·安全技术· 文章编号：1000-3428(2016)08-0107-05 文献标志码：A 中图分类号：TP309

移动网络中隐私保护的付费机制

鲍传松，许 艳，黄丛林

（安徽大学 计算机科学与技术学院，合肥 230601）

摘 要： 由于无线网络的开放性，在移动设备和服务器的交互过程中可能存在用户身份及服务信息的隐私泄露问题。为此，提出一种保护移动网络中用户隐私的付费机制。服务器采用密文策略属性加密方法向用户发送请求结果，相比采用传统加密方法更加高效。使用假名实现多用户联合请求某一种或多种服务，在实现隐私保护同时降低用户的成本。分析结果表明，该机制能够保护用户身份隐私，实现通信安全，降低服务器端的计算和通信代价。

关键词： 移动社交网络；移动用户；隐私保护；付费服务；属性加密

中文引用格式： 鲍传松，许 艳，黄丛林. 移动网络中隐私保护的付费机制[J]. 计算机工程，2016，42(8)：107-111，116.

英文引用格式： Bao Chuansong，Xu Yan，Huang Conglin. Privacy-preserving Payment Mechanism in Mobile Network[J]. Computer Engineering，2016，42(8)：107-111，116.

Privacy-preserving Payment Mechanism in Mobile Network

BAO Chuansong，XU Yan，HUANG Conglin

（School of Computer Science and Technology，Anhui University，Hefei 230601，China）

【Abstract】 Due to the openness of wireless network，user identity and service information may leak in the interaction between mobile devices and servers. Therefore，this paper puts forward a payment mechanism to protect the privacy of mobile network users. In this mechanism，servers adopt the method of Ciphertext Policy Attribute Based Encryption（CP-ABE）to send results to users，which is more efficient than using the traditional encryption method. Furthermore，by using pseudonyms，multiple users can make an joint request to get one or more services，which reduces the cost for users while protecting their privacy. Analysis results show that the mechanism can protect the privacy of user identity，realize secure communication，and reduce the cost of server-side computation and communication.

【Key words】 mobile social network；mobile user；privacy-preserving；paid service；attribute encryption

DOI： 10.3969/j.issn.1000-3428.2016.08.020

1 概述

随着移动设备的普及，越来越多的用户选择使用移动终端来获取服务。从市场角度看，服务通过移动网络技术提供给移动设备端有着很大的市场需求。因此，为移动设备提供高效、便捷和清晰的数据访问服务有着重要的实际应用价值。然而，由于无线网络的开放性，使用移动终端来获取服务可能存在安全隐患，如何安全可靠地享受移动服务是隐私保护领域的研究热点。文献[1-2]提出 k-匿名模型，之后，已有学者采用 k-匿名的方式[3-5]来单独访问服务器获取服务，这种方式虽然简便，但是没有实现用户利益最大化。文献[6]提出在移动支付模式下设计签名方案来保证移动支付的公平性和不可抵赖性。

目前，服务提供商除了提供多种不同性质的免费服务，也有专门为付费用户提供的付费服务。如何安全提供移动付费服务，并实现用户利益最大化是本文的研究内容。例如移动用户向服务器请求某一需付费的学术论文，该用户为了降低费用，可以广播该项请求，有相同需求的用户就会聚合起来，一起向服务器请求，平摊服务费用。本文机制将实现多用户联合请求某种付费服务，以降低用户成本，同时考虑用户的隐私保护问题。

基金项目： 国家自然科学基金资助项目(61173188)；安徽省科技攻关计划基金资助项目(1401b042015)；安徽省高校自然科学研究基金资助重点项目(KJ2013A017)。

作者简介： 鲍传松(1990－)，男，硕士研究生，主研方向为网络与信息安全；许 艳，博士；黄丛林，硕士研究生。

收稿日期： 2015-06-30 **修回日期：** 2015-08-10 **E-mail：** chuansong06@163.com

在属性加密机制[7]中,只有属性集合满足访问控制策略的用户能够进行正确解密操作,具有细粒度访问控制的能力,特别适用于本文研究场景。文献[8]提出密钥策略属性加密方案(Key Policy Attribute Based Encryption,KP-ABE),密文和属性集合关联,而用户密钥和访问结构树相关。2007 年,文献[7,9]分别提出更接近实际访问控制系统的密文策略属性加密(Ciphertext Policy Attribute Based Encryption,CP-ABE)。在 CP-ABE 中,密文关联访问结构,而用户密钥由属性集合决定。

属性加密已广泛用于安全访问控制。文献[10]提出基于 CP-ABE 算法的云存储数据访问控制,在服务提供商不可信的前提下,保证在开放环境下云存储系统中数据的安全性。文献[11]基于属性加密方案提出社交网络中用户隐私保护方案。该方案能够保证移动用户的位置隐私。文献[12]基于属性加密提出了一个分布式认证系统,可用于移动医疗系统中为患者提供医疗服务,同时保护患者身份隐私。文献[13]提出一个更加灵活的属性加密方案,使用户能够独立地对数据加密,并且不需要依赖在线的可信机构,采用代理重加密和延迟重加密技术保护用户隐私。文献[14]使用属性加密来保护面向社交网络的隐私保护方案,该方案能够避免社交网络服务提供商与系统内部非授权用户的合谋攻击,且不泄漏用户的任何属性信息。

本文基于属性加密方案设计一个多用户联合请求付费服务的隐私保护机制,以有效保护用户隐私,同时减少用户的访问代价。在该机制中,服务器仅需使用一次属性加密即可实现多个用户服务的传递,减少服务器的计算代价和通信代价。

2 预备知识

2.1 双线性对映射

假设 G 和 G_T 是椭圆曲线上点所构成的 q 阶循环群(q 是一个大素数),g 是 G 的生成元,则映射 e:$G\times G\rightarrow G_T$ 称为这 2 个循环群之间的一个双线性对[15],具备如下 3 个性质:

(1)双线性性:对于所有的 $g_1,g_2\in G$ 和 $a,b\in Z_q^*$,满足 $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$。

(2)非退化性:$e(g,g)\neq 1$。

(3)可计算性:在有效的算法,对于任意的 $g_1,g_2\in G$ 能够计算出 $e(g_1,g_2)$。

2.2 密文策略属性加密

在密文策略属性加密[9]中,密文对应于一个访问结构,而密钥对应于一个属性集合,当且仅当属性集合中的属性能够满足此访问结构时即可解密。在该加密系统中,首先 TA 运行安全参数生成主密钥 MK 和公钥 PK,然后数据拥有者构造访问控制属性树 Γ,把访问者需要访问的数据 m 加密成密文 CT,数据访问者将自己的属性提交给可信中心,可信中心根据用户的属性产生密钥 SK 发给用户,用户使用密钥来解密密文 CT。

2.3 网络模型

本文方案的系统模型如图 1 所示。

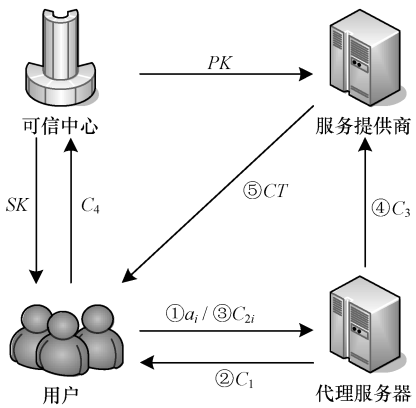

图 1 本文系统模型

本文方案主要由 4 个实体组成,即可信权威机构(Trusted Authority,TA)、移动用户(Mobile Users)、服务提供商(Server Provider,SP)、代理(Proxy)。TA 用于系统初始化以及各参与方产生纠纷时进行仲裁。移动用户通过代理向 SP 请求服务。移动用户的属性和身份信息在注册时提交给 TA,TA 为移动用户生成私钥。SP 是服务提供商,为移动用户提供服务。Proxy 用于收集移动用户的请求,并转发给 SP。

本文做以下假设:

(1)移动用户和服务提供商遵守服务规则,但具有好奇心。

(2)代理通过 TA 认证,具有很高的可信度。

(3)所有参与用户都需要在 TA 中注册。

2.4 设计目标

本文模型主要用于移动用户在向服务提供商请求服务时,SP 能够准确有效地提供服务,同时减少服务器的计算代价,最大程度上保护移动用户的隐私,提高服务质量,降低移动用户请求服务的代价。同时保护移动用户的身份隐私,通信信息的安全,使其达到匿名性、非关联性、防伪造攻击和防合谋攻击。

2.5 符号描述

本文方案所使用的符号描述如表 1 所示。

表 1　符号描述

符号	描述
SP'	CP-ABE 的主密钥
PK	服务提供商使用 CP-ABE 的公钥
CT	CP-ABE 中的密文
SK	CP-ABE 中的密钥
PID_{ij}	移动用户 U_i 的假名
a_i	U_i 请求
C_1	用户请求组
C_{2i}	参与聚合 U_i 请求
p_i	U_i 价格承诺
C_3	聚合请求
C_0	带有属性的请求
T	访问控制结构
j_i	U_i 的属性
p_l	L 服务价格

2.6　风险模型

移动用户是随机的,一旦有移动用户请求服务,移动用户就遵守协议规则,但可以观察收集其他移动用户隐私的信息。增加一个半可信的代理来集中所用移动用户的请求服务。

3　本文方案

3.1　系统初始化

TA 输入安全参数 λ,生成素数 q,设 G 是 q 阶加法循环群,G_T 是 q 阶乘法循环乘法群,g 是 G 的生成元。双线性映射 $e: G \times G \rightarrow G_T$,选取哈希函数 $H: \{0,1\}^* \rightarrow Z_q$。TA 选择一个安全对称加密算法 Enc,如 AES,选择 2 个随机参数 $\alpha, \beta \in Z_q$,计算 $h = g^{\beta}, f = g^{1/\beta}$。

TA 选择随机数 $s \in Z_q^*$,计算 $P_{\text{pub}} = g^s$。公开系统参数 $\{q, g, G, G_T, e, e(g,g)^{\alpha}, h, f, P_{\text{pub}}\}$ 保密系统主密钥 $MK = (\beta, g^{\alpha})$。移动用户 u_i、服务提供商和代理初始化时使用非对称加密 RSA 算法生成各自的公私钥,公开公钥并保存私钥。

3.2　用户私钥的产生

用户私钥的产生过程如下:

(1)移动用户 u_i 向 TA 提交真实的用户名 ID_i 和属性集合 s_i。

(2)TA 选随机数 r_{ij} $(j = 1, 2, \cdots)$,计算 $s_0 = H(s)$ 和 $PID_{ij} = Enc_{s_0}(ID_i \| r_{ij})$。用户 u_i 的假名为 $PID_i = \{PID_{i1}, PID_{i2}, \cdots\}$。随后 TA 通过可信通道把假名发送给 u_i。

(3)TA 执行以下步骤,生成 u_i 的私钥:

1)TA 选择随机数 $r \in Z_q$,为每个属性 $j \in S$ 选择随机数 $r_j \in Z_q$。

2)TA 计算 $D = g^{(\alpha + r)/\beta}$,为每个属性计算 $D_j = g^r \cdot H(j)^{r_j}, D'_j = g^{r_j} (j \in S)$。

3)TA 将 $SK = (D, D_j, D'_j)$ 作为 u_i 的私钥,秘密地发送给 u_i。

3.3　通信过程

不失一般性,假设用户 u_1 请求收费服务 l。

(1)u_1 首先向周围用户广播请求 l 服务的信息。随后,计算服务请求 $a_1 = E_{pk_p}(l \| PID_{1j} \| t_l \| k)$ 并发送给 Proxy。其中,pk_p 为 Proxy 的公钥;t_1 为该请求的有效时间;k 为用户请求聚合时的最少用户数。

(2)用户 u_i 收到 u_1 的服务请求广播后,如果也想请求服务 l,那么向 Proxy 发送服务请求 $a_i = E_{pk_p}(l \| PID_{ij} \| \varepsilon_{ij})$,其中,$\varepsilon_{ij}$ 为随机数。

(3)Proxy 统计时间 t_1 内收到的用户请求数 k_l,若满足 $k_l \geqslant k$,则计算 $C_1 = Sig_{sk_p}(l \| k_l \| H(PID_1 \| \varepsilon_{1j}) \| H(PID_2 \| \varepsilon_{2j}) \| \cdots \| H(PID_{k_l} \| \varepsilon_{kjl}))$ 并广播,其中,sk_p 为 Proxy 的私钥。

(4)用户 u_i 收到 C_1 后,若 u_i 请求 l 服务,计算 $C_{2i} = E_{pk_p}(l \| PID_i \| \varepsilon_{ij} \| E_{pk_s}(j_i \| p_i))$ 并发送给 Proxy。其中,pk_s 为 SP 的公钥;p_i 为用户 u_i 为请求服务 l 所付费用。

(5)Proxy 收到 k 个用户请求后,比较同一用户 2 次请求时的随机数 ε_{ij} 是否相同,如果相同,那么整合 $C_3 = E_{pk_s}(l \| E_{pk_s}(j_1 \| p_1) \| E_{pk_s}(j_2 \| p_2) \| \cdots \| E_{pk_s}(j_{k_l} \| p_{k_l}) \| t)$ 并发给 SP。其中,t 为时间戳,防止重放攻击。

(6)SP 收到 Proxy 发来的 C_3,执行如下操作:

1)计算所有用户为请求服务 l 所付费用 $P_l = \sum_{i=1}^{k_l} p_i$,并判断是否满足 SP 提供 l 服务的价格。

2)若满足,SP 根据所有请求 l 服务的用户属性集合生成访问结构 Γ,并使用该访问结构 Γ 对 l 服务的内容进行加密,得到加密消息 C,并广播。

(7)用户 u_i 收到 SP 广播的加密消息 C 后,如果 u_i 是合法的付费用户,则 u_i 的属性集合 S_i 能满足 SP 指定的访问结构 Γ,从而 u_i 能够正确地解密 C,从而获得请求的 l 服务的内容。

4　性能分析

4.1　用户隐私分析

移动用户在使用属性加密来实现传输过程中的信息安全,特别是用户隐私的安全。本文安全目标是用户真实身份的隐私安全、通信过程中信息的安全以及未付费的用户无法获得服务内容。

4.1.1 匿名性

移动用户 u_i 在注册时,向 TA 提交真实的用户名 ID_i,TA 计算用户的假名。对于用户 u_i 的其中一个假名 $PID_{ij}=Enc_{s_0}(ID_i\|r_{ij})$,其中,$r_{ij}$ 为随机数;$s_0=H(s)$;Enc 为 TA 保密的对称加密函数,除非攻破 TA,否则其他用户无法获得其 r_{ij} 和 Enc。用户使用假名通信,保护了用户的身份不被泄露,实现用户身份的匿名。

4.1.2 非关联性

移动用户每进行一次请求服务的通信,都会更换之前使用的假名 PID,用户在连续 2 次请求服务时使用不同的假名,这使得攻击者不能连续跟踪同一用户的 2 次请求,保障了用户身份的不可连接性。

4.1.3 防伪造攻击

参与合作的每个移动用户 u_i 都需要在 TA 上注册,来获取所需的假名 PID_i 和私钥 $SK=(D,D_j,D'_j)$。当攻击者 u'_i 冒充 u_i 来获取服务信息内容时,由于每个私钥都是使用不同的属性集合生成的,因此 u'_i 必须使用 u_i 的私钥 SK 来解密密文 C。实际上每个用户所拥有的私钥是唯一的,除非攻击者 u'_i 攻破 TA 或者 u_i,否则无法伪造用户 u_i 的私钥。

4.1.4 防合谋攻击

当多个未付费的用户一起来攻击付费用户 u_i 时,攻击者想要获取服务的内容,因而需要付费用户的私钥 SK,由于每个私钥都是使用不同的属性集合生成的,因此多个攻击者也无法确定他们所组合的属性集合是否为 u_i 的属性,除非攻击者攻破 TA 或者 u_i,否则无法伪造用户 u_i 的私钥。

4.2 费用分析

本文方案使用多用户联合向 SP 请求付费服务,实现了服务费用的均摊,从而能够减轻单个用户的费用负担。服务 l 的价格为 P_l,那么有 k 个用户联合请求该服务,则每个用户的费用为 P_l/k。随着用户增多,每个用户承担的服务费用将变小。

4.3 安全分析

4.3.1 防服务信息泄露的方法

在本文方案中,没有向服务提供商提供有效的属性和价格的用户是无法解密密文 CT。因为此时该用户的属性不满足服务提供商用于信息加密的属性树策略,从 TA 获得的私钥 SK 中的属性和服务提供商所产生的属性树 Γ 不匹配;同理,没有在 TA 授权的用户也无法解密密文。

4.3.2 防用户欺骗的方法

本文加入一个半可信代理服务器来转发信息,可以有效地防止移动用户的伪造信息,即可以防止发起者匿名自己的请求。若没有采用代理服务器,u_i 在发起请求 l 服务时,其他 $k-1$ 个用户把请求消息发给 u_i,此时 u_i 可以隐藏自己的请求,公告请求用户个数为 $k-1$,这样就可以免费得到 l 服务,加入代理服务器之后,则可以有效地防止此类攻击的发生。

4.3.3 防重放攻击的方法

在每次请求服务时,代理向服务提供商发送带有时间戳 t 的消息,这样使得每次请求具有时效性。服务提供商每次收到代理发来的用户请求时都会检查请求中的时间戳 t 是否有效,如果有效,则执行用户请求的要求;否则丢弃该条消息。

4.3.4 防推断攻击的方法

对于攻击者是一个聪明的对手,拥有大量的数据集。在理想的条件下,攻击者获得某一用户 u_i 的假名 PID_i。假设在一次通信过程中,攻击者会获得 Proxy 广播的签名 C_1,使用 Proxy 公钥来获得参与通信的服务类型 l 和人数 k_l。攻击者伪装合法用户 u_i,使用 u_i 假名 PID_i 向 Proxy 发送请求 $C'_{2i}=E_{pk_p}(l\|PID_i\|\varepsilon'_{ij}\|E_{pk_s}(j_i\|0))$,Proxy 收到 C'_{2i}的消息后,根据假名 PID_i 判断 2 次的随机数是否相同,即 $\varepsilon_{ij}=\varepsilon'_{ij}$是否成立,若成立,则为同一用户,接收其所包含的信息;否则丢弃该数据包。攻击者无法准确获取用户 u_i 参与通信的随机数 ε_{ij},因此,攻击者无法采用这种攻击方法来获取服务信息。

假设攻击者在某一位置长期监听移动用户参与合作的信息,获得丰富的加密数据,攻击者根据这些数据来获取服务信息,则需要破解 RSA 算法或者 CP-ABE 算法,来攻破 Proxy 或者 SP。RSA 算法的理论基础是一种特殊的可逆模指数运算,它的安全性是基于分解大整数的困难性,只要选择足够长的密钥,对于当前的计算机水平,选择 1 024 位长的密钥(相当于约 300 位十进制数字)就可认为是无法攻破的。属性加密算法的安全性是建立在判定双线性 Diffie-Hellman(DBDH)困难问题上,CP-ABE 算法在此基础上采用访问控制属性树 Γ 的策略,因次,攻击者必须获得 Γ 才能破解 CP-ABE 算法,这使得攻击者需要攻破 SP,是困难的。因此,攻击者无法获得移动用户私钥来获取服务信息,保障了通信信息的安全。

4.4 效率分析

本文方案的部分功能使用 C++仿真模拟,在仿真实验中每个移动用户都能计算数据以及相互交流。假设有 100 个移动用户分布在 $S=\{1\ km\times1\ km,1.5\ km\times1.5\ km\}$ 的区域内,分别代表用户稀疏的区域和用户稠密区域,每个用户的移动速度 $v=\{1,2\}$ m/s,在 S 区域内按照点模型移动,每个用户的通信半径 $tr=50$ m,评估移动用户向代理发送服务请求时达到 k-匿名的等待时间。假设移动用户在该区域需要请求服务的概率为 p 为 25% 。假设用

户 u_1 在时刻为 0 时停止移动并广播请求服务信息，之后其他用户 u_i 收到请求并停止移动，向代理发送同样的请求消息。

在不同的参数设置下进行仿真实验，每次运行 30 min，平均结果运行 1 000 次。图 2 显示了在请求合作过程中参与用户的数量 k 与等待时间之间的关系。从图中可以看到，在同等密度区域的条件下与相同的等待时间内，用户移动的速度越大参与合作用户数量 k 的数量越多。在相同的速度条件下，在某一区域内用户的密度越大参与合作用户数 k 的数量越多。

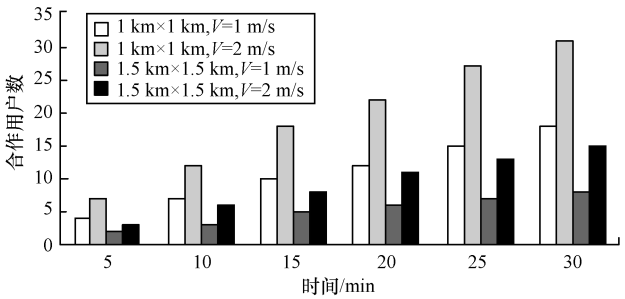

图 2　代理收到参与用户数 k 与时间的关系

系统中服务提供商使用 CP-ABE 加密算法进行一次加密即可完成所有用户需要的信息密文，不需要给每个用户单独加密减轻了服务提供商端的计算代价和通信代价。CP-ABE 加密算法的主要时间开销来自于属性树的增加，即随着属性的增加，构造访问控制属性树 Γ 的时间也随之增加，因此，服务提供商加密的时间也随之增加。

通过仿真实验来验证服务提供商在属性加密过程中的计算时间。实验平台是 Window7 系统，处理器为 Intel(R) Core(TM) i5-4430 CPU 3.00 GHz，内存 RAM 为 4.00 GB。在 MyEclipse10 编译平台下使用 Java 编写代码，代码使用基于双线性加密(jPBC)库版本 jPBC-API 2.0.0 控制策略来仿真实验。为了减少实验误差，所有的仿真数据都经过 200 次实验取平均值，如图 3 所示服务提供商属性加密计算时间，可以看出，随着略增加的属性数量，本文方案的计算时间增加得较为缓慢。

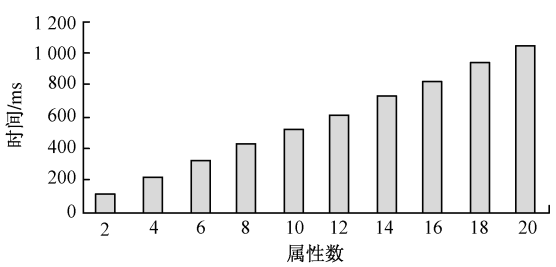

图 3　服务提供商属性加密计算时间

5　结束语

随着移动设备的普及，移动用户使用移动设备联合获取服务的方式能够使用户利益最大化。但难免存在隐私泄露等安全问题。本文提出使用假名来实现多用户联合请求某一种或多种服务，在降低用户成本的同时实现隐私保护。分析结果表明，使用 CP-ABE 算法，能够减少服务提供商的计算开销和通信代价，同时说明了在攻击者拥有大数据集的情况下本文方案仍然是安全的。下一步将研究基于多种属性无代理的用户隐私保护方案。

参考文献

[1] Sweeney L. K-anonymity: A Model for Protecting Privacy[J]. International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, 2002, 10(5): 557-570.

[2] Samarati P. Protecting Respondents Identities in Microdata Release[J]. IEEE Transactions on Knowledge and Data Engineering, 2001, 13(6): 1010-1027.

[3] Um J H, Kim Y K, Lee H J, et al. K-nearest Neighbor Query Processing Algorithm for Cloaking Regions Towards User Privacy Protection in Location-based Services[J]. Journal of Systems Architecture, 2012, 58(9): 354-371.

[4] Liu Xinxin, Liu Kaikai, Guo Linke, et al. A Game-theoretic Approach for Achieving K-anonymity in Location Based Services[C]//Proceedings of IEEE INFOCOM'13. Washington D. C., USA: IEEE Press, 2013: 2985-2993.

[5] Lu Rongxing, Lin Xiaodong, Shi Zhiguo, et al. PLAM: A Privacy-preserving Framework for Local-area Mobile Social Networks[C]//Proceedings of IEEE INFOCOM'14. Washington D. C., USA: IEEE Press, 2014: 763-771.

[6] Lan T. Secure Mechanism Based on Concurrent Signature for Mobile Payment Services[C]//Proceedings of the 3rd IEEE International Conference on Communication Software and Networks. Washington D. C., USA: IEEE Press, 2011: 435-438.

[7] Bethencourt J, Sahai A, Waters B. Ciphertext-policy Attribute-based Encryption[C]//Proceedings of EEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2007: 321-334.

[8] Goyal V, Pandey O, Sahai A, et al. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2006: 89-98.

[9] Cheung L, Newport C. Provably Secure Ciphertext Policy ABE[C]//Proceedings of ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2007: 456-465.

[10] 孙国梓，董　宇. 基于 CP-ABE 算法的云存储数据访问控制[J]. 通信学报，2011，32(7)：835-152.

(下转第 116 页)

5 结束语

本文针对认知无线电网络中存在恶意用户的情况,提出一种基于防伪码鉴定机制的数据伪造攻击检测方法。该方法为每个用户的感知信息都附加了一段防伪码来删除虚假信息,同时,为降低系统能耗,对防伪码长度进行了优化。仿真结果表明,该方法能有效提高存在恶意用户时网络的感知效率。本文方法是在假定报告信道误码率为定值的情况下进行的,时变误码率情况下认知无线电网络中恶意用户的检测将是下一步的研究方向。

参考文献

[1] Haykin S. Cognitive Radio: Brain-empowered Wireless Communications[J]. IEEE Journal on Selected Areas in Communications,2005,23(2):201-220.

[2] Mitola J, Maguire J G Q. Cognitive Radio: Making Software Radios More Personal [J]. IEEE Personal Communications,1999,6(4):13-18.

[3] Ghasemi A, Sousa E S. Spectrum Sensing in Cognitive Radio Networks: Requirements, Challenges and Design Trade-offs[J]. IEEE Communications Magazine,2008,46(4):32-39.

[4] Chen Qian, Motani M, Wong W C, et al. Cooperative Spectrum Sensing Strategies for Cognitive Radio Mesh Networks[J]. IEEE Journal of Selected Topics in Signal Processing,2011,5(1):56-67.

[5] Letaief K, Zhang Wei. Cooperative Communications for Cognitive Radio Networks[J]. Proceedings of the IEEE, 2009,97(5):878-893.

[6] Mu Hua, Tugnait J K. Joint Soft-decision Cooperative Spectrum Sensing and Power Control Multiband Cognitive Radios [J]. IEEE Transactions on Signal Processing,2012,60(10):5334-5346.

[7] Burbank J L. Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security [C]//Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications. Washington D. C., USA: IEEE Press,2008:1-7.

[8] Chen Ruiliang, Park J M, Hou Y T, et al. Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks[J]. IEEE Communications Magazine, 2008, 46(4):50-55.

[9] Wang Wenkai, Li Husheng, Sun Yan, et al. Securing Collaborative Spectrum Sensing Against Untrustworthy Secondary Users in Cognitive Radio Networks [J]. EURASIP Journal on Advances in Signal Processing, 2009,2010(1):1-15.

[10] Rawat A S, Anand P, Chen H, et al. Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks[J]. IEEE Transactions on Signal Processing,2011,59(2):774-786.

[11] Vempaty A, Agrawal K, Varshney P, et al. Adaptive Learning of Byzantines' Behavior in Cooperative Spectrum Sensing[C]//Proceedings of IEEE Wireless Communications and Networking Conference. Washington D. C., USA: IEEE Press, 2011:1310-1315.

[12] He Xiaofan, Dai Huaiyu, Ning Peng. Hmm-based Malicious User Detection for Robust Collaborative Spectrum Sensing[J]. IEEE Journal on Selected Areas in Communications,2013,31(11):2196-2208.

[13] Srinu S, Sabat S L. Cooperative Wideband Sensing Based on Cyclostationary Features with Multiple Malicious User Elimination [J]. AEU——international Journal of Electronics and Communications,2013,67(8): 702-707.

[14] 逄德明,胡 罡,徐 明. 基于能量指纹匹配的无线认知网络仿冒主用户攻击检测[J]. 计算机科学,2011, 38(3):28-33.

[15] Zhang Linyuan, Wu Qihui, Ding Guoru, et al. Performance Analysis of Probabilistic Soft SSDF Attack in Cooperative Spectrum Sensing[J]. EURASIP Journal on Advances in Signal Processing,2014,(1):1-9.

[16] Zhang Wei, Mallik R K, Letaief K. Optimization of Cooperative Spectrum Sensing with Energy Detection in Cognitive Radio Networks [J]. IEEE Transactions on Wireless Communications,2009,8(12):5761-5766.

[17] Kaligineedi P, Khabbazian M, Bhargava V K. Malicious User Detection in a Cognitive Radio Cooperative Sensing System[J]. IEEE Transactions on Wireless Communications,2010,9(8):2488-2497.

编辑 刘 冰

(上接第 111 页)

[11] Guo Linke, Zhu Xiaoyan, Zhang Chi, et al. Privacy-preserving Attribute-based Friend Search in Geosocial Networks with Untrusted Servers[C]//Proceedings of GLOBECOM'13. Washington D. C., USA: IEEE Press, 2013:629-634.

[12] Guo Linke, Zhang Chi, Sun Jinyuan, et al. PAAS: A Privacy-preserving Attribute-based Authentication System for eHealth Networks [C]//Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2012:224-233.

[13] Sun Wenhai, Yu Shucheng, Lou Wenjing, et al. Protecting Your Right: Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud[C]//Proceedings of IEEE INFOCOM'14. Washington D. C., USA: IEEE Press, 2014:226-234.

[14] 吕志泉,洪 澄,张 敏,等. 面向社交网络的隐私保护方案[J]. 通信学报,2014,35(8):23-32.

[15] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing [C]//Proceedings of CRYPTO'01. Berlin, Germany: Springer-Verlag, 2001:213-229.

编辑 刘 冰