次的正常访问都会导致 c 清 0，从而缓解对其的追踪威胁。

4.4 去同步化

在该协议中，无论标签读取过程如何，利用之前描述的更新方式总能保持标签与后台数据库之间关于 IDv 的记录一致性。

但也有可能发生意外，例如由于某些未知因素干扰，导致步骤(5)未能完成，则会使标签更新与后台数据库不同步，要解决这个问题，只需要付出更多的存储空间，在后台数据库中同时保留上一次以及这一次的更新链，下一次读取时再根据参数 c 来确定优先搜索哪一条更新链。因此对于去同步化问题，该协议也是安全的。

5 协议效率分析

与其他协议不同，本文协议中后台数据库的主要计算负荷在于对 IDv_i 链的更新和维护。以一个标签总量为 N 的系统为例，读取一个标签，后台数据库平均需要执行 $N/2+1$ 次比较操作以及 1 次流密码算法，相对于文献[11]的方案，计算负荷更小，可以更快地做出反应。而与后台数据库的计算能力直接相关的是对应 IDv_i 链的长度，即参数 w 的大小，其与整个系统安全性、并发性的关系，以及如何在效率与安全之间取得较好的折中，都值得作进一步的研究。

6 结束语

本文应用流密码算法构造了一个安全的 RFID 认证协议，能够抵抗假冒攻击、重传攻击，在一定程度上抵抗追踪，解决了电子标签与后台数据库之间的去同步化问题，适用于分布式数据库环境，并且在降低标签门限复杂度，提高整个系统的响应速度上有较大改进。之后将针对各种不同应用环境中参数 w 的安全取值以及如何解决参数 c 所产生的追踪隐患做进一步的研究和改进。

参考文献

[1] Juels A. RFID Security and Privacy: A Research Survey[J]. IEEE Journal on Selected Areas in Communication, 2006, 24(2): 381-394.

[2] Sarma S, Weis S, Engels D. RFID Systems and Security and Privacy Implications[C]//Proc. of the 4th Int'l Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2002: 454-469.

[3] 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, Germany: Springer, 2003: 201-212.

[4] Ohkubo M, Suzuki K, Kinoshita S. Hash-chain Based Forward-secure Privacy Protection Scheme for Low-cost RFID[C]//Proc. of 2004 Symposium on Cryptography and Information Security. Berlin, Germany: Springer, 2004: 719-724.

[5] Rhee K, Kwak J, Kim S, et al. Challenge-response Based RFID Authentication Protocol for Distributed Database Environment[C]// Proc. of the 2nd Int'l Conference on Security in Pervasive Computing. Berlin, Germany: Springer, 2005: 70-84.

[6] Henrici D, Mauller P. Hash-based Enhancement of Location Privacy for Radio-frequency Identification Devices Using Varying Identifiers[C]//Proc. of the 2nd IEEE Annual Conference on Pervasive Computing and Communications. Los Alamitos, USA: IEEE Computer Society, 2004.

[7] Lee S M, Hwang Y J, Lee D H, et al. Efficient Authentication for Low-cost RFID Systems[C]//Proc. of the International Conference on Computational Science and Its Applications. Berlin, Germany: Springer, 2005: 619-627.

[8] 王少辉, 王高丽. RFID 认证协议 ULAP 的被动攻击分析[J]. 计算机工程, 2010, 36(22): 17-19.

[9] Canniere C D, Preneel B. Trivium Specifications[EB/OL]. [2011-05-20]. http: //www.ecrypt.eu.org/stream.

[10] Feldhofer M, Wolkerstorfer J. Hardware Implementation of Symmetric Algorithms for RFID Security[M]//Kitsos P, Zhang Y. RFID Security: Techniques, Protocols and System-on-Chip Design. [S. l.]: Springer, 2008: 373-415.

[11] Berbain C, Billet O, Etrog J, et al. An Efficient Forward Private RFID Protocol[C]//Proc. of the 16th ACM Conference on Computer and Communications Security. [S. l.]: ACM Press, 2009: 43-53.

编辑 张 帆

(上接第 125 页)

6 结束语

针对无线传感器网络的数据安全收集问题，本文提出一种结合秘密共享算法和安全多路径技术的 MERS 算法。该算法对汇聚节点没有正确收到的数据项编号进行复用并反馈给源节点，以此来确认相对安全的路由。实验结果显示，与同类算法相比，本文算法在增加有限网络能耗的情况下，较大地提高了网络数据收集的质量。未来的工作将注重以下 2 个方面：(1)充分利用各节点缓存中和错误数据项反馈的信息进行入侵检测，对恶意节点进行定位。(2)在更加复杂的网络环境中，对本文算法做进一步验证和改进。

参考文献

[1] 杨 庚, 王安琪, 陈正宇, 等. 一种低耗能的数据融合隐私保护算法[J]. 计算机学报, 2011, 34(5): 792-800.

[2] 邓文元. 基于功率控制的 WSN 数据收集可靠性分析[J]. 计算机工程, 2009, 35(20): 100-102.

[3] Marina M K, Das S R. On-demand Multipath Distance Vector Routing in Ad Hoc Networks[C]//Proc. of IEEE Int'l Conf. on Network Protocols. [S. l.]: IEEE Press, 2001: 14-23.

[4] Ye Zhenqiang, Krishnamurthy S V, Tripathi S K. A Framework for Reliable Routing in Mobile Ad Hoc Networks[C]//Proc. of INFOCOM'03. [S. l.]: IEEE Press, 2003: 270-280.

[5] Lou Wenjing, Liu Wei, Fang Yuguang. Spread: Enhancing Data Confidentiality in Mobile Ad Hoc Networks[C]//Proc. of INFOCOM'04. [S. l.]: IEEE Press, 2004: 2404-2413.

[6] Lou Wenjing, Kwon Y. H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks[J]. IEEE Transactions on Vehicular Technology, 2006, 55(4): 1320-1330.

[7] Nasser N, Chen Yunfeng. SEEM: Secure and Energy-efficient Multipath Routing Protocol for Wireless Sensor Networks[J]. Computer Communications, 2007, 30(11/12): 2401-2412.

[8] Shu Tao, Liu Sisi, Krunz M. Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes[C]//Proc. of INFOCOM'09. [S. l.]: IEEE Press, 2009: 2846-2850.

[9] Mao Yunxin, Wei Guiyi. A Feedback-based Secure Path Approach for Wireless Sensor Network Data Collection[J]. Sensors, 2010, 10(10): 9529-9540.

编辑 张 帆