基于多证明者交互证明模型的RFID安全协议的研究

陆 尧 廖明宏 李贵林
(厦门大学软件学院 厦门 361005)

摘 要 RFID技术因其操作便捷等优点在当今得到广泛的应用,但是由于其安全模型的缺陷,使得RFID技术在高安全需求的领域仍未得到应用。提出了一个改进的适用于RFID的多证明者交互证明模型,其相对于单证明者交互模型具有更高的安全性。在此模型的基础上进一步提出了一个适用于分布式RFID环境的基于椭圆曲线门限秘密共享方案的RFID安全协议。经理论分析证明,该协议可以较好地解决克隆攻击、重传攻击、标签跟踪等几种常见的RFID安全问题。

关键词 RFID,安全模型,身份认证,安全协议
中图法分类号 TP309 **文献标识码** A

Research of Security Authentication Protocol of the RFID Based on the Multi-prover Model

LU Yao LIAO Ming-hong LI Gui-lin
(Software School of Xiamen University, Xiamen 361005, China)

Abstract RFID technology is widely used in today's society. However, due to the shortcomings of its security model, RFID technology is still not applied in some areas very well. We proposed a new RFID security model-RFID multi-prover model. It can compensate for deficiencies in the original model. We also proposed a security protocol based on this model. It can solve many RFID security problems, such as cloning attack, replay attack, tag tracking, and etc.

Keywords RFID, Security model, Identification authentication, Security protocol

1 引言

无线射频识别技术(Radio Frequency Identification, RFID)是一种利用射频通信实现的非接触式双向通信技术,可达到自动识别目标对象并获取相关数据的目的,可识别高速运动的物体并可同时识别多个目标,具有精度高、适应环境能力强、抗干扰性强、操作快捷等众多优点,在许多方面都有广泛应用。例如RFID可以应用于保险箱防盗系统中[1]。这些保险箱的控制系统嵌入了读写器(Reader),当用户开启保险箱时,读写器比较钥匙内嵌的标签(Tag)是否为保险箱的计算机所承认的合法标签。如果标签不能通过认证,则其控制系统不会开启。这就为保险箱的防盗增加了另一道安全措施。攻击者可以轻易仿制一把普通钥匙,但是他不能得到一个正确的标签,因此无法开启保险箱,这样就对安全起到了很好的保护作用。

不过因为信息安全问题的存在,RFID应用尚未普及到至为重要的关键任务中。因此我们认为对高安全需求的RFID技术的研究是必要的。如果能在理论上对高安全需求的RFID安全技术的研究有所突破,势必对RFID技术在新的领域开辟更有价值的应用起到积极的推动作用。

正是基于这样的认识,本文首先建立一个安全的RFID多证明者交互证明模型;进一步在此模型的基础上提出一个基于椭圆曲线门限秘密共享方案的RFID安全协议。

秘密共享[2,3]的基本思想就是把一个密钥拆分成多分,分开进行保管,这样可以防止系统密钥的遗失、损坏和攻击,减少密钥持有者包括个人或服务器的责任,同时可以降低对方破译密钥的成功率,显然要比只有单独一个密钥具有更高的安全性。

不妨假定这样的环境:不再是一个标签与读写器之间的验证,而是多个标签与读写器之间的验证。此时满足以下安全需求:1)单个标签无法通过验证,只有足够数量的标签互相合作才能通过验证;2)即使已知一个甚至多个合法标签的内容,也不能由此推断出或伪造成其他合法标签成员。本文称这种用来作为证明者的标签为证明者标签(Prover-tag)。这种涉及到多个标签验证的问题的模型即为RFID多证明者交互证明模型(Multi-prover Model)。显然,多证明者交互证明模型有其特殊的应用背景,而且相比单证明者交互证明模型更加具有安全性。

本文第2节介绍一些相关工作,包括介绍RFID多证明者模型以及系统合法成员。第3节详细介绍本文提出的RFID安全协议,包括具体的详细步骤及其证明。第4节针对RFID协议面临的主要安全问题,从理论上进行了安全性分

到稿日期:2010-06-12 返修日期:2010-11-14 本文受国家自然科学基金(60803148)资助。
陆 尧(1987—),男,硕士生,CCF会员,主要研究方向为信息安全、普适计算,E-mail:luyao_87@163.com;廖明宏(1966—),男,教授,博士生导师,主要研究方向为智能嵌入式软件、网络智能技术、普适计算;李贵林(1979—),男,博士,助教,主要研究方向为嵌入式软件、数据库与信息处理、无线自组网数据管理、传感器网络查询处理。

析及性能分析。

2 RFID 多证明者交互证明模型

目前针对 RFID 安全性机制所采用的方法主要有物理机制和密码机制两种[4]。物理机制包括消除标签数据(kill tag)、阻塞器标签(blocker tag)[5]、跳频通信技术(frequency hopping spread spectrum)等。但这些物理方法增加了额外的物理设备或元件,既不方便还增加了成本。

鉴于物理安全机制存在的种种缺点,在最近的 RFID 安全机制的研究中,学者们提出了许多基于密码技术的安全机制。例如 Sarma 等人的 Hash-Lock 协议[6]、Weis 等人的随机化 Hash-Lock 协议[7]、Henrici 等人的基于杂凑 ID 变化协议[8]、Juels 等人的重加密机制[9]、Lee 等人的防追踪和克隆的轻量级协议[10]、Burmester 等人的可组合的 RFID 安全认证机制[11]、Avoine 等人的基于树型结构的认证机制[12]、Castro 等人的强身份验证和完整性协议[13]、Lopez 等人的基于轻量级块密码的认证机制[14]等。

经过研究发现,这些协议都是基于单证明者交互证明模型[15],如图 1 所示。

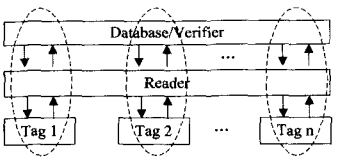

图 1 RFID 单证明者交互证明模型

然而,即使在对多个标签进行认证的情况下,单证明者交互证明模型中每个标签的认证过程仍是独立的。而多证明者交互证明模型(见图 2)与单证明交互证明者模型不同的是:单证明者交互证明模型的证明是由一个个体生成的,而多证明者交互证明模型的证明是由多个成员合作生成的。因此多证明者交互证明模型能够具有更高的安全性。多证明者交互证明模型和单证明者交互证明模型的验证都是由单个个体完成的。

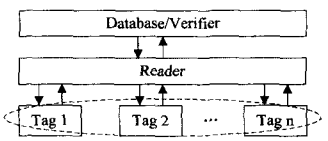

图 2 RFID 多证明者交互证明模型

由于 RFID 本身有其局限性:有限的计算能力、有限的存储空间、外形很小、电源供给有限等,所有这些特点和局限性使得设计者对密码机制的选择受到很多限制,也对 RFID 系统安全机制的设计带来了特殊的要求。

在本文的 RFID 模型系统中,将会有以下几个合法成员。

1)服务器:服务器是一个值得信赖的实体,知道和维护所有有关标签的信息,比如各个标签对应的公有密钥等。这里不妨假定服务器为物理安全的,不易受到攻击。为了简单起见,假设一个单一的逻辑服务器可以实现多个相关物理服务器的功能。

2)读写器:读写器是对标签进行读取和写入操作的设备。这里假定所有服务器和读写器之间的通信都是通过安全信道完成的。此外,服务器和读写器保持松散的时钟同步,两者都有足够的存储、计算和通信能力。

3)证明者标签:每个标签的密钥由两部分组成:一是群组密钥的子秘密,用来合成群组密钥;二是标签自身的密钥,用来标识标签身份。标签具有一定的存储、计算和通信能力。当证明者标签数量到达一定数量时,可以生成有效的签名,以通过验证单元的验证。

方案中把一个密钥拆分成若干子密钥,分别存储到各个标签中。使用的时候,只有多个标签合作才能生成合法的签名并通过认证。每个标签对消息使用自己的子密钥签名得到部分签名,签名合成者每次合成 t 个部分签名可获得整个签名。这样任何少于 t 个的部分签名均不能获得整个签名的任何信息;并且已知部分签名不能获得密钥和子密钥的任何信息。

4)验证单元:验证单元是最终认证单元,具有一定的存储、计算和通信能力,用来判断证明者标签是否通过认证。

下一节将对协议具体过程进行详细说明。

3 协议设计

3.1 符号和定义

使用表 1 所列符号来标识整个协议。

表 1 本文定义的一些符号和术语

T	RFID 标签	k	标签生成的随机数
R	RFID 读写器	m	待签名的消息
S	后台服务器	CA	可信中心
V	验证单元	DC	签名合成者
h()	单向 hash 函数	P	椭圆曲线上的一个基点
IDi	标签 T_i 的身份标识	Q_{pub}	组 L 的组公钥
L	组 $L=\{T_1,T_2,\cdots,T_n\}$ n 个证明者标签的集合	Q_i	每个 T_i 获得的组私钥的子秘密对应的公钥
B	L 中成员数为 t 的子集	X_i	每个 T_i 自身的私钥
SL	组 $L=\{T_1,T_2,\cdots,T_n\}$ 的组私钥	Y_i	每个 T_i 自身的私钥对应的公钥
s_i	每个 T_i 获得的组私钥的子秘密	C_i	Lagrange 插值系数

3.2 详细介绍

设计一个适用于分布式 RFID 环境下的基于椭圆曲线的门限签名方案的 RFID 安全协议。本协议同时具有门限签名方案的优点。下面对此进行详细介绍。

3.2.1 初始化阶段

在初始化阶段,设定逻辑服务器包含一个可信中心 CA 和一个指定的签名合成者 DC。CA 选取有限域 F_q 上一条安全的椭圆曲线 $E(F_q)$,保证该椭圆曲线的离散对数问题是难解的。在 $E(F_q)$ 上选一个基点 P,P 的阶数为 p(p 为一个大素数)。另外,CA 还选择一个单向 Hash 函数 $h()$。

令一组证明者的成员 $L=\{T_1,T_2,\cdots,T_n\}$ 是 n 个证明者的集合,令 B 为成员数是 t 的子集($B\subset L$,$\{B\}=t$)。对于任意的 $T_i\in B$,定义 Lagrange 插值系数 $C_i=\sum_{j=1,j\neq i}^{t}\frac{ID_j}{ID_j-ID_i}$。$ID_i$ 为证明者 T_i 的身份标识,是不等于零的正整数,且不同的签名者 T_i 具有不同的身份标识 ID_i,即当 $i\neq j$ 时,$ID_i\neq ID_j$。

设门限为 t,CA 随机产生 $t-1$ 次多项式:$f(x)=a_0+a_1x+\cdots+a_{i-1}x^{i-1}\in F_q(x)$,其中 $a_0=s_L$,$s_i=f(ID_i)$。CA 选取 s_L 作为组 $L=\{T_1,T_2,\cdots,T_n\}$ 的私钥,组 $L=\{T_1,T_2,\cdots,T_n\}$ 的公钥为 $Q_{pub}=s_LP\in E(F_q)$。分发秘密 s_L 给每个证明者标签。每个证明者 T_i 得到一个 s_i 作为他的子秘密。对应的验证公钥 $Q_i=s_iP$。每个 T_i 随机选择一个整数 $x_i\in F_q$ 作为他的私

钥，并公布对应的公钥 $Y_i=x_iP$。

由 $s_i=f(ID_i)$ 可知，在此方案中，当有新的证明者成员需要加入时，服务器只需要根据新成员提供的唯一公开身份 ID，计算标签的私钥发送给他即可，而系统和老成员的相关参数全都不用改动。当需要删除成员时，只需要将其 ID 通知为无效的 ID，因而整个系统能够具有较好的稳定性。

3.2.2 验证阶段

本协议的验证过程如图 3 所示。

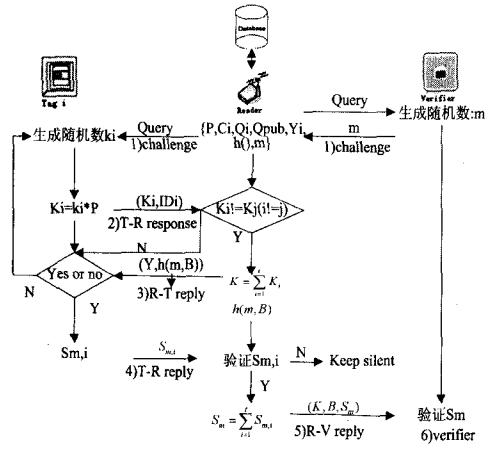

图 3 本协议的验证过程

步骤 1 challenge

服务器对验证单元发送 Query 请求，验证单元随机产生消息 m，并将 m 发送给服务器。同时读写器发送 Query 至证明者标签 T_i，作为认证请求。

步骤 2 T-R Response

证明者标签 $T_i(i=1,2,\cdots,t)$ 随机生成一个随机数 k_i，$1\leqslant k_i\leqslant p-1$，并计算 $K_i=k_iP$，将 (K_i,ID_i) 发送给读写器。

步骤 3 R-T Reply

读写器通过验证 $K_i\neq K_j(i\neq j)$ 来判断 T_i,T_j 是否选择了相同的随机数。如果 T_i,T_j 选择了相同的随机数，则读写器向标签 T_i 发送 Resend 信息，通知它们重新选取新的随机数并计算 K_i；否则读写器计算 $K=\sum_{i=1}^{t}K_i$。且令每个 $ID_i\in B$ 并计算 $h(m,B)$，将 $h(m,B)$ 发送给标签 $T_i(i=1,2,\cdots,t)$。

步骤 4 T-R Reply

证明者标签 $T_i(i=1,2,\cdots,t)$ 计算 $S_{m,i}=k_i+(C_is_i+x_i)h(m,B)$，将 $S_{m,i}$ 发送给读写器。本方案中证明者标签执行的计算只需要生成伪随机数及一次加密运算。

步骤 5 R-V Reply

读写器判断方程

$$S_{m,i}P-K_i=(C_iQ_i+Y_i)h(m,B) \tag{1}$$

是否成立。若所有 $S_{m,i}$ 都通过验证，绑定生成 S_m，$S_m=\sum_{i=1}^{t}S_{m,i}$。将 (K,B,S_m) 发送给验证单元。

由于标签 T_i 的部分签名是由私钥 s_i 和 x_i 加密而成的，因此可以利用 T_i 对应的公钥 Q_i 和 Y_i 解密来检验签名的有效性。

定理 1 如果方程(1)有效，则 $T_i(i=1,2,\cdots,t)$ 的部分签名有效。

证明：

$$\begin{aligned}S_{m,i}P-K_i&=[k_i+(C_is_i+x_i)h(m,B)]P-K_i\\&=k_iP+(C_is_i+x_i)h(m,B)P-K_i\\&=K_i+(C_is_i+x_i)h(m,B)P-K_i\\&=(C_is_i+x_i)h(m,B)P\\&=(C_is_iP+x_iP)h(m,B)\\&=(C_iQ_i+Y_i)h(m,B)\end{aligned}$$

步骤 6 Verifier

验证单元收到 (K,B,S_m) 后，检查方程

$$S_mP=h(m,B)(Q_{pub}+\sum_{i=1}^{t}Y_i)+K \tag{2}$$

是否成立。如果成立，则通过认证，否则认证失败。

由于门限签名由私钥 s_L 和 $\sum_{i=1}^{t}x_i$ 加密而成，因此可以利用其对应的公钥 Q_{pub} 和 $\sum_{i=1}^{t}Y_i$ 解密来验证门限签名的有效性。

定理 2 如果方程(2)成立，则门限签名 (K,B,S_m) 有效。

证明：

由 Lagrange 插值公式可知

$$s_L=\sum_{i=1}^{t}s_i\Big(\sum_{j=1,j\neq i}^{t}\frac{ID_j}{ID_j-ID_i}\Big)=\sum_{i=1}^{t}s_iC_i$$

则有

$$\begin{aligned}S_mP&=\sum_{i=1}^{t}S_{m,i}P=\sum_{i=1}^{t}[k_i+(C_is_i+x_i)h(m,B)]P\\&=\sum_{i=1}^{t}k_iP+\sum_{i=1}^{t}(C_is_i+x_i)h(m,B)P\\&=K+(\sum_{i=1}^{t}C_is_i+\sum_{i=1}^{t}x_i)h(m,B)P\\&=K+(s_LP+\sum_{i=1}^{t}x_iP)h(m,B)\\&=h(m,B)(Q_{pub}+\sum_{i=1}^{t}Y_i)+K\end{aligned}$$

本文特地使用标签自身的私钥 x_i 来标识各个标签，而不仅仅使用群密钥的子秘密。这样在验证时需要验证签名者的身份，就无法冒充其他成员进行签名。因此就不会出现这样的情况：任意 t 个成员合谋可以产生有效的门限签名，而不必承担任何责任(无法确定签名者的身份)。

如此一来，如果对方不能拥有多个证明者标签，就不能伪造签名；即使它收买了多个证明者标签，也不能伪造其他成员组的门限签名。日志会将每个访问者的 ID 都记录下来，可供日后查证之用。

4 分析

4.1 安全性分析

安全问题会出现在 RFID 标签、读写器、传输网络和数据存储等各个环节，但主要集中在标签与读写器的数据交换过程中。如图 4 所示，从 RFID 读写器到标签的前向信道(Forward Channel)和从标签到读写器的后向信道(Backward Channel)都是不安全信道。而在一般情况下，读写器和后台业务应用与管理系统之间的通讯是有线传输信道，可以认为是安全可靠的[16]。

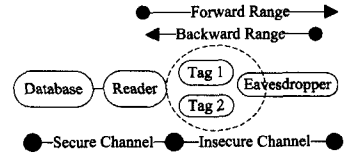

图 4 RFID 系统安全分析

因此，本文主要对标签与读写器之间的安全问题进行分析。下面根据文献[17,18]提出的几种 RFID 攻击进行分析。在本文的方案中，这几种攻击在理论上都能得到很好的解决。

(1)克隆攻击(Cloning Attack)

攻击者假冒读写器来克隆标签的响应，之后攻击者用该响应去响应合法的读写器，使得该合法的读写器误认为是真正的标签。而实际上真正的标签已经离去。通常来讲，解决克隆攻击问题的主要途径是执行认证协议和数据加密。

首先攻击者伪装成合法的读写器通过前向信道 $R \rightarrow T$ 向标签发送 Query 和 m。攻击者获取标签的响应(K_i，ID_i)和 $S_{m,i}$。

在下一次认证会话中，当真正合法的读写器发送 Query 时，攻击者通过后向信道 T→R 响应 $S_{m,i}$。

由于每一次认证会话中标签会产生新的伪随机数，即 $k_i \neq k_i'$，并且每一次认证会话中的 $S_{m,i} \neq S'_{m,i}$，标签使用其自身的密钥加密，别人无法获得，因此攻击者无法克隆合法标签进行克隆攻击。所以，本协议对克隆攻击具有安全性。

(2)重传攻击(Replay Attack)

攻击者通过中途截取读写器和标签之间通信的有效信号，而后将该有效信号在 RFID 系统中进行重传，从而对系统进行攻击。通常来讲，解决重传攻击问题需要用到挑战-响应机制，计时和计数的机制也经常用来抵御重传攻击。

在读写器通过前向信道向标签发送 Query 和 m 之后，攻击者获取标签的响应(K_i，ID_i)和 $S_{m,i}$。

在以后的认证会话中，攻击者通过后向信道响应(K_i，ID_i)和 $S_{m,i}$，从而对后端服务器发动重传攻击。

由于每一次认证会话中的 m 是 Verifier 随机产生的随机数，即 $m \neq m'$，不仅如此，加密时使用随机数 k_i 生成 $S_{m,i}$，即使在 m 相同的情况下每一次认证会话中的 $S_{m,i} \neq S'_{m,i}$，因此本协议对重传攻击具有安全性。

(3)跟踪攻击(Tracking Attack)

不同于前面的两种攻击，标签跟踪是一种对人有威胁的安全问题，攻击者通过标签的响应信息来追踪标签。因此，一个 RFID 系统应该满足不可分辨性和前向安全。不可分辨性是包含在 ID 匿名中的一个概念，意味着一个标签所发出的信息与其他标签所发出的信息具有不可分辨性。前向安全则是指，如果一个攻击者获取了该标签先前发出的信息，那么攻击者用该先前获取的信息不能够确定该标签。通常来讲，Hash 函数的随机特性和随机数被用来解决该类问题。

在伪装成合法的读写器通过前向信道向标签发送 Query 之后，攻击者获取标签的响应(K_i，ID_i)，并通过分析该响应来追踪发出该响应的标签。

由于在每一次认证会话中，标签都产生新的随机数 k_i，因此攻击者每次收到的标签的响应都不同。所以，本协议对追踪具有安全性。

4.2 性能分析

对于密码算法的 RFID 标签应用的选择准则包括以下两个方面[19,20]：安全性和硬件实现代价。密码算法的安全性包括算法抗密码分析的强度、稳定的数学基础、算法输出的随机性与其他算法比较的相对安全性；硬件实现代价主要包括实现芯片面积(或等效门数)、功耗和计算时间，是评估的另一个重要因素。

由于椭圆曲线加密算法所需的密钥长度较短，目前主流的看法是 163～283bits 长度即已基本满足要求，从而对芯片所能提供的计算资源要求较少，在存储时所需的内存和通讯时所需的带宽都较节约。目前与其它加密算法相比，椭圆加密算法在芯片晶体管数量较少、功率较小的某些设备上日益受到青睐。因此可以说椭圆加密算法是一个非常适合在 RFID 芯片上实现的公钥加密技术[21]。

本方案中标签运行的计算包括生成伪随机数和一轮椭圆曲线加密运算。因此在椭圆加密算法适用于 RFID 的前提下，提出用于实现 RFID 芯片与读写器之间的安全方案是完全可行的。具有相同安全性的密码算法所需的密钥长度对比如表 2 所列。

表 2　不同密码算法具有相同安全强度的密钥长度要求

Security (bits)	Symmetric Encryption Algorithm	Hash Algorithm	Mini Size of Public keys(bits)		
			DSA/DH	RSA	ECC
80	——	SHA-1	1024	1024	160
112	3DES	——	2048	2048	224
128	AES-128	SHA-256	3072	3072	256
192	AES-192	SHA-384	7680	7680	384

此外，椭圆曲线上双线性对的使用，能使方案以较短的密钥得到同等安全强度。另外，非超奇异椭圆曲线离散对数问题的难度远远超过有限域上离散对数问题(DLP)的难度，因而椭圆曲线密码可使用长度小得多的密钥，这样可使本文方案以更少的计算和传输量达到同等的安全要求。

结束语　RFID 技术有着传统技术不可比拟的优势，然而安全和成本这对不可调和的矛盾也正成为 RFID 技术面对的重要问题。由于安全和隐私的级数需要依赖于具体的应用，因此并不存在普遍适用的解决方案。而安全需求越高的应用，对硬件及成本的要求就越高。本文试图从软件的角度，通过安全模型的研究和安全协议的设计，提出一套安全性更高的 RFID 安全系统方案。本文主要工作有：

①提出一个改进的适用于 RFID 的多证明者交互证明模型，它比单证明者交互证明模型具有更高的安全性。

②提出一个适用于分布式 RFID 环境的基于椭圆曲线的门限秘密共享 RFID 安全协议。理论分析表明，该协议可以很好地解决克隆攻击、重传攻击、标签跟踪等常见的 RFID 安全问题。

受客观条件所限，该协议在实现方面还需要进一步优化和改进，以期将来能更加完善。随着电路制造工艺的不断提升，RFID 的生产成本将会越来越低，也就使得 RFID 标签上将会有越来越多的计算资源可用于安全方面，因此我们相信这个领域的研究会有更多的突破，也将开辟出新颖而有价值的应用领域。

参 考 文 献

[1] Thornton F, Haines B, Das A M, et al. RFID Security [M]. Canada: Andrew Williams, 2006: 69-71

[2] Shamir A. How to Share a Secret [J]. Communication of Association for Computing Machinery, 1979, 22(11): 612-613

[3] 李国文. 门限签名体制的研究[D]. 济南：山东大学，2007：54-55

[4] 周永彬，冯登国. RFID 安全协议的设计与分析[J]. 计算机学报，

2006,29(4):581-589

[5] Juels A, Rivest R, Szydlo M. The blocker tag: Selective blocking of RFID tags for consumer privacy [C]// Proc of the 8th ACM Conf on Computer and Comm Security. New York: ACM, 2003: 103-111

[6] Sarma S, Weis S, Engels D. RFID systems and security and privacy implications [C]// Proc of the 4th Int Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2002: 454-469

[7] Weis S A, Sarma S E, Rivest R L, et al. Security and privacy aspects of low-cost radio frequency identification systems [C]// Proc of the 1st Security in Pervasive Computing. Berlin: Springer, 2003: 201-212

[8] Henrici D, Mauller P. Hash-based enhancement of location privacy for radio-requency identification devices using varying identifiers [C]// Proc of the 2nd IEEE Annual Conf on Pervasive Computing and Communications Workshops. Los Alamitos, CA: IEEE Computer Society, 2004

[9] Juels A, Pappu R. Squealing euros: Privacy-protection in RFID-enabled banknotes [C]// Proc of the Financial Cryptography. Berlin: Springer, 2003: 103-121

[10] Lee Y-C, Hsieh Y-C, You P-S, et al. A New Ultralightweight RFID Protocol with Mutual Authentication [C] // Proc. of WASE09. Volume 2. ICIE. 2009: 58-61

[11] Burmester M, Van Le, De Medeiros T, et al. Universally composable RFID identification and authentication protocols [J]. ACM Trans. Inf. Syst. Secur, 2009, 12(4): 21-33

[12] Avoine G, Tchamkerten A. An Efficient Distance Bounding RFID Authentication Protocol: Balancing False-acceptance Rate and Memory Requirement [C] // Information Security Conference-ISC09. volume 5735 of Lecture Notes in Computer Science, Pisa, Italy, 2009

[13] Hernandez-Castro J C, Tapiador J M E, Peris-Lopez P, et al. Cryptanalysis of the SASI Ultralightweight RFID Authentication Protocol with Modular Rotations [C]// Proc. of WCC'09. Lofthus, Norway, 2009: 10-15

[14] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. Shedding. Some Light on RFID Distance Bounding Protocols and Terrorist Attacks [C]// arXiv. org. Computer Science, Cryptography and Security, 2009

[15] Ben-or M, Goldwasser S, Kilian J, et al. Multi-prover Interactive Proofs: How to Remove Intractability Assumptions [C]// 20th ACM Symposium on the Theory of Computing. Chicago: Ilion is Association for Computing Machinery, 1988

[16] Rhee K, Kwak J, Kim S, et al. Challenge-response based RFID authentication protocol for distributed database environment [C]// Proc of the 2nd Int Conf on Security in Pervasive Computing. Berlin: Springer, 2005: 70-84

[17] 丁振华,李锦涛,冯波. 基于 hash 函数的 RFID 安全认证协议研究[J]. 计算机研究与发展, 2009, 46(4): 583-592

[18] Lee S. Mutual authentication of RFID system using synchronized secret information [D]. Daejeon, Korea: School of Engineering, Information and Communications University, 2005

[19] 高磊. 基于椭圆曲线密码的 RFID 安全协议[D]. 上海:上海交通大学, 2007: 45-46

[20] Wolkerstorfer J. Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags? [C]// Workshop on RFID and Lightweight Crypto. Graz, Austria, 2005

[21] 刘丹. 基于 ISO 18000-6C 协议的 RFID 安全标签的研究与开发[D]. 复旦大学, 2009: 35-37

(上接第 59 页)

[4] Goldsmith A, Wicker S. Design Challenges for Energy-constrained Ad Hoc Wireless Networks[J]. IEEE Communi-cations, 2002, 9(4): 8-27

[5] Rugin R, Mazzini G. A simple and efficient MAC-routing integrated algorithm for sensor network [C]// 2004 IEEE Int'l Conf. on Communications. 2004: 3499-2503

[6] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor net_works[A]// Proc. of the 33rd Annual Hawaii Int'l Conf. on System Sciences[C]. IEEE Computer Society, 2000: 3005-3014

[7] Heinzelman W R, Chandrakasan A, Balakrishnan H. An Application-specific Protocol Architecture for Wireless Micro_ sensor Networks[J]. IEEE Trans on Wireless Communications, 2002, 1(4): 660-670

[8] Younis O, Fahmy S. HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks [J]. IEEE Transactions on Mobile Computing, 2004, 3(4): 336-379

[9] Bandyopadhyay S, Coyle E J. An Energy Efficient Hierar_chical Clustering Algorithm for Wireless Sensor Networks [A]// INFOCOM Communications Societies[C]. IEEE, 2003: 1713-1723

[10] 李成法,陈贵海,叶懋,等. 一种基于非均匀分簇的无线传感器网络路由协议[J]. 计算机学报, 2007, 30(1): 27-36

[11] Gungor V C, Vuran M C, Akan O B. On the cross-layer interactions between congestion and contention in wireless sensor and actor networks[J]. Ad Hoc Networks, 2007, 5: 897-909

[12] Bai Yuebin, Liu Shujuan, Sha Mo, et al. An Energy Optimization Protocol Based on Cross-Layer for Wireless Sensor Networks [J]. Journal of Communications, 2008, 3(6): 27-34

[13] Lin Xiao-hui, Kwok Y-K, Wang Hui. Cross-layer design for energy efficient communication in wireless sensor networks [J]. Wirel. Commun. Mob. Comput., 2009, 9: 251-268

[14] Bouabdallah F, Bouabdallah N, Boutaba R. Cross-Layer Design for Energy Conservation in Wireless Sensor Networks [A]// IEEE International Conference on Communications (ICC '09) [C]. 2009, 6: 1-6

[15] Sohrabi K, Gao J, Ailawadhi V, et al. Protocols for self-organization of a wireless sensor network[J]. IEEE Personal Communications, 2000, 7(5): 16-27

[16] CC1000 A unique UHF RF Transceiver [EB/OL]. http://focus. ti. com/lit/ds/symlink/cc1000. pdf

[17] http://www. omnetpp. org

[18] Galluccio L, Leonardi A, Morabito G, et al. A MAC/Routing cross-layer approach to geographic forwarding in wireless sensor networks[J]. Ad Hoc Networks, 2007, 5: 872-884