文章编号：1004-4353(2014)01-0058-05

一种改进的 RFID 双向安全认证协议

王彦， 李永珍*
（延边大学工学院 计算机应用技术学科网络与信息安全研究室，吉林 延吉 133002）

摘要：现有的 RFID 认证协议大部分都建立在阅读器和后台数据库为安全通信这一假设上，通过对现有协议以及 RFID 发展趋势的分析，取消这种假设，提出了一种改进的双向安全认证协议. 该协议采用异或运算和 Hash 函数对通信的消息进行加密，通过自动更新标签 ID、共享密钥等方法抵抗重放攻击、假冒攻击、系统内部攻击等. 性能分析表明，新协议能在较低成本的基础上抵抗各种攻击，可以保证通信的安全性和正确性.

关键词：RFID；双向认证；安全协议；会话密钥
中图分类号：TP309.2 **文献标识码**：A

An improved RFID mutual authentication protocol

WANG Yan， LI Yongzhen*
（*Network and Information Security Lab.*, *Dept. of Computer Application Technology*, *College of Engineering*, *Yanbian University*, *Yanji* 133002, *China*）

Abstract: Most of the existing authentication protocols are based on the assumption that the communication between the reader and the background database is safe. Through the analysis of the existing protocols and the development trend of RFID, we cancel this assumption and propose a new improved mutual authentication protocol. It uses the XOR operation and Hash algorithm to encrypt the messages. Through updating the ID of the tag automatically and sharing the keys, it resists the replay attack, counterfeit attack, internal system attack and so on. The performance analysis shows that this protocol can resist all kinds of attacks and guarantee the security and correctness of the communication on the basis of low cost.

Key words: RFID; mutual authentication; secure protocol; session key

RFID 是一种通过无线广播进行非接触式双向通信的自动识别技术，它具有精度高、操作简单、感知能力强等优点[1]，但同时 RFID 技术也面临着保密、重放攻击、假冒攻击、前向可追踪、系统内部攻击等安全问题，因此安全和隐私保护是 RFID 应用时首先要解决的关键问题之一. 现有的协议大部分建立在阅读器和后台数据库为安全通信的假设上，但是在实际应用中无线阅读器[2-3]的应用越来越广泛，而无线阅读器和后台数据库之间是通过不安全的无线信道进行通信，因此需要设计一种协议来确保通信的安全性. 文献[4]提出了 MRPPS-IoT 协议，此协议综合运用 Hash 函数、异或运算、对称加密、身份加密等方法来实现标签、无线阅读器和后台数据库之间的相互认证，但由于这个协议采用的对称加密、身份加密等方法比较复杂，因此 MRPPS-IoT 协议效率不是很高. 为了提高认证的效率，本文采用轻量级加密函数(Hash 函数和异或运算)来加密通信过程中的信息，并采用自动更新标签 ID、标签和阅读器共享密钥、标签和阅读器分别与后台数据库共享密

收稿日期：2013 - 09 - 26
* **通信作者**：李永珍(1971—)，男，博士，副教授，研究方向为网络安全、无线网络协议.

钥[5-6]等方法来实现双向认证并确保通信安全.

1　相关协议介绍

文献[7]提出了一种 RFID 双向安全认证协议，该安全认证协议中使用的符号见表 1，协议的认证过程如图 1 所示. 在图 1 中 $M=\mathrm{H}(T_i \oplus R)$，$N=\mathrm{H}(M_{\mathrm{L}} \| R \| IDS_i) \oplus IDS_{i+1}$，$key_{i+1}=key_i \oplus (R_{\mathrm{L}} \| M_{\mathrm{L}})$，$IDS_{i+1}=E_{key\,i+1}(ID)$.

表 1　文献[7]中使用的一些符号

符号	定　义
R	阅读器向标签发送的随机数
T	一个临时值，因为标签不能产生随机数，所以用 T 来代替
ID	标签的唯一标识
IDS	对 ID 进行一次对称加密后所得的值，代替 ID 值在通信中进行传输，以防 ID 泄露
Info	后台数据库中存储的相应标签的详细信息
RID	阅读器的唯一标识
M_{L}	M_{L} 为 M 的左半部分，M 是标签计算的值，后台数据库验证标签合法性时用 M_{L}
M_{R}	M 值的右半部分
N	由后台数据库计算得到，标签收到后通过 N 获得 IDS_{i+1}，进而验证收到信息的合法性
key	key 为对称加密的密钥，后台数据库通过对称加密来更新 IDS
$Pre\text{-}x$	上次通信时 x 的值，x 代表某个变量如 key、IDS 等，$Pre\text{-}x$ 可表示 $Pre\text{-}key$、$Pre\text{-}IDS$ 等
$Cur\text{-}x$	本次通信中 x 的值，x 在这里代替某一个变量如 key、IDS 等

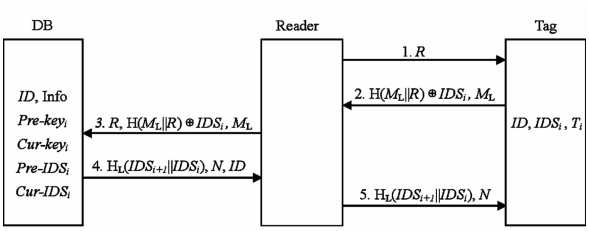

图 1　文献[7]中协议的认证过程

文献[7]的协议虽然是建立在阅读器和后台数据库为安全通信的假设上，大大减少了后台数据库的运算量(只需要 $O(1)$ 的工作量)，但是通过分析可以发现此协议存在如下问题：

1) 随着无线阅读器越来越广泛的应用，后台数据库和阅读器之间的通信不再是安全的，所以文献[7]提出的协议具有一定的局限性.

2) Hash 函数是一种公开函数，攻击者可以获得其算法. 如果攻击者窃听到认证过程的第 2 步信息：M_{L}，R 和 $\mathrm{H}(M_{\mathrm{L}} \| R) \oplus IDS_i$，且已知 Hash 函数的计算方法，那么他就可以通过计算 $\mathrm{H}(M_{\mathrm{L}} \| R)$ 进而获得 IDS_i. 同理，攻击者也可以获得 IDS_{i+1}，ID 等保密信息，这时此协议既无法满足保密性也无法抵抗跟踪、假冒、重放等攻击.

3) 在设计上未考虑系统内部攻击，因此无法抵抗内部攻击.

4) 协议中没有对阅读器进行合法性的验证，任何攻击者都可以假冒阅读器读取标签的信息.

2　改进的 RFID 双向安全认证协议

2.1　新协议中使用的符号

本文在文献[7]的基础上提出了一种改进的认证协议，协议中使用的相关符号见表 2.

表 2　新协议中使用的符号

符号	定　义
R	阅读器向标签发送的随机数
ID	标签的唯一标识，存储在标签中，为了防跟踪 ID 需要动态更新
ID_{old}	标签上次通信时使用的标识，存储在后台数据库中
ID_{new}	标签本次通信应该使用的标识，存储在后台数据库中
RID	阅读器的唯一标识
T_{td}	标签与后台数据库共享的密钥，用于防系统内攻击
R_{rd}	阅读器与后台数据库共享的密钥，用于防系统内攻击
T_{t}	标签标识，用来防重放和假冒攻击
T_{r}	阅读器标识，用来防重放和假冒攻击
$\mathrm{H_r}()$	做 Hash 运算后取所得值的右半部分
$\mathrm{H_l}()$	做 Hash 运算后取所得值的左半部分

2.2　新协议的初始化过程

首先由后台数据库产生标签和阅读器的各项信息(如表 2)，然后将(ID、T_{td}、T_{t})存入相应的标签，将(RID、R_{rd}、T_{r})存入相应的阅读器. 同时在后台数据库建立一个 ID 表和一个 RID 表，ID 表中每一项存储相应标签的(ID_{old}，ID_{new}，T_{td})，RID 表中每一项存储相应阅读器的(RID，R_{rd})，

其中$ID_{old}=ID_{new}=ID$，$T_r=T_t=0$.

2.3 新协议的认证过程

协议的认证过程如图 2 所示，具体过程如下：

1）阅读器产生随机数R，然后令$T_r=1$，并发送R给标签.

2）标签收到R之后，首先检验T_t是否为 0. 若$T_t=0$，则令$T_t=1$，然后计算$H(R\oplus ID\oplus T_{td})$，保存$H_l(R\oplus ID\oplus T_{td})$，将$H_r(R\oplus ID\oplus T_{td})$发送给阅读器；若$T_t!=0$，则停止认证.

3）阅读器收到标签的响应信息后，首先检验其存储器中是否存有R，若没有则停止认证，若存有则检验T_r是否为 1. 若$T_r=1$，则计算$H(R\oplus RID\oplus R_{rd})$，保存$H_l(R\oplus RID\oplus R_{rd})$，将$H_r(R\oplus RID\oplus R_{rd})$、$R$和收到的$H_r(R\oplus ID\oplus T_{td})$发送给后台数据库，然后令$T_r=0$；若$T_r!=1$，令$T_r=0$并停止认证.

4）首先验证阅读器的合法性. 遍历RID表，对表中的每一项计算$H(R\oplus RID\oplus R_{rd})$，并将$H_r(R\oplus RID\oplus R_{rd})$与收到的信息作比较. 若遍历完所有项仍没有相同的，则阅读器不合法，停止认证；若有使两者相同的项RID'，则阅读器合法. 然后验证标签的合法性. 首先在所有的ID_{new}中进行查找，对每一项计算$H(R\oplus ID_{new}\oplus T_{td})$，然后将$H_r(R\oplus ID_{new}\oplus T_{td})$与收到的$H_r(R\oplus ID\oplus T_{td})$比较. 若$ID_{new}$中有使两者相同的项$ID_{new}'$，则标签合法，更新相应的$ID_{old}'=ID_{new}'$，$ID_{new}'=H(ID_{old}'\oplus R)$；若$ID_{new}$中没有相同项，则继续在所有的$ID_{old}$中查找，方法与前一步相同. 若在$ID_{old}$中找到相同项$ID_{old}'$，则标签也合法，保持$ID_{old}'$不变，更新相应的$ID_{new}'=H(ID_{old}'\oplus R)$. 如果$ID_{new}$和$ID_{old}$中都没有相同项，则标签不合法，认证失败. 如果阅读器和标签都合法，后台数据库将$H_l(R\oplus RID'\oplus R_{rd})$和$H_l(R\oplus ID_{old}'\oplus T_{td})$发送给阅读器.

5）阅读器将收到的$H_l(R\oplus RID'\oplus R_{rd})$与先前保存的$H_l(R\oplus RID\oplus R_{rd})$作比较，若相同，则确定信息合法，然后删除存储器中的R，并将收到的$H_l(R\oplus ID_{old}'\oplus T_{td})$发送给标签；如果不相同，则停止认证.

6）标签收到信息后令$T_t=0$，并将收到的$H_l(R\oplus ID_{old}'\oplus T_{td})$与保存的$H_l(R\oplus ID\oplus T_{td})$作比较，若不同则信息不合法，认证失败；若相同，则确定信息合法，并更新$ID=H(ID\oplus R)$完成整个认证过程.

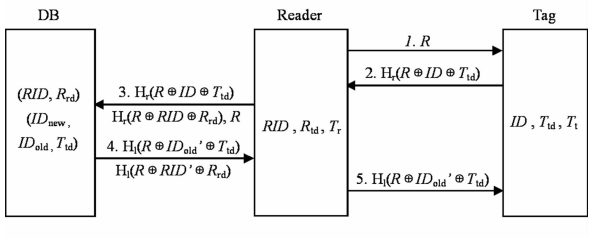

图 2 新协议的认证过程

2.4 改进型安全认证协议

基于文献[7]，本文提出如下新协议：

1）新协议主要采用 Hash 函数做加密运算，由于 Hash 函数的单向性，攻击者很难从中得到重要信息，如ID、RID、T_{td}、R_{rd}等.

2）标签只采用 Hash 函数和异或运算加密信息，取消了串联运算，这样可以降低标签成本.

3）在新协议的阅读器和后台数据库中存储合法阅读器的唯一标识RID，后台数据库通过RID来验证阅读器的合法性，以此确保只有合法的阅读器才能读取标签的信息.

4）标签和阅读器分别与后台数据库共享一个密钥值T_{td}和R_{rd}，这两个值是绝对保密的，用来防止系统内部的攻击.

5）标签和阅读器在传送信息时，保存计算值的左半部分，首先只传送计算值的右半部分，后台数据库通过收到的右半部分的值验证标签和阅读器的合法性，然后后台数据库发送相应值的左半部分，标签和阅读器通过比对收到的值与保存的值是否相同来确定收到信息的合法性，这样可以减少标签和阅读器的计算量.

6）在标签和阅读器中各存储一个状态值T_t和T_r，通过判断这些值是 1 还是 0，可以更快速有效地防止重放和假冒攻击.

3 性能分析

3.1 后台数据库和标签同步更新

在通信过程中，可能由于攻击者的破坏或其他外来因素，标签没能收到最后一步的信息，使标签的ID无法更新，致使标签和后台数据库无法同

步更新 ID 值. 在本协议中，后台数据库同时存放标签的新旧 ID：ID_{old} 和 ID_{new}，ID_{old} 为标签在上一次通信时使用的 ID，ID_{new} 为上次通信完成后标签更新的 ID. 这样即使后台数据库和标签更新未能同步，在下一次通信时标签依然可以在后台数据库的 ID_{old} 中找到匹配项，不会影响后台数据库对标签的合法性验证.

3.2　安全性分析

1) 保密性. 本文协议中发送的消息都是通过 Hash 函数和异或运算加密的，由于 Hash 函数的单向性，攻击者很难获得 ID、RID 等保密信息，所以本协议具有很好的保密性.

2) 重放攻击. 首先分析重放阅读器请求. 如果攻击者在认证过程中重放阅读器请求，由于标签只在 $T_t=0$ 的时候才会响应，而 T_t 在整个认证过程中始终等于 1，所以重放无效. 如果攻击者重放阅读器的请求时标签没有进行其他的认证，在标签响应后攻击者截获响应信息，并假装已经通过第 3、第 4 步的认证，然后向标签发送伪造的 $H_1(R \oplus ID \oplus T_{td})$，由于在上一次的通信过程中标签的 ID 已经更新，所以在最后标签验证时标签收到的信息与保存的信息不同，认证失败，重放攻击无效.

重放标签响应的分析. 攻击者如果在本次认证过程中重放标签响应，由于阅读器只在 $T_r=1$ 时才会做出回应，而当攻击者重放标签响应的时候，阅读器的标识 T_r 已经变成了 0，所以阅读器不会响应，重放无效. 如果攻击者在认证过程中重放上一次认证过程中标签的响应信息，由于随机数 R 与标签 ID 不同，在后台数据库中认证时会导致失败，重放无效. 如果阅读器已经结束本次认证，并且在攻击者重放标签响应时阅读器没有进行其他的认证过程，则由于阅读器中没有存放随机数 R 而不做出回应，重放无效. 所以本协议具有抗重放攻击的能力.

3) 假冒攻击. 如果攻击者截获阅读器的请求信息并假冒阅读器发给标签，标签响应后向攻击者发送 $H_r(R \oplus ID \oplus T_{td})$，由于攻击者不知道如何计算 $H_r(R \oplus RID \oplus R_{rd})$，所以在攻击者将 $H_r(R \oplus ID \oplus T_{td})$ 和伪造的 $H_r'(R \oplus RID \oplus R_{rd})$ 发送给后台数据库时，认证失败. 如果攻击者不做第 3、第 4 步直接向标签发送伪造的 $H_1'(R \oplus ID \oplus T_{td})$，则在标签处认证失败.

如果攻击者截获标签的响应信息，然后假冒标签将截获的信息发送给阅读器，阅读器按照正常步骤将信息发送给后台数据库，通过认证后，阅读器发送信息给标签，攻击者截获此信息后假装认证通过. 认证完成后，阅读器和后台数据库进行通信时，阅读器读到的依然是正确标签的信息，所以此攻击无效.

4) 前向不可追踪性. 理想情况下，攻击者可以通过截获状态信息对标签进行攻击. 由于本协议中的信息是通过 Hash 函数和异或运算进行加密后传递的，而且每次通信标签的 ID 都动态更新，这样，标签每次响应的信息都不同，所以攻击者很难将截获的信息与某个特定标签联系，无法跟踪标签位置.

5) 系统内部攻击. 系统内部攻击包括系统内合法标签 B 假冒合法标签 A 和合法阅读器 B 假冒合法阅读器 A. 首先分析前者. 标签 A 和 B 的标识分别为 ID_a 和 ID_b，A 和 B 与后台数据库分别共享密钥 T_{td}^a 和 T_{td}^b. 认证开始后，阅读器向标签发送请求和随机数 R，标签 B 假冒 A 向阅读器发送 $H_r(R \oplus ID_a \oplus T_{td}^b)$，后台数据库在验证标签的合法性时只能找到 $H_r(R \oplus ID_a \oplus T_{td}^a)$ 和 $H_r(R \oplus ID_b \oplus T_{td}^b)$，这与收到的 $H_r(R \oplus ID_a \oplus T_{td}^b)$ 不相同，所以认证失败. 失败的主要原因是 T_{td}^a 是标签 A 和后台数据库私有的，而标签 B 无法知道，因此标签 B 无法计算出正确的 $H_r(R \oplus ID_a \oplus T_{td}^a)$，从而认证失败. 若系统内合法阅读器 B 假冒合法阅读器 A，由于 RID_a 只有阅读器 A 与后台数据库知道，而阅读器 B 不知道，因此阅读器 B 无法计算出正确的 $H_r(R \oplus ID_a \oplus T_{rd}^a)$，认证失败. 可见本协议可以很好地防止系统内部攻击.

将新协议与文献[3]、[6] 和[7] 中的协议做安全性方面的对比，结果如表 3 所示（× 表示不具备此安全性能，○ 表示具备此安全性能）. 由表中各项可知新协议在保留文献[7] 轻量级加密结构的同时能抵抗各种攻击，具有最好的安全性.

表 3 RFID 认证协议的安全性比较

认证协议	保密性	重放攻击	假冒攻击	前向不可追踪	轻量级加密	系统内部攻击	适用于无线阅读器
文献[3]	×	×	×	×	○	×	○
文献[6]	○	○	○	○	×	○	×
文献[7]	×	×	×	×	○	×	×
新协议	○	○	○	○	○	○	○

3.3 效能分析

将新协议与文献[3]、[6]和[7]中的协议做计算量和存储量方面的对比,结果如表 4 所示(Hash、Ran、Xor、Ser 和 E_k 分别表示散列函数、随机数产生、异或运算、串联运算和对称加密运算;N_1 和 N_2 分别表示阅读器和标签的数量,其中 N_2 远远大于 N_1).由表 4 可知:新协议中标签和阅读器的计算量大大减少,很好地满足了低成本的要求;虽然后台数据库的计算量增加,但是增加的这部分计算量提高了协议的整体保密性和抗攻击能力.新协议中标签的存储量相对于文献[3]和[7]虽没有变化,但是比文献[6]减少了很多,并且后台数据库的存储量相对于其他协议也有所减少.可见,新协议在计算量和存储量上具有很高的优越性.

表 4 RFID 认证协议的效能比较

认证协议	计算量			存储量		
	标签	阅读器	后台数据库	标签	阅读器	后台数据库
文献[3]	5Hash+9Xor	6Hash+1Ran+5Xor+5Ser	$O(1)$	3	1	N_1+5N_2
文献[6]	1Hash+1Ran+4E_k	1Ran+1Ser+1E_k	$O(1)$	$2+2N_1$	2	N_1+4N_2
文献[7]	4Hash+4Xor+4Ser	0	$O(1)$	3	0	$5N_2$
新协议	2Hash+3Xor	1Hash+2Xor	$O(N_1+N_2)$	3	3	$2N_1+3N_2$

4 结束语

本文在文献[7]的基础上提出了一种改进的 RFID 双向认证协议,为确保协议中阅读器与标签、阅读器与后台数据库之间通信的安全性,新协议采用了 Hash 函数、异或运算、动态更新标签 *ID* 的方法来防跟踪、防窃听、防重放和假冒攻击,而且通过在阅读器和后台数据库、标签和后台数据库之间共享密钥来防止系统内部攻击,同时通过在标签和阅读器中设置状态值 T_t 和 T_r 能够更快捷有效地防重放攻击.效能分析表明,本文协议成本低,而且能抵抗窃听攻击、重放攻击、假冒攻击、系统内部攻击等,具有很好的安全性和实用性.

参考文献:

[1] 潘涛,左开中,郭良敏,等.基于异或运算的低成本 RFID 双向认证协议[J].计算机工程,2012,38(9):278-281.

[2] He Jialiang, Xu Zhiqiang. A mutual RFID security protocol for wireless reader[J]. International Journal of Security and Its Applications, 2013,7(5):43-52.

[3] Sandhya M, Rangaswamy T R. A Practical Approach for Enhancing Security in Mobile RFID Environment[C]//2011 International Conference on Future Information Technology ICFIT 2011. Singapore, 2011.

[4] 朱炜玲,喻建平.物联网移动 RFID 系统隐私保护方案[J].系统工程理论与实践,2011,31(S2):119-123.

[5] 郭建庆.RFID 系统的安全认证协议的研究[D].南京邮电大学,2012:19-40.

[6] 裴云.RFID 安全认证协议研究[D].华中科技大学,2012:10-25.

[7] He Jialiang, Ouyang Dantong, Xu Youjun, et al. An efficient RFID authentication protocol supporting tag ownership transfer[J]. International Journal of Advancements in Computing Technology, 2012, 4(4):244-253.