·安全技术· 文章编号：1000-3428(2017)08-0173-05 文献标志码：A 中图分类号：TP393

基于假名标识的加密 RFID 系统无线密钥生成协议

苏 庆，李 倩，彭家进，刘富春

（广东工业大学 计算机学院，广州 510006）

摘 要： 针对无线射频识别（RFID）系统密钥生成过程中存在的密钥托管、无线信道不安全和标签成本过高的问题，提出一种 RFID 系统密钥无线生成协议。在前、后向信道均可被窃听的假设前提下，通过引入假名标识以防止秘密信息泄露，仅采用简单位运算降低标签成本与计算量，利用异或和移位运算对通信信息进行加密传输，从而保证协议的安全性，并运用 GNY 逻辑对协议进行形式化证明。分别在单标签个体密钥生成、批量标签个体密钥生成以及群组标签组密钥生成 3 种应用下对协议进行安全与性能分析，结果表明，该协议具有较高的安全性和较低的成本。

关键词： 无线射频识别；密钥生成；密钥托管；假名标识；加密；窃听；GNY 逻辑

中文引用格式： 苏 庆，李 倩，彭家进，等. 基于假名标识的加密 RFID 系统无线密钥生成协议[J]. 计算机工程，2017，43(8)：173-177，183.

英文引用格式： Su Qing，Li Qian，Peng Jiajin，et al. Wireless Key Generation Protocol for Encrypted RFID System Based on Pseudonym Logo[J]. Computer Engineering，2017，43(8)：173-177，183.

Wireless Key Generation Protocol for Encrypted RFID System Based on Pseudonym Logo

SU Qing，LI Qian，PENG Jiajin，LIU Fuchun

（College of Computer Science，Guangdong University of Technology，Guangzhou 510006，China）

【Abstract】 In view of the problems including the key escrow，the insecurity of the wireless channel and the high cost of the tag in the key generation process of Radio Frequency Identification（RFID） system，an wireless key generation protocol for RFID system is proposed. On the premise that the forward and backward channels can be eavesdropped，the paper introduces the pseudonym logo to prevent the disclosure of secret information. The paper only uses simple bit operations to reduce the tag cost and computation，and it uses Exclusive OR（XOR） and shift operations to encrypt and transmit information，which aims to ensure the security of protocol. The proposed protocol is formally proved by using GNY logic. The security and performance of the protocol are analyzed under three kinds of applications，which are the single label individual key generation，batch label key generation and group label key generation. It is proved that the proposed protocol has higher security and lower cost.

【Key words】 Radio Frequency Identification（RFID）；key generation；key escrow；pseudonym logo；encryption；eavesdrop；GNY logic

DOI： 10.3969/j.issn.1000-3428.2017.08.029

0 概述

无线射频识别（Radio Frequency Identification，RFID），俗称电子标签，是一种无需接触的自动识别技术，是物联网的重要支持技术[1]。RFID 系统主要由标签、读写器以及后端数据库组成，其中标签具有耐磨损、非接触、体积小型化等优点，因此，RFID 技术广泛应用于身份识别、交通运输、防伪系统、物流和仓库管理等各个领域[2]。

密钥生成是指利用交互式协议构造一个共享密钥的过程。共享密钥用于在 2 个不同实体之间建立机密的通信通道或提供数据完整性，保证协议的安全进行[3]。在 RFID 标签上安全生成密钥是一项非常具有挑战性的工作，难点在于：1）如何选择密钥生

基金项目： 国家自然科学基金（61502108，61273118）；广东省重大科技专项（2014B010111007）；广东省公益研究与能力建设专项（2016A010101027）。

作者简介： 苏 庆（1979—），男，副教授、硕士，主研方向为信息安全、软件安全与保护、可视计算；李 倩，硕士研究生；彭家进，本科生；刘富春，教授、博士。

收稿日期： 2016-07-08 **修回日期：** 2016-08-30 **E-mail：** 1014664490@qq.com

成方。如果是制造商在标签出厂之前就预先设置好密钥,会带来密钥托管问题[4],在监管不当的情况下容易造成密钥信息的泄露;如果是读写器以无线的方式直接将密钥写入标签,那么由于读写器和标签之间是无线通信,容易受到攻击者的攻击。攻击主要分为 2 种:一种是被动攻击。攻击者嗅探或窃听读写器和标签之间的通信,然后根据获得的数据进行分析或进行跟踪等;另一种是主动攻击。攻击者在读写器和标签之间作为第三人存在,截获读写器和标签之间交互的数据,然后通过重放或篡改的方式发送给另一方,最终导致密钥信息被窃取[5]。2)标签成本限制。在大规模实际应用中,大多采用的标签都是低成本无源标签,其依靠读写器发出的射频信号来获取工作所需的电源能量[6]。若采用计算过程复杂的传统密钥协商协议算法,标签接收到的信号强度将难以支持其内部电路完成计算所需要的功耗,因此,传统的密钥协商协议不能直接应用到标签成本受限的 RFID 系统中。

因此,设计高安全和轻量级的 RFID 系统密钥生成协议是目前 RFID 系统中要解决的主要问题。在这种背景下,本文提出一种 RFID 系统密钥无线生成方法,该方法基于超轻量级运算,并引入假名标识和来加密通信。

1 相关研究

基于物理机制和基于密码机制的密钥生成方法是 2 种传统的密钥生成方法。基于物理机制的方法主要有法拉第网罩法[7]和有线连接写入[8]等,但法拉第网罩方法由于受到自身网罩空间大小的限制,很难实际运用于 RFID 系统中。有线连接写入方法必须要有硬件接口,才能建立两端信号的连接,而 RFID 标签没有硬件接口提供支持,所以此方法也不适用于 RFID 系统。基于密码机制的方法,主要是以公钥密钥学的密钥协商[9]为基础,但此类方法需要花费较大的计算量和较多的存储空间,在大规模 RFID 标签应用中并不实用。

采用证书机制的普通公钥体制下密钥管理技术[10](Public Key Infrastructure,PKI)和身份的密钥管理技术[11](Identity Based Encryption,IBE)以及不需要第三方认证的组合公钥体制下密钥管理技术[12](Combined Public Key,CPK)逐步应用到 RFID 系统中,对 RFID 系统初始化、密钥生成、密钥分配和数据安全传输等方面提供了新的方法。其中,PKI 技术密钥生成方法大多以 RSA 公钥加密算法为核心,来产生一对公、私钥;IBE 技术利用哈希函数和用户身份信息 ID 生成密钥;CPK 技术通过公钥因子矩阵计算密钥。这些技术大多依赖于第三方认证或是密钥管理中心的参与,如果应用于 RFID 系统中则存在计算复杂、通信消耗大、效率低等问题。

文献[13]提出了一种在 RFID 标签上进行密钥安全无线生成的方法(Wireless Key Generation,WiKey),WiKey 的基本思想是利用 RFID 系统前、后向信道的非对称性,使得其具有以下优点:1)无线生成密钥,无需物理接口;2)适用于低成本的 RFID 标签;3)可抵抗多种攻击;4)密钥生成过程可由非专业人员操作。但是,文献[13]提出了“后向信道不可窃听”的观点,基于该观点,协议中后向信道的传输信息均采用明文传输。而事实上,上述假设具有一定局限性,不能完全符合实际应用场合。后向信道在一定情况下是可窃听的,这会造成信息的泄露,导致密钥被破解。

2 RFID 信道可窃听

文献[14]对攻击者可能的窃听范围进行了不同的定义,窃听范围距离依次递增,如图 1 所示。

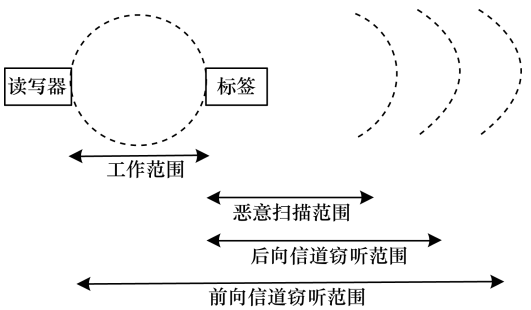

图 1 读写器和标签窃听范围分类

工作范围(Operation Range):RFID 标准和规范规定的读写器和标签之间的安全工作范围。

恶意扫描范围(Malicious Scanning Range):攻击者使用带有更大功率输出和更多天线部件的读写器可以增加实际的读写距离,在这个范围内可用较低的代价进行恶意窃听。

后向信道窃听范围(Backward Channel Eavesdropping Range):标签向读写器发送信息的通信信道称为后向信道(Backward Channel)。通常无源标签是由读写器产生的输入信号来获得工作所需的能量,而标签发射响应信号的强度较弱,所以攻击者实施后向信道的窃听比对前向信道的窃听更困难,但是后向信道往往传输更为重要的响应信息,因此攻击者更关注此信道。

前向信道窃听范围(Forward Channel Eavesdropping Range):读写器向标签发送信息的通信信道称为前向信道(Forward Channel)。由于读写器通常是有源装置,其发出的射频信号强度远远大于标签回复的信号强度,因此攻击者在此范围内能窃听读写器给标签发送的响应或密钥更新消息等。

针对文献[13]所描述“后向信道不可窃听”并不完全符合实际应用。例如,在后向信道窃听范围内攻击者窃听标签对合法读写器的响应消息,即使需要在距离标签较近的位置,攻击者也完全有可能

窃听成功。因为在合法读写器向标签提供工作所需的信号能量之后,攻击者这时使用假冒读写器进行窃听,不需要再发射任何信号,就可以窃听到标签的响应消息,后向信道窃听成功。又如,文献[15]对 RFID 信用卡实施了成功的窃听攻击。他们在读写器旁放置用于窃听的接收天线,将标签响应的后向信道射频信号进行接收并处理,最终得到了信用卡片持有人的名字、卡号、卡有效期,甚至包括卡上运行的软件版本和支持的通信协议。所以后向信道也是完全有可能被窃听的。

综上所述,文献[13]在"后向信道不可窃听"假设下所提出的密钥生成协议存在安全漏洞与不足。在安全性方面,协议中密钥的无线生成仅仅依赖于随机数 r_1,r_2,并且它们均采用明文传输,并未作加密处理,这就在"后向信道可被窃听"的情况下造成信息的泄露,最终密钥被攻击者破解。在标签成本问题上,由于协议标签端产生随机数,那么标签端门电路的使用增多,标签成本增加。所以文献[13]并没有完全达到其所描述的高安全性和低成本性。

3　新的密钥无线生成协议

针对实际生活应用中存在"后向信道可被窃听"的情况本文提出一种基于假名标识的加密 RFID 系统密钥无线生成协议。在本协议中引入标签假名标识 IDS,避免攻击者窃听整个通信过程,泄露标签唯一标识符 ID;系统中的通信数据不再明文传输,而是利用超轻量级异或、移位运算进行加密传输并实现通信双方的双向认证功能,以保证系统在"后向信道可被窃听"的情况下的安全性。并且在本协议中标签不再产生随机数,而是由读写器产生 2 个随机数,减少标签端门电路使用,以达到降低标签成本的目的。

3.1　协议符号定义

为了简化协议通信过程描述,首先对本文协议使用到的各种符号进行定义说明,详见表 1。

表 1　协议符号定义

符号	含义
D	RFID 系统的数据库
R	RFID 系统的读写器
T	RFID 系统的标签
ID	标签唯一标识
IDS_i	标签假名标识
l	密文的长度
$\oplus$	异或运算
$X>>a$	右循环移位运算
k	标签与读写器之间的共享密钥
r_1,r_2	读写器生成的随机数
A,B,C,D,E,F,X,Y,Z	标签与读写器的通信数据

3.2　协议执行过程

与其他协议类似作出如下假设:后端数据库与读写器之间的通信信道是安全的,因此,可以将后端数据库和读写器看成一个整体;与读写器之间的通信信道是不安全的[16]。另外在协议初始状态中,标签保存数据(IDS,ID),读写器保存数据{(IDS_i,ID_i)}。

下面描述在 3 种不同场景下的协议执行过程:单个标签的个体密钥生成,批量标签个体密钥生成以及群组标签的组密钥生成。

3.2.1　单个标签密钥生成

读写器为一个标签生成一个共享密钥的协议过程如图 2 所示。

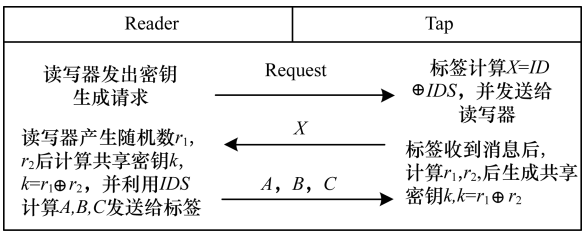

图 2　单个标签密钥生成协议

1)读写器向一个标签发出密钥生成请求。

2)标签在收到请求后,根据自身 ID 和假名 IDS,计算 $X=ID\oplus IDS$,并将 X 发送给读写器。

3)读写器在收到 X 后,根据后端数据库中存储的信息验证 X 的值,如果找到对应的信息(IDS_i,ID_i),生成随机数 r_1,r_2,之后计算共享密钥 k_i,利用 IDS 计算 A,B,C 并发送给标签;如果未找到对应信息,说明标签是假冒的,协议终止。

$$A=r_1\oplus IDS,B=r_2\oplus IDS$$

$$C=(r_1\oplus r_2)>>l,k_i=r_1\oplus r_2$$

4)标签收到消息 A,B,C 后,根据自身假名 IDS 计算 r_1,r_2 的值,并验证 C 的值,如果相等生成共享密钥 k_i;如果不相等说明读写器假冒,协议终止。

$$r_1=A\oplus IDS,r_2=B\oplus IDS$$

$$k_i=r_1\oplus r_2$$

3.2.2　批量标签密钥生成

读写器同时为大量不同的标签生成各自独立的共享密钥,议过程如图 3 所示。

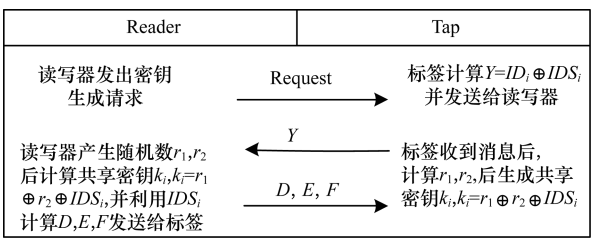

图 3　批量标签密钥生成协议

批量标签的密钥生成与单个标签密钥生成协议相似,唯一的不同即是:标签端和读写器端共享密钥

k_i 的生成中需要加入每个标签不同的假名信息 IDS，来区分不同密钥，也即 $k_i = r_1 \oplus r_2 \oplus IDS$。

3.2.3 群组标签密钥生成

读写器为一组标签 $T_1, T_2, \cdots, T_n$，生成一个唯一的共享密钥协议过程如图 4 所示。

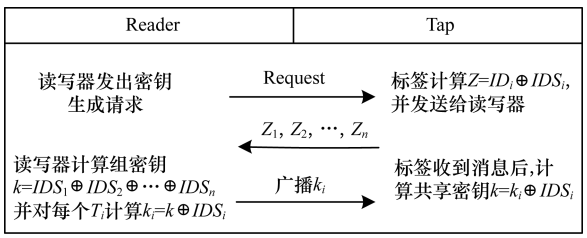

图 4 群组标签密钥生成协议

1）读写器向全组标签 $T_1, T_2, \cdots, T_n$ 广播发出密钥生成请求。

2）组内标签在收到请求后，根据自身 ID 和假名 IDS，开始计算 $Z_1, Z_2, \cdots, Z_n$：$Z_1 = ID_1 \oplus IDS_1$，$Z_2 = ID_2 \oplus IDS_2$，$\cdots$，$Z_n = ID_n \oplus IDS_n$ 并发送给读写器。

3）读写器收到标签回复信息后，将收到的信息与后端数据库中所存储的信息（IDS_i, ID_i）计算进行对比，判断是否完全相同。若完全相同，说明组内所有标签此刻均是合法标签且都已应答，协议继续执行，读写器开始计算生成群组唯一共享密钥 k，$k = IDS_1 \oplus IDS_2 \oplus \cdots \oplus IDS_n$，并为每一个标签 T_i 生成密钥因子 k_i，$k_i = k \oplus IDS_i$，之后广播发送给标签；若有不相同的信息，则表明组内有标签未应答或是存在非法标签，读写器重新发送请求以重启密钥生成过程或终止协议。

4）标签收到密钥因子信息后，根据自身 IDS_i 计算群组共享密钥 k，$k = k_i \oplus IDS_i$。

4 协议形式化证明

GNY 逻辑[17]作为公认的第一个扩展 BAN 逻辑，是一种基于规则和假设的形式逻辑分析方法，本文根据 GNY 逻辑的推理法则，最终得到协议的形式化证明。

由于 3 种不同场景协议过程类似，本节只对单个标签密钥生成协议作具体证明，其余 2 种情况将不做重复描述。

1）单个标签密钥生成协议过程形式化模型

在本协议中使用 T，R 表示主体，即标签为 T，读写器为 R，用逻辑化形式语言来描述本协议中的消息。

$M_1: R \lhd * F_1[IDS, ID]$

$M_2: T \lhd * F_2[r_1, IDS]$，$T \lhd * F_3[r_2, IDS]$

2）单个标签密钥生成协议过程初始化假设

设 P_1，P_2 表示标签、读写器的拥有；P_3，P_4 表示标签、读写器对数据新鲜性的相信；P_5，P_6 表示标签和读写器相信各自的信息是可以识别的。

$P_1: T \in (IDS, ID)$；$P_2: R \in (IDS, ID)$

$P_3: T \mid \equiv \#(IDS, ID)$；$P_4: R \mid \equiv \#(IDS, ID, r_1, r_2)$

$P_5: T \mid \equiv \varphi(IDS, ID)$；$P_6: R \mid \equiv \varphi(r_1, r_2)$

3）单个标签密钥生成协议过程安全目标

本协议的安全目标有 3 个，分别为读写器对标签的身份信息 IDS，ID 的识别；标签对读写器传递信息新鲜性的相信。

$D_1: R \mid \equiv \varphi F(IDS, ID)$

$D_2: T \mid \equiv R \mid \sim \#F_1(r_1, IDS)$

$D_3: T \mid \equiv R \mid \sim \#F_2(r_2, IDS)$

4）单个标签密钥生成协议过程分析证明

从读写器收到消息 M_1 开始，当读写器收到消息 IDS 和 ID 的异或消息后与后台数据库的信息（IDS_i，ID_i）验证是否匹配，如果匹配成功，则读写器预认证标签成功，即：$R \mid \equiv \varphi(IDS, ID)$，再根据可识别规则 $R1$：

$$\frac{P \mid \equiv \varphi(X)}{P \mid \equiv \varphi(X, Y), P \mid \equiv \varphi(F(X))}$$

得到 $R \mid \equiv \varphi F(IDS, ID)$，预期目标 D_1 实现。

当标签收到消息 M_2 后，由已知结论 $T \mid \equiv \#(IDS)$ 和新鲜性规则 F_1：

$$\frac{P \mid \equiv \#(X)}{P \mid \equiv \#(X, Y), P \mid \equiv \#(F(X))}$$

得到 $T \mid \equiv \#(IDS, r_1)$，继续使用新鲜性规则 F_1，可得到 $T \mid \equiv \#F(IDS, r_1)$；同理，根据已知结论 $T \mid \equiv \#(IDS)$ 和新鲜性规则 F_1，有 $T \mid \equiv \#(IDS, r_2)$，继续使用新鲜性规则 F_1，得到 $T \mid \equiv \#F(IDS, r_2)$，预期目标 D_2，D_3 实现。

5 协议安全性分析

在前、后向信道都可被攻击者窃听攻击的实际应用中，分别对 3 种不同情况下的 RFID 系统密钥无线生成协议做具体抵抗被动攻击和主动攻击分析。

5.1 单个和批量标签密钥生成协议安全性分析

前 2 种协议抵抗被动和主动攻击的能力都依赖于读写器端动态更新随机数的新鲜性以及随机数、假名标识 IDS 的加密传输和双向认证功能的实现。

5.1.1 被动攻击

攻击者企图通过窃听整个通信过程，窃取标签与读写器的全部通信数据，以获取共享密钥。但由于数据是加密传输，攻击者不知道每个标签的假名标识 IDS，更无法从已获得的信息中得到 2 个随机数，计算共享密钥，因此攻击者窃取共享密钥失败，协议可以抵抗此种被动攻击方式。

攻击者企图截取响应信息 $A \sim F$，对其进行跟踪活动，最终非法获取标签与读写器端的共享密钥。但因为读写器端每轮通信过后，动态更新 2 个随机数并且每次传输过程中随机数都是密文传输，攻击者想要获取构成共享密钥信息的关键值（随机数）是不可能的，所以攻击者窃取共享密钥失败，协议可以抵抗此种被动攻击方式。

5.1.2　主动攻击

攻击者企图通过重放或篡改的方式发送消息给另一方,最终导致密钥信息被窃取。但是由于随机数的动态更新保证了信息的新鲜性,当攻击者重放上一轮的消息 $A \sim F$ 时,随机数 r_1,r_2 早已更新,导致认证失败,协议终止,攻击者主动攻击失败。

5.2　群组标签密钥生成协议安全性分析

对于第 3 种群组密钥生成协议,抵抗被动和主动攻击能力依赖于引入的标签假名标识 *IDS* 和双向认证功能的实现。

5.2.1　被动攻击

攻击者企图通过被动攻击,窃听消息 $Z_1,Z_2,\cdots,Z_n$,获取和共享密钥相关的信息。但是读写器是利用所有标签的 *IDS* 计算群组密钥,而在整个通信过程中,标签的 *IDS* 信息全部进行加密处理,因此,攻击者无法获取共享密钥。即使攻击者通过某些手段获取某些标签的 *IDS*,但是只要其中一个信息出错,攻击者仍然得不到正确的共享密钥。所以,协议可以抵抗被动攻击。

5.2.2　主动攻击

攻击者企图通过主动攻击,伪装成合法的读写器,来获取共享密钥。但因攻击者没有全部标签的 (IDS_i,ID_i),无法对群组内的每个标签验证成功,协议终止;更无法计算正确共享密钥 $k = IDS_1 \oplus IDS_2 \oplus\cdots\oplus IDS_n$,攻击失败。

攻击者企图通过主动攻击,假冒成合法的标签,来获取共享密钥。读写器首先向群组标签发送密钥生成请求,但假冒标签只有部分 (IDS_i,ID_i) 信息,即使能做异或加密运算后将残缺的 Z_1, $Z_2,\cdots,Z_n$ 作为响应信息发给读写器。但当读写器收到此消息后,则会立即识别出标签为假冒,协议终止,而此时攻击者还没有获得任何有用的信息,无法计算出正确的共享密钥,攻击失败。

综上所述,本文提出的 RFID 系统密钥无线生成协议在 3 种不同实际应用情况下能更全面地抵抗被动攻击和主动攻击,下面给出文献[13]协议与本文协议的安全性对比,见表 2,在表 2 中,√表示满足安全性;/表示部分满足安全性。

表 2　协议安全性对比

攻击类型	文献[13]协议	本文协议
被动攻击	/	√
主动攻击	/	√

6　协议性能分析

本节分别对 3 种不同情况下的 RFID 系统密钥无线生成协议,从标签的计算量、存储量和通信量 3 个方面与文献[13]协议进行性能分析对比,其中,文献[13]协议与本文协议标签端的通信量相同,表中就不进行赘述,具体差异对比详见表 3 ~ 表 5。

表 3　单个标签密钥生成协议性能对比

单个标签协议	计算量	存储空间
文献[13]协议	*XOR* + *PRNG*	*I* + *X*
本文协议	5*XOR* + *R*	2*I* + *X*

表 4　批量标签密钥生成协议性能对比

批量标签协议	计算量	存储空间
文献[13]协议	*XOR* + *PRNG*	*I* + *X*
本文协议	6*XOR* + *R*	2*I* + *X*

表 5　群组标签密钥生成协议性能对比

群组标签协议	计算量	存储空间
文献[13]协议	*XOR*	*I* + *X*
本文协议	(*n* + 1)*XOR*	2*I* + *X*

在表 3 ~ 表 5 中,*XOR* 表示异或运算,*R* 表示移位运算,*PRNG* 表示随机数产生器,假名标识 *IDS* 标识、标签唯一标识 *ID*、密钥 *k*、随机数的长度都是 *I*,*X* 表示认证过程中的临时存储空间。

通过表 3 ~ 表 5 可以看出,对于单个和批量标签密钥生成协议,在标签通信量相同的情况下,本文协议标签计算量更优,因为本文协议标签端不再使用随机数发生器产生随机数,大大减少了标签端计算量,并且降低标签成本,实现密钥快速生成。对于群组标签密钥生成协议,虽然标签端计算量比文献[13]协议增加,但本文协议采用加密传输使得系统具有更高的安全性,对于高安全要求的应用场合具有明显优势。

7　结束语

本文提出一种基于假名标识的 RFID 系统密钥无线生成协议。分别对 3 种不同情况下的 RFID 密钥无线生成协议进行安全性与性能分析,并根据 GNY 逻辑对协议进行形式化证明。分析结果表明,该协议引入标签假名标识并与其进行异或加密传输,保证协议在前、后向信道都可被窃听情况下的安全性;在标签端通信量不变的前提下,实现标签和读写器端的双向认证功能,强化协议安全性;标签不再使用随机数发生器产生随机数,降低了标签成本与计算量。但系统密钥生成后,读写器和标签通信双方如何继续进行高安全、低成本的双向认证过程,将是下一步的研究方向。

参考文献

[1]　毛雅佼,孙达志. 一种新的 RFID 标签所有权转移协议[J]. 计算机工程,2015,41(3):147-150.

[2]　赵庚申,低成本柔性电子标签的设计和设备研究[D]. 大连:大连理工大学,2005.

[3]　师鸣若,姜中华. 一种无线认证密钥协商协议[J]. 计算机工程,2009,35(7):142-149.

(下转第 183 页)

结果表明,网络越稀疏,抵制相互作用过程的破坏力越强,但相互作用过程中级联故障子过程破坏力也会得到增强。当网络稀疏性确定后,降低网络聚类系数可以减弱相互作用过程的破坏力。本文的研究结论对保护 Internet 网络具有指导意义。

参考文献

[1] 蒙在桥,傅秀芬. 基于在线社交网络的动态消息传播模型[J]. 计算机应用,2014,34(7):1960-1963.

[2] 胡宝安,李　兵,李亚玲. 具有时滞的 SIR 计算机病毒传播模型[J]. 计算机工程,2016,42(5):168-172.

[3] 黄宏程,蒋艾玲,胡　敏. 基于社交网络的信息传播模型研究[J]. 计算机应用研究,2016,33(9):2738-2742.

[4] Borge-Holthoefer J, Meloni S, Gonçalves B, et al. Emergence of Influential Spreaders in Modified Rumor Models[J]. Journal of Statistical Physics, 2013, 151(1):383-393.

[5] Wang Wenxu, Chen Guanrong. Universal Robustness Characteristic of Weighted Networks Against Cascading Failure[J]. Physical Review E,2008,77(2).

[6] Lin Guoqiang, Di Zengru, Fan Ying. Cascading Failures in Complex Networks with Community Structure[J]. International Journal of Modern Physics C,2014,25(5):323-337.

[7] 彭兴钊,姚　宏,张志浩,等. 基于节点蓄意攻击的无标度网络级联抗毁性研究[J]. 系统工程与电子技术,2013,35(9):1974-1978.

[8] 刘漳辉,陈国龙,汤振立,等. 加权复杂网络相继故障的节点动态模型研究[J]. 小型微型计算机系统,2013,34(12):2800-2804.

[9] Coffman J E G,Ge Zihui,Misra V,et al. Network Resilience: Exploring Cascading Failures Within BGP[C]//Proceedings of the 40th Annual Allerton Conference on Communications, Computing and Control. Berlin, Germany: Springer, 2002: 65-193.

[10] Ouyang Bo,Jin Xinyu,Xia Yongxiang,et al. Dynamical Interplay Between Epidemics and Cascades in Complex Networks[J]. Europhysics Letters,2014,106(2):205-211.

[11] 欧阳博,金心宇,夏永祥,等. 疾病传播与级联失效相互作用的研究:度不相关网络中疾病扩散条件的分析[J]. 物理学报,2014,63(21):434-443.

[12] 欧阳博. 复杂网络上的级联失效及其与病毒传播相互作用的研究[D]. 杭州:浙江大学,2014.

[13] 秦　李,黄曙光,陈　骁. 病毒传播下的因特网级联故障模型构建与仿真[J]. 计算机应用研究,2016,33(4):1228-1231.

[14] 何郁郁,邹艳丽,许旋风,等. 可变聚类无标度网络上的谣言免疫策略[J]. 计算物理,2014,31(6):751-756.

[15] Holme P, Kim B J. Growing Scale-free Networks with Tunable Clustering[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics,2002,65(2).

[16] Singh A, Singh Y N. Rumor Spreading and Inoculation of Nodes in Complex Networks[C]//Proceedings of the 21st International Conference on World Wide Web. New York, USA: ACM Press, 2012: 675-678.

[17] Puzis R, Elovici Y, Zilberman P, et al. Topology Manipulations for Speeding Betweenness Centrality Computation[J]. Journal of Complex Networks, 2015, 3(1):84-112.

编辑　顾逸斐

(上接第 177 页)

[4] 隋　雷,郭渊博,姜文博,等. 基于无线信道特征的密钥生成与提取研究[J]. 计算机科学,2015,42(2):137-141.

[5] 金永明,吴棋滢. 基于 PRF 的 RFID 轻量级认证协议研究[J]. 计算机研究与发展,2014,51(7):1506-1514 .

[6] 李娅莉. RFID 系统的认证与密钥协商协议研究[D]. 上海:上海交通大学,2010.

[7] Kuo C,Luk M,Negi R,et al. Message-in-a-bottle: User Friendly and Secure Key Deployment for Sensor Nodes[C]// Proceedings of the 5th International Conference on Embedded Networked Sensor Systems. New York, USA: ACM Press, 2007: 233-246.

[8] Stajano F, Anderson R. The Resurrecting Duckling: Security Issues for Ubiquitous Computing[J]. Computer, 2002,35(4):22-26.

[9] Wang Rangding, Jiang Gangyi, Chen Jin'er. A New Method of Audio-digital Watermarking Based on Trap Strategy[J]. Journal of Computer Research and Development,2006,43(4):613-620.

[10] 刘伟峰,陈怀义. 基于面向对象技术的 PKI 密钥的软件生成[J]. 计算机工程与科学,2004,26(11):26-32.

[11] Shamir A. Identity-based Cryptosystems and Signature Schemes[C]//Proceedings of LNCS 196: Advances in Crypotogy-Crypto'84. Berlin, Germany: Springer-Verlag, 1984:47-53.

[12] 黄　灿,刘　丹,彭春林. RFID 系统下基于组合公钥的密钥管理应用研究[J]. 微电子学与计算机,2013,30(12):104-107.

[13] 鲁　力. RFID 系统密钥无线生成[J]. 计算机学报,2015,38(4):822-832.

[14] Ranasinghe D C, Cole P H. Confronting Security and Privacy Threats in Modern RFID Systems[C]// Proceedings of the 14th Asilomar Conference on Signals, Systems and Computers. Washington D. C., USA: IEEE Press,2006:2058-2064.

[15] Heydt-Benjamin T S, Bailey D V, Fu K, et al. Vulnerabilities in First-generation RFID-enabled Credit Cards[C]//Proceedings of FC'07. Berlin, Germany: Springer-Verlag,2007:2-14.

[16] 胡德新,王晓明. 基于 RFID 标签的所有权转移认证协议[J]. 计算机工程与设计,2014,35(3):819-824.

[17] 李　杰. RFID 安全认证协议研究与设计[D]. 西安:西安电子科技大学,2012.

编辑　刘　冰　顾逸斐