一种改进的满足后向隐私的RFID认证协议

刘道微 凌 捷 杨 昕
(广东工业大学计算机学院 广州 510006)

摘 要 针对在物联网应用中,现有的RFID安全认证协议存在安全缺陷和认证效率低等问题,提出了一种满足后向隐私的RFID双向认证协议,它通过Rabin加密算法的运算单向性来解决同步以及后向隐私的问题,并采用随机数使标签保持信息的新鲜性。采用BAN逻辑方法对协议进行了形式化证明。将该协议与现有的此类安全认证协议进行了安全性和成本比较,结果表明该协议不仅具有防跟踪、抗暴力破解、防重放攻击等特点,而且因为门电路的减少,使得成本下降,适用于低成本的RFID系统。

关键词 物联网,Rabin算法,射频识别,BAN形式化分析

中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.8.027

Improved RFID Authentication Protocol with Backward Privacy

LIU Dao-wei LING Jie YANG Xin
(School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China)

Abstract In the application of Internet of things, aiming at the security flaws of existing RFID security authentication protocol and low authentication efficiency, this paper proposed a meet to RFID privacy after two-way authentication protocol, which uses Rabin operation of one-way encryption algorithm to solve the problem of synchronization and later to the privacy, and uses random number to keep the label information of freshness. BAN logic method is used to the formal agreement. Compared the security and cost of the proposed protocol with the existing security authentication protocols, the results show that this protocol not only has the anti tracking, anti brute force crack, and anti replay attack etc, but also because of the reduction of the gate circuit, reduces the cost of protocol, and is suitable for low-cost RFID system.

Keywords Internet of things, Rabin algorithm, RFID, BAN formal analysis

1 引言

无线射频识别技术(Radio Frequency Identification, RFID)是一种利用射频信号实现的无接触信息传输,并且通过所传输的信息来达到识别的目的。作为一种快速、准确地收集和处理信息的高新技术,通过对实体对象的唯一有效的标识,RFID技术被广泛应用于生产、物流、国防、交通等各个领域[1-3]。

RFID技术由于利用无线射频通道来交换数据,因此很容易受到外部环境的干扰以及攻击者的恶意攻击。如果RFID标签中存放的个人信息或者商业情报等被恶意的攻击者非法获取,就会给使用者带来巨大的损失[4-6]。因此设计一种安全的RFID双向认证协议具有重大的意义。

文献[7]提出的认证方案其实质是一个搜索协议,而不是一个双向认证协议;文献[8]中提出的认证方案不能提供向后的隐私安全性;文献[9]提出的认证方案不能抵抗去同步攻击,攻击者可以通过重放消息,使阅读器与标签两者之间的密钥不一致,从而破坏两者之间的后续认证;文献[10]提出的认证方案不能抵抗主动攻击,攻击者通过不断地询问标签来分析标签的回复信息,从而完全推导出标签存放的所有密钥信息;文献[11]中提出的方案不能抵抗暴力破解攻击,攻击者很容易获取r1和r2,采用穷举法可以推导出标签中存放的密钥信息。在此基础之上,提出了一种改进的满足后向隐私的基于Rabin算法的RFID安全认证协议。该协议在存储、计算需求以及门电路要求方面要优于现有的方案,通过分析门电路的个数,并且采用BAN逻辑形式化方法证明了该协议的安全性。本协议适用于低成本的RFID系统。

2 改进的RFID认证协议

文献[11]给出的认证方案存在暴力破解安全缺陷,由于标签产生的随机数r2与阅读器产生的随机数r1都是明文传输,且Hash函数算法是公开的,因此攻击者可以在阻断标签与阅读器通信的前提下,采用穷举法使用暴力破解手段来穷举出密钥Key的值,从而获取标签存放的信息;标签和阅读

到稿日期:2015-07-20 返修日期:2015-10-26 本文受广东省科技计划项目(2013B040401017,2014A010103029,2015B010108002),广州市科技计划项目(2014J4100201,201508010026)资助。

刘道微(1989—),男,硕士生,主要研究方向为信息安全,E-mail:995565519@qq.com;凌 捷(1964—),男,博士,教授,CCF会员,主要研究方向为网络信息安全技术;杨 昕(1992—),男,硕士生,主要研究方向为信息安全。

器都是采用随机数发生器来产生随机数，从而导致门电路增多；而 Hash 函数的使用，将更进一步使门电路个数增多，从而使 RFID 标签成本提高。针对以上存在的问题，提出一种改进的基于 Rabin 算法的 RFID 安全认证协议，该协议将使用异或运算来传输标签产生的随机数，以抵抗存在的暴力破解攻击；采用线性反馈移位寄存器 LFSR 代替随机数发生器来产生随机数，LFSR 的使用将会减少门电路的个数；用 Rabin 算法取代 Hash 函数加密，文献[12]提出的优化以后的 Rabin 加密算法实现所需要的门电路数要远远少于实现 Hash 函数所用的门电路个数，同时文献[13]证明了 Rabin 加密算法的安全性，其也具有 Hash 函数计算单向性的特点，从而可以抵抗去同步攻击。

与其他认证协议一样，假设：阅读器与后台数据库之间的通信是安全的，数据库与标签之间共享的密钥 KEY 和 ID 是安全的。本协议认证过程包括初始化阶段和认证阶段。

2.1 初始化阶段

首先给出本协议中各符号的含义。

R：阅读器；

T：标签；

DB：后台数据库；

ID：标识符；

$KEYnew$：本轮的共享密钥；

$KEYold$：上一轮的共享密钥；

k：密钥的长度；

M：选择的梅森数，$M=2^{2K}-1$；

Rr：阅读器产生的随机数；

Rt：标签产生的随机数；

$\oplus$：异或运算；

$//$：与运算。

2.2 认证阶段

RFID 协议认证过程如图 1 所示。

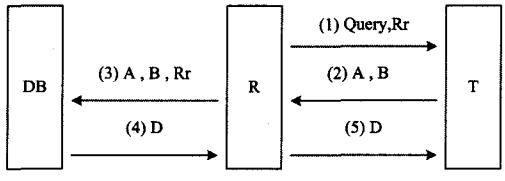

图 1　改进的协议

改进的协议中 A,B,D 的说明如下：

$A=KEY\oplus Rt$；

$B=[(Rr//Rt//ID)^2 \bmod M]_K$，表示取运算结果的前 K 位；

$D=[KEY^2 \bmod M]_K//Rt$，表示首先取[]运算结果的前 K 位，然后再与 Rt 进行与运算。

整个协议的认证步骤描述如下：

1)首先阅读器产生一个 k 位数的随机数 Rr，接着阅读器将随机数 Rr 连同请求认证 Query 命令一同发送给标签。

2)标签接收到阅读器发送来的信息后，首先产生一个随机数 Rt，然后再计算 A 和 B 的值，将计算结果一并传给阅读器。

3)阅读器接收到标签发送来的信息后，再将自身产生的随机数 Rr 一并传送给后台的数据库。

4)数据库在接收到阅读器发来的信息后，首先计算 $A\oplus KEYnew$，然后验证是否存在($ID,KEYnew$)满足以下等式：

$[(Rr//(A\oplus KEYnew)//ID)^2 \bmod M]_K$

如果存在，则进行步骤 5)；如果不存在，则检查是否存在(ID，KEYold)满足以上等式，若找到，则用(ID，KEYold)来代替(ID，KEYnew)进行步骤 5)，否则标签是伪造的，协议终止。

5)后台数据库计算 D 的值，并把 D 值发送给阅读器，然后更新密钥：$KEYold=KEYnew$；

$KEYnew=[KEY^2 \bmod M]_K$

6)阅读器收到后台数据库发送来的信息后，马上将该信息转发给标签。标签通过计算来验证 D 是否正确，若正确，则更新密钥为$[KEY^2 \bmod M]_K$，否则说明阅读器是伪造的，认证协议终止。

3 BAN 逻辑形式化分析

本文采用 BAN 逻辑形式化分析方法对本文协议进行安全性证明，BAN 逻辑是由 Burrows 等人提出的。模态逻辑由一些命题和推理规则组成，其中命题表示主体对消息的知识或信念，而推理规则可以从已知的知识或信念推导出新的知识和信念。

采用 BAN 逻辑对协议进行形式化分析，证明过程如下。

首先给出协议的理想化模型：

消息 1　$R\rightarrow T:Query,Rr$

消息 2　$T\rightarrow R:A,B$

消息 3　$R\rightarrow T:D$

下面给出协议的初始假设：

$P_1:R|\equiv R\overset{KEY}{\leftrightarrow}T$，$R$ 相信 R 和 T 共享密钥值 KEY。

$P_2:T|\equiv R\overset{KEY}{\leftrightarrow}T$，$T$ 相信 R 和 T 共享密钥值 KEY。

$P_3:R|\equiv R\overset{ID}{\Leftrightarrow}T$，$R$ 相信 R 和 T 共享标识符 ID。

$P_4:T|\equiv R\overset{ID}{\Leftrightarrow}T$，$T$ 相信 R 和 T 共享标识符 ID。

$P_5:R|\equiv\#(Rr)$，R 相信随机数 Rr 的新鲜性。

$P_6:T|\equiv\#(Rr)$，T 相信随机数 Rr 的新鲜性。

$P_7:R|\equiv\#(Rt)$，R 相信随机数 Rt 的新鲜性。

$P_8:T|\equiv\#(Rt)$，T 相信随机数 Rt 的新鲜性。

$P_9:R|\equiv T|\Rightarrow A$，$R$ 相信 T 对 A 的管辖权。

$P_{10}:R|\equiv T|\Rightarrow B$，$R$ 相信 T 对 B 的管辖权。

$P_{11}:T|\equiv R|\Rightarrow D$，$T$ 相信 R 对 D 的管辖权。

安全目标：

$G_1:R|\equiv A$，R 相信 A。

$G_2:R|\equiv B$，R 相信 B。

$G_3:T|\equiv D$，T 相信 D。

分析推理：

由消息 2 得 $R\triangleleft\{A\}$(R 曾经收到消息 A)，并且由初始假设 P_1 及消息含义法则 $\dfrac{P|\equiv P\overset{K}{\leftrightarrow}Q,P\triangleleft\{X\}_K}{P|\equiv Q|\sim X}$(若主体 P 相信主体 P 和 Q 的共享秘钥 K，且 P 曾经收到用 K 加密的密文 X，则 P 相信主体 Q 发送过来的消息 X，得到 $R|\equiv T|\sim A$。

由假设 P_5、P_7 及消息新鲜性法则 $\dfrac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$(如果一个消息的一部分是新鲜的，则整个消息也是新鲜的)，得 $R|\equiv\#(A)$。

由已经推导出来的 $R|\equiv T|\sim A$，$R|\equiv\#(A)$及随机数验

证法则$\frac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$，得到$R|\equiv T|\equiv A$。

由$R|\equiv T|\equiv A$，初始化假设P_9以及管辖法则$\frac{P|\equiv Q\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$，可得$R|\equiv A$。因此，目标$G_1$得证。

运用上述条件和法则，同理可证得G_2和G_3。此处不再赘述。

4 安全性分析

4.1 假冒攻击

因为标签每次产生的随机数是不一样的，即使攻击者伪装成阅读器，也无法获得密钥KEY和ID，最终标签仍然可以鉴别阅读器的真伪；而攻击者在无法获知密钥KEY和ID的前提下，无法伪装成合法的标签，且阅读器每次发送过来的随机数并不相同，很容易鉴别出标签的真伪，因此协议可以抵抗假冒攻击。

4.2 追踪攻击

攻击者伪装成合法的阅读器向标签发送信息，可以获得标签响应的信息：A，B，企图根据响应的信息来跟踪标签的活动。但是标签每次产生的随机数Rt都是不一样的，并且每次传输过程中随机数Rt都是密文传输，再加上Rabin加密算法运算单向性的特点，攻击者想要获取密钥值KEY和ID是不可能实现的，因此协议可以抵抗追踪攻击。

4.3 重放攻击

在整个协议认证过程中，阅读器和标签都是通过线性反馈移位寄存器LFSR来产生随机数，并且攻击者不可能提前知晓每次产生的随机数，从而可以保证标签和阅读器每次通信的信息的新鲜性，攻击者想要获取密钥值KEY和ID是不可能实现的，因此协议可以抵抗重放攻击。

4.4 暴力破解攻击

协议中标签每次产生的随机数Rt都是先与密钥KEY进行异或运算后再传输的，攻击者在不知密钥KEY的前提下，无法通过穷举法知晓随机数Rt，从而就不可能采用暴力破解法穷举手段来攻击标签获得密钥KEY，即使攻击者阻断标签与阅读器之间的通信，反复发送相同的随机数Rr来获得标签响应的信息，但标签每次产生的随机数都是不相同的，因此标签每次响应的信息也是不同的，根本无法分析出有用的信息，因此协议可以抵抗暴力破解攻击。

4.5 后向安全性

在认证过程中，虽然攻击者可以通过某些手段获取当前标签的密钥信息$KEYnew$，但是如果攻击者没有时时刻刻跟踪标签，就会错过标签的密钥更新过程；再由于Rabin加密算法的运算单向性，使得通过Rabin加密得到的输出结果具有无关性，后继时刻标签的密钥值和当前时刻的密钥值不可区分，因此即使攻击者能破解当前的密钥信息，也没有办法破解以前的回话信息，因此该协议具有后向安全性。

4.6 去同步化

为了破坏标签端和数据库之间密钥的一致性，攻击者可以通过以下方式进行攻击：1）攻击者使标签端进行密钥的更新，而数据库没有进行更新；2）攻击者使标签端和数据库都进行了密钥的更新，但是两者之间更新使用的参数不一致。

在新协议中，假如攻击者想要使标签进行密钥更新，则必须要能够生成合法认证消息$D=[KEY^2 \bmod M]_K // Rt$。因为$D$中需要本次认证过程中标签生成的随机数$Rt$，但是每次标签生成的随机数$Rt$都是不一样的，导致攻击者根本不能重放以前获得的消息，所以攻击者无法通过上述两种方式进行去同步攻击，因此该情况下本协议可以抵抗去同步攻击。

表1是本文协议与其他几种RFID认证协议之间进行的安全性对比的情况。

表1 协议的安全性比较

攻击类型	文献[8]	文献[9]	文献[10]	文献[11]	本文协议
假冒攻击	√	√	√	√	√
追踪攻击	√	√	√	√	√
重放攻击	√	√	×	√	√
暴力破解攻击	√	√	√	×	√
后向攻击	×	√	√	√	√
同步破坏攻击	√	×	√	√	√

注：√表示能够抵抗，×表示无法抵抗。

5 性能分析

表2是本文协议与文献[11]进行的成本性能比较，比较的对象为标签，比较的内容包含存储空间、计算量、门电路总个数。

表2 协议的性能比较

协议	存储空间	计算量	门电路总个数
文献[11]	3k	4XOR+1PRNG+4H()	1700～2145
本文协议	3k	1XOR+3XAND+1LFSR+3R()	545～1090

表2中密钥KEY、标识符ID、随机数Rt的长度均为K。PRNG表示随机数产生器，LFSR表示线性移位寄存函数，XOR表示异或运算，XAND表示与运算，H()表示哈希运算，R()表示Rabin加密运算。其中Rabin加密运算的计算量远远小于哈希运算的计算量，因为梅森数M的计算量很小，可以忽略，因此不予考虑。

由表2中数据分析可以得知，本文协议与文献[11]在标签中存储空间相同，但是本文协议在标签端的计算量要比文献[11]的计算量小很多。其中异或运算量和与运算量是等量级的运算，但是R()运算量和H()运算量却不相同，R()运算量要远远小于H()运算量，因此本文协议在计算方面优于文献[11]。本文协议与文献[11]在标签端所使用的门电路的总个数相差较大，使得标签的成本降低。采用LFSR模块来取代PRNG模块，可以减少门电路的个数，采用Rabin加密运算来代替哈希运算，使实现Rabin加密运算所需的门电路个数远远少于实现哈希运算所需的门电路个数，再一次减少门电路的个数，因此可以降低标签的成本。

结束语 本文针对文献[11]等提出了一种改进的基于Rabin加密算法的RFID认证协议。本文协议与文献[11]给出的协议相比较，不仅能够抵抗常见的攻击，并且还可以抵抗文献[11]所不能抵抗的暴力破解攻击，而且标签在计算方面运算量减少很多，门电路的总个数也减少很多。改进的协议舍弃PRNG模块，采用LFSR模块产生的随机数来保持标签的信息新鲜性，从而减少门电路的使用；Rabin加密算法的使用，减少了计算量，最终达到了标签成本降低的目的，同时采用BAN逻辑形式化方法证明了本文协议的安全性。

（下转第158页）

[5] Dai Fei, Li Tong, Xie Zhong-wen, et al. Research on Structure Soundness of Software Processes Based on EPMM[J]. Computer Science, 2013, 40(8): 186-190(in Chinese)
代飞,李彤,谢仲文,等. 基于 EPMM 的软件过程结构合理性研究[J]. 计算机科学,2013,40(8):186-190

[6] ISO, IEC. ISO/IEC 12207: Standard for Information Technology-software Life Cycle Processes[S]. 1998

[7] Osterweil L J. Software Processes are Software Tool[C]// Proc. of the 9th International Conference on Software Engineering. Monterey. USA: ACM Press, 1987: 2-13

[8] Wang Qing, Li Juan. The challenge for software evolution from the Internet[J]. Communications of the CCF, 2009, 5(12): 27-37 (in Chinese)
王青,李娟. 互联网对软件演化的挑战[J]. 中国计算机学会通讯,2009,5(12):27-37

[9] Herbsleb J D, Moitra D. Guest Editors' Introduction: Global Software Development[J]. IEEE Software, 2001, 18(2): 16-20

[10] Li Tong. An approach to modelling software evolution processes [M]. Berlin: Springer-Verlag, 2008

[11] Milner R. A Calculus of Communicating Systems[M]. Lecture Notes in Computer Science, Springer-Verlag, 1980

[12] Milner R. 通信与移动系统 π 演算[M]. 北京:清华大学出版社, 2009

[13] Xiao Fang-xiong, Li Yan, Huang Zhi-qiu, et al. Modeling and Analyzing Web Services Composition Using Timed Probabilistic Priced Process Algebra [J]. Chinese Journal of Computers, 2012, 1(5): 918-936(in Chinese)
肖芳雄,李燕,黄志球,等. 基于时间概率代价进程代数的 Web 服务组合建模和分析[J]. 计算机学报,2012,1(5):918-936

[14] Xiao Fang-xiong, Huang Zhi-qiu, Cao Zi-ning, et al. Process Algebra Extended with Price Information[J]. Journal of Nanjing University of Aeronautics and Astronautics, 2009, 41(1): 69-74 (in Chinese)
肖芳雄,黄志球,曹子宁,等. 一种扩展了价格信息的进程代数[J]. 南京航空大学学报,2009,41(1):69-74

[15] Qian Ye. An Approach to Modelling, Properties Verification and Performance Analysis of Software Evolution Process[D]. Kunming: Yunnan University, 2014(in Chinese)
钱晔. 一种软件演化过程建模、性质验证及性能分析方法[D]. 昆明:云南大学,2014

[16] Wu Shuai. The Research on Translating UML Diagram to B-Method Formal specification and 1st Application[D]. Nanchang: Jiangxi Normal University, 2007(in Chinese)
吴帅. UML 模型图到 B 方法形式规约的转换研究与应用[D]. 南昌:江西师范大学,2007

(上接第 130 页)

参 考 文 献

[1] Ding Zhen-hua, Li Jin-tao, Feng Bo. Research on hash-based RFID security authentication protocol [J]. Journal of computer Research and Development, 2009, 46(4): 583-592(in Chinese)
丁振华,李锦涛,冯波. 基于 Hash 函数的 RFID 安全认证协议研究[J]. 计算机研究与发展,2009,46(4):583-592

[2] Ma Chang-she. Low cost RFID authentication protocol with forward privacy [J]. Chinese Journal of Comptuers, 2011, 34(8): 1388-1398(in Chinese)
马昌社. 前向隐私安全的低成本 RFID 认证协议[J]. 计算机学报,2011,34(8):1388-1398

[3] International Telecommunication Union. ITU Internet Reports 2005: The Internet of Things [R]. Geneva: ITU, 2005

[4] Zhou Yong-bin, Feng Deng-guo. Design and analysis of cryptographic protocols RFID [J]. Chinese Journal of Computers, 2006, 29(4): 581-590(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

[5] Jin Yong-ming, Wu Qi-ying, Shi Zhi-qiang, et al. RFID Lightweight Authentication Protocol Based on PRF [J]. Journal of Computer Research and Development, 2014, 51(7): 1506-1514 (in Chinese)
金永明,吴棋滢,石志强等. 基于 PRF 的 RFID 轻量级认证协议研究[J]. 计算机研究与发展,2014,51(7):1506-1514

[6] Ohkubo M, Suzuki K, Kinoshta S. Hash-chain based for-ward-secure privacy protection scheme for low-cost RFID[C]// Proceedings of the 2004 Symposium on Cryptography and Information Security. Berlin: Springer-Verlag, 2004: 719-724

[7] Miyaji A, Rahman M S. KIMAP: Key-insulated mutual authentication protocol for RFID [J]. Int Journal of Automated Identification Technology, 2011, 3(2): 61-74

[8] Alomair B, Cuellar J, Poovendran R. Scalable RFID systems: A privacy-preserving protocol with constant time identification [J]. IEEE Trans on Parallel and Distributed Systems, 2012, 23 (8): 1-10

[9] Godor G, Imre S. Hash-based mutual authentication protocol for low-cost RFID systems[C]// Proc of the 18th EUNICE Conf on Information and Communications Technologies. Berlin: Springer, 2012: 76-87

[10] Mamun M S I, Miyaji A, Rahman M S. A secure and private RFID authentication protocol under SLPN problem[C]// Proc of the 6th Int Conf on Network and System Security. Berlin: Springer, 2012: 476-489

[11] Wang Shao-hui, Liu Su-juan, Chen Dan-wei. Scalable RFID Mutual Authentication Protocol with Backward Privacy [J]. Journal of computer Research and Development, 2013, 50(6): 1276-1284(in Chinese)
王少辉,刘素娟,陈丹伟. 满足后向隐私的可扩展 RFID 双向认证方案[J]. 计算机研究与发展,2013,50(6):1276-1284

[12] Shamir A. SQUASH-A new MAC with provable security properties for highly constrained devices such as RFID tags [C]// Proc of Fast Software Encryption. Berlin: Springer, 2008: 144-157

[13] Gosset F, Standaert F X, Quisquater J J. FPGA implementation of SQUASH[C]// Proc of the 29th Sysp on Information Theory in the Benelux. Leuven: Werkgemeenschap Informatie, 2008: 1-8