一种 RFID 空中接口安全认证算法①

杨　顺　章　毅　陶　康 (辽宁工程技术大学 电子与信息工程学院 辽宁 葫芦岛 125000)

摘　要： 射频识别技术是一种非接触式的自动识别技术，对 RFID 的现有技术进行了分析，对现存问题做了改进，并在此基础上提出了一种空中接口通信安全认证算法，通过 ID 更新来保证标签的匿名性，并且解决了一般 RFID 空中接口算法中采用 ID 刷新机制容易导致的数据更新不同步问题。

关键字： 射频识别；空中接口；认证

A RFID Air Interface Security Authentication Algorithm

YANG Shun, ZHAN Yi, TAO Kang

(School of Electronic and Communications Engineering, Liaoning Technical University, Huludao 125000, China)

Abstract: Radio frequency identification technology (RFID) is a non-contact automatic identification technology. The existing RFID technology is reviewed and its problem is addressed. An air interface communications security authentication algorithm is put forward, which solves the problem of updated key with changing ID.

Keywords: RFID; air interface; authentication

1　引言

射频识别(Radio Frequency Identification，RFID)[1]技术是一种非接触式的自动识别技术，它通过射频信号自动识别目标对象并获取相关数据。

由于无线通信本身的脆弱性，未授权的阅读器可以读取其作用范围内标签的相关信息，通过信息积聚和关联达到获取消费者隐私的目的。如何在标签计算速度、通信能力文章)和存储空间非常有限的情况下，设计较好的安全机制，提供安全性和隐私性保护，防止各种恶意攻击对 RFID 系统的安全研究具有重要意义。

2　现有的RFID协议及其性能分析

2.1 询问－应答算法

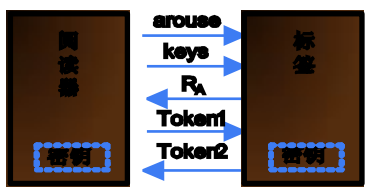

图 1　算法流程图

其中图 2 执行过程如下：

(1) 阅读器对标签进行唤醒；

(2) 阅读器读取标签的序列号 ID，利用 ID 计算得到该标签的密钥 key；

(3) 进行标签对阅读器的认证。

标签向阅读器发送随机数 R_A，阅读器向标签发送编码数据包 Token1，其中 $R_A' = ek(key, R_A)$，ek 是一种加密算法；标签重新计算得 R_A''，即

$$R_A'' = ek(key, R_A)$$

标签比较 R_A'' 和 R_A' 相等，则阅读器通过验证；

(4) 进行阅读器对标签的认证，方法与标签对阅读器的认证方式是一样的。

2.2 询问－应答算法的缺点

上述算法中没有动态 key 刷新机制，且 key 是以明文[2]通过不安全的信道，一旦攻击者获得标签的 key 就可以假冒标签；而且任何阅读器发出查寻都可能得到标签的 key，攻击者可以对标签持有者进行跟踪；

2.3 基于杂凑的 ID 变化协议[3]

如图 2 所示，TID 是最后一次回话号，LST 是最

① 收稿时间:2009-06-13

后一次成功的回话号[2]。

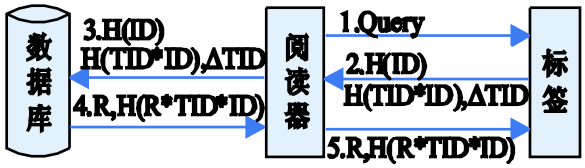

图 2　基于杂凑的 ID 变化协议

执行过程如下：

(1) 阅读器向标签发送 Query 请求；

(2) 标签将当前回话号加1，将H(ID)，H(TID*ID)，ΔTID 发送给阅读器；

(3) 阅读器将 H(ID)，H(TID*ID)，ΔTID 转发给数据库；

(4) 如果所收到数据有效，则产生随机数 R，并将(R，H(R*TID*ID))发送给阅读器。然后数据库更新该标签 ID 为 ID⊕R，并相应地更新 TID 和 LST；

(5) 阅读器将 R，H(R*TID*ID)转发给标签；然后标签验证接收信息的有效性。

2.4 基于杂凑的 ID 变化协议的缺点

标签在接收到消息 5 且验证通过之后才更新其 ID 和 LST，在此之前，数据库已经成功地完成信息的更新。如此时进行攻击，数据库和标签之间数据不同步。

3　空中接口通信安全认证算法

算法要求在使用前对阅读器方和系统所使用的标签进行初始化操作。

标签：Tag 中设有 96-bit 可写存储区，分别被写入标识符 ID(64-bit)、认证口令 P_key(32-bit)，ID 作为索引号。阅读器方：阅读器方存有一张包含系统内所有标签的表单，每个标签的表单中包含有(ID_0，P_key_0，ID_1，P_key_1，Data)。初始化时 ID_0=ID，P_key_0=P_key，ID_1、P_key_1 中填充 0。其中 ID_0、ID1 是标签标识符，作为索引号；P_key_0，P_key_1 是认证口令，Data 是标签的私密信息数据，具体算法流程如下所述[3]：

(1) [阅读器询问] 阅读器向标签发送 Query 询问；

(2) [标签响应 ID] 标签响应(ID，CRC(ID))，其中 CRC(ID)用来校验 ID 在传输过程中有没有差错；

(3) [阅读器方发送认证信息] 阅读器方先计算 CRC(ID)校验 ID 传输是否正确，若没有差错，则在数据库中查询检索列 ID_0 和 ID_1，只要找到某行的 ID_0 或 ID_1 等于 ID(记为 ID_x，x=1 或 0)，则得到对应的 P_key_x，阅读器产生随机数 R_1、R_2(可以是阅读器产生，也可以是数据库产生)，其中 R_1、R_2 均为 32-bit 的随机数；计算

$$A=CRC(P\_key \times R_1 \oplus R_2)$$

$$B=f(ID_x, 32) \oplus P\_key_x R_1$$

$$C=R_1 \oplus R_2$$

记　$M=A||B||C$；

其中 $f(ID_x, 32)$表示从 ID_x 从中抽取任意的 32 个比特(可以是前 32 个比特，也可以是后 32 比特或者中间部分的 32 比特，但标签和阅读器方抽取的比特位要一致)；阅读器方发送(M，CRC(M))，其中 CRC(M)用来校验 M 传输过程有没有差错；

(4) [标签验证阅读器方] 标签先校验 M，若没有差错，则开始计算

$$R_1=f(ID, 32) \oplus P\_key \oplus B$$

$$R_2=R_1 \oplus C$$

$$A'=CRC(P\_key \oplus R_1 \oplus R_2)$$

如果 A′=A，则标签认为阅读器方是可信的，之后标签发送(D=CRC(P_key ⊕ R_1)，CRC(D))给阅读器方；如果 A′≠A，认证失败，标签停止响应；

(5) [阅读器方验证标签并更新] 阅读器方先计算 CRC(D)校验 D 传输过程，若没有差错，开始计算

$$D'=CRC(P\_key_x \oplus R_1)$$

若 D′=D，则标签是合法的；然后阅读器方更新：

$$ID_{1-x}=ID_{n+1}=ID_n \oplus ((R_1 \oplus R_2) \oplus CRC(P\_key_x \oplus R_1) \oplus CRC(P\_key_x \oplus R_2))$$

$$P\_key_{1-x}=P\_key_{n+1}=P\_key_x \oplus (R_1 \oplus R_2)$$

即阅读器方更新其标签标识符、认证口令中与标签中的不匹配的那部分；同时发送 OK 给标签。

(6) [标签更新] 标签收到 OK 后更新：

$$ID_{n+1}=ID_n \oplus ((R_1 \oplus R_2) \oplus CRC(P\_key_n \oplus R_1) \oplus CRC(P\_key_n \oplus R_2))$$

$$P\_key_{n+1}=P\_key_x \oplus (R_1 \oplus R_2)$$

4　本算法在实际应用中的性能分析

本算法在实际应用中完成一次认证和更新，标签只需进行 13 次异或运算和 6 次 CRC-16，而没有采

用哈希算法、对称加密算法等相对来说成本较高的密码机制，标签计算负担较小，非常适合在低成本标签中应用，其性能分析如下：

(1) 标签的匿名性[4]

虽然只要阅读器放送 Query 询问，标签都会发送标识符 ID，但由于每次认证完成后 ID 都要更新：$ID_{n+1}=ID_n \oplus ((R_1 \oplus R_2) \oplus CRC(P\_key_n \oplus R_1) \oplus CRC(P\_key_n \oplus R_2))$，攻击者无法根据得到的大量不同的 ID 推算出它们中间的联系，从而也无法跟踪同一标签，因此标签有很好的匿名性。

(2) 数据机密性

机密数据 Data 保存在后端数据库，标签上只存有用作索引的标签标识符 ID，而且标签标识符 ID 每次认证完都会更新，另外在标签认证阅读器时，传输的数据 $M=A||B||C$，其中 $A=CRC(P\_key_x \oplus R_1 \oplus R_2)$，$B=f(ID_x, 32) \oplus P\_key_x \oplus R_1$，$C=R_1 \oplus R_2$，在计算 A 时认证口令 P_key_x、随机数 R_1、R_2 经过异或运算后又进行了 CRC，由于 CRC 函数的单向性，比较好的隐藏了它们；在计算 B、C 时也用了异或运算来隐藏数据。

(3) 数据完整性

标签与阅读器方之间通信的数据都包含了 CRC 校验值，若数据传输过程发生错误或攻击者修改其中的某些数据，接收方通过做 CRC 校验会发现错误。

(4) 双向认证

本算法中，先进行标签对阅读器的认证(算法流程第 4 步)，以防非授权阅读；再进行了阅读器对标签的认证(算法流程第 5 步)，确认标签的合法性。

(5) 前向安全性

假设标签泄漏了信息，即攻击者可以获得标签的数据(ID，P_key)，由于 ID 每次认证完更新为

$$ID_{n+1}=ID_n((R_1R_2) \oplus CRC(P\_key_nR_1) \oplus CRC(P\_key_nR_2))$$

加上以前通信过程中监听的(M，D)值，由于随机数 R_1，R_2 几乎每次都不一样，而且每次通信过程都通过异或运算或 CRC 运算隐藏了，攻击者无法得知，所以攻击者无法根据泄露的标签信息和以前窃听的大量信息来追踪标签，所以本算法有很好的前向安全性。

(6) 抗中间人攻击

由于 P_key 和 R_1、R_2 进行了 CRC 运算和多次异或，攻击者很难解密出 P_key，而解密不了 P_key，只根据窃听到的 ID 无法成功地进行中间人攻击。

(7) 抗重放攻击

由于采用了随机数，攻击者重放上一次窃听或截获的消息，即便上次标签没有更新成功，在认证的第 5 步阅读器对标签进行认证时通过的概论几乎等于零，因为重放的消息为(D=CRC(P_keyR1)，CRC(D))，其中的 R_1 为随机数，这一次 R_1 与前一次 R_1 相等的概率几乎为零，所以本算法可以很好的抵抗重放攻击。

(8) 数据同步问题

在本算法中，阅读器方存储的标签数据表中，包含(ID_0，P_key_0，ID_1，P_key_1)，且每次更新时，阅读器方总是更新其标签标识符、认证口令中与标签中的不匹配的那部分(ID_{1-x}，P_key_{1-x})，即本次与标签成功进行双向认证所使用的标签标识符和认证口令(ID_x，P_key_x)仍然保留在表单中，如果本次通信中第 5 步“OK”被攻击者截获或是因为其它原因标签没有更新成功，下次标签仍然可与可信阅读器方正常通信。而且，即便出现多次异常导致标签没有更新，但由于上次进行通信的 ID_x 和 P_key_x 还保存在阅读器方的表单中，所以标签依然可以与可信阅读器方正常通信，而不会出现合法标签无法通过认证和识别的系统异常。

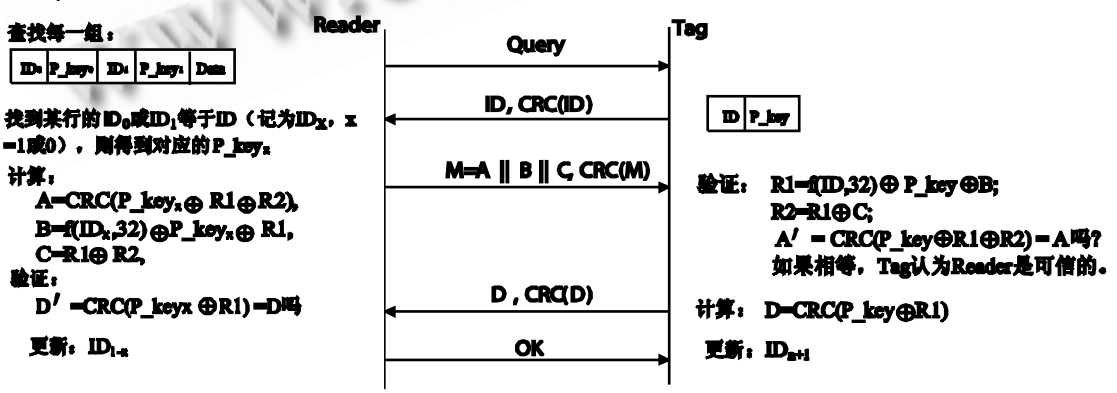

图 3　本算法算法流程示意图

(下转第 220 页)

(上接第 196 页)

5 总结

本文总结了现有两种 RFID 算法，并分析现有协议中的缺点，从机密性、完整性等方面分析本算法。在此基础上提出一种 RFID 安全认证算法，通过 ID 更新来保证标签匿名性，解决一般 RFID 空中接口算法中采用 ID 刷新机制容易导致数据更新不同步问题，并对算法在实际应用中的性能作以分析。

参考文献

1 Henrici D, Muller P. Hash2based enhancement of location privacy for radio frequency identification devices using varying identifiers. Proc. of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04). Washington, DC, USA, 2004.149 – 153.

2 Sarma SE, Weis SA, Engels DW. RFID systems and security and privacy implications. Kaliski BS, Koc CK , Paar C eds. Proc. of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002). Lectures Notes in Computer Science 2523. Berlin: Springer-Verlag, 2003.454 – 469.

3 Sarma SE, Weis SA, Engels DW. Radio frequency identification: Secure risks and challenges. RSA Laboratories Crypto bytes, 2003,6(1):2 – 9.

4 Molnar D, Wagner D. Privacy and security in library RFID: Issues, practices, and architectures. In: Proc. of the 11th ACM Conference on Computer and Communications Security (CCS'04), Washington, DC, USA, 2004.210 – 219.