计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20180075
55(7):1432-1439,2018

物联网中超轻量级RFID电子票据安全认证方案

王 悦[1] 樊 凯[2]
[1](西安文理学院信息工程学院 西安 710065)
[2](西安电子科技大学网络与信息安全学院 西安 710071)
(ywang@xawl.edu.cn)

Ultra-Lightweight RFID Electronic Ticket Authentication Scheme in IoT

Wang Yue[1] and Fan Kai[2]
[1](*College of Information Engineering*, *Xi'an University*, *Xi'an* 710065)
[2](*School of Cyber Engineering*, *Xidian University*, *Xi'an* 710071)

Abstract With the increasing popularity of IoT application technologies, one of the key technologies, called the radio frequency identification (RFID) technology, has been applied to more and more application scenarios in various fields. The electronic tickets apply RFID technology to traditional tickets, which makes the traditional tickets have the characteristics of being storable and identifiable as well as verifiable, bringing a great deal of convenience and efficiency to people's daily life. Although, RFID systems in the application of electronic tickets still face many potential security risks, such as privacy leakage. To solve the security problems in the application of electronic tickets, an ultra-lightweight RFID security authentication scheme is presented in this paper. Compared with some schemes that use complex cryptographic algorithms, this scheme adopts simple logic operation and timestamp synchronization upgrade mechanism, which can effectively resist asynchronous attack and replay attack, and besides it can effectively prevent information leakage. At the same time, the method that the time stamp matches the label information in the database in this scheme greatly improves the efficiency of information searching in database. Through the analysis of security and efficiency, and the performance comparison and simulation, the proposed scheme has higher security and efficiency than some existing schemes.

Key words radio frequency identification (RFID); security authentication; ultra-lightweight; electronic ticket; IoT

摘 要 随着物联网应用技术的日益普及,作为其中重要技术之一的无线射频识别(radio frequency identification, RFID)技术在各个领域的应用场景越来越丰富.电子票据将RFID技术应用于传统票证,使得传统票证具备可存储、可识别、可验证等特性,在很大程度上给人们的日常出行带来了巨大的便捷和高效.尽管如此,RFID系统在电子票证上的应用仍然面临着许多安全风险,比如隐私泄露.针对RFID技术在电子票据应用中存在的安全问题,提出了一种超轻量级的安全高效的认证方案.和一些采用复杂加密运算的方案相比,该方案采用简单的逻辑运算和时间戳同步升级机制,可有效抵抗失同步

收稿日期:2018-01-31;**修回日期**:2018-05-04
基金项目:国家自然科学基金项目(61772403,U1401251);西安市科技计划项目(CXY1352WL30)
This work was supported by the National Natural Science Foundation of China (61772403, U1401251) and the Science and Technology Plan Project in Xi'an of China (CXY1352WL30).

攻击和重放攻击,并可有效防止信息泄露.同时,该方案在数据库中采用时间戳匹配标签信息的方法,极大地提高了数据搜索效率.经过对安全性和高效性方面的分析以及对性能的仿真比较,可知所提方案相比现有方案在安全性和效率上均有较大提升.

关键词　无线射频识别;安全认证;超轻量级;电子票据;物联网

中图法分类号　TP393

随着云计算、大数据以及新一代移动通信技术的普及应用,物联网技术也得以快速发展,该技术可应用的领域也越来越多.物联网是一种通过信息传感设备,把任何物品与互联网相连接,按约定的协议进行信息交换和通信,以实现智能化识别、定位、跟踪、监控和管理的网络.无线射频识别(radio frequency identification, RFID)技术是物联网的关键技术之一,也在诸多物联网场景中被广泛应用.RFID 是一种非接触式自动识别技术,具有快速高效等特点,可以快速、实时和精确地识别、采集并处理相关对象的信息.近年来,国内的 RFID 技术发展迅速,已被广泛应用于公共交通、自动收费站、社会保障等领域[1].

在票据领域,RFID 广泛应用于获取电子票据的信息认证和隐私保护等方面,是电子票据应用技术的重要组成部分.通过将 RFID 技术应用于传统的票据,电子票据比纸质的标签能提供更高效、便利的服务[2].但在节约工作成本和提高效率的同时,也带来了一系列潜在的安全威胁.

在实际应用中,使用 RFID 技术的电子票据体现了物联网的智能化识别和检测.但这一过程存在多种安全问题,比如身份隐私泄露和安全认证等问题.由于电子标签和读卡器之间通过无线链路来交换数据信息,这种无线通信工作于开放环境中,其固有的脆弱性使得传输的数据信息被完全地暴露出来,容易受到外部的干扰和攻击,使标签的隐私信息存在极大的安全隐患[3],如攻击者可以通过跟踪电子标签,追踪用户的位置,从而泄露用户的位置信息[4].此外,攻击者还可以通过窃听获取到电子标签的隐私信息,并对信息分析后进行攻击,也就进一步影响了后续的安全认证.

RFID 的安全问题制约着电子票据系统的发展和应用,解决 RFID 安全问题的有效手段是引入具有隐私保护的安全认证机制.与此同时,由于电子标签的计算能力、存储空间、通信容量、逻辑门的数量和电源供给能力等多方面的资源限制,一些成熟复杂的加密算法不能应用在 RFID 安全认证系统中,因此轻量级安全认证协议得到了广泛的应用,也成为了当前电子票据安全认证协议研究的重点.

为解决 RFID 技术在电子票证中存在的安全问题,通过分析研究,本文提出了一个超轻量级的 RFID 安全认证方案,使得电子票证的隐私保护和安全认证等方面的需求得以保障.本方案采用计算复杂度较简单的逻辑运算用于信息的加密,在保障系统信息安全的同时,可以降低计算开销,能够更好地适用于无源标签系统.方案采用时间戳同步升级机制,可有效解决失同步攻击和重放攻击等安全问题,并可有效防止信息泄露.另外,为了提高信息匹配的速度,后端数据库采用时间戳匹配标签信息的方法,极大地提高了数据搜索效率.

1　相关工作

物联网技术正在快速发展,在不同的应用场景中,人们的安全意识和需求也都在逐步提升.物联网的安全主要是指保护在其系统中软硬件的数据免受泄露、篡改、破坏等安全问题,从而使得整个系统稳定、安全且高效地运行.

由于 RFID 技术在物联网中应用广泛,系统应用的安全问题一直以来都是该领域研究人员重点关注的问题.随着 RFID 技术的发展,为了进一步扩大轻量级的 RFID 系统的应用场景和应用领域,一些低成本的 RFID 安全认证方案先后陆续被提出.早在 2003 年,文献[5]就曾基于 Hash 函数提出过 Hash-lock 协议.在该方案中,标签的身份信息是匿名的,尽管如此,匿名化的身份信息在每轮会话过程中是保持不变的,在保护用户身份隐私的同时,却失去了抵抗追踪的能力.该协议整体设计较为简单,安全防御能力还有待提升.随后, Hash-chain 协议[6]被提出,该协议是基于 Hash-lock 改进的方案,尽管解决了之前协议的不足,却也带来了一些新的安全问题,比如无法抵抗重放攻击等.

2006 年,RFID 轻量级安全认证协议 SPAP[7]被提出,但该协议不仅不能抵抗重放攻击,且容易泄

露标签的敏感信息. 2007 年提出的超轻量级 RFID 认证协议(SASI)[8]能抵抗重放攻击,并且提供强认证性和强集成性,却不能有效抵抗拒绝服务攻击. 一旦有攻击者反复认证 IDS 信息,会使数据库一直处于忙碌状态,带来资源消耗严重,从而影响正常数据的通信. 此外,和 SPAP 协议相似,SASI 协议也容易泄露标签的敏感信息. 2012 年,文献[9]提出了基于时间戳的认证协议,该协议实现了双向认证. 此外,在该协议中,标签的 ID 信息在传送时都经过了 Hash 运算,可以保证标签身份的机密性. 但是该协议存在一定的缺陷,不能有效抵抗去同步攻击,甚至在失同步的情况下还会进一步遭受重放攻击. 2013 年文献[10]提出了一个抵抗去同步攻击的协议,但该协议数据库中对同一个标签存储数据过多且不便于查找. 以上这些方案或多或少均存在一些安全不足,因此如何设计更安全、成本更低的方案仍然是当前研究的重点. 针对 RFID 技术在电子票据应用场景中存在的安全问题,本文提出了一种安全高效的轻量级认证方案,可以有效地防止重放攻击、去同步攻击等常见的安全威胁,并极大地提高了数据的搜索效率.

2 轻量级 RFID 电子票据安全认证方案

2.1 电子票证的安全特征

一个完善的票证防伪认证系统应当具备匿名访问、票证防伪、防追踪等 3 种基本的特征[11].

1) 匿名性

票证和读卡器之间是通过无线链路来交换数据信息的,而无线通信固有的脆弱性使得传输的数据信息完全地暴露出来,容易受到外部的干扰和攻击,导致一些信息被泄露. 而票证中有很多敏感信息,一旦泄露会给用户造成一定的威胁,如用户的身份信息、当前位置等. 在读卡器对票证进行读写和通信的过程中要对重要信息进行加密,不能出现有关这些数据的明文信息,以保证信道中信息传输的机密性. 票证在与外界设备的交互过程中也不能直接将自身敏感信息直接传输,而是要经过一些匿名处理,实现对票证的随机化访问控制,即使攻击者通过无线信道截获了交互消息,在未知解密密钥和解密方法的情况下也无法获知票证中的重要信息. 而在认证的过程中,每次票证请求时,请求消息中的认证标识符都不相同,从而实现了用户身份的匿名性[12].

2) 票证防伪

RFID 技术的票证中都内嵌有独立的芯片,由于芯片制造过程中产生的差异本身具有不可模仿和复制的特性,所以芯片的复制难度极高,并且芯片内存储有唯一的 ID,结合通信前的相互认证过程,没有通过认证的票证不能进行下一步操作. 芯片 ID 和双向认证共同作用使票证具有防伪的功能[13].

一般说来,RFID 的安全隐私问题与非法的读卡器从合法的标签上读取重要信息有关. 因此,解决 RFID 安全问题的有效手段是引入安全认证机制. 即在电子标签和读卡器进行重要信息交换之前先通过一定的手段进行双向认证,认证通过后才可以进一步操作[14].

3) 防追踪

由于票证发送的信息中可能包含某种固有的或者有规律的能唯一标识身份的信息,如 ID 序列号,攻击者可以根据票证响应读卡器的响应信息对票证进行跟踪分析. 因此,当用户没有改变时,攻击者就可以通过跟踪票证追踪用户的位置,从而泄露用户的位置信息[15],因此,在协议交互的过程中不能使用 ID 的明文信息,需要将 ID 进行变换,混淆 ID 信息,防止追踪.

2.2 方案设计

轻量级 RFID 电子票据安全认证方案在电子标签与读卡器进行有效的数据传输前,会先进行双向认证,只有通过认证后,电子标签才会把身份信息等数据发送给读卡器. 双方传输的数据信息用异或、置换变换、循环移位等超轻量级逻辑运算进行加密. 电子标签和服务器中存储有相应的时间戳信息,既可以防止失同步问题的出现,又可以提高检索效率. 在认证的过程中,一旦发现不能匹配的信息,电子标签、读卡器和后台服务器可随时终止协议.

由于认证期间,只需要传输时间戳作为认证的标识,可以很大程度上减少电子标签的开销.

在电子标签向后台服务器传输数据时,没有直接传输明文 ID 或者 ID 的部分明文,而是将 ID 进行加密、变换后再进行传输,防止标签的重要信息泄露.

时间戳的更新分别在电子标签和服务器中完成,更新后的数据没有在不安全信道上传输,被攻击者窃听到的几率大大减小.

2.3 符号说明

为方便方案描述,协议中需要用到的符号和操作说明如表 1 所示:

Table 1　Notations

表 1　符号说明

Notation	Description
R	Reader
T	Tag
DB	Datatbase
SID	Tag's secure ID
T_l	Timestamp stored in the tag
T_o	The old timestamp used in the last successful authentication
T_n	The updated timestamp after last successful authentication
K_l	The secret key of the tag
K_o	The old secret key used in the last successful authentication
K_n	The updated secret key after last successful authentication
$Per()$	The permutation operation
$f(ID,X,Y)$	A function that can extract some bits from X to Y in the ID
$Rot(x,y)$	The left rotation of x according to the hamming weight of y

2.4　方案介绍

本方案涉及到 3 个实体:电子标签、读卡器和后台服务器.读卡器和服务器之间的数据交互基于有线信道,故而是安全可靠的;而读卡器和电子标签之间的数据传输是在无线开放环境中进行的,因此是不安全的.

在电子标签和后台服务器进行通信的过程中,标签运算只涉及加法、异或、置换、循环移位 4 种简单的位操作.置换变换可以有效地应用在无源标签上,减少标签的计算开销.

2.4.1　置换变换

定义 1. 置换变换 $Per(A,B)$.假设 A,B 是 2 个均为 l 位长的字符串,且

$$A=a_1a_2\cdots a_l,a_i\in\{0,1\},i=1,2\cdots,l,$$

$$B=b_1b_2\cdots b_l,b_j\in\{0,1\},j=1,2\cdots,l,$$

B 中 1 的个数为 m,即:

$$b_{k1}=b_{k2}=\cdots=b_{km}=1,b_{km+1}=b_{km+2}=\cdots=b_{kl}=0,$$

其中,$1\leqslant k_1<k_2<\cdots<k_m\leqslant l,1\leqslant k_{m+1}<k_{m+2}<\cdots<k_l\leqslant l$,则:

$$Per(A,B)=\tilde{a}_{k1}\tilde{a}_{k2}\cdots\tilde{a}_{km}a_{kl}a_{kl-1}\cdots a_{km+2}a_{km+1}.$$

例如 $A=10110101,B=11010110$,即可得到 $Per(A,B)=01001101$.

设指针 p_A 和 p_B 分别指向字符串 A,B,且同步地从字符串的第 1 位到最后一位,当 p_B 指向 1 时,就将 p_A 指向的位取反并复制到第 3 个字符串中,直到 p_A,p_B 都同时指向最后一位,如图 1 阴影部分所示.然后 p_A,p_B 同时从最后一位向第 1 位同步移动,当 p_B 指向 0 时,就将 p_A 指向的位复制到第 3 个字符串中,直到 p_A,p_B 都同时指向第 1 位,计算结果如图 1 所示 $Per(A,B)$.

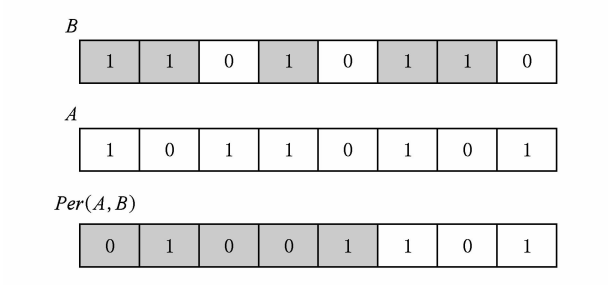

Fig. 1　Permutation operation

图 1　置换变换

2.4.2　协议步骤

本方案包括 2 个阶段:初始化阶段和认证阶段.

1) 初始化阶段.该阶段实现标签和后台服务器存储数据的初始化.

① 标签的初始化.系统为每个标签指定唯一的 l 位长的身份认证信息(Secure ID, SID)和本次认证的密钥信息 K_l.将 SID,K_l 和时间戳 T_l 存储在每个标签中.

② 后台服务器的初始化.系统将每个电子标签的 SID 信息、K_l 和时间戳 T_l 存储在后台服务器 Database 中,并将上次成功认证的时间戳 T_o 和上次成功认证的密钥 K_o 置为 0.

2) 认证阶段.方案的认证过程如图 2 所示.协议共分为 6 步,每一步的认证过程如下所示:

① 读卡器发送询问信号.电子标签接收到询问信号后,将上次更新的时间戳信息 T_l 发送给读卡器,读卡器将 T_l 和随机数 R_1 发送给后台数据库.

② 搜索后台数据库中保存的时间戳信息.如果 T_l 匹配到的是上次成功认证的时间戳信息 T_o,那么可能是标签上次认证未更新时间戳,而密钥信息是否更新未知,为了保证标签和数据库中数据的一致性,将 K_o 的值赋给 K_l;如果 T_l 匹配到的是更新后的时间戳 T_n,则将 K_n 的值赋给 K_l.通过加密运算 $Per(R_1,K_l)$ 对 R_1 进行加密后传输.

③ 读卡器接收到后台数据库发送的消息 P 后,将 P 发送给电子标签.标签通过相应的逆置换变换 P^{-1} 得到 R_1,产生随机数 R_2,计算 $V=Per(K_l\oplus R_2,R_1),SID'=Rot(SID\oplus V,R_2),R'=f(SID',$

$1, R_1) \| f(SID', R_2, l)$. 电子标签将计算得到的信息 V 和 R' 发送给读卡器.

④ 读卡器将 V 和 R' 发送给后台数据库. 后台数据库从 V 中得到 R_2, 计算 $SID'=Rot(SID \oplus V, R_2)$, 得到 $f(SID', 1, R_1) \| f(SID', R_2, l)$, 将其与标签发送的数据 R' 进行比较是否匹配, 如果匹配成功, 则计算 $R''=f(SID', R_1, R_2)$, 将 R'' 发送给读卡器. 然后更新 $T_o \leftarrow T_l$, $K_o \leftarrow K_l$, $K_n \leftarrow Rot(K_l \oplus R_1, R_1)$, $T_n \leftarrow T_l + Per(K_n, R_1)$.

⑤ 读卡器将 R'' 发送给电子标签. 标签计算 $f(SID', R_1, R_2)$, 并与 R'' 比较, 如果相等, 则发送"OK"给读卡器, 然后更新 $K_l \leftarrow Rot(K_l \oplus R_1, R_1)$, $T_l \leftarrow T_l + Per(K_l, R_1)$; 否则发送"No find"信息给读卡器.

⑥ 如果读卡器收到的是"OK"信息, 那么就将信息转发给后台数据库, 数据库将发送 SID 信息给读卡器; 否则, 读卡器终止协议.

在协议认证的过程中, 如果有多个电子标签同时对读卡器的询问信号做出响应, 那就会产生干扰, 影响认证的进行. 因此在本协议中使用 BMSA(breadth-first-search m-ary split algorithm)来解决标签碰撞问题[16].

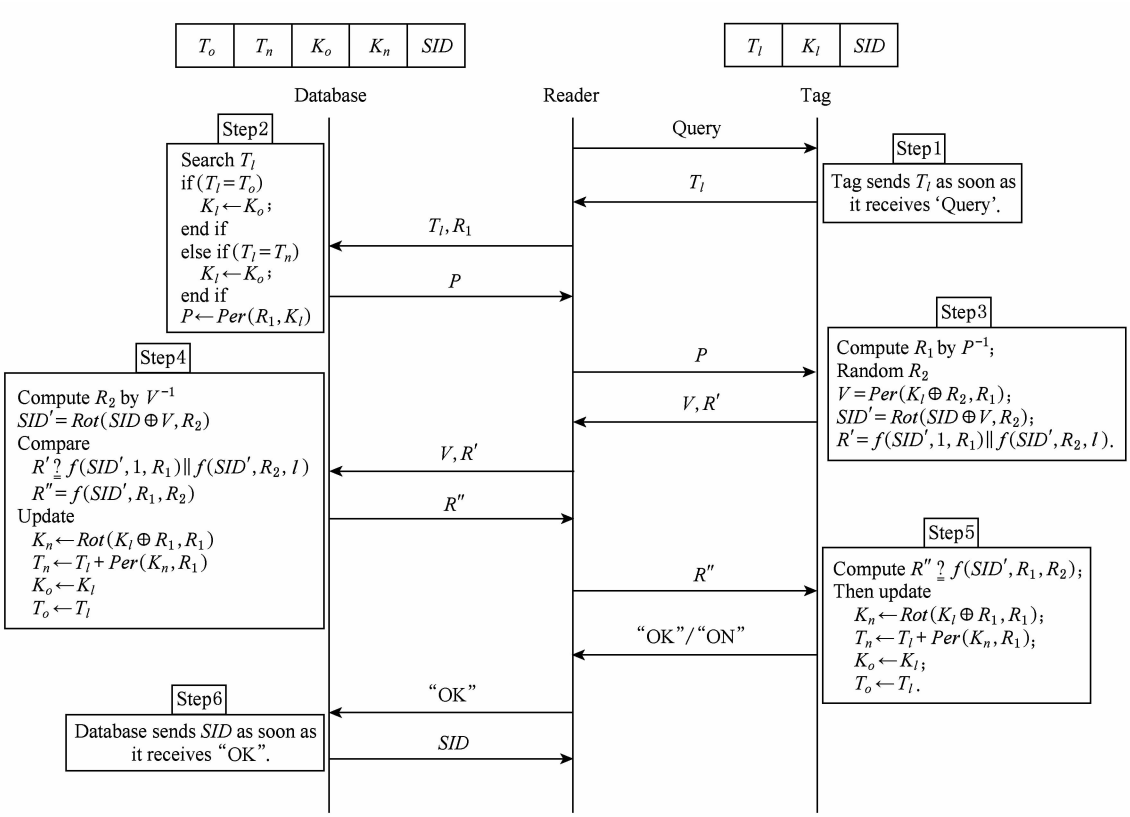

Fig. 2 Ultra-lightweight RFID electronic ticket authentication scheme in IoT

图 2 物联网中超轻量级 RFID 电子票据安全认证方案

3 安全性分析

本文对 SPAP 协议、SASI 协议和本文提出的协议进行了分析比较, 3 种方案的比较如表 2 所示. SPAP 协议中, 电子标签中的 SID 信息仅仅通过简单的取子串和异或的方法就进行发送, 一旦被攻击者窃听到, 就容易泄露相应的 ID 信息. 在 SASI 协议中, 由于 ID 信息是以明文的形式在无线链路中传输, 因此也容易造成信息泄露. 本方案中后台数据库是用时间戳信息搜索电子标签的, 标签的 ID 信息得到保护. 本方案在安全性方面具有 7 个特点:

1) 标签匿名且不可追踪. 在整个协议的认证期间, 攻击者能获取到的值只有 T_l, P, V, R', R''. 而 T_l 只有时间戳的意义, 不包含其他有关电子标签身份的信息. 对于系统来说, 时间戳只是起到便于后台数据库搜索标签的作用. 所以对攻击者来说, 即使截获了时间戳, 也不能最终通过和后台数据库之间的认证过程. 而 P, V, R' 和 R'' 均会受到随机数的影响, 也无法追踪.

Table 2　Comparison of Various Authentication Protocols

表 2　安全认证协议比较

Protocol	SPAP	SASI	Proposed Protocol
Arithmetic operation	$\oplus, OR, PID$	$+, \oplus, OR, Rot$	$\oplus, +, Rot, Per$
The storage overhead of the tag	$2l$	$7l$	$3l$
The storage overhead of the database	l	$4l$	$5l$
Tag anonymity	No	Yes	Yes
Resistance to replay attacks	No	Yes	Yes
Resistance to desynchronization attacks	No	Yes	Yes
Forward secrecy	Yes	Yes	Yes
Backward secrecy	Yes	Yes	Yes

2) 双向认证. 后台服务器通过 T_l 和 R' 实现对电子标签的认证,电子标签通过 R'' 实现对后台数据库和读卡器的认证. 只有存储密钥 K 的标签和数据库才能完成对 R', R'' 的认证.

3) 防止重放攻击. 攻击者可能会截获标签和读卡器之间传输的消息,但这些消息依赖于每次认证都会更新的密钥和随机数. 所以即使攻击者重放消息,也不能通过数据库和标签的认证.

4) 防止去同步攻击. 后台数据库中不仅存储当前通信需要的时间戳、密钥,还存储着上次认证成功的时间戳和密钥. 防止 R'' 被攻击者截获导致标签更新失败后合法的标签不能通过再次认证的问题.

5) 防止隐私泄露. 电子标签和读卡器间传输的信息 $Per(R_1, K_l)$, $Per(K_l \oplus R_2, R_1)$ 是加密后的数据,因为很多对 K_l, R_1 都会得到相同的 $Per(R_1, K_l)$ 值,所以即使攻击者截获 $Per(R_1, K_l)$,也不能计算出随机数 R_1 和密钥 K_l 的值. 同理通过 $Per(K_l \oplus R_2, R_1)$ 也不能得到 R_1, R_2 和 K_l.

6) 前向安全性. 后台数据库和电子标签使用随机数分别更新时间戳和密钥信息. 因此,即使当前的密钥泄露,攻击者也不能推测出以前的密钥信息.

7) 后向安全性. 即使攻击者获取到后台数据库和电子标签之间当前传输的交互信息 P, V, R' 和 R'',也不能从当前信息中推测出更新电子标签的信息 K_l,因此不能更新假冒标签的信息.

4　性能分析

本文提出的协议只需要标签进行简单的逻辑运算、位运算,可大大减少对标签的软硬件要求. 下面将详细论述本方案中标签和后台服务器的开销.

1) 标签的通信开销. 在本协议中,电子标签只涉及随机数发生器,简单的加法 $+$、异或 XOR $\oplus$、循环移位 Rot、置换变换 Per 等操作,计算简单高效.

2) 标签的存储开销. 在本协议中,身份信息 SID、时间戳 T_l、密钥信息 K_l 都是 l 位的,那么标签共需要 $3l$ 位的空间存储信息.

3) 后台服务器的查找开销. 在 SPAP 协议中,数据库需要在每个可能标签信息中查找请求标签的 SID 信息,并进行计算后与 $PID'_{1L} \oplus PID'_{2R}$ 比较是否匹配,造成后台数据库的开销过大. SASI 协议需要先计算数据 A, B, C 的值后才能进行相互认证,浪费较多的数据库资源、开销大. 而本方案中,在初步匹配到时间戳信息之后仅进行简单的计算,发送加密的数据,实现对标签的进一步认证.

5　仿真分析

本文采用 MATLAB 软件对协议进行模拟仿真. 图 3 和图 4 分别对认证时间和攻击次数进行了

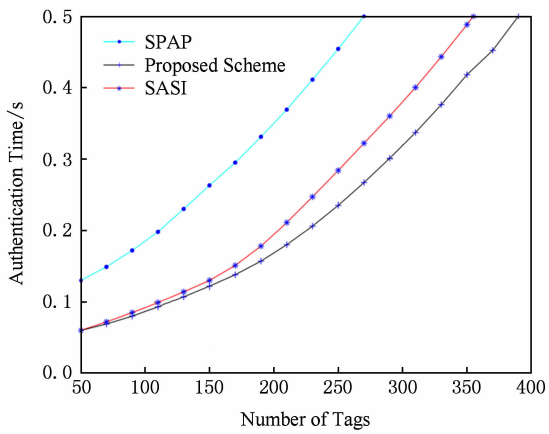

Fig. 3　Authentication time versus the number of tags

图 3　认证时间和标签数量的关系图

仿真,将 SASI 协议、SPAP 协议与本方案进行了分析比较.

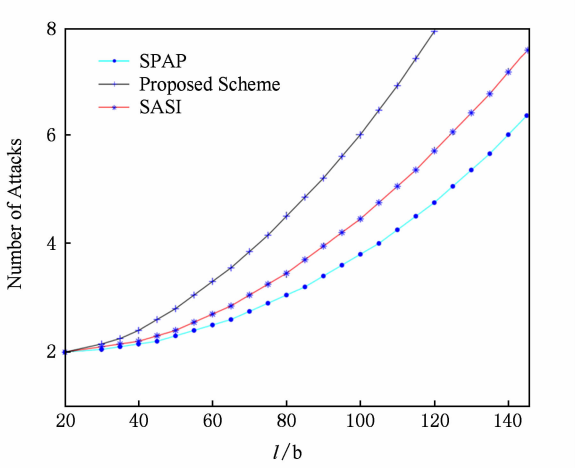

Fig. 4 The number of attacks versus the length of l

图 4 攻击次数和 l 长度的关系图

由图 3 可知,随着数据库中存储标签个数的增加,标签通过后台数据库认证的时间也随之增加.在后台数据库认证标签的时间开销方面,本文提出的协议的认证时间较短、认证速度较快,具有较好的性能.由图 4 可知,随着每个标签中 SID,K_i 长度的增加,为了获取标签的隐私信息需要攻击的次数也在不断增加,可见本文提出的协议安全性较高,抵抗攻击性较强.

6 总 结

物联网旨在实现万物相连,将传统票证电子化也是将其物联网化的一种应用.针对物联网中 RFID 技术在电子票据应用中存在的安全问题,本文对现有的 RFID 认证方案进行了优化与改进,提出了一种轻量级安全高效的认证方案.该方案实现了电子标签和读卡器间的双向认证,具有机密性和标签匿名性,可有效抵抗重放攻击、失同步攻击,同时具有前向安全性,基本满足了低成本 RFID 系统的要求.另外,性能分析和仿真结果均表明,该方案在保证一定安全性的同时,具有较高的性能和较低的资源消耗.

参 考 文 献

[1] Wang Pei. The design and application of combinational RFID positioning system based on multi-frequency [D]. Xi'an: Xidian University, 2014 (in Chinese)
(王沛. 基于多频 RFID 组合定位系统设计与应用[D]. 西安:西安电子科技大学, 2014)

[2] You Xiangbai, Liu Yimin. Research on cryptographic protocols for RFID [J]. Video Engineering, 2012, 36(15): 104-107 (in Chinese)
(游相柏, 刘毅敏. RFID 安全认证协议研究[J]. 电视技术, 2012, 36(15): 104-107)

[3] Cai Shaoying, Li Yingjiu, Li Tieyan, et al. Attacks and improvements to an RFID authentication protocol and its extensions [C] //Proc of the WISEC'09. New York: ACM, 2009: 51-58

[4] Zhang Longxiang. Security analysis of a RFID authentication protocol based on physically unclonable function [J]. Journal of Computer Applications, 2012, 32(8): 2280-2282 (in Chinese)
(张龙翔. 一种基于不可复制功能的 RFID 认证协议的安全性分析[J]. 计算机应用, 2012, 32(8): 2280-2282)

[5] Sarma S E, Weis S A, Engels D W. RFID systems and security and privacy implications [C] //Proc of Int Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2002: 454-469

[6] Ohkubo M, Suzuki K, Kinoshita S. Hash-chain based forward-secure privacy protection scheme for low-cost RFID [C] //Proc of the SCIS'04. Berlin: Springer, 2004: 719-724

[7] Li Yongzhen, Cho Youngbok, Um Namkyoung, et al. Security and privacy on authentication protocol for low-cost RFID [C] //Proc of IEEE Int Conf on Computational Intelligence and Security. Piscataway, NJ: IEEE, 2006: 1101-1104

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

[9] Zhang Bing, Ma Xinxin, Qin Zhiguang. Design and analysis of a lightweight mutual authentication protocol for RFID [J]. Journal of University of Electronic Science and Technology of China, 2013, 42(3): 425-430 (in Chinese)
(张兵, 马新新, 秦志光. 轻量级 RFID 双向认证协议设计与分析[J]. 电子科技大学学报, 2013, 42(3): 425-430)

[10] Xie Wei, Xie Lei, Zhang Chen, et al. Cloud-based RFID authentication [C] //Proc of the 2013 IEEE Int Conf on RFID (RFID). Piscataway, NJ: IEEE, 2013: 168-175

[11] Deng Miaolei, Ma Jianfeng, Zhou Lihua. Design of anonymous authentication protocol for RFID [J]. Journal on Communications, 2009, 30(7): 20-26 (in Chinese)
(邓淼磊, 马建峰, 周利华. RFID 匿名认证协议的设计[J]. 通信学报, 2009, 30(7): 20-26)

[12] Dang Lanjun, Kou Weidong, Cao Xuefei, et al. Mobile IP registration protocol with user anonymity [J]. Journal of Xidian University (Natural Science), 2008, 35(2): 282-287 (in Chinese)
(党岚君, 寇卫东, 曹雪菲, 等. 具有用户匿名性的移动 IP 注册协议[J]. 西安电子科技大学学报:自然科学版, 2008, 35(2): 282-287)

[13] Bassil R, El-Beaino W, Kayssi A, et al. A PUF-based ultra-lightweight mutual-authentication RFID protocol [C] //Proc of the 2011 IEEE Internet Technology and Secured Transactions. Piscataway, NJ: IEEE, 2012: 495-499

[14] Bao Guihao, Zhang Minggao, Liu Jiuwen, et al. The design of an RFID security protocol based on RSA signature for E-ticket [C] //Proc of the 2nd IEEE Int Conf on Information Management and Engineering. Piscataway, NJ: IEEE, 2010: 636-639

[15] Zhang Longxiang. Security analysis of a RFID authentication protocol based on physically unclonable function [J]. Journal of Computer Applications, 2012, 32(8): 2280-2282 (in Chinese)
(张龙翔. 一种基于不可复制功能的 RFID 认证协议的安全性分析[J]. 计算机应用, 2012, 32(8): 2280-2282)

[16] Zhou Shijie, Zhang Zhen, Luo Zongwei, et al. A lightweight anti-desynchronization RFID authentication protocol [J]. Information Systems Frontiers, 2010, 12(5): 521-528

Wang Yue, born in 1982. Master, engineer. Her main research interests include information and telecommunication engineering, IoT security, information security.

Fan Kai, born in 1978. PhD, associate professor. His main research interests include IoT security, information security.