基于循环移位的轻量型相互认证协议研究

张学军[1,2],王 玉[1],王锁萍[2],孙知信[2]
(1.南京邮电大学电子科学与工程学院,江苏南京 210003;2.南京邮电大学宽带无线通信与传感网技术教育部重点实验室,江苏南京 210003)

摘 要: 安全隐私是射频识别系统的关键问题,该文在轻量型相互认证协议的基础上,根据阅读器产生的随机数对将要传送的信息进行循环左移,提出了基于循环移位的轻量型相互认证协议(CSLMAP 协议),并用 GNY 逻辑对协议的安全性进行了证明.结果显示,所提出的 CSLMAP 协议解决了轻量型相互认证协议中的安全隐私问题,提高了认证协议的执行效率,降低了标签的应用成本.

关键词: 射频识别技术; 安全隐私; 轻量型认证协议
中图分类号: TN92 **文献标识码:** A **文章编号:** 0372-2112 (2012)11-2270-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.11.020

Research on the Cyclic Shift Lightweight Mutual Authentication Protocol

ZHANG Xue-jun[1,2], WANG Yu[1], WANG Suo-ping[2], SUN Zhi-xin[2]
(1. *School of Electronic Science and Engineering, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*;
2. *Key Laboratory of Broadband Wireless Communication and Sensor Network Technology of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*)

Abstract: The security and privacy has become key issues in the RFID system. The information to be transmitted needs to rotate left according to the random number generated by reader, a cyclic shift of the lightweight mutual authentication protocol (CSLMAP) is put forward on the basis of Lightweight Mutual Authentication Protocol (LMAP), and then GYN logic is used to prove the safety of the proposed protocol. The result shows that the new protocol solves the problem of security and privacy in the Lightweight Mutual Authentication Protocol, and improves the efficiency of the authentication protocol, thus reducing the cost of the application of tags.

Key words: radio frequency IDentification (RFID); security and privacy; lightweight authentication protocol

1 引言

射频识别技术 (Radio Frequency IDentification, RFID) 是一种利用射频信号通过空间耦合(交变磁场或电磁场)实现无接触信息传递并通过所传递的信息达到识别目标的技术.射频识别系统通常由电子标签(射频标签)、阅读器和后端数据库组成[1].RFID 技术和传感器技术、纳米技术、智能嵌入技术并称为物联网的四大核心技术[2],随着物联网应用研究的深入,RFID 系统的安全和隐私问题受到广泛的关注.RFID 的安全问题通常有窃听、消息拦截、假冒和针对 RFID 系统的中间人攻击等,这些攻击可分为主动攻击和被动攻击.主动攻击通常是以建立 RFID 系统和 RFID 标签的拒绝服务为目标,如中间人攻击和假冒攻击.而窃听和信息窃取是被动攻击[3].由于低成本标签的处理能力、存储空间、电源供给有限等局限性[4],加大了强安全机制实现的难度,设计一种安全、高效、轻量型的 RFID 安全认证协议具有很重要的实际意义.本文在轻量型相互认证协议(Lightweight Mutual Authentication Protocol, LMAP)[5]的基础上,根据阅读器产生的随机数将要传送的信息进行循环左移,提出了一种新的安全协议——基于循环移位的轻量型相互认证协议(Cyclic Shift Lightweight Mutual Authentication Protocol, CSLMAP),并用 GNY 逻辑[6]对协议的安全性进行了证明.结果显示,所提出的 CSLMAP 协议解决了 LMAP 协议中的安全隐私问题,提高了认证协议的执行效率,降低了标签的应用成本.

2 LMAP 协议及安全分析

在 RFID 系统中,目前广泛采用基于密码的安全协

收稿日期 2011-11-17;修回日期:2012-06-09
基金项目:国家自然科学基金(No.60973140, No.61001077, No.61170276);江苏省高校自然科学基金(No.08KJB510015)

议,这一类安全协议主要分为基于散列函数的认证协议和轻量型的认证协议两类.

在基于散列函数的认证协议中,所有的秘密值都是通过散列函数加密后进行通信.散列函数具有随机性和不可逆转性,加密后的信息可以安全地在无线信道中传输.这一类安全协议主要有:Hash 锁协议[7]、随机化 Hash 协议[8]、Hash 链协议[9]等.轻量型的认证协议仅用简单的位运算,而不用高代价的乘法运算和 Hash 函数,随机数发生器也只在阅读器执行,大大减少标签的逻辑门数量,但是在强大的攻击下很容易被攻击.这一类安全协议主要有:轻量型相互认证协议(Lightweight Mutual Authentication Protocol,LMAP)、强认证和强完整性(Strong Authentication and Strong Integrity, SASI)协议[10~12]、最低限要求的相互认证协议(Minimalist Mutual Authentication Protocol, M^2AP)[13]、高效的相互认证协议(Efficient Mutual Authentication Protocol, EMAP)[14]]、匿名 RFID 认证协议(Anonymous RFID Authentication Protocol, ARAP)[15]和无服务器匿名相互认证(Serverless Anonymous Mutual Authentication, SAMA)[16]等.在 LMAP 协议中,标签和阅读器共享 1 个密钥 K,这个密钥分成 4 个部分($K = K1 \parallel K2 \parallel K3 \parallel K4$),每一部分都是 96 位,1 个动态的索引假名 IDS(96 位),每个标签都拥有唯一的标识符 ID.IDS 和 K 在每次认证结束后都要进行更新,协议认证过程分为 3 个阶段,如图 1 所示.

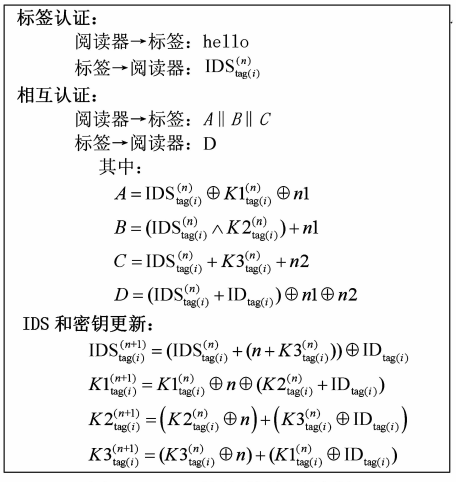

图1　LMAP协议的认证过程

LMAP 协议能够实现相互认证,能够保证数据安全性、标签匿名性、数据机密性、前向安全性,能够抵制重传攻击等,但不能抵御去同步攻击和整体揭露攻击.具体攻击步骤见文献[17].

3　基于循环移位的轻量型相互认证协议——CSLMAP 协议

CSLMAP 协议是在 LMAP 协议基础上,将阅读器发送的信息根据随机数值进行循环左移,实现信息简单加密的方法来抵御去同步攻击;通过在标签中设置状态标志 S 来抵御整体揭露攻击.在 CSLMAP 协议中只用了异或($\oplus$)、或($\vee$)、与($\wedge$)、模 2^m 加法(+)和移位等简单的位操作,符合轻量型协议的要求.为表述方便,下文中所涉及标记符号的含义见表 1.

表 1　标记符号的含义

标记	描述
R	阅读器
T	标签
n	随机数
ID	标签标识符
IDS	标签索引假名
K	密钥值
S	标签中的状态标志
Rot_L(X, Y)	将 X 循环左移 Y 位

在 CSLMAP 协议中,每个标签都有两个标识符:一个是用于在数据库中搜索对应数据的索引假名 IDS(96 位),IDS 在每次协议运行结束后都会进行更新;另一个是标签自身的标识符 ID(96 位),每个标签的 ID 是唯一的,在协议的运行过程中不改变.新协议中,每个标签还增加了一个 2 位的状态标志 S(初始状态为 00),用于记录标签在认证过程中的状态.标签和阅读器共享 1 个密钥 K,每个密钥由 3 部分组成($K = K1 \parallel K2 \parallel K3$,每部分均为 96 位).对应于每个标签,在数据库都要存储[IDS,ID,$K1$,$K2$,$K3$]的信息.由于大多数低成本标签都是无源的,协议的执行必须从阅读器开始,假设前向信道和后向信道都可以被攻击者监听,假设阅读器和后端数据库之间的信道是安全的.CSLMAP 协议的认证过程分为 3 个阶段,如图 2 所示.

标签认证阶段:

(1)阅读器发送查询命令 Hello.

(2)标签响应并将当前的 IDS 发送给阅读器,同时标签将标志位 S 置为 01.

(3)阅读器根据接收到的标签 IDS,在后端数据库中查找相应的密钥值 K.

相互认证阶段:

(4)阅读器生成一个随机数 n(96 位).根据图 2 中的式(1)和式(2),结合索引假名 IDS 和密钥值 $K1$、$K2$ 分别计算生成 A 和 B,再将 B 循环左移 n 位后的值与 B 异或得到 $M1$,阅读器将 $A \parallel M1$ 发送给标签.

(5)标签接收到 $A \parallel M1$ 后,将状态标志 S 置为 11,并从 A 中计算出阅读器生成的随机数 n',将 n' 代入图 2 中的式(2),计算出 B',再将 B' 循环左移 n' 位后的值与 B' 异或得到 $M1'$.比较 $M1$ 与 $M1'$,若不等,标签发送 Fail 信号给阅读器,认证阅读器失败,结束认证;若相等,标签认证阅读器成功,标签计算 C' 值,并将 C' 循环

左移 n' 位得到 $M2'$,标签将 $M2'$ 发送给阅读器.

(6)阅读器接收到 $M2'$ 后,计算 C,并将 C 值循环左移 n 位得到 $M2$. 阅读器比较 $M2$ 与 $M2'$,若相等,相互认证成功,结束认证;若不等,阅读器认证标签失败,结束认证.

索引假名和密钥更新阶段:

(7)相互认证成功后,标签和阅读器都对索引假名和密钥进行下列更新,更新时标签将状态标志 S 重新置为 00.

$$IDS_{tag(i)}^{(n+1)} = (IDS_{tag(i)}^{(n)} + (n + K3_{tag(i)}^{(n)})) \oplus ID_{tag(i)}$$

$$K1_{tag(i)}^{(n+1)} = K1_{tag(i)}^{(n)} \oplus n \oplus (K2_{tag(i)}^{(n)} + ID_{tag(i)})$$

$$K2_{tag(i)}^{(n+1)} = (K2_{tag(i)}^{(n)} \oplus n) + (K3_{tag(i)}^{(n)} \oplus ID_{tag(i)})$$

$$K3_{tag(i)}^{(n+1)} = (K3_{tag(i)}^{(n)} \oplus n) + (K1_{tag(i)}^{(n)} \oplus ID_{tag(i)})$$

在 CSLMAP 协议中,当状态标志 S 为 00 时,标签只能接收阅读器的请求信号;当状态标志 $S=01$ 时,标签只能接收由阅读器发送的 $A \| M1$;而当状态标志 $S=11$ 时,标签只能接收阅读器发送的认证成功或失败的信号.

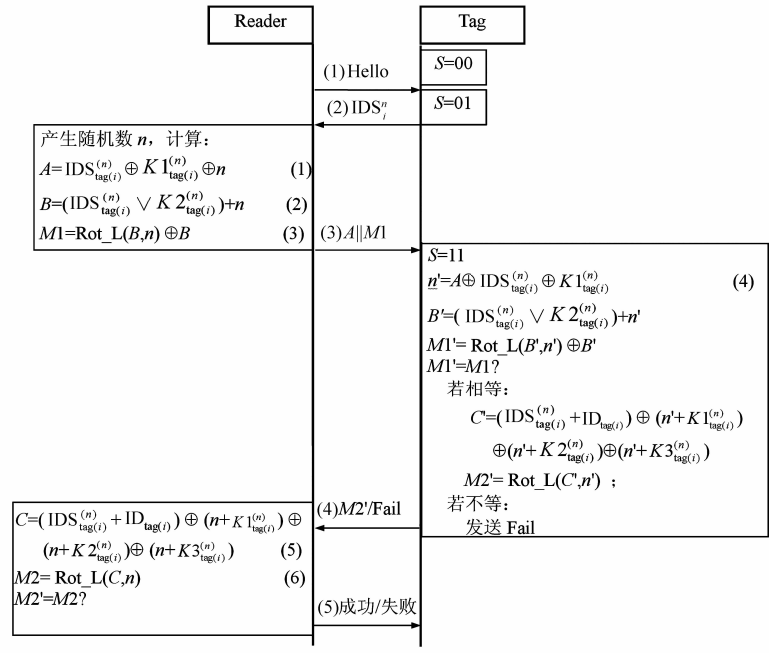

图2 CSLMAP协议的认证过程

4 CSLMAP 协议安全性及性能分析

4.1 安全性分析

相互认证:在协议执行过程中,阅读器通过发送 $A \| M1$ 信息来实现对标签的认证,而标签通过发送 $M2'$ 信息来实现对阅读器的认证,实现了阅读器与标签间的相互认证.

标签匿名性:标签在计算 C' 时隐藏了标签的识别码 ID,而标签向阅读器发送的认证信息 $M2'$ 是将 C' 循环左移 n' 位后得到的. 随机数是由阅读器生成后与密钥值计算得到 A、B 后,通过 $A \| M1$ 发送给标签,并且索引假名和密钥的更新也包含有随机数. 由于每轮传输信息的随机数不同,对于攻击者来说,传输的信息是随机的,所以 CSLMAP 协议可以保证标签的匿名性.

数据机密性:标签的识别码 ID 是利用索引假名 IDS、密钥 K 和随机数运算得到 C',并经过随机的循环左移后发送的. 对于攻击者来说,标签 ID 不是以明文传输的,始终处于加密状态,所以可以保证静态识别码 ID 的安全,即保证了用户数据的机密性.

前向安全性:在每一轮相互认证之后,标签和阅读器都会对当前的 IDS 和 K 进行更新,并且这些更新操作都是不可逆的,即使攻击者成功攻击了当前的标签并获取了 IDS 和 K,也无法推算出先前的传输信息,保证了标签的前向安全性.

重传攻击:在 RFID 系统中,重传攻击主要包括两种方式:(1)伪装成阅读器,重传阅读器对标签的认证请求;(2)伪装成标签,重传标签对阅读器的认证响应. 本协议中,在标签和阅读器完成相互认证后,索引假名和密钥都要更新,所以即使攻击者窃听了所有的信息,重新发送时不会使标签和阅读器失去同步.

去同步攻击:在 LMAP 协议中,攻击者通过篡改信息 A、B、C 实现去同步攻击. 在 CSLMAP 协议中,只要标签能够识别出接收到的 A、B 是否被篡改过,就可以抵御去同步攻击. 由于在 CSLMAP 协议中标签没有直接发送信息 B,因此攻击者不能采用同时修改信息 A、B 的方法来欺骗标签. 但攻击者可能从下述两个方面考虑实施攻击.

方案 1 攻击者考虑从阅读器发送的 $A \| M1$ 中计算出 B 值. 下面通过例子来说明这种攻击方案是不可行的. 首先随机数 n 对攻击者是未知的,假设 $n=3$,且假设所有的信息值都是 8 位,$B=(n7,n6,n5,n4,n3,n2,n1,n0)$,$M1=(11100101)$. 将 B 循环左移 3 位,即 $Rot\_L(B,3)=(n4,n3,n2,n1,n0,n7,n6,n5)$,再将 B 和 $Rot\_L(B,3)$ 异或得到 $M1$,如图 3 所示. 由 $M1$ 可以得到 B 和 $Rot\_L(B,3)$ 对应位的逻辑关系,但并不能确定 B 的每一位的值.

Rot_L(B,3)	n4	n3	n2	n1	n0	n7	n6	n5
⊕								
B	n7	n6	n5	n4	n3	n2	n1	n0
M1	1	1	1	0	0	1	0	1

图3 数值未被修改的逻辑关系

方案 2 攻击者考虑对 $M1$ 进行适当修改,得到等式 $(Rot\_L(B,3))(B)' = Rot\_L(B',3)(B')$,那么也就成功实施了去同步攻击. 若攻击者将 A 值的第 j 位($0 \leqslant j \leqslant 95$)翻转,那么标签中得到的 n' 和 B' 值的第 j 位也相应地被翻转. 假设攻击者将 A 的最后 1 位翻转,那么 n' 和

B'的最后 1 位也发生了翻转,n'的值相当于被加 1 或减 1.下面仍用上述例子来说明该攻击方案是不可行的,最后 1 位被翻转后的逻辑关系分别如图 4(相当于 n'的值加 1)和图 5(相当于 n'的值减 1)所示.

Rot_L(B',4)	$n3$	$n2$	$n1$	$n0'$	$n7$	$n6$	$n5$	$n4$
⊕								
B'	$n7$	$n6$	$n5$	$n4$	$n3$	$n2$	$n1$	$n0'$
$M1'$	×	×	×	×	×	×	×	×

图4　数值被修改后的逻辑关系（n'+1）

Rot_L(B',2)	$n5$	$n4$	$n3$	$n2$	$n1$	$n0'$	$n7$	$n6$
⊕								
B'	$n7$	$n6$	$n5$	$n4$	$n3$	$n2$	$n1$	$n0'$
$M1'$	×	×	×	×	×	×	×	×

图5　数值被修改后的逻辑关系（n'-1）

攻击者如果截获了 $M1$,只能得到 B 和 Rot_L(B,3)对应位的关系.当攻击者将 A 改成 A'后,n'的值被加 1 或减 1,将 B'进行循环左移的位数也发生了变化,此时再与 B'进行异或后,攻击者无法得到 $M1'$,也就无法对 $M1$ 进行修改.由于标签在第一次接收到 $A \parallel M1$ 信息后,就将状态标志 S 置为 11,此时标签只能识别阅读器最后发送的成功或失败信号,因此攻击者也不可能采用不断向标签发送可能的 $M1'$的方法来实施攻击.只要标签成功认证了阅读器,就可以确定 $A \parallel M1$ 没有被修改过,所以 CSLMAP 协议可以抵制去同步攻击.

整体揭露攻击:整体揭露攻击是去同步攻击的扩展.在对 LMAP 协议的攻击中,攻击者首先假扮成合法的阅读器,获取当前标签的 IDS,然后假扮成标签,并利用这个合法的 IDS 从合法的阅读器获得信息 $A \parallel B \parallel C$.接着,攻击者将所有可能的 $A' \parallel B' \parallel C$ 发送给标签,若接收到的信息是 D,那么 $n1$ 的第 j 位与 B 的第 j 位相等;否则,由此可推断出 $n1$ 的值[17].

表 2　几种轻量型协议的安全性比较

协议 / 安全性	SASI	T2MAP	EMAP	Gossamer Protocol	LMAP	CSLMAP
数据机密性	○	×	○	○	○	○
标签匿名性	○	×	○	○	○	○
数据完整性	○	×	△	△	△	○
相互认证	○	○	○	○	○	○
前向安全性	×	○	○	○	○	○
抵御重传	○	○	○	○	○	○
抵御假冒	○	○	○	○	○	○
抵御去同步	×	×	×	×	×	○
抵御整体揭露	×	×	×	×	×	○

注释:○满足,△部分满足,×不满足

在 CSLMAP 协议中,C'值是通过 Rot_L(C',n')加密后发送的,而 n'是随机数,攻击者不可能从 Rot_L(C',n')中获得 C'的值,这样隐藏于 C'中的 ID 得到了保护.协议中还设置了状态标志 S,可以记录标签的状态.因此,在协议未完成时,攻击者不能假扮成阅读器发送请求信号获取下次会话的 IDS,也就无法假扮标签,骗取下次会话的 $A \parallel M1$ 值,所以攻击者就不能通过数学推导得出标签的 ID 值.表 2 中从前向安全性、去同步化和整体揭露攻击等安全问题,将 CSLMAP 协议与已有的 RFID 认证协议的安全性进行了分析和比较,可见 CSLMAP 协议具有比其它轻量型协议更高的安全性能.

4.2　性能分析

下面从计算开销、存储开销和通信开销三个方面对 CSLMAP 协议的性能进行分析,并与 LMAP 协议进行比较.

(1)计算开销　低成本的标签具有体积小、计算能力低、存储空间少、能源供给有限等局限性,标签只能存储长度为 32 ~ 128 位的密钥,用于安全协议的门电路不超过 2000 个[18].基于散列函数的认证协议,占用的资源较多,且阅读器端的计算量与标签的数量成比例,所以不能应用于低成本的标签中.在 CSLMAP 协议中没有使用 Hash 函数等复杂的函数,仅用了异或、或、取模和移位等简单的位操作,满足低成本的要求的.该协议中要计算 9 个数值,而 LMAP 协议中也需要计算 9 个数值,可见,在 CSLMAP 协议并没有增加计算的开销;而且在 CSLMAP 协议中只需要 1 个随机数,这样也在一定程度上减轻了计算开销.

(2)存储开销　每个 RFID 标签至少有 1 个不可修改的、特有的标识符 ID,它是存储在 ROM 中的.在 CSLMAP 协议中为每个标签分配了 1 个索引假名 IDS(96 位)和 1 个由 3 部分组成的密钥 K(3 × 96 位),再加上状态标志 S(2 位),这样共需要 386 位的可读可写内存.而在 LMAP 协议中,每个标签也分配了 1 个索引假名 IDS(96 位)和 1 个由 4 部分组成的密钥 K(4 × 96 位)共需要 480 位的可读可写内存.可见,CSLMAP 协议节省了存储开销.

(3)通信开销　在 CSLMAP 协议执行过程中,共需要 5 次信息传输,其中 2 次用于在标签和阅读器相互认证的过程.考虑到低成本标签一般是无源的,标签识别过程就是防碰撞阶段的一部分,所以,协议认证阶段只执行了 3 次信息传输,大大减少了 RFID 系统通信的次数[17].LMAP 协议的认证阶段也只需 3 次信息传输,所以 CSLMAP 协议继承了 LMAP 协议通信量小的优点.

5　CSLMAP 协议安全性证明

本节运用 GNY 逻辑来证明 CSLMAP 协议的安全性.协议认证过程的最终目的是使得阅读器与标签之间相互信任,假设阅读器与后端数据库之间的通信信道是安全的,因此 CSLMAP 协议的证明可以不考虑后端数据库的参与,即通过抽象将其定位于阅读器与标签之间的双方认证协议.

5.1 GNY 逻辑的常用基本原理[6]

下面仅介绍 GNY 逻辑中与本文证明 CSLMAP 协议相关的两个规则. 其中, P 表示对象, X、Y 表示一般意义的公式, K 表示密钥.

(1)已收到规则(Being-told Rules)

规则 1(记为 $T1$): $\frac{P\triangleleft(X,Y)}{P\triangleleft(X)}$ 如果 P 收到过 X 和 Y 的集合,则 P 收到过 X.

规则 2(记为 $T2$): $\frac{P\triangleleft\{X\}_K, P\ni K}{P\triangleleft(X)}$ 如果 P 收到过加密后的 $\{X\}_k$ 且 P 拥有密钥 K,则可视为 P 收到过 X.

(2)拥有规则(Possession Rules)

规则 1(记为 $P1$): $\frac{P\triangleleft X}{P\ni X}$ 如果 P 收到过 X,则 P 拥有 X.

规则 2(记为 $P2$): $\frac{P\ni X, P\ni Y}{P\ni(X,Y), P\ni F(X,Y)}$ 如果 P 拥有 X 和 Y,则 P 拥有 X 和 Y 的合集,且 P 拥有 X 和 Y 的合集的函数运算结果.

5.2 CSLMAP 协议中已成立的命题

(1)标签 T 成立的命题

$T\ni ID$, T 拥有身份信息 ID;

$T\ni K_i$, T 拥有密钥 $K_i(i=1,2,3)$;

$T|\equiv\varphi(K_i)$, T 认为 K_i 是可以被识别的;

$T|\equiv\varphi(IDS)$, T 认为 IDS 是可以被识别的;

$T|\equiv T\overset{K_i}{\leftrightarrow}R$, T 认为 K_i 是 T 和 R 之间良好密钥.

(2)阅读器 R 成立的命题

$R|\equiv\varphi(Hello)$, R 相信命令 Hello 是可被识别的;

$R\ni K_i$, R 拥有密钥 $K_i(i=1,2,3)$;

$R|\equiv\varphi(K_i)$, R 认为 K_i 是可以被识别的;

$R\ni n$, R 可以产生随机数 n;

$R|\equiv\#(n)$, R 相信随机数是新鲜的;

$R|\equiv\varphi(n)$, R 认为 n 是可以被识别的;

$R|\equiv R\overset{K_i}{\leftrightarrow}T$, R 认为 K_i 是 R 和 T 之间良好密钥.

(3)CSLMAP 协议要达到的两个安全目标

目标 1: $T\ni n$ 标签 T 能够获得随机数 n;

目标 2: $R\ni ID$ 阅读器 R 能够获得标签 T 的识别码 ID.

5.3 形式化分析

在分析了安全协议中的各组成部分的成立命题,明确了协议要达到的目标后,利用 GNY 逻辑的推理规则证明安全协议能够从已成立的命题出发,经过运行最终达到协议要求的安全目标,来证明协议的安全性和完备性.

(1)由图 2 中步骤 1,阅读器 R 向标签 T 发送 Hello 命令,可以形式化为

$$T\triangleleft *Hello, R|\equiv\varphi(Hello)$$

由已收到规则 $T1$,可得 $T\triangleleft Hello$

由拥有规则 $P1$,可得 $T\ni Hello$

(2)由图 2 中步骤 2,阅读器 R 接收到标签 T 回复的索引假名 IDS,可以形式化为

$$R\triangleleft *IDS, T|\equiv\varphi(IDS)$$

由已收到规则 $T1$,可得 $R\triangleleft *IDS$

由拥有规则 $P1$,可得 $R\ni IDS$

(3)由图 2 中步骤 3,标签 T 接收到阅读器 R 发送的两个串联计算值 $A\parallel M1$,可以形式化为

$$T\triangleleft *A|M1$$

而 $A=\{n, IDS\}_{K1}$,即 A 是由随机数 n,索引假名 IDS 通过密钥值 $K1$ 加密得到的消息.

$$T\triangleleft *A|M1, T|\equiv T\overset{K_i}{\leftrightarrow}R$$

由已收到规则 $T1$,可得 $T\triangleleft A|M1$

由已收到规则 $T2$,可得 $T\triangleleft n$

由拥有规则 $P1$,可得 $T\ni n$

则目标 1 证毕.

(4)由图 2 中步骤 4,阅读器接收到标签回复的 $M2$,可以形式化为

$$R\triangleleft *M2, 即\ R\triangleleft *C$$

而 $C=\{n, ID, IDS\}_K$,即 C 是由随机数 n、标签标识 ID 和索引假名 IDS 通过密钥 K 加密得到的消息.

$$R\triangleleft *\{n, ID, IDS\}_K, R|\equiv R\overset{K_i}{\leftrightarrow}T$$

由已收到规则 $T1$,可得 $R\triangleleft\{n, ID, IDS\}_K$

由已收到规则 $T2$,可得 $R\triangleleft ID$

由拥有规则 $P1$,可得 $R\ni ID$

则目标 2 证毕.

由上述分析可见,CSLMAP 协议可以达到预期的目标,协议是安全的.

6 结束语

本文提出的 CSLMAP 协议是一种适用于低成本标签的相互认证协议,该协议是在 LMAP 协议的基础上,根据阅读器产生的随机数将要传送的信息进行循环左移,克服了 LMAP 协议的缺陷,有效地抵御了去同步攻击和整体揭露攻击,系统的安全性能提高了,但标签的硬件资源并没有增加,符合轻量型 RFID 安全协议的要求. 文章最后运用 GNY 逻辑,从理论上证明了 CSLMAP 协议的安全性.

参考文献

[1] 张学军,蔡文琦,王锁萍. 改进型自适应多叉树防碰撞算法研究[J]. 电子学报,2012,40(1):193 - 198.
Zhang Xue-jun, Cai Wen-qi, Wang Suo-ping. One Anti-colli-

sion algorithm based on improved adaptive multi-tree search [J]. Acta Electronica Sinica, 2012, 40(1): 193 – 198. (in Chinese)

[2] 宁焕生,徐群玉.全球物联网发展及中国物联网建设若干思考[J].电子学报,2010,38(11):2590 – 2599.
Ning Huan-sheng, Xu Qun-yu. Research on global internet of things developments and its construction in China [J]. Acta Electronica Sinica, 2010, 38(11): 2590 – 2599. (in Chinese)

[3] Mubarak M F, Manan J A, Yahya S. A critical review on RFID system towards security, trust, and privacy (STP) [A]. IEEE 7th International Colloquium on Signal Processing and its Applications[C]. Penang, Malaysia, Mar. 2011. 39 – 44.

[4] Hoopad Mobahat. Authentication and lightweight cryptography in low cost RFID [A]. 2nd International Conference on Software Technology and Engineering[C]. San Juan, PR, Oct. 2010 (V2): 123 – 129.

[5] 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[A]. Proc. Second Workshop on RFID Security[C]. Graz, Austria, July 2006.

[6] Gong Li, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols [A]. Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy [C]. IEEE Computer Society Press, Los Alamitos, CA. 1990: 234 – 248.

[7] Sarma S E, Weis S A, Engels D W. RFID systems and security and privacy implications [A]. In B. Kaliski, editor, CHES′02, volume 2523 of Lectures Notes in Computer Science [C]. Berlin: Springer-Verlag, 2003. 454 – 469.

[8] S A Weis. Security and privacy in radio-frequency identification devices[D]. Master′s thesis, MIT, Cambridge, MA 02139, May 2003.

[9] Miyako Ohkubo, Koutarou Suzuki, Shingo Kinoshita. Hash-chain based forward-secure privacy protection scheme for low-cost RFID[A]. Proceedings of the 2004 Symposium on Cryptography and Information Security (SCIS 2004) [C]. Sendai, Japan, 2004. 719 – 724.

[10] H Y Chien. SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity [J]. IEEE Trans. Dependable and Secure Computing, 2007, 4 (4): 337 – 340.

[11] Paolo D′Arco, Alfredo De Santis. On ultralightweight RFID authentication protocols [J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(4): 548 – 563.

[12] Hung-Min Sun, Wei-Chih Ting, King-Hang Wang. On the security of Chien′s ultralightweight RFID authentication protocol [J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(2): 315 – 317.

[13] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan Estevez-Tapiador, et al. M2AP: A minimalist mutual authentication protocol for low-cost RFID tags[A]. International Conference on Ubiquitous Intelligence and Computing-UIC′06, volume 4159 of Lecture Notes in Computer Science [C]. Berlin: Springer-Verlag, September 2006. 912 – 923.

[14] Tieyan Li, Robert Deng. Vulnerability Analysis of EMAP-An efficient RFID mutual authentication protocol [A]. In IFIP SEC 2007[C]. sandton, Gauteng, South Africa, May 2007.

[15] Jian Shen, Dongmin Choi, Sangman Moh, et al. A novel anonymous RFID authentication protocol providing strong privacy and security[A]. 2010 International Conference on Multimedia Information Networking and Security [C]. Nanjing, China, 2010. 584 – 588.

[16] Myneni S, Misra S, Guoliang Xue. SAMA: Serverless Anonymous mutual authentication for low-cost RFID tags[A]. 2011 IEEE International Conference on Communications [C]. Kyoto, Japan, June 2011. 1 – 5.

[17] Li T, Deng R H, Wang G. The security and improvement of an ultra-lightweight RFID authentication protocols[J]. Security and communication networks, 2008, 1(2): 135 – 146.

[18] 唐静,姬东耀.基于 LPN 问题的 RFID 安全协议设计与分析[J].电子与信息学报,2009,31(2):439 – 443.
Tang Jing, Ji Dong-yao. Design and analysis of security protocols for RFID based on LPN problem[J]. Journal of Electronics &Information Technology, 2009, 31(2): 439 – 443. (in Chinese)

作者简介

张学军(通讯作者)　男,1969 年 8 月出生于江苏南通. 1993 年、2001 年、2011 年分别在中国石油大学、东南大学和南京邮电大学获工学学士、硕士和博士学位. 现为南京邮电大学副教授,硕士生导师,中国电子学会高级会员. 主要研究方向为无线射频识别技术、通信网络的性能分析、流量控制、QoS 理论与技术.
E-mail: xjzhang@njupt.edu.cn

王　玉　女,1989 年 10 月出生于江苏盐城. 南京邮电大学硕士研究生. 主要研究方向为无线射频识别技术、通信网络的性能分析等.
E-mail: jadewy@sina.cn