一种低成本超轻量级RFID双向认证协议

杨 昕 凌 捷
(广东工业大学计算机学院 广州 510006)

摘 要 针对射频识别系统存在的安全问题和成本问题,提出了一种低成本超轻量级RFID双向认证协议。采用BAN逻辑形式化证明方法对协议进行了形式化证明,并进行了安全性分析,结果表明本协议能够有效抵抗拒绝服务攻击、去同步化攻击、假冒攻击等多种恶意攻击,具有安全性较好、成本低和需要的运算与存储资源少等优点。

关键词 RFID,超轻量,双向认证,交叉位运算,CRC
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.4.032

Low-cost Ultralightweight RFID Mutual-authentication Protocol

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

Abstract Aiming at the security problems and tag's cost problems of RFID, a low-cost ultralightweight RFID mutual-authentication protocol was proposed, and this protocol was proved to be safe by BAN logic formal analysis method. Besides, security analysis shows that the protocol possesses robust security and can defend against malicious attacks such as disclosure attack, desynchronization attacks, impersonation attack, etc. It has advantages of better security, low cost and less consumption resource of computing and storage.

Keywords RFID, Ultralightweight, Mutual-authentication, Crossover, CRC

1 引言

射频识别(Radio Frequency Identification, RFID)是一种自动识别人或物的非接触式技术,这种识别无需物理接触或其它任何可见的接触。如今,RFID系统广泛应用于供应链管理场合、数字图书馆管理场合、防伪造的电子护照系统,甚至能用于构建智能自组网络环境等。

RFID系统包含后端数据库、读写器及标签3部分。后端数据库和读写器之间的通信信道一般被认为是安全可靠的[1]。读写器和标签之间的信道暴露在空气中,极易被监听,进一步地还可以对读写器或标签进行伪造欺骗。所以需要为读写器和标签之间的通信设计可靠的双向认证协议,用以保证整个RFID系统的安全。

为了降低标签的生产成本,在设计更加安全的双向认证协议时,同时也要考虑低成本标签的有限计算能力和存储空间。标签的大规模生产使得降低标签成本的需求越来越突出。然而,标签成本的降低,往往需要在设计系统时牺牲一定的安全性。那么,在低成本和安全性之间取得一个可以接受的折中,就成为时下研究的热点问题。

二代标签在2006年作为ISO18000-6C标准被采纳,并将应用于主流的RFID系统[2]。二代标签包含一个伪随机数产生器并使用循环冗余校验码(Cyclic Redundancy Check, CRC)来保证信息的完整性。其存储空间被划分为4个部分:保留存储区、产品电子编码区(EPC)、标签ID区和用户区。二代标签通过电线接收来自阅读器的供电。

文献[3]提出了认证协议LMAP,协议只使用了简单的异或(XOR)、与(AND)、或(OR)以及模二加(+)运算,有效地降低了标签的生产成本。LMAP协议后来被称为超轻量级认证协议。然而,经过研究发现LAMP协议并不完善,存在安全漏洞[5]。

超轻量认证协议SASI[4]引入了左循环位移运算 $Rot(X,Y)$:将 X 循环左移 $wt(y)$ 位,$wt(y)$ 为 Y 的汉明重量。Rot运算提高了协议加密算法的复杂程度,增强了认证的安全性。然而文献[6]提出该协议的输出结果具有很大的偏重性,导致标签的隐私性不强且易受跟踪攻击。此后,文献[7]引入MIXBITS函数提出了Gossamer协议,但最终文献[8]发现其存在拒绝服务攻击。

文献[9]根据遗传算法的相关知识提出了交叉位运算 $Cro(X,Y)$,并结合XOR、Rot运算提出了CURAP协议。但是CURAP在运算方面过于简单,安全性略显不足。基于现有研究成果,本文结合CRC和Cro运算提出了一种新的超轻量级RFID双向认证协议,力求在不增加标签成本的前提下提高认证的安全性。

到稿日期:2015-02-10 返修日期:2015-05-28 本文受广东省自然科学基金重点项目(S2012020011071),广东省教育部产学研合作项目(2013B040401017),广州市科技计划项目(2013J4300058)资助。

杨 昕(1992-),男,硕士生,主要研究方向为网络与信息安全,E-mail:xy300007@163.com;凌 捷(1964-),男,博士,教授,主要研究方向为网络与信息安全。

2 协议的提出

2.1 协议说明

设 X、Y 是两个具有偶数 L 位的二进制数，$X=x_1x_2x_3\cdots x_L$，$Y=y_1y_2y_3\cdots y_L$，x_i，y_i 取值范围为{0,1}，$i=1,2,\cdots,L$，本文用到的交叉位运算 $Cro(X,Y)$ 是指由 X 的奇数位和 Y 的偶数位相互交叉形成新的 L 位数组[9]。交叉位运算可在标签中有效实现：定义两个指针 $p1$ 和 $p2$ 分别指向 X 和 Y，当 $p1$ 指向 X 的奇数位时，把此位置上的值赋予运算结果的偶数位；当 $p2$ 指向 Y 的偶数位时，则把此位置上的值赋予运算结果的奇数位。

$Cro(X,Y)$ 的详细运算过程如图 1 所示。这里取长度 $L=12$，设 $X=111000110110$，$Y=011001011100$。$Cro(X,Y)=110110111001$。

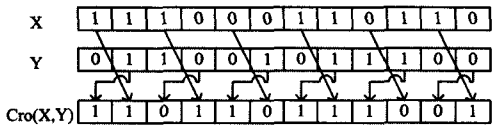

图 1 $Cro(X,Y)$计算过程

$CRC\text{-}16(X)$即循环冗余校验码是一个有效的校验和算法。本文协议中，X 作为输入被分为多个 16bit 的分组，每个分组都将经过 CRC 加密，最后所有得到的分组将组合为一个新的结果。CRC 方法在本协议中实现单向散列函数的作用，能够在不增加标签成本的前提下减少数据之间的关联性。

2.2 协议通信流程

标签和后端数据库共同持有标签的真实身份标识 ID，当前的会话密钥 K_1、K_2、K_3 以及标签的临时身份标识 TID，即 $\{ID, TID^{new}, K_1^{new}, K_2^{new}, K_3^{new}\}$，且后端数据库将保存前一次会话的信息 $\{ID, TID^{old}, K_1^{old}, K_2^{old}, K_3^{old}\}$。下面给出协议中常用的符号。

ID：标签身份标识

TID^{old}：上一轮标签临时身份标识

TID^{new}：最新标签临时身份标识

K_i^{old}：标签和阅读器间的上一轮共享密钥($i=1,2,3$)

K_i^{new}：标签和阅读器间的最新共享密钥($i=1,2,3$)

N_i：读写器生成的随机数($i=1,2$)

$A-E$：读写器和标签之间的交换信息

⊕：按位异或运算

$Cro(X,Y)$：交叉位运算

$CRC\text{-}16(X)$：循环校验函数，用来加密 X 的值

本协议的通信流程包括标签识别、双向认证、更新操作 3 个阶段，如图 2 所示。

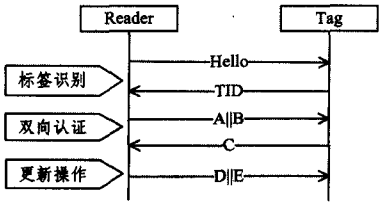

图 2 协议通信流程

标签识别阶段：读写器向标签发送“Hello”信号以发起认证请求。标签收到认证请求后，返回 TID 给读写器，读写器在后端数据库中检索 TID，若此 TID 存在，则取得与之相匹配的密钥 K_i，并开启双向认证阶段；否则读写器将重新发送请求信号。

双向认证阶段：读写器搜索到 TID 后，生成两个随机数 N_1、N_2。利用相匹配的密钥 K_i 计算 A、B，并发送 $A\|B$ 至标签。标签收到 $A\|B$ 后，提取出 N_1，并用同样的方法计算 B'。比较 B' 和 B，若两者不相等，则标签认证读写器失败，协议终止；若两者相等，则认证读写器成功，标签计算 C，并发送给读写器。

读写器接收 C，并用同样的方式计算 C'，比较 C' 和 C 是否相等。若两者相等，则读写器成功认证标签，双向认证完成，进入更新阶段；否则，认证失败，协议终止。

更新阶段：读写器认证标签后，生成 D、E，发送 $D\|E$ 至标签。之后，读写器进行更新操作。标签收到 D、E 后，从 D 中提取出 N_2，并计算 E'。如果 E' 和 E 相等，则认证 N_2 成功，进行更新操作；否则，认证失败，不做更新。

为防止拒绝服务攻击瘫痪标签和读写器之间的通信，后端数据库将保存上一轮通信过程中的 TID 和密钥 K_i。在认证期间，读写器若发现标签的 TID 为 TID^{old}，那么将会采用上一轮的 K_i^{old} 和标签进行接下来的认证。

具体的通信协议如图 3 所示。

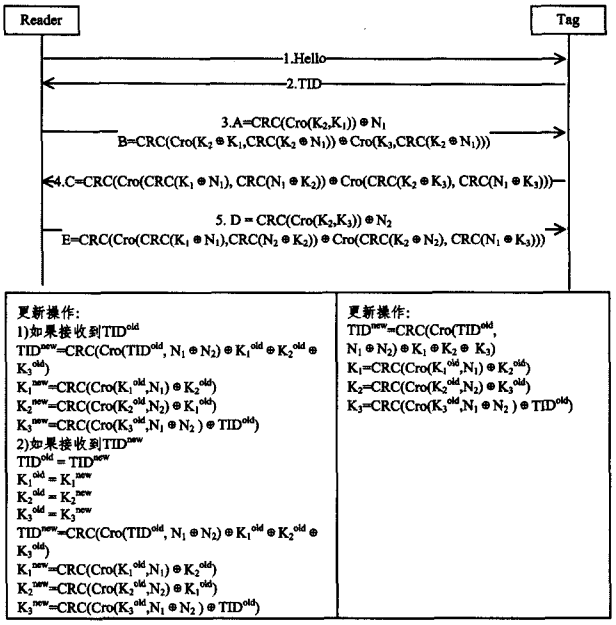

图 3 具体通信协议

3 BAN 逻辑形式化分析

本文采用 BAN 逻辑分析方法对协议进行形式化证明。BAN 逻辑是由 Burrows、Abadi 和 Needha 提出的基于信念的模态逻辑，模态逻辑由一些命题和推理规则组成，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和信念推导出新的知识和信念，在文献[11]中详细描述了其语法、推理法则及推理步骤。使用 BAN 逻辑对协议进行形式化分析，过程如下所示。

首先给出协议的理想化模型：

消息① $R \rightarrow T: Hello$

消息② $T \rightarrow R: TID$

消息③ $R \rightarrow T: \{A, B\}$，$A$ 和 B 中都包含随机数 N_1，并都是用秘钥 K_i 加密过后的密文

消息④ $T \rightarrow R: \{C\}$，D 中包含随机数 N_i，并都是用秘钥 K_i 加密过后的密文

消息⑤ $R \rightarrow T: \{D, E\}$，$D$ 和 E 中都包含随机数 N_i，且都是用秘钥 K_i 加密过后的密文

下面给出协议的初始假设：

$P_1: R \models R \overset{Ki}{\leftrightarrow} T$，$R$ 相信 R 和 T 共享秘钥 K_i

$P_2: T \models R \overset{Ki}{\leftrightarrow} T$，$T$ 相信 R 和 T 共享秘钥 K_i

$P_3: R \models R \overset{TID}{\Leftrightarrow} T$，$R$ 相信 R 和 T 共享秘密信息 TID

$P_4: T \models R \overset{TID}{\Leftrightarrow} T$，$T$ 相信 R 和 T 共享秘密信息 TID

$P_5: R \models \#(N_i)$，R 相信随机数 N_i 的新鲜性

$P_6: T \models \#(N_i)$，T 相信随机数 N_i 的新鲜性

$P_7: T \models R \mid \Rightarrow B$，$T$ 相信 R 对 B 的管辖权

$P_8: R \models T \mid \Rightarrow C$，$R$ 相信 T 对 C 的管辖权

$P_9: T \models R \mid \Rightarrow E$，$T$ 相信 R 对 E 的管辖权

安全目标：

$G_1: R \models C$，R 相信 C

$G_2: T \models B$，T 相信 B

$G_3: T \models E$，T 相信 E

分析推理：

由消息④得 $R \triangleleft \{C\}$（R 曾经收到消息 C），并且由初始假设 P_1 及消息含义法则 $\dfrac{P \models P \overset{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \models Q \mid \sim X}$（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 $R \models T \mid \sim C$。

由假设 P_5 及消息新鲜性法则 $\dfrac{P \models \#(X)}{P \models \#(X,Y)}$（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 $R \models \#(C)$。

由已经推导出来的 $R \models T \mid \sim C$、$R \models \#(C)$ 及随机数验证法则 $\dfrac{P \models \#(X), P \models Q \mid \sim X}{P \models Q \models X}$，得到 $R \models T \models C$。

由 $R \models T \models C$、初始化假设 $P8$ 以及管辖法则 $\dfrac{P \models Q \Rightarrow X, P \models Q \models X}{P \models X}$，可得 $R \models C$。因此，目标 G_1 得到了证明。

运用上述条件和法则，同理可得 $T \models B$ 和 $T \models E$，也就是说目标 G_2 和 G_3 得到了证明。此处不再赘述。

4 协议的安全性分析

4.1 数据可靠性

本文协议通过使用标签和读写器间的共享密钥 K_i 生成通信信息 $A-E$。此外，通信信息使用了随机数 N_i 来帮助加密，这使得双方每次的通信信息都是不会重复的。第三方无法通过篡改或者重放的方式骗过认证，确保了数据的可靠性。

4.2 标签的匿名性和不可跟踪性

协议运行过程中使用的都是标签的临时身份 TID，攻击者不可能从截获的消息中提取出标签的真实身份 ID，所以本文协议具有匿名性；同时，若攻击者根据截取到的 TID 对标签进行跟踪，因为每次协议运行结束时，标签都会利用随机产生的 N_i 计算新的 TID，所以攻击者对标签进行跟踪是毫无意义的，因此本文协议具有不可跟踪性。

4.3 抵抗拒绝服务攻击

本文协议考虑到可能存在第三方拒绝服务攻击，使后端数据库保存上一次通信的 TID 和密钥 K_i。当发生拒绝服务攻击时，攻击者截获 D、E，标签内数据更新失败，标签内存储的是上一轮通信的 TID 和密钥 K_i。读写器再次向标签请求通信时，将发现标签的 TID 为 TID^{old}，那么会采用上一轮的密钥和标签进行通信认证。

4.4 抵抗去同步化攻击

文献[10]证明了针对 UAPP 协议可能存在的去同步化攻击。为了抵抗去同步化攻击，应当使得针对通信信息的任何修改在认证阶段都会发生雪崩效应。本文协议采用 CRC-16 协议来降低可能发生的风险，并且这不会增加标签的成本。

4.5 抵抗假冒攻击

当攻击者企图假冒读写器（标签）来发送截获的信息欺骗标签（读写器）时，由于本文协议每次会生成新的随机数 N_i，并利用读写器和标签的共享密钥 K_i 来生成认证信息，攻击者无法计算出一致的认证信息，使其本身被标签（读写器）认证。

4.6 抵抗重传攻击

每当协议运行一轮结束时，读写器和标签将计算新的 TID 和共享密钥 K_i，而且每次会话所使用的随机数 N_i 都是不同的，即使攻击者截获到了前一轮通信的交互信息 $A-E$ 并在以后的会话中重放，也不会通过认证。

4.7 抵抗暴露攻击

本文协议运行时，所有的密文均不会暴露给攻击者。协议运行中，攻击者可能通过某种手段获得 $Cro(K_1, K_2)$，进而可提取出 K_i 的奇/偶位，但是并不能获取完整的 K_i。攻击者无法破解有随机数 N_i 参与生成的 $A-E$，从而保证了密文不会暴露给攻击者。

5 协议的性能分析

主要从标签的计算量、存储空间和通信量 3 个方面来考察超轻量 RFID 双向认证协议的性能。

计算需求：本文协议只包含 3 种简单的位运算，都可以在便签中很好地实现；除此之外，伪随机数的生成由读写器负责，标签只需简单的位运算提取信息，使标签的计算量得到了有效降低。

存储空间：标签存储有标签的真实身份 ID 和协议每轮的会话信息 $\{TID^{new}, K_1, K_2, K_3\}$，若将协议中各信息长度设为 L，标签所需存储空间为 $5L$。

通信量：本文协议运行过程中总共传输了请求信息“Hello”和 TID 以及读写器与标签的交互信息 $A-E$，而标签的传输消息只有 TID 和认证消息 C，若同样设传输的消息长度为 L，标签的总通信量为 $2L$。

（下转第 172 页）

[11] Benavides D, Segura S, Ruiz-Cortés A. Automated analysis of feature models 20 years later: A literature review[J]. Information Systems, 2010, 35(6): 615-636

[12] Schobbens P, Heymans P, Trigaux J. Feature Diagrams: A Survey and A Formal Semantics[M]// Proceedings of 14th IEEE International Conference on Requirements Engineering. Washington: IEEE Computer Society, 2006: 139-148

[13] Clarke E M, Emerson E A. Design and synthesis of synchronization skeletons using branching time temporal logic[M]// Logic of Programs: Workshop, Yorktown Heights, New York, May 1981. London: Springer-Verlag, 1981: 52-71

[14] Pnueli A. The temporal logic of programs[C]// Proceedings of the 18th Annual Symposium on Foundations of Computer Science. Washington: IEEE, 1977: 46-57

[15] Nicola R D, Vaandrager F. Action versus state based logics for transition systems[J]// Lecture Notes in Computer Science, 1990, 469: 407-419

[16] Glenn B, Patrice G. Model Checking Partial State Spaces with 3-Valued Temporal Logics[J]. 11th International Conference on Computer Aided Verification(CAV'99). 1999: 274-287

[17] Classen A, Cordy M, Heymans P, et al. Model checking software product lines with SNIP[J]. International Journal on Software Tools for Technology Transfer, 2012, 14(5): 589-612

[18] Chen J J, Wei O. Approximation of multi-valued models via reduction[J]. Computer Science, 2014, 41(6): 125-130(in Chinese)
陈娟娟，魏欧. 基于分解的多值模型的逼近关系[J]. 计算机科学，2014，41(6)：125-130

[19] Shi Y F, Wei O, Zhou Y. Model checking of software product line based on bilattices[J]. Computer Science, 2015, 42(2): 167-172(in Chinese)
石玉峰，魏欧，周宇. 基于双格的软件产品线模型检测[J]. 计算机科学，2015，42(2)：167-172

[20] Classen A, Boucher Q, Heymans P. A text-based approach to feature modelling: Syntax and semantics of TVL[J]. Science of Computer Programming, 2011, 76(12): 1130-1143

(上接第 162 页)

本文协议与其他几种超轻量认证协议的性能比较结果见表 1。

表 1 超轻量级 RFID 认证协议性能的比较

协议	计算需求	存储空间	通信量
SASI	∧ ∨ ⊕ + Rot	7L	2L
Gorssamer	⊕ + Rot MixBits	7L	2L
CURAP	⊕ Rot Cro	4L	2L
本协议	⊕ CRC Cro	5L	2L

结束语 本文提出了一种低成本超轻量级 RFID 双向认证协议，通过在标签端使用简单的 CRC 运算和交叉位运算实现了标签和阅读器之间的双向认证，并且在降低计算代价的同时，使协议能够有效抵抗拒绝服务攻击、去同步化攻击、假冒攻击等多种恶意攻击，确保在资源受限的低成本标签上完成双向认证。通过 BAN 逻辑形式化分析，验证了本协议的正确性和安全性。通过性能分析说明与已有的超轻量级 RFID 认证协议相比，所提协议减少了标签所需的存储空间。

参 考 文 献

[1] Zhou Y B, Feng D G. Design and Analysis of Cryptographic Protocols for RFID[J]. Chinese Journal of Computers, 2006, 29(4): 581-589(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

[2] Sun H M, Ting W C. A Gen2-based RFID authentication protocol for security and privacy[J]. IEEE Trans Mob Comput, 2009, 8(8): 1052-1062

[3] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags[C]// Proceedings of the 2nd Workshop on RFID Security. New Jersey, USA: IEEE Press, 2006: 137-148

[4] Chien H Y. SASI: A New Ultra-lightweight RFID Authentication Protocol Providing Strong Authentication and Strong Intergrity[J]. IEEE Trans. Dependable and Secure Computing, 2007, 4(4): 337-340

[5] Bagheri N, Safkhani M, Naderi M, et al. Security Analysis of LMAP++, an RFID Authentication Protocol[C]// Abu Dhabi. 6th International Conference on Internet Technology and Secured Transactions. 2011: 689-694

[6] Phan R C W. Cryptanalysis of a New Ultralightweight RFID Authentication Protocol—SASI[J]. IEEE Trans. on Dependable and Secure Computing, 2009, 6(4): 316-320

[7] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. Advances in Ultra-Lightweight Cryptography for Low-cost RFID Tags: Gossamer Protocol[C]// 9th International Workshop on Information Security Applications. 2009: 56-68

[8] Peng P, Zhao Y M, Han W L, et al. Ultra-lightweight RFID Mutual Authenticaiton Protocol[J]. Computer Engineering, 2011, 37(16): 140-142(in Chinese)
彭朋，赵一鸣，韩伟力，等. 一种超轻量级 RFID 双向认证协议[J]. 计算机工程，2011，37(16)：140-142

[9] Du Z Y, Zhang G A, Yuan H L. Crossover Based Ultra-lightweight RFID Authentication Protocol[J]. Computer Science, 2013, 40(11): 35-37(in Chinese)
杜宗印，章国安，袁红林. 基于交叉位运算的超轻量 RFID 认证协议[J]. 计算机科学，2013，40(11)：35-37

[10] Gao L J, Ma M D, Shu Y T, et al. An ultralightweight RFID authentication protocol with CRC and permutation[J]. Journal of Network and Computer Applications, 2014, 41: 37-46

[11] Yang S P. Analysis and Research of Security Protocol with BAN Logic[D]. Guiyang: Guizhou University, 2007: 54-73(in Chinese)
杨世平. 安全协议及其 BAN 逻辑分析研究[D]. 贵阳：贵州大学，2007：54-73

[12] Tian Y, Chen G L, Li J H. A new ultralightweight RFID authentication protocol with permutation[J]. Communications Letters IEEE, 2012, 16(5): 702-705