共享密钥与位运算的移动 RFID 认证协议

梅松青 邓小茹
(广州医科大学 广东 广州 510006)

摘 要 移动 RFID 系统中,可移动读写器与后台数据库之间是通过无线方式进行通信,该信道不安全可靠,传统的 RFID 认证协议并不能适用于移动 RFID 系统中。为解决该问题,提出一种基于共享密钥与按位运算的超轻量级的移动无线射频识别双向认证协议 MAP(Mutual Authentication Protocol)。MAP 基于按位运算机制,采用超轻量级的位替换运算对传输信息进行加密,利用随机数保持传输信息及共享密钥的新鲜性。一次通信过程中标签、读写器、后台数据库三方之间进行认证以此来抵抗攻击者的蓄意破坏。安全性分析表明,MAP 能够实现共享密钥动态更新及抵抗去同步化等攻击。通过 GNY 逻辑对 MAP 进行形式化数学推理,性能分析表明,MAP 具有较低的计算量,适用于低成本的移动 RFID 系统中。

关键词 物联网 无线射频 共享密钥 位替换运算 双向认证

中图分类号 TP393.08 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.07.050

MOBILE RFID AUTHENTICATION PROTOCOL BASED ON SHARED PRIVATE KEY AND BITWISE OPERATION

Mei Songqing Deng Xiaoru
(*Guangzhou Medical University*, *Guangzhou 510006*, *Guangdong*, *China*)

Abstract In the mobile RFID system, the mobile reader and the background database communicate by wireless way. The channel is not secure and reliable, and the traditional RFID authentication protocol cannot be applied to the mobile RFID system. In order to solve the above problem, we propose an ultra-lightweight mutual authentication protocol(MAP) of mobile RFID based on shared key and bit operation. Based on the bitwise operation mechanism, MAP adopted ultra-lightweight bit replacement operation to encrypt the transmission information, and used random numbers to maintain the freshness of the transmission of information and shared key. During a communication process, the tag, the reader and the background database were authenticated to resist the sabotage of the attacker. The security analysis shows that MAP can achieve dynamic update of the shared key and resist attacks such as desynchronization. The formal mathematical reasoning of MAP is carried out by GNY logic. The performance analysis indicates that MAP has a lower computational complexity, and it is suitable for low-cost mobile RFID systems.

Keywords Internet of Things RFID Shared key Bit replacement operation Mutual authentication

0 引 言

RFID 是一种使用非物理性接触实现对象识别和数据交换的技术,兴起于 20 世纪,并在 20 世纪 90 年代末得到大规模的应用[1-2]。

现有的 RFID 系统一般由标签、读写器、后台数据库三部分构成。在传统的 RFID 系统中,读写器一般是固定式,因此读写器与后台数据库之间的通信基于有线信道完成,同时被认为该信道安全可靠[3-4]。伴随着移动智能终端的快速发展,将读写器嵌入移动智能终端中从而形成移动 RFID 系统。在移动 RFID 系

收稿日期:2019-05-15。广东省教育厅"2017 年广东高校重点平台及科研项目"特色创新类项目(自然科学)(2017KTSCX156)。
梅松青,讲师,主研领域:信息安全,生物信息分析。**邓小茹**,副研究员。

统中,读写器不再是固定式,而是可移动的,因此读写器与后台数据库之间的信息传输亦只能通过无线方式完成;无线信道易被攻击者窃听,使得两者之间的信息传输不再安全可靠[5-6]。

基于上述描述,显然传统的 RFID 认证协议并不适用于移动 RFID 系统。为此,提出一种基于共享密钥及按位运算的移动无线射频识别系统双向认证协议 MAP。

1　相关工作

文献[7]提出一个移动双向认证协议,且考虑了后台服务器与移动读写器之间的信道安全问题,引入后台服务器对移动读写器身份认证步骤,适用于移动读写器的认证场景。但对协议进行深入分析发现:协议没有提供标签与移动读写器两者之间的认证,从而导致协议并不能抵抗攻击者发起的假冒攻击。

文献[8]提出一种移动认证协议,该协议未采用计算量较大的哈希函数,而是采用位运算进行信息的加密。对协议进行研究发现:攻击者通过物理入侵的方式获取密钥,从而假冒标签或移动读写器发起假冒攻击。

文献[9]提出了一种超轻量级的移动认证协议,分析发现该协议不能抵抗标签端的重放攻击。文献[10]中提出一种基于 Hash 函数的移动认证协议,分析发现协议无法防范标签伪造且存在中间人攻击及重放攻击。文献[11]提出三方认证的移动协议,但分析得知,协议使得后台数据库一直处于大负荷工作状态,且该协议无法抵抗拒绝服务攻击。

文献[12]基于物理不可克隆设计出一种适用于轻量级的移动 RFID 双向认证协议,协议主要基于物理不可克隆特征进行信息加密。对协议进一步研究分析:协议无法抵抗攻击者发起的去同步化攻击,攻击者截获信息后,重放该消息,经过几轮重放之后,标签一端的密钥会与后台服务器之间的密钥失去同步性。文献[13]提出了基于共享密钥的移动认证协议,分析发现该协议在整个认证过程中并未实现标签对读写器的认证,使得协议存在假冒攻击威胁。

鉴于现有众多方案的缺陷,本文针对移动无线射频识别系统提出了一种基于共享密钥与按位运算的移动 RFID 系统双向认证协议 MAP。MAP 在整个认证过程中,先验证消息源的真伪,再进行后续操作,从而可以抵抗攻击者的蓄意破坏;采用按位运算对信息进行加密,使得 MAP 可以达到超轻量级别,能够有效减少 RFID 系统的计算量;从安全性及性能角度分析表明,MAP 适用于低成本的移动 RFID 系统中。

2　MAP 设计

2.1　初始条件及符号说明

位替换运算定义:为了便于用符号描述,约定用符号 $Sub(X,Y)$ 表示位替换运算符号。位替换运算 $Sub(X,Y)$ 定义如下:设 X、Y 是两个长度均为 L 位的二进制数,$X = x_1x_2\cdots x_L$,$Y = y_1y_2\cdots y_L$。获取二进制数 Y 中为 1 的位,二进制数 X 中与之对应的位元素取反将其替换,则二进制数 X 中共有 $n = wt(Y)$ 个元素被替换,其中 $wt(Y)$ 为 Y 的汉明重量。

位替换运算在标签中实现时,采用文献[14]中所提出的指针形式,从而使得它比直接采用逻辑门效率更高。引入两个指针,一个记为 P_X,另一个记为 P_Y,其中 P_X 指向二进制数 X,P_Y 指向二进制数 Y。当 P_X 从二进制数 X 最高位开始遍历的时候,P_Y 同时从二进制数 Y 最高位开始遍历。当 P_Y 指向二进制数 Y 中元素为 0 时,P_X 所指二进制数 X 中元素不变;当 P_Y 指向二进制数 Y 中元素为 1 时,P_X 所指二进制数 X 位上元素用取反(0 的反为 1)替换。最后 $Sub(X,Y)$ 即为被替换后的二进制数 X。比如:$L = 8$,$X = 00001100$,$Y = 01100101$,则 $Sub(X,Y) = 01101001$,具体过程如图 1 所示。

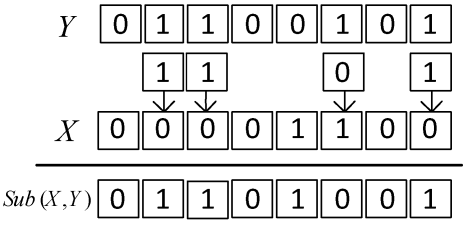

图 1　位替换运算流程图

本文提出的 MAP 移动认证协议主要基于以下假设前提:

1)低成本标签的计算能力及存储空间是受限制的;移动读写器及后台数据库具备较强的计算能力及存储空间。

2)标签与移动读写器之间无线信道通信,被认为不安全;移动读写器与后台数据库之间无线信道通信,同样被认为不安全。

3)协议中采用的位替换运算是安全的。

4)标签、读写器、后台数据库初始化时存放的信息是安全可靠的。

在 MAP 执行之前,移动 RFID 系统中所有实体需初始化内存单元。初始化结果如下:

标签端存放 Key_L、Key_R、ID_T,即形成一个三元

组(Key_L,Key_R,ID_T)。移动读写器端存放 Key_L、Key_R、ID_R,即形成一个三元组(Key_L,Key_R,ID_R)。后台数据库端存放 Key_L、Key_R、ID_T、ID_R,即形成一个四元组(Key_L,Key_R,ID_T,ID_R)。

MAP 所使用的符号定义及说明如表 1 所示。

表 1 符号说明

符号	含义
T	标签
R	移动读写器
DB	后台数据库
ID_T	标签的标识符
ID_R	读写器的标识符
Key	移动读写器、标签、后台数据库三者之间的共享密钥
Key_L	共享密钥的左半部分
Key_R	共享密钥的右半部分
Key_old	移动读写器、标签、后台数据库上轮认证共享密钥
Key_new	移动读写器、标签、后台数据库本轮认证共享密钥
r_T	标签生成的随机数
r_R	读写器生成的随机数
r_{DB}	后台数据库生成的随机数
⊕	按位“异或”运算
&	按位与运算
Sub(X,Y)	位替换运算

2.2 MAP 认证流程

MAP 认证流程如图 2 所示。图 2 中 M0 至 M12 公式具体含义说明如表 2 所示。

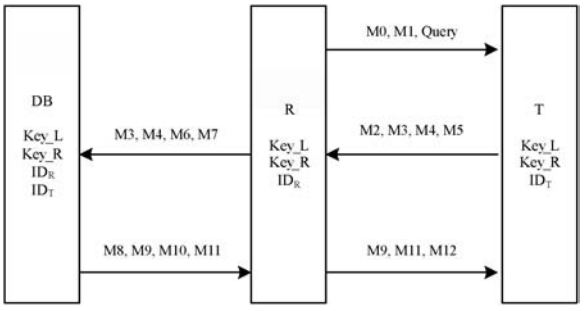

图 2 MAP 认证流程图

表 2 公式说明

符号	含义
M0	$r_R \oplus$ Key_R
M1	$r_R \oplus$ Key_L
M2	$r_R \oplus r_T$
M3	$r_T \oplus ID_T$
M4	*Sub*(r_T& Key_L,$r_T \oplus$ Key_R)
M5	*Sub*(r_T& r_R,r_T& Key_L)
M6	$r_R \oplus ID_R$
M7	*Sub*(r_R&ID_R& Key_L,r_R&ID_R& Key_R)
M8	$r_R \oplus r_{DB} \oplus ID_R$
M9	$r_T \oplus r_{DB} \oplus ID_T$
M10	*Sub*(r_R,r_{DB})
M11	*Sub*(r_T,r_{DB})
M12	r_R&r_{DB}

MAP 认证流程详细步骤描述如下:

步骤 1 首先移动读写器生成一个随机数 r_R,然后读写器计算 M0 和 M1 的值,最后将 M0、M1 及认证请求命令 Query 发送给标签。

步骤 2 标签接收到信息后,首先计算 M0 ⊕Key_R、M1 ⊕ Key_L 的值,然后比对 M0 ⊕ Key_R 与 M1 ⊕ Key_L 两者值是否相等。若相等,则标签验证移动读写器通过,进行步骤 3;否则,说明移动读写器是伪造的,MAP 立刻终止。

步骤 3 标签通过计算得到随机数 r_R,然后标签生成一个随机数 r_T,接着标签计算 M2、M3、M4、M5 的值,最后将(M2、M3、M4、M5)传送给移动读写器。

步骤 4 移动读写器接收到信息后,首先计算 M2 ⊕ r_R 的值,然后计算 M5′的值,最后比较 M5′与 M5 的值是否相等。若相等,则移动读写器验证标签通过,进行步骤 5;否则,说明标签是伪造的,MAP 立刻终止。其中:M5′ = *Sub*(((M2 ⊕ r_R) & r_R),((M2 ⊕ r_R) & Key_L))。

步骤 5 移动读写器通过计算得到随机数 r_T,然后读写器计算 M6、M7 的值,最后将(M3、M4、M6、M7)传送给后台数据库。

步骤 6 后台数据库对移动读写器的认证。

(1) 数据库接收到信息后,首先计算 M6 ⊕ ID_R 的值,然后计算 M7′的值,最后比对 M7′与 M7 的值是否相等。若相等,则数据库验证移动读写器通过,进行步骤(3);否则,进行步骤(2)。其中:M7′ = *Sub*((M6 ⊕ ID_R)&ID_R& Key_L,(M6 ⊕ ID_R)&ID_R& Key_R)。

(2) 数据库用 Key_old 代替 Key_new 进行步骤(1)中的计算。若相等,则数据库验证读写器通过,进行步骤(3);否则,说明移动读写器是伪造的,MAP 立刻终止。

(3) 数据库通过计算得到随机数 r_R,然后进行步骤 7。

步骤 7　后台数据库对标签的认证。

(1) 数据库验证移动读写器通过后,然后计算 $M3 \oplus ID_T$ 的值,再计算 M4′的值,最后比对 M4′与 M4 的值是否相等。若相等,则数据库验证标签通过,进行步骤(3);否则,进行步骤(2)。其中:$M4' = Sub((M3 \oplus ID_T)\& Key\_L, (M3 \oplus ID_T) \oplus Key\_R)$。

(2) 数据库用 Key_old 代替 Key_new 进行步骤(1)中的计算。若相等,则数据库验证标签通过,进行步骤(3);否则,说明标签是伪造的,MAP 立刻终止。

(3) 数据库通过计算得到随机数 r_T,然后进行步骤 8。

步骤 8　数据库生成一个随机数 r_{DB},然后计算 M8、M9、M10、M11 的值,接着开始更新共享密钥信息 Key_old = Key、Key = Key_new,最后将(M8,M9,M10,M11)传送给移动读写器。其中:$Key\_new = Sub((r_{DB} \oplus r_T \oplus r_R), (r_{DB}\& r_T \& r_R))$。

步骤 9　移动读写器接收到信息后,首先计算 $M8 \oplus r_R \oplus ID_R$ 的值,然后计算 M10′的值,最后比对 M10′与 M10 的值是否相等。若相等,则移动读写器验证后台数据库通过,进行步骤 10;否则,说明后台数据库是伪造的,MAP 立刻终止。其中:$M10' = Sub(r_R, (M8 \oplus r_R \oplus ID_R))$。

步骤 10　移动读写器计算 M12 的值;然后更新共享密钥信息,即 Key_old = Key、Key = Key_new;最后将(M9,M11,M12)传送给标签。其中:$Key\_new = Sub((r_{DB} \oplus r_T \oplus r_R), (r_{DB}\& r_T \& r_R))$。

步骤 11　标签对移动读写器的验证。

(1) 标签接收到信息后,标签首先计算 $M9 \oplus r_T \oplus ID_T$ 的值,然后计算 M12′的值,最后比对 M12′与 M12 的值是否相等。若相等,则标签验证移动读写器通过,进行步骤(2);否则,说明移动读写器是伪造的,MAP 立刻终止。其中:$M12' = r_R \& (M9 \oplus r_T \oplus ID_T)$。

(2) 标签对后台数据库的验证:标签计算 M11′的值,比对 M11′与 M11 的值是否相等。若相等,则标签验证后台数据库通过,进行步骤(3);否则,说明后台数据库是伪造的,MAP 立刻终止。其中:$M11' = Sub(r_T, (M9 \oplus r_T \oplus ID_T))$。

(3) 标签开始更新共享密钥信息,即 $Key = Sub((r_{DB} \oplus r_T \oplus r_R), (r_{DB}\& r_T \& r_R))$。到此标签、移动读写器、后台数据库三方之间的认证结束。

3　安全性分析

(1) 重放攻击。在每次认证过程中,标签都会产生随机数 r_T。认证消息(M2,M3,M4,M5)计算过程中都有包含 r_T。若攻击者采用旧的上述消息,则标签在验证(M9,M11,M12)时会使用新产生的随机数 r_T。这样使得标签在验证移动读写器及后台数据库时就会失败,MAP 立刻终止,阻止了攻击者完成后续认证过程,故 MAP 可以抵抗重放攻击。

(2) 异步攻击。异步攻击是指移动读写器(或后台数据库)与标签在认证过程中,由于攻击者的蓄意破坏,使得两者之间的共享密钥不同步,异步攻击也称为去同步化攻击。为了能够抵抗异步攻击,MAP 存放了上一轮认证过程中用到的共享密钥 Key_old 用来现实与标签恢复同步。后台数据库通过(M3,M4,M6,M7)对标签及移动读写器进行认证时,首先调用 Key_new 进行计算,若验证无法通过,再调用 Key_old 进行计算,从而抵抗攻击者的去同步化攻击。故 Key_new 及 Key_old 的存在使得 MAP 能够抵抗异步攻击。

(3) 中间人攻击。该种攻击方式比较常见的攻击方法是替换消息、篡改消息等。根据协议应用的场景,攻击者可以获取标签、移动读写器、后台数据库三者之间所有的通信信息集合 MS = {M0,M1,M2,M3,M4,M5,M6,M7,M8,M9,M10,M11,M12}。上述消息都是加密之后的信息,因此即便是攻击者获取上述消息,并不能推导出有用信息。攻击者虽然可以对其中某个消息进行修改或篡改,但 MAP 在每个步骤中都将会对其进行验证,简单的验证便会发现消息已被篡改。同时上述消息计算过程中与随机数 r_R、r_T、r_{DB} 有关联,且随机数是秘密产生的,并具备无法预测性,使得攻击者修改消息难度进一步增大。故 MAP 可以抵抗中间人攻击。

(4) 前向安全。因后台数据库存放有上一轮的认证共享密钥,所以这里仅仅讨论标签端的前向安全性。若攻击者想要获取标签的当前共享密钥值,则攻击者需要从获得的上次消息来解密出以前的认证消息。但攻击者无法成功,原因如下:攻击者无法破解采用按位操作加密的消息,因为密文中至少有两个量对于攻击者来说是未知的;MAP 在认证结束后,会立刻更新共享密钥值,前后共享密钥值之间并无关联,同时共享密钥值的计算与 r_R、r_T、r_{DB} 三个随机数都有关联,攻击者是不可能获取这三个随机数的。故 MAP 能够确保标签的前向安全。

(5) 假冒攻击。若攻击者假冒标签,发送消息给移动读写器。由于攻击者假冒的标签并不知晓当前共享密钥值 Key_R、Key_L,因此攻击者无法计算出正确的随机数 r_R 的值,从而攻击者传送给移动读写器

(M2、M5)信息也会被移动读写器识别为错误,认证立刻终止。攻击者假冒标签失败。

若攻击者假冒移动读写器,则发送消息给标签。由于攻击者假冒的移动读写器并不知晓当前共享密钥值 Key_R、Key_L,因此攻击者计算出来的(M0、M1)必定是错误的,传送给标签后,标签进行简单计算即可识别出攻击者假冒移动读写器。

若攻击者假冒移动读写器,则发送消息给后台数据库。由于攻击者假冒的移动读写器并不知晓移动读写器标识符 ID_R,因此攻击者计算出来的(M6、M7)必定是错误的。消息传送给后台数据库之后,验证移动读写器失败,攻击者被发现。

若攻击者假冒后台数据库,发送消息给移动读写器。由于攻击者假冒的后台数据库并不知晓移动读写器标识符 ID_R、标签标识符 ID_T,因此攻击者根本无法解密出正确的随机数 r_R、r_T,攻击者计算得到的(M8、M9、M10、M11)亦是错误的,移动读写器验证后台数据库无法通过,攻击者假冒失败。综上描述,MAP 能够抵抗攻击者的各种假冒攻击。

(6) 双向认证。因在移动 RFID 系统中,标签与读写器之间、读写器与后台数据库之间都是通过无线信道进行通信的,均不安全,因此每次信息传输都需要先对其进行认证。

- 标签对读写器的认证。读写器第一次传送消息给标签,标签通过步骤 2 完成对读写器的第一次验证;读写器在步骤 10 中第二次传送消息给标签,标签在步骤 11 中完成对读写器的第二次认证。
- 读写器对标签的认证。标签在步骤 3 中发送消息给读写器,读写器在步骤 4 中完成对标签的真伪鉴定。
- 读写器对后台数据库的认证。后台数据库在步骤 8 中向读写器传送消息,读写器在步骤 9 中完成对后台数据库真伪的鉴定。
- 后台数据库对读写器、标签的认证。为了能够抵抗去同步攻击,后台数据库同时存放 Key_new、Key_old 的值。在步骤 5 中读写器向后台数据库传送消息后,后台数据库在步骤 6 中实现对读写器的认证,在步骤 7 中实现对标签的认证。

通过上述描述,标签、读写器、后台数据库之间可以实现任意两者之间的相互认证,故 MAP 能够实现双向认证。

表 3 为本文 MAP 与其他移动 RFID 认证协议之间的安全性比较。

表 3 认证协议安全性比较

攻击类型	文献[7]	文献[8]	文献[9]	文献[10]	文献[12]	文献[13]	本文协议
重放攻击	√	√	×	×	√	√	√
异步攻击	√	√	√	√	×	√	√
中间人攻击	√	√	√	×	√	√	√
前向安全	√	√	√	√	√	√	√
假冒攻击	×	×	√	√	√	×	√
双向认证	√	√	√	√	√	×	√

注:×表示不能抵抗;√表示能够抵抗。

4 GNY 逻辑形式化证明

(1) 协议形式化描述。为使 MAP 协议便于用 GNY 形式逻辑语言描述,现作如下约定:R 表示移动读写器,T 表示标签,DB 表示后台数据库。MAP 协议流程如下:

Msg1:$R \xrightarrow{\{M0,M1,Query\}} T$;表示标签 T 接收到{M0,M1,Query}信息。

Msg2:$T \xrightarrow{\{M2,M3,M4,M5\}} R$;表示读写器 R 接收到{M2,M3,M4,M5}信息。

Msg3:$R \xrightarrow{\{M3,M4,M6,M7\}} DB$;表示后台数据库 DB 接收到{M3,M4,M6,M7}信息。

Msg4:$DB \xrightarrow{\{M8,M9,M10,M11\}} R$;表示移动读写器 R 接收到{M8,M9,M10,M11}信息。

Msg5:$R \xrightarrow{\{M9,M11,M12\}} T$;表示标签 T 接收到{M9,M11,M12}信息。

用 GNY 形式逻辑语言规范以上协议,可以描述如下:

Msg1:$T < *\{M0,M1,Query\}$。

Msg2:$R < *\{M2,M3,M4,M5\}$。

Msg3:$DB < *\{M3,M4,M6,M7\}$。

Msg4:$R < *\{M8,M9,M10,M11\}$。

Msg5:$T < *\{M9,M11,M12\}$。

(2) 协议初始化假设。MAP 协议假设如下:R、DB、T 表示主体,即 R 表示移动读写器,T 表示标签,DB 表示后台数据库。

Sup1:$T \ni (Key\_R, Key\_L, ID_T, r_T)$;表示标签 T 拥有共享密钥值 Key_R、Key_L,拥有自身标识符 ID_T 及自身产生的随机数 r_T。

Sup2:$R \ni (Key\_R, Key\_L, ID_R, r_R)$;表示移动读写器 R 拥有共享密钥值 Key_R、Key_L,拥有自身标识符 ID_R 及自身产生的随机数 r_R。

Sup3:DB ∋ (Key_R,Key_L,ID_R,ID_T,r_{DB});表示后台数据库 DB 拥有共享密钥值 Key_R、Key_L,拥有移动读写器 R 的标识符 ID_R 及标签 T 的标识符 ID_T,拥有自身产生的随机数 r_{DB}。

Sup4:R |≡ #(r_R,r_T,r_{DB});表示移动读写器 R 相信随机数 r_R、r_T、r_{DB}是新鲜的。

Sup5:T |≡ #(r_R,r_T,r_{DB});表示标签 T 相信随机数 r_R、r_T、r_{DB}是新鲜的。

Sup6:DB |≡ #(r_R,r_T,r_{DB});表示后台数据库 DB 相信随机数 r_R、r_T、r_{DB}是新鲜的。

Sup7:T |≡ R $\xleftrightarrow{Key\_R,Key\_L}$ T;表示标签 T 相信标签 T 与移动读写器 R 之间共享的信息 Key_R、Key_L。

Sup8:R |≡ T $\xleftrightarrow{Key\_R,Key\_L}$ R;表示移动读写器 R 相信移动读写器 R 与标签 T 之间共享的信息 Key_R、Key_L。

Sup9:DB |≡ R $\xleftrightarrow{Key\_R,Key\_L,IDR}$ DB;表示后台数据库 DB 相信后台数据库 DB 与移动读写器 R 之间共享的信息 Key_R、Key_L、ID_R。

Sup10:R |≡ DB $\xleftrightarrow{Key\_R,Key\_L,IDR}$ R;表示移动读写器 R 相信移动读写器 R 与后台数据库 DB 之间共享的信息 Key_R、Key_L、ID_R。

Sup11:DB |≡ T $\xleftrightarrow{Key\_R,Key\_L,IDT}$ DB;表示后台数据库 DB 相信后台数据库 DB 与标签 T 之间共享的信息 Key_R、Key_L、ID_T。

Sup12:T |≡ DB $\xleftrightarrow{Key\_R,Key\_L,IDT}$ T;表示标签 T 相信标签 T 与后台数据库 DB 之间共享的信息 Key_R、Key_L、ID_T。

(3) 协议证明目标。MAP 协议的证明目标主要有 5 个,即标签、移动读写器、后台数据库之间对彼此交互信息新鲜性的信任。目标的证明公式如下:

Goal1:T |≡ R |~ #(M0,M1);

Goal2:R |≡ T |~ #(M2,M3,M4,M5);

Goal3:DB |≡ R |~ #(M3,M4,M6,M7);

Goal4:R |≡ DB |~ #(M8,M9,M10,M11);

Goal5:T |≡ R |~ #(M9,M11,M12)。

(4) 协议证明过程。MAP 协议的证明是在初始化假设的基础之上进行的,证明过程遵循文献[15]中的逻辑推理规则、告知规则、新鲜规则、拥有规则,消息解释规则遵循文献[15]中 GNY 逻辑推理规则的书写形式,分别用 T、P、F 及 I 表示。

因协议证明目标 Goal2、Goal3、Goal4、Goal5 的证明过程与协议证明目标 Goal1 的证明过程相似,故本节以协议证明目标 Goal1 为例,证明过程如下描述:

∵ 规则 P1:$\frac{P<X}{P\ni X}$和 Msg1:T < ∗ {M0,M1}

∴ T ∋ {M0,M1}

∵ 规则 F1:$\frac{P\mid\equiv(X)}{P\mid\equiv(x,y),P\mid\equiv\#F(X)}$以及 Sup4:R |≡ #($r_R$,$r_T$,$r_{DB}$)

∴ T = #{M0,M1}

∵ 规则 P2:$\frac{P\ni X,P\ni Y}{P\ni(X,Y),P\ni F(X,Y)}$, Sup1:T ∋ (Key_R,Key_L,$ID_T$,$r_T$)和 Sup2:R ∋ (Key_R,Key_L,ID_R,r_R)

∴ T ∋ {M0,M1}

∵ 规则 F10:$\frac{P\mid\equiv(X),P\ni X}{P\mid\equiv\#(H(X))}$以及推导出来的 T = #{M0,M1}、T ∋ {M0,M1}

∴ T |≡ #{M0,M1}

∵ 规则 I3:$\frac{P<H(X,<S>),P\in(X,S),P\mid\equiv P\leftrightarrow Q,P\mid\equiv\#(X,S)}{P\mid\equiv Q\mid\sim(X,S),P\mid\equiv Q\sim H(X,<S>)}$

又∵ Sup7:T |≡ R $\xleftrightarrow{Key\_R,Key\_L}$ T、Sup8:R |≡ T $\xleftrightarrow{Key\_R,Key\_L}$ R 以及 Msg1:T < ∗ {M0,M1}

∴ T |= R ~ {M0,M1}

∵ 新鲜性定义以及推导出来的 T = #{M0,M1}、T |= R ~ {M0,M1}

∴ Goal1:T |≡ R |~ #(M0,M1)得证明。

5　性能分析

移动 RFID 系统中包含标签、移动读写器、后台数据库,因后两者具备较强的计算能力及较大的存储量,对协议的性能影响不大,所以这里只针对标签一端的计算量及存储量进行分析。RFID 认证协议的性能分析主要从以下 4 个方面进行:标签端的计算量、标签端的存储量、会话次数、协议的通信量。表 4 为本文 MAP 与其他认证协议之间的性能比较结果。

表 4　认证协议性能比较

文献	计算量	存储量	通信量	会话次数
文献[7]	5PR + 3N	4 l	11 l	5
文献[8]	PR + C	3 l	16 l	7
文献[10]	3H	3 l	14 l	5
文献[11]	2H	2 l	13 l	5
文献[12]	3PR + 2N + 2P	5 l	14 l	5
文献[13]	3S + H	2 l	12 l	5

表 4 中:H 表示哈希函数运算;M 表示标量乘运

算;S 表示随机数运算;Sub 表示位替换运算;N 表示求余运算;PR 表示伪随机数运算;P 表示物理不可克隆函数运算;C 表示交叉运算。由上文叙述可得,H、M、S、N、PR、P 属于轻量级运算,而 Sub、C 属于超轻量级运算,即前者的运算量要比后者运算量大很多。考虑到按位"异或"运算、按位与运算的计算开销很小,因此在进行性能分析时予以忽略。设定共享密钥 Key、标识符 ID、各运算结果(各运算是指 H、M、S、N、PR、P、Sub、C)的长度均为 l。

(1) 标签的存储量及计算量。本文 MAP 中标签端只需要存放共享密钥 Key、标签的标识符 ID_T 两个量,根据前面的约定可知,标签端存储量为 $2l$。相对于文献[7,10,12]来说,本文协议标签端的存储量已有所降低;相对于文献[8,11,13]来说,本文协议标签端的存储量与其相当。

在标签端的计算量方面,针对按位"异或"运算及按位与运算因计算开销小,不予考虑,故本文协议在标签端的计算量要远少于其他文献。本文协议标签端并未使用计算量较大的哈希函数或标量乘运算对信息进行加密,而是采用超轻量级的按位操作对信息进行加密,从而减少标签的计算量。综上描述,在标签的存储量及计算量方面,本文协议相比其他协议均有所改进。

(2) 通信量及会话次数。本文协议在通信量方面相对文献[7,10-11,13]而言,略大于上述文献中的通信量,但上述文献中均存在一些安全隐患,而本文协议弥补了上述文献中协议存在的缺陷问题。本文协议在通信量方面与文献[8,12]相当,同时解决了它们中存在的安全问题。

会话次数方面,众多协议大多是 5 次通信,本文协议在会话次数方面并无优势。综上所述,本文协议在整个通信量及会话次数两方面改进不大,相对其他协议并无优势,但解决了其他协议中存在的安全缺陷问题,故本文协议仍具备一定的实用价值。

6 结 语

本文描述传统 RFID 系统与移动 RFID 系统的不同点,指出传统 RFID 系统认证协议无法适用于移动 RFID 系统的特点,从而提出一种适用于移动 RFID 系统的认证协议 MAP。阐述当前一些适用于移动 RFID 系统的认证协议中存在的缺陷及不足,然后提出改进的认证方案。所提 MAP 协议摒弃哈希函数加密的方法,采用按位操作对信息进行加密,使得协议可以达到超轻量级的级别;位替换运算的使用,增加了攻击者破解协议的难度;通过安全性及性能分析,表明了协议的安全性及优势之处所在;GNY 逻辑形式化证明了 MAP 的正确性。MAP 不仅适用于移动 RFID 系统,传统 RFID 系统也同样适用。下一步的研究方向:对 MAP 协议进行优化,合理降低整个通信的通信量;将采用 MAP 的移动 RFID 系统原型实现出来,搞清楚实现所需门电路总个数、一个完整通信时间等问题,做到理论与实际相结合。

参 考 文 献

[1] Wang W C, Yona Y, Diggavi S N, et al. Design and analysis of Stability Guaranteed PUFs[J]. IEEE Transactions on Information Forensics and Security, 2017, 13(4): 978-992.

[2] Lai Y C, Hsiao L Y, Chen H J, et al. A novel query tree protocol with bit tracking in RFID tag identification[J]. IEEE Transactions on Mobile Computing, 2013, 12(10): 2063-2075.

[3] 刘道微,凌捷. 一种改进的满足后向隐私的 RFID 认证协议[J]. 计算机科学,2016,43(8):128-130,158.

[4] 石乐义,贾聪,宫剑,等. 基于共享秘密的伪随机散列函数 RFID 双向认证协议[J]. 电子与信息学报,2016,38(2): 361-366.

[5] Huth C, Aysu A, Guajardo J, et al. Secure and private, yet lightweight, authentication for the IoT via PUF and CBKA [C]//International Conference on Information Security and Cryptology(ICISC),2016:28-48.

[6] 张朝晖,刘悦,刘道微. 基于标签 ID 的 RFID 系统密钥无线生成算法[J]. 计算机应用研究,2017,34(1):261-263,269.

[7] Sundaresan S, Doss R, Piramuthu S, et al. A secure search protocol for low cost passive RFID tags[J]. Computer Networks,2017,122:70-82.

[8] Fan K, Jiang W, Li H, et al. Lightweight RFID protocol for medical privacy protection in IoT[J]. IEEE Transactions on Industrial Informatics, 2018,14(4):1656-1665.

[9] 汪杰,汪学明. 改进的轻量级移动 RFID 双向认证协议[J]. 计算机工程与设计,2018,39(4):912-917.

[10] Gope P, Lee J, Quek T Q S, et al. Resilience of DoS attacks in designing anonymous user authentication protocol for wireless sensor networks[J]. IEEE Sensors Journal, 2017, 17(2):498-503.

[11] Xie R, Ling J, Liu D W. Wireless key generation algorithm for RFID system based on bit operation[J]. International Journal of Network Security, 2018,20(5):938-949.

[12] 孙子文,李松. 采用 PUF 保护位置隐私的轻量级 RFID 移动认证协议[J]. 计算机科学与探索,2019,13(3):418-428.

(下转第 323 页)

由图 4 可以清晰地看出,沥青路面结构温度随时间变化而呈现出明显的周期性趋势,其温度在 13:00 左右达到最高值,随后其温度随着热辐射和环境气温的降低而逐渐减弱,并在 5:00 左右达到一天的最低值。出现这一变化规律的原因是外界环境温度和辐射对路面温度分布影响较大,如从图 2 中可以看出外界温度从 7:00 开始逐渐升高,且沥青路面温度也从 7:00 开始升高。

从沥青埋入深度的角度分析,可以发现结构内部温度随着测量深度的变化而变化,20 mm 和 100 mm 两种深度的最大温差出现时间与路面结构最高温度出现时间一致。这与本文所采用的仿真模拟方法具有较高的一致性,也证明了本文方法的准确性和可靠性。

4　结　语

本文采用多物理场仿真模拟与实验相结合的方法,探究了沥青混合料路面结构的温度演变规律,得到了如下主要结论:

(1) 随着深度的增加,路面结构温度逐渐下降,并且其最大温差与结构最大温差在相同时间出现。

(2) 沥青混合料路面结构温度变化具有明显的周期性,随着时间的增加,沥青路面结构温度先增加后降低。结构最高温度出现在 13:00 左右,最低温度出现在 5:00 左右,且同一时间条件下不同结构深度的最大温度差与结构最高温度同时出现。

本文建立的 ANSYS 模型与实测数据较为吻合,可靠性较高。今后沥青路面运营使用过程中,为避免较大的温度差破坏沥青结构,可利用该模型进行分析预警,提前对结构薄弱处采取洒水降温等措施。

参 考 文 献

[1] 康海贵,郑元勋,蔡迎春,等. 实测沥青路面温度场分布规律的回归分析[J]. 中国公路学报,2007,20(6):13 – 18.

[2] 艾长发,邱延峻,毛成,等. 考虑层间状态的沥青路面温度与荷载耦合行为分析[J]. 土木工程学报,2007,40(12):99 – 104.

[3] 李雪毅,邹晓翎,吁新华. 热风循环式就地热再生沥青路面温度场[J]. 中外公路,2018,38(2):69 – 74.

[4] 韦璐,陶明霞,马志平,等. 行车荷载与温度综合作用下沥青路面疲劳损伤分析[J]. 公路,2018(2):1 – 6.

[5] 马翔,徐成,徐旭光,等. 新铺沥青混凝土温度衰变规律及强度特性[J]. 铁道科学与工程学报,2018,15(10):70 – 75.

[6] 顾海荣,梁奉典,李金平,等. 沥青路面加热过程中温度分布的随机性研究[J]. 筑路机械与施工机械化,2018,35(5):160 – 165,170.

[7] 赵毅,梁乃兴. 沥青路面沥青层偏应力分布研究[J]. 公路,2018,63(3):1 – 9.

[8] 宋小金,樊亮. 沥青路面结构温度随深度变化规律研究[J]. 土木工程学报,2017,50(9):110 – 117.

[9] 郭学东,常孟元,孙明志,等. 季节性冻土地区沥青路面温度场的预估模型[J]. 科学技术与工程,2017,17(10):294 – 298.

[10] 李强,黄葵阳,王朝晖. 沥青路面内部温度预估方法与预估模型[J]. 中外公路,2017,37(5):56 – 61.

[11] 夏明,徐邱彬. 沥青混合料摊铺碾压温度场模拟分析[J]. 交通运输研究,2009(18):85 – 89.

[12] 建筑保温墙体薄空气间层空气湿度对传热影响的实验研究[D]. 合肥:安徽建筑大学,2015.

[13] 蒋甫. 考虑对流传热的多孔沥青路面降温性能[J]. 土木工程学报,2011,44(10):138 – 142.

[14] 延西利,李绪梅,孙毅,等. 基于傅立叶导热定律的沥青混合料热传导试验[J]. 交通运输工程学报,2013(6):1 – 6.

[15] 白琦峰,陈荣生,杜骋. 半刚性基层沥青混凝土路面反射裂缝模拟试验及有限元分析[J]. 公路,2004(8):97 – 101.

(上接第 291 页)

[12] Zhu H F, Zhang Y. An efficient chaotic maps-based deniable authentication group key agreement protocol[J]. Wireless Personal Communications, 2017, 96(1): 217 – 229.

[13] Kumar A, Tripathi S. A pairing free anonymous certificateless group key agreement protocol for dynamic group[J]. Wireless Personal Communications, 2015, 82(2): 1027 – 1045.

[14] Zhang Q K, Wang X M, Yuan J L, et al. A hierarchical group key agreement protocol using orientable attributes for cloud computing[J]. Information Sciences, 2019, 480: 55 – 69.

[15] Tan H W, Chung I Y. A secure and efficient group key management protocol with cooperative sensor association in WBANs[J]. Sensors, 2018, 18(11): 3930.

(上接第 308 页)

[13] 王国伟,贾宗璞,彭维平. 基于动态共享密钥的移动 RFID 双向认证协议[J]. 电子学报,2017,45(3):612 – 618.

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

[15] Gong L, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols[C]//IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, US, 1990: 234 – 248.