第34卷 第20期 计 算 机 工 程 2008年10月
Vol.34 No.20 Computer Engineering October 2008
·安全技术· 文章编号：1000—3428(2008)20—0151—03 文献标识码：A 中图分类号：TP393.08

一种基于随机序列的RFID安全协议

林贵彬[1,2]，王永华[1]，詹宜巨[3]
(1. 中山大学信息科学与技术学院，广州 510275；2. 中兴通讯股份有限公司CDMA研究所，深圳 518009；
3. 中山大学工学院，广州 510275)

摘 要：提出一种新的RFID安全协议，利用已存储的随机序列产生伪随机数的机制代替随机数产生器。该协议采用阅读器和电子标签双方互相验证的机制，可以防止跟踪、非法阅读器读取标签数据、标签假冒、重放攻击等威胁。在保证安全等级的情况下减少了标签硬件电路的复杂程度，有效降低了RFID标签的设计成本。建立协议的理想化模型，利用BAN逻辑对该协议进行形式化分析，在理论上证明其安全性。

关键词：安全协议；随机数；BAN逻辑

RFID Secure Protocol Based on Random Sequence

LIN Gui-bin[1,2], WANG Yong-hua[1], ZHAN Yi-ju[3]
(1. School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510275;
2. CDMA Research Institute, ZTE Corporation, Shenzhen 518009;
3. School of Engineering, Sun Yat-sen University, Guangzhou 510275)

【Abstract】 This paper proposes a new RFID secure protocol which uses the mechanism that the random sequence stored in the tag produces the pseudo random number to replace the random value generator. With both tag-to-reader and reader-to-tag authentication, the protocol can prevent the RFID system from some malicious attack, such as tracking, spoofing, forgery, and replay attack. It reduces the tag designing cost while ensuring the security grade. After setting up an idealized protocol model, a process of formal analysis of this protocol is presented and the security is proved theoretically by using the BAN logic.

【Key words】 secure protocol; random value; BAN logic

RFID是一种利用射频信号进行信息通信的非接触式自动识别技术，具有抗干扰能力强、信息量大、非视觉范围读写、寿命长等特点。但由于RFID的信息通过自由空间传输，因此引发了一些信息安全问题。虽然已有多种基于密码学理论的RFID安全协议，但其实用性较低、成本较高。目前缺少针对RFID安全协议的形式化分析和证明。本文提出一种新的协议并利用BAN逻辑[1]对该协议进行形式化分析。

1 RFID安全协议

基于密码学的RFID安全协议能有效加强RFID系统的安全性能、保护消费者隐私、防止信息泄漏。下文将介绍4种RFID安全协议，并分析其优缺点。

1.1 定读取控制Hash锁协议

在定读取控制Hash锁协议[2]中，阅读器向电子标签发出*ID*访问请求，标签发送*metaID*，阅读器回复根据*metaID*计算*K*值。标签计算*hash*(*K*)，若*metaID*=*hash*(*K*)，则阅读器通过验证，解锁并发送*ID*值给阅读器。若*ID*值与数据库的*ID*相同，则对标签的验证通过。因为每次询问后射频标签的反应固定，所以存在被跟踪的危险，且协议中的随机密钥*K*和标签*ID*通过明文传输，容易被窃听并受到假冒攻击和重传攻击。

1.2 随机读取控制Hash锁

在随机读取控制Hash锁协议[2]中，标签向阅读器发出的*metalID*是变化的。随机读取控制Hash锁可以避免被跟踪，但阅读器每次识别一个标签都需要搜索并计算所有标签*ID*，系统资源消耗过大，容易受到拒绝服务攻击。阅读器通过不安全的无线信道传输*IDk*的明文，如果被截取，就会受到标签假冒攻击。

1.3 Hash链

在Hash链协议[3]中，与阅读器进行第*i*次交换时，射频标签对其初始值*Si*，发送*ai*=*G*(*Si*)给阅读器，并根据原有*Si*更新密钥*Si*+1=*H*(*Si*)。Hash链的方法容易遭受重传攻击，只要截获一个*ai*值，就可进行重放攻击。

1.4 David的数字图书馆RFID协议

在David的数字图书馆RFID协议[4]中，后端数据库和每个标签之间在系统运行前，需要预先共享一个秘密值*s*，f_s表示用*s*加密的安全伪随机函数。该协议执行过程如下：(1)阅读器向标签发送认证请求及其生成的随机数*Rr*；(2)标签生成随机数*Rt*，使用自己的*ID*和秘密值*s*计算$\sigma = ID \oplus f_s(0, Rr, Rt)$，并将$(Rt, \sigma)$发送给阅读器；(3)阅读器将$(Rt, \sigma)$转发给后端数据库；(4)数据库检查是否有某个*IDj*，使$IDj = \sigma \oplus f_s(0, Rr, Rt)$成立，若有，则对标签的认证通过，并将$\beta = IDj \oplus f_s(1, Rr, Rt)$发送给阅读器；(5)阅读器将$\beta$转发给标签；(6)标签验证$ID = \beta \oplus f_s(1, Rr, Rt)$是否成立，若成立，则对阅读器的认证

基金项目：广东省自然科学基金资助项目(06023131)；中山大学“985”二期基金资助项目(90013-3272240)
作者简介：林贵彬(1981－)，男，硕士，主研方向：通信系统，RFID及信息安全；王永华，博士研究生；詹宜巨，教授、博士生导师
收稿日期：2007-12-30 **E-mail：**zhanyiju@mail.sysu.edu.cn

通过。该协议没有明显的安全漏洞，但必须在标签电路中包含实现随机数生成及安全伪随机函数 2 个功能模块，因此，不适用于低成本RFID标签系统。

2 基于随机序列的 RFID 安全协议

在使用大量电子标签的场合中，降低标签成本是一个需要重点考虑的因素。在保证安全性的前提下，应尽可能简化标签设计。根据上述协议的优缺点，本文设计了一种新的 RFID 安全协议。

假设攻击者可能窃听到无线信道里阅读器和标签间的所有电文，而阅读器和数据库之间是用成熟的网络安全机制加以保证的安全信道。*ID* 表示标签的唯一性代号，*X* 表示标签里的敏感信息，数据库和每个合法的标签间共享一个密钥 *k*，$H_k(X)$ 表示用密钥 *K* 对消息 *X* 进行单向杂凑运算。基于随机序列的 RFID 安全协议如图 1 所示。

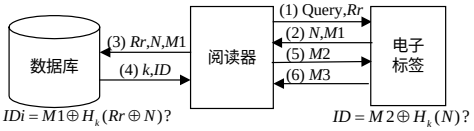

图 1 基于随机序列的 RFID 安全协议

其中，$N = N' + n_i$ ；$M1 = H_k(Rr \oplus N) \oplus ID$ ；$M2 = H_k(N) \oplus ID$ ；$M3 = H_k(N \oplus Rr) \oplus X$ 。

对图 1 说明如下：

(1)阅读器发出询问指令 Query，并将阅读器产生的一个随机数 *Rr* 发送给电子标签。

(2)标签利用出厂初始化时储存好的随机序列值 n_i ($0 \le i \le L$)产生一个伪随机数 $N = N' + n_i$ ，*N'*为前一个 *N* 的值，将当前 *i* 值修改为 *i*＋1 并储存，当 *i*>*L* 时，*i*=1。标签将随机数 *Rr*, *N* 及自身的序列号 *ID* 进行与或运算及基于共享密钥 *K* 的单向杂凑函数运算，将得到的密文 $M1 = H_k(Rr \oplus N) \oplus ID$ 连同明文 *N* 一起发送给阅读器。

(3)阅读器发送 *Rr* 并转发 *N*, *M*1 给后台服务器的数据库系统。

(4)后台系统根据储存在数据库中的 *ID* 及其密钥 *k* 值，计算是否有 *ID* 使 $ID = M1 \oplus H_k(Rr \oplus N)$ 成立，若有，就找到了标签的 *ID* 和 *k* 值，并证明了电子标签的合法性。后台系统将 *ID* 及密钥 *k* 通过安全的通道传送给阅读器。

(5)阅读器利用 *k* 值计算出密文 $M2 = H_k(N) \oplus ID$ 后发送给标签。

(6)标签验证 $ID = M2 \oplus H_k(N)$ 是否成立，若成立，则证实了阅读器的合法性，并给阅读器发送加密过的信息 $M3 = H_k(N \oplus Rr) \oplus X$ ；若不成立则保持静寂。

3 协议安全性

本文 RFID 安全协议可防止 4 类安全威胁，即跟踪、监听、欺骗、重放攻击。

假设在无线信道上的一切消息都在攻击者的控制下，攻击者可以任意读取、插入、删除、篡改、延迟发送或重放任何消息，也可以在任意时刻发起与阅读器或标签的任意对话。本文遵循一切秘密寓于密钥之中的原则，假设攻击者知道除了密钥 *k* 以外的协议流程和算法。

在本文协议中，标签对询问的反应是变化的，可防止扫描跟踪 *ID* 值获取标签位置。*N* 的值每次都改变，根据存储在标签内一定长度的随机序列数进行跳转。每个标签储存不同随机序列，有自己的跳转规律，在 *N* 的长度为 *k* bit 时，输出结果有 2^k 种，对攻击者而言是不确定的，使其难以实施跟踪。

在无线信道上，利用随机数和单向杂凑函数生成一次插入的随机密钥，进行与或运算的数据流加密。除随机数 *Rr* 和伪随机数 *N* 是明文外，其他信息都是经过加密处理的密文。攻击者在不知道密钥的情况下，难以根据 *Rr* 和 *N* 计算杂凑值 $H_k(Rr \oplus N)$, $H_k(N)$, $H_k(N \oplus Rr)$ ，即不能破解其中的明文，无法得知 *ID* 或 *X* 值。由于单向杂凑函数的特点是反向运算极困难，因此可以有效保护各种秘密信息，防止监听和非法读取标签数据。

本文采用阅读器和电子标签相互验证，双方在通信中加入了己方信任的随机数因子进行加密，保证消息的新鲜性，可防止重放攻击。假冒标签缺少密钥 *k*，无法完成对阅读器 *Rr* 的正确响应 *M*1，不能通过阅读器的身份验证程序。同理，非法阅读器企图直接读取或改写标签内容时，难以对标签发出的 *N* 值作出正确的反映 *M*2，标签进入静寂状态，可防止非法阅读器通过多次查询，试图用暴力攻击手段，如穷举搜索等方法找到 *N*, *ID* 和 *M*2 的对应关系。

以上安全性讨论是在假设密钥 *k* 绝对保密的情况下实现的，在系统设计和工程实施阶段都要注意对密钥的保护。

4 安全性推导与分析

4.1 BAN 逻辑简介

BAN逻辑[1]是用于分析安全协议的一种逻辑手段，其规则简洁且直观，推导过程根据最初的假设条件利用基本逻辑推理规则，逐步推导出协议的最终目的。

BAN 逻辑表达式描述如下：$P \mid\equiv X$ 表示 *P* 相信 *X*；$P \lhd X$ 表示 *P* 收到过 *X*；$P \Rightarrow X$ 表示 *P* 对 *X* 有仲裁权；$P \mid\sim X$ 表示 *P* 说过 *X*；$\#(X)$表示 *X* 是新鲜的；$P \xleftrightarrow{K} Q$ 表示 *P* 和 *Q* 共享一个密钥 *K*；$\{X\}_K$ 表示用密钥 *K* 加密消息 *X* 的密文。

BAN 逻辑的几条基本逻辑推理规则如下：

(1)消息意义规则 $\dfrac{P \mid\equiv Q \xleftrightarrow{K} P, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$

(2)随机数验证规则 $\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$

(3)仲裁规则 $\dfrac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$

(4)信仰规则 $\dfrac{P \mid\equiv (X, Y)}{P \mid\equiv X, P \mid\equiv Y}$

(5)信仰规则 $\dfrac{P \mid\equiv X, P \mid\equiv Y}{P \mid\equiv (X, Y)}$

(6)新鲜规则 $\dfrac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)}$

4.2 形式化分析

共有 3 方参与协议，即电子标签 *A*、阅读器 *B*、后台服务器的数据库系统 *S*。*A* 与 *S* 之间在初始化时已共享一个密钥 *K*。笔者将阅读器和数据库系统之间的安全信道模型假设为 *B* 与 *S* 利用一个可靠的良好密钥 *Kbs* 加密信息，为了简化分析过程，忽略 RFID 安全有线信道良好密钥的新鲜性问题，可以增加一条良好密钥规则：

(7) $\dfrac{P \mid\equiv Q \xleftrightarrow{GoodKey(K)} P, P \lhd \{X\}_K}{P \mid\equiv Q \mid\equiv X}$

增加规则(7)对于讨论 RFID 的无线信道安全性问题没有

大的影响。整个协议的目的是验证 A 和 B 的合法性。

首先建立协议的初始假设集合：

$A|\equiv A\xleftrightarrow{K}S$, $B|\equiv B\xleftrightarrow{Kbs}S$, $B|\equiv GoodKey(Kbs)$

$S|\equiv A\xleftrightarrow{K}S$, $S|\equiv B\xleftrightarrow{Kbs}S$, $S|\equiv GoodKey(Kbs)$

$B|\equiv S\Rightarrow ID$, $A|\equiv S\Rightarrow B\xleftrightarrow{Kbs}S$

$B|\equiv \#Rr$, $A|\equiv \#N$, $S|\equiv B|\equiv \#Rr$, $S|\equiv A|\equiv \#N$

然后建立协议的理想化模型：

a: A－>B：$N,\{Rr,N,ID\}_K$

b: B－>S：$\{Rr,N,\{Rr,N,ID\}_K\}_{Kbs}$

c: S－>B：$\{ID,K\}_{Kbs}$

d: B－>A：$\{N,B\xleftrightarrow{Kbs}S\}_K$

其中，a,b,c,d 表示 4 条消息，消息 c 中的 ID 表明了标签的合法性；消息 d 中 $B\xleftrightarrow{Kbs}S$ 说明阅读器是合法的。

上述协议的预期目标是 $A|\equiv B\xleftrightarrow{Kbs}S$, $B|\equiv ID$ ，其实际意义是经过阅读器和标签双方验证后，两者均能得知对方是合法的。

根据上述模型，运用 BAN 逻辑表达式进行推理：

(1)由模型中的消息 a，可以得到 $B\triangleleft N$, $B\triangleleft\{Rr,N,ID\}_K$ ，B 无法理解加密后的内容，但可以转发给 S。

(2)由消息 b 可知 $S\triangleleft\{Rr,N,\{Rr,N,ID\}_K\}_{Kbs}$ ，加上初始假设 $S|\equiv B\xleftrightarrow{Kbs}S$, $S|\equiv GoodKey(Kbs)$ ，利用规则(7)，可知 $S|\equiv\{Rr,N,\{Rr,N,ID\}_K\}$ 。由规则(4)可得 $S|\equiv Rr$, $S|\equiv N$, $S|\equiv\{Rr,N,ID\}_K$ 。由假设 $S|\equiv A\xleftrightarrow{K}S$ ，利用规则(1)可得 $S|\equiv A|\sim\{Rr,N,ID\}$ 。由假设 $B|\equiv \#Rr$, $S|\equiv B|\equiv \#Rr$ 及规则(6)，得到 $B|\equiv \#\{Rr,N,ID\}$, $S|\equiv \#\{Rr,N,ID\}$ ，得 $S|\equiv \#Rr$, $S|\equiv A|\sim\{Rr,N,ID\}$, $S|\equiv ID$ 。S 发出消息 c。

(3)由消息 c，即 $B\triangleleft\{ID,K\}_{Kbs}$ ，且 $B|\equiv B\xleftrightarrow{Kbs}S$, $B|\equiv GoodKey(Kbs)$ ，利用规则(7)可推得 $B|\equiv S|\equiv\{ID,K\}$ ，利用规则(4)可得 $B|\equiv S|\equiv ID$ 。假设 $B|\equiv S\Rightarrow ID$ ，利用规则(3)得到 $B|\equiv ID$ 。

(4)由消息 d，即 $A\triangleleft\{N,B\xleftrightarrow{Kbs}S\}_K$ ，根据规则(1)，有 $A|\equiv S|\sim\{N,B\xleftrightarrow{Kbs}S\}$ 。由假设 $A|\equiv \#N$ 及规则(6)得到 $A|\equiv \#\{N,B\xleftrightarrow{Kbs}S\}$。利用规则(2)可得 $A|\equiv S|\equiv\{N,B\xleftrightarrow{Kbs}S\}$，利用规则(4)可得 $A|\equiv S|\equiv B\xleftrightarrow{Kbs}S$ 。根据假设 $A|\equiv S\Rightarrow B\xleftrightarrow{Kbs}S$ 并利用规则(3)，可知 $A|\equiv B\xleftrightarrow{Kbs}S$ 。

(5)最终可得 $A|\equiv B\xleftrightarrow{Kbs}S$, $B|\equiv ID$ ，即证明了该协议实现了其预期目标，安全性得到保证。

5 结束语

本文 RFID 安全协议利用已存储的随机序列代替随机数产生器，可以有效简化电路。此协议适用于低成本电子标签系统，具有较高实用价值。

参考文献

[1] Burrows M A, Needham R. A Logic of Authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18-36.

[2] Stephen A W, Sanjay E S, Ronald L R, et al. Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems[C]// Proceedings of International Conference on Security in Pervasive Computing. Boppard, Germany: [s. n.], 2003.

[3] Gao Xingxin, Xiang Zhe, Wang Hao, et al. An Approach to Security and Privacy of RFID System for Supply Chain[C]//Proceedings of the IEEE International Conference on E Commerce Technology for Dynamic E Business. [S. l.]: IEEE Press, 2004.

[4] Molnar D, Wagner D. Privacy and Security in Library RFID: Issues, Practices, and Architectures[C]//Proceedings of the 11th ACM Conference on Computer and Communications Security. [S. l.]: ACM Press, 2004.

(上接第 150 页)

阶段 2 虽然增加了 1 个 Hash，却减少了 3 个对称加密，相较于文献[1]不但没有增加终端的负担，而且没有增加信息传送次数。在文献[1]中信息至少需传输 10 次，造成了对无线稀缺频谱资源的浪费。

表 1 改进后 AKA 与原 3G 中 AKA 安全性比较

	防止中间人攻击	VLR、HLR 间密文传输	是否有双向验证	对 IMSI 保密	对网络端同步调整	对终端同步调整	防止 HLR 遭受回放攻击	f1 和 f1*	f5 和 f5*	异或器	ECC
本文 AKA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
3G 中 AKA	N	N	Y	N	Y	N	N	N	N	N	N

表 2 身份认证中 MS 所负担计算量比较

	公钥加密	私钥解密	对称加解密	签名	签名验证	Hash
本文的 AKA	1	0	1	0	1	2
文献[4]阶段 2 的AKA	1	0	4	1	0	1
文献[1]的SSL AKA	1	0	0	1	1	3

5 结束语

通过对原有 3G 入网认证标准和 WPKI 所存在的漏洞进行分析，提出了基于混合密码体制入网认证机制，弥补了原有 3G 中安全方面的不足，并针对在下一代异构网络中实现统一安全问题，提出了大体的 PKI 体系架构。整个方案没有增加通信次数。且利用移动商务中 ECC 的使用，对已具备商务功能的终端没有增加设备或芯片的数量。终端和 HLR 却减少了 f1, f1*, f5, f5*和一个异或器。鉴于 PKI 越来越广泛的普及和 ECC 芯片的大量生产，此方案具有一定的可实现性。

参考文献

[1] Kambourakis G, Rouskas A, Gritzalis S. Performance Evaluation of Public Key-based Authentication in Future Mobile Communication Systems[J]. Journal on Wireless Communications and Networking, 2004, 1(1): 184-197.

[2] Jiang Yixin, Lin Chuang, Shen Xuemin, et al. Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks[J]. IEEE Trans. on Wireless Communication, 2006, 5(9): 2569-2577.

[3] Zheng Yu, He Dake, Xu Lixing et al. Security Scheme for 4G Wireless Systems[C]//Proceedings of International Conference on Communications, Circuits and Systems. [S. l.]: IEEE Press, 2005: 397-401.

[4] Zheng Yu, He Dake, Tang Xiaohu, et al. AKA and Authorization Scheme for 4G Mobile Networks Based on Trusted Mobile Platform Information[C]//Proceedings of the 5th International Conference on Communication and Signal. [S. l.]: IEEE Press, 2005: 976-980.