一种适用于多跳认知无线电网络的高效IBE方案

于 雍[1,2] 雷凤宇[3] 秦玉化[3] 张沙沙[3]
(解放军理工大学通信工程学院 南京 210007)[1] (第二炮兵装备研究院 北京 100085)[2]
(解放军75741部队 广州 510510)[3]

摘 要 研究了认知无线网络的安全方案。针对认知无线网络存在的安全问题,结合网络的特点,提出了一种基于身份的安全解决方案,即Yu-IBE方案。该方案无需在线可信第三方即可实现认知节点的身份认证,其功能与PKI类似,但认证链却简单很多。该安全解决方案能通过较少的基础设施实现系统密钥的分发、密钥定期更换、域内及跨域通信等功能。将Yu-IBE总体安全解决方案与已有的两种知名数据融合方案进行了对比仿真,结果显示,Yu-IBE方案在所列攻击类型下均具有较好的稳定性,认知正确率始终保持较高水平。

关键词 认知无线网络,密码体制,基于身份的加密,公钥基础设施
中图法分类号 TP309 **文献标识码** A

Efficient and Provably Secure IBE Scheme Suitable for Multi-hop Cognitive Radio Networks

YU Yong[1,2] LEI Feng-yu[3] QIN Yu-hua[3] ZHANG Sha-sha[3]
(Institute of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China)[1]
(The Second Artillery Equipment Research Institute, Beijing 100085, China)[2]
(PLA UNIT 75741, Guangzhou 510510, China)[3]

Abstract Aiming at cognitive wireless network security issues and combining with the characteristics of the network, an identity-based security solution named Yu-the IBE scheme was proposed. The solution can realize cognitive node authentication without online trusted third party. Its function is similar with PKI, but certification chain is much simpler than the PKI. This security solution can realize the function of system key distribution, key regularly replace, domain and cross-domain communication with less infrastructure. In addition, this paper compared overall security solution of Yu-IBE with the existing two well-known data integration program. The simulation results show that the Yu-IBE program has better stability, and cognitive correct rate has remained relatively high level.

Keywords Cognitive wireless network, Cryptosystem, IBE, PKI

1 引言

随着信息技术和网络技术的发展,无线网络已经渗透到社会的各个领域,在现代社会经济发展中的战略作用越来越重要。无线技术的飞速发展,进一步促进了无线网络宽带化、高速化、异构化及泛在性。为了解决无线网络频谱资源利用率、异构网络标准化、网络用户接入以及网络管理等方面的问题,提出了认知无线电的思想。认知无线电作为一种新的学科领域,具有一系列的认知学习能力,如感知、分析、推理、自适应以及学习能力等,能进行频谱感知(Spectrum Sensing,检测可用频带、寻找频谱空洞)、频谱分析(Spectrum Analysis,对感知得到的频谱空洞特征进行分析)和频谱决策(Spectrum Decision,根据用户需求和频谱特征选择工作频段),可以解决固定频谱分配策略下对频谱资源利用率低的问题,在不影响主用户正常通信的情况下,动态地利用频谱资源,机会接入空闲频段,从而提高频谱使用效率。

由于认知无线电是无线通信的一种,因此它具有传统无线通信的所有安全问题,如非法授权访问、破坏数据完整性、无线信号被截获和篡改、冒充合法用户、干扰系统正常运行、传播网络病毒、线路侦听等[1-4]。此外,"认知"的引入带来了一些新的安全隐患,如模仿主用户攻击(PUE, Primary User Emulation)[1]、拒绝服务攻击、自私行为攻击[5]、集中式频谱策略数据库攻击、干扰主用户攻击[6]、公共控制信道干扰攻击等。因此,随着认知无线电技术的发展,信息安全就成为决定认知无线电应用前景的关键因素。

对认知无线电网络的研究是近年内才逐渐兴起的,目前国内外对认知无线电网络安全问题的研究尚处于初级阶段,成熟的解决方案较少,现有的认知无线电网络安全性主要依赖于通信机制的健壮性和可靠性。

文献[1]提出了一种检测PUE的方法,但该方法仅能检

到稿日期:2012-03-15 返修日期:2012-08-12 本文受"973"项目(2009CB320403),国家自然科学基金(60832008,60832006)资助。
于 雍(1982—),女,博士生,工程师,主要研究方向为认知无线网络,E-mail:free-sky@126.com;雷凤宇(1980—),女,博士,主要研究方向为公钥密码、可证明安全性、密码学理论和实践等;秦玉化(1979—),男,主要研究方向为公钥密码、数字签名、可证明安全性等;张沙沙(1974—),女,高级工程师,主要研究方向为密码学。

测攻击者的存在，没有完善的安全解决方案，对于如何预防、在检测到 PUE 攻击后如何找出并隔离攻击者无能为力。另外两种频谱感知技术：滤波器匹配和特征旋转检测同样不足以对抗 PUE 攻击。

针对控制信道的攻击行为，文献[7]提出了一种分布式协调机制，用户自组织成多个协调组，每个组用户协调使用一个控制信道，以防止由于控制信息拥塞造成通信中断，但是如果所有可用信道都阻塞，则该方案失败。文献[7,8]提出的检测攻击和确定攻击节点的方案可供借鉴，但是在多跳认知无线电网络环境下，需要进行大量的扩展和改进。在集中式认知无线电网络中，IEEE 802.22 提出使用安全子层保证对 MAC 帧提供机密性和身份认证[2]。但在多跳认知无线电网络中，由于无可信第三方进行密钥分发，安全问题面临更大挑战，需要有完善的密钥管理方案来解决这一难题。

2 一种基于身份的安全解决方案

在传统有线网络中，PKI 安全解决方案是 X.509 国际标准，已广泛应用于电子商务和电子政务等网络，但是 PKI 需要有固定的基础设施做支撑，而且需要有可信第三方负责密钥管理，其认证链非常复杂，无法应用于缺少固定基础设施保护的认知无线电网络，尤其是多跳式认知无线电网络。

1984 年，Shamir 提出了 IBE(Identity-based Encryption，基于身份的加密)的概念[9]，它和 PKI 公钥密码体系不同。IBE 方案以用户唯一身份标识信息如用户唯一的身份证号码、电子邮件地址等私人信息作为公钥进行加密，即发送方只要确认接收方的身份信息，就可实现身份认证。IBE 公钥密码方案可以实现与 PKI 等同的功能，且无需可信第三方即可实现密钥分发和身份认证，可为集中式或多跳式认知无线电网络提供完善的安全解决方案，适用于缺乏固定基础设施支持的认知无线电网络，尤其是多跳式认知无线电网络。

虽然 IBE 方案在系统结构和性能方面都具有巨大的优越性，但是由于其自身存在不完善的地方，一直没有得到实际应用。2001 年，Boneh 提出了第一个实用的 IBE 方案[10]，利用 MOV 规约的数学特点，提出双线性映射的概念，其有效地解决了 IBE 发展中长期面临的问题。2004 年，Boneh 又提出了两个 IBE 方案，并在标准模型下进行了安全性证明[11,12]。随后，Waters[13] 和 Gentry[14] 分别提出了两种综合效率更高的 IBE 方案，即它们不仅具有有效的规约，而且具有常数量的时间复杂度和密文长度。上述 IBE 方案已经具有实用性，但是无法直接应用于认知无线电网络，需要考虑以下问题：1)私钥安全分发问题，2)用户身份确认问题，3)密钥更换问题，4)大数据报文传输加密问题，5)各环节无缝对接问题。针对认知无线电网络中存在的安全问题和攻击方式，本文提出了一种实用的 IBE 安全解决方案，称之为 Yu-IBE 解决方案。

本方案中，只有少量的安全基础设施，称为认证中心，其由身份认证机构、密钥管理机构、权限管理机构 3 个分机构组成，其中，密钥管理机构只用于密钥分发，密钥分发完成后，设置为离线状态。

2.1 定义和前提假设

定义 1(身份认证机构) 负责验证用户身份，完成用户注册、注销等工作，并管理用户的唯一标识符。

定义 2(密钥管理机构) 为系统的核心机构，为合法用户生成与其唯一标识符对应的私钥，并完成密钥分发及定时更换。

定义 3(权限管理机构) 当认知节点在域间移动时，解决跨域授权问题，并确保合法用户在域内获得服务和资源的使用权限。

本方案基于以下假设：

(1)身份认证机构、密钥管理机构和权限管理机构均为可信机构；

(2)身份认证机构、密钥管理机构和权限管理机构之间相互信任；

(3)身份认证机构、密钥管理机构和权限管理机构之间通信为无缝连接，即 3 个机构之间为安全通信；

(4)认证中心掌握所有域认证中心的公钥信息，并能建立信任连接；

(5)经过身份认证机构认证的用户均为合法用户；

(6)本方案不讨论密码体制的安全性，其安全性为另一个领域论题。

该安全解决方案的体系结构如图 1 所示。

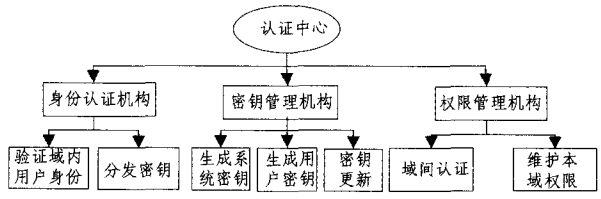

图 1 基于身份的安全方案体系结构

2.2 密钥分发过程

2.2.1 系统初始化

为了增加系统的可扩展性，本系统以域为单位进行管理。系统初始化需要对系统参数和域内用户参数进行初始化。

(1)系统参数初始化

选取有限域 $F_p(p>3)$，$a,b\in F_p$ 且满足 $4a^3+27b^2\neq 0(\mathrm{mod}\ p)$，设 $E:y^2=x^3+ax+b$ 为 F_p 上的椭圆曲线，则 E 为 $y^2=x^3+ax+b$ 同余式 $y^2\equiv x^3+ax+b$ 解 $(x,y)\in F_p\times F_p$ 的集合。

设椭圆曲线密码系统参数为：$T=(p,a,b,G,K_{pub},K_{id},K_{pr},q,n)$，其中 G 为椭圆曲线 $E(F_p)$ 上的基点，q 为 G 点的阶，$n=\#E(F_p)/n$($\#E$ 为椭圆曲线 E 上点的个数)，且满足：$\#E(F_p)\neq p$；$p^t\neq 1(\mathrm{mod}\ n)$，其中 $1\leqslant t<20$；$h\geqslant 4$，p,n 满足 $p=2\ \mathrm{mod}\ 3$ 且 $p=6n-1$；设随机数 $s\in Z_n^*$ 为密钥管理机构私钥，则其对应公钥为 $K_{pub}=s\cdot G$。假设身份认证机构和权限管理机构的唯一标识符分别为 ID_{id} 和 ID_{pw}，私钥分别为 s_{id} 和 s_{pw}，则对应的公钥分别为 $K_{id}=s_{id}\cdot G$，$K_{pw}=s_{pw}\cdot G$。

(2)用户参数初始化

认知节点(设为用户 U)接入认知无线电网络前，需提供唯一标识符及其他验证信息到身份认证机构注册认证。用户身份认证后，由身份认证机构激活该用户，为用户发放系统参数：$T=(p,a,b,G,K_{pub},K_{id},K_{pr},q,n)$，$U$ 选择一个随机数 $s_u\in Z_q^*$ 作为自己的私钥，用于将来与认证中心之间通信；然后根据系统给定的参数 T 计算出对应公钥 $K_U=s_u\cdot G$，并将 K_U 发送给身份认证机构保存。

2.2.2 认知节点身份验证

完成初始化后，各认知节点可以向认证中心请求发放私钥。由前提假设可知，身份认证机构、密钥管理机构和权限管理机构之间互相信任，为了确保密钥管理机构的绝对安全性，通常情况下该机构为离线状态，身份认证以及系统参数的发放等与认知节点直接交互的过程均由身份认证机构处理。在完成身份认证后，由密钥管理结构生成密钥，并由身份认证机构将其转发给认知节点，具体流程如下。

(1)认知节点 U 使用系统提供的参数 T 加密数据报 M，生成密文 C。

$$M=\{ID_{id},K_{id},F_{U_{id}},ID_U,K_U,t,w\}$$

式中，ID_{id} 为身份认证机构唯一标识符，$F_{U_{id}}$ 为认知节点所在域的标识，ID_U 为用户 U 的唯一标识符，K_U 为认知节点 U 的公钥(与认证中心之间通信用)，t 为时间戳，w 为功能代码，表示该报文功能为请求发放私钥。

由于该数据报 M 较短，可以直接使用身份认证机构提供的参数 T 加密数据报，生成密文 C。加密过程为：根据系统参数 T，利用身份认证机构的公钥 K_{id} 计算密文 $C=EC(M,K_{id},ID_{id},K_U)$，其中函数 EC 为椭圆曲线加密算法。认知节点 U 使用与认证中心通信的私钥 s_u 对密文进行签名，得到 $X=SIG_u(hash(C),K_U,ID_U)$。

(2)身份认证机构收到密文 X 后，通过 U 的唯一标识符 ID_U 在密钥分配表中查找对应的公钥，利用 U 的公钥验证其签名，并得到密文 C。身份认证机构再用自己的私钥 s_{id} 解密报文 C，得到明文 $M=DC(C)$，DC 为椭圆曲线解密函数，若解密成功，则确认；否则表示不成功，拒绝该密文。

解密后，身份认证机构依次验证域标识 $F_{U_{id}}$、接收者公钥 K_{id} 是否正确，判断认知节点 U 是否为合法用户。若验证通过，则表明身份验证成功；否则失败。

(3)验证认知节点 U 身份后，身份认证机构给该节点发送应答报文：$M_1=(ID_U,t,w_1,\alpha)$，其中 w_1 为功能代码，表示该报文为对私钥发放请求报文的应答报文；字段 α 表示结果，当 $\alpha=1$ 表示身份验证通过，$\alpha=0$ 表示身份验证失败。

同理，应答报文以密文的形式发送，加密和签名过程为：身份认证机构使用认知节点 U 与认证中心通信的公钥 K_U 加密报文 M_1，得到密文 $C_1=EC(M_1,ID_U,K_{id},K_U)$，并使用身份认证机构的私钥 s_{id} 进行签名，得 $X_1=SIGs_{id}(hash(C_1),K_{id},ID_{id})$，并将 X_1 发送给认知节点 U。

2.2.3 认知节点密钥生成及分发

身份认证机构安全地完成对认知节点 U 的身份认证后，若验证通过，则把节点 U 的请求发送给密钥管理机构，由密钥管理机构为节点 U 生成对应于其唯一标识符 ID_U 的私钥并发回给身份认证机构，由身份认证机构将密钥转发给认知节点。在本系统中，密钥管理机构只信任身份认证机构认证过的域内用户，并给受信任用户发放私钥。为了便于节点之间实现基于身份的认证，本系统结合 CPK(Combined Public Key，组合公钥)[15] 的思想，统一生成密钥种子矩阵(key seed matrix，密钥种子矩阵)，通信双方可以使用对方唯一标识符作为公钥实现身份认证。密钥生成和分发过程如下。

(1)密钥种子矩阵初始化

为了确保密钥的绝对安全性，密钥种子矩阵由密钥管理机构离线生成。矩阵每一个因子表示一个密钥变量，令矩阵为 $u\times v$ 矩阵(u 行 v 列)，则表示一共有 v 列，每列包括 u 个密钥变量。

1)密钥种子矩阵构建。由密钥管理机构生成 $u\times v$ 阶私钥种子矩阵 SK：

$$SK=\begin{pmatrix} r_{1,1} & \cdots & r_{1,v} \\ \vdots & \ddots & \vdots \\ r_{u,1} & \cdots & r_{u,v} \end{pmatrix}$$

式中，$r_{i,j}$ 在 Z_q^* 内随机选取。

与私钥种子矩阵对应的公钥种子矩阵为 PK：

$$PK=\begin{pmatrix} r_{1,1}\cdot G & \cdots & r_{1,v}\cdot G \\ \vdots & \ddots & \vdots \\ r_{u,1}\cdot G & \cdots & r_{u,v}\cdot G \end{pmatrix}$$

式中，私钥种子矩阵 SK 中的元素 r_{ij} 为随机数的集合，即私钥的集合，公钥种子矩阵中的元素则为与私钥 r_{ij} 对应的椭圆曲线 E 上的点 $r_{ij}\cdot G$。密钥管理机构生成公、私钥种子矩阵后，私钥种子矩阵需要绝对保密，公钥种子矩阵对外公布。

2)映射算法。密钥种子矩阵中，密钥管理机构采用映射算法计算认知节点的公/私钥对。本系统中，采用随机映射的方式。根据认知节点的唯一标识符计算出对应的映射值，在 $u\times v$ 矩阵中，每列均为 u 个元素，设映射算法为 $H_i(U_{id})$，其中 H_i 表示映射函数，可以是采用不同密钥的加密或散列函数，如 DES 或 AES 加密算法等；U_{id} 表示认知节点 U 的唯一标识符。则映射过程为：

$$H_1(U_{id}) \bmod u=maping(1)$$

$$H_2(U_{id}) \bmod u=maping(2)$$

$$\cdots\cdots$$

$$H_v(U_{id}) \bmod u=maping(v)$$

3)密钥计算。对用户唯一标识符映射后，可获得 v 个映射值，再根据映射值依次对应的元素计算出认知节点的公/私钥。设映射层次为 v，认知节点 U 的 v 个映射值 $maping(1)$，$maping(2),\cdots,maping(v)=(x_1,x_2,\cdots,x_v)$，对应每一列 k ($k=1,2,\cdots,v$)，分别取出对应私钥种子矩阵 SK 中第 x_k($k=1,2,\cdots,v$)行元素 $r_{x_k k}$，即该映射表示第一列的 x_1 行，第二列的 x_2 行，…，第 v 列的 x_v 行，可以根据私钥因子矩阵 SK 取出 v 个元素为：$r_{x_1 1},r_{x_2 2},\cdots,r_{x_v v}$。

认知节点 U 的私钥为：

$$S_k(U)=(r_{x_1 1},r_{x_2 2},\cdots,r_{x_v v}) \bmod u$$

式中，$S_k(U)$ 表示认知节点 U 的私钥。

当认知节点之间相互通信时，需要通过用户的公钥来进行加密或使用公钥验证对方的签名。计算用户公钥的方法与计算私钥方法一致。设要计算认知节点 U 的公钥，根据用户唯一标识符，通过映射算法 $H_i(U_{id})$ 计算出与认知节点 U 相对应的 v 个映射值：

$$maping(1),maping(2),\cdots,maping(v)=(x_1,x_2,\cdots,x_v)$$

同样，从公钥种子矩阵 PK 中取出对应于 $r_{x_1 1},r_{x_2 2},\cdots,r_{x_v v}$ 的 v 个公钥元素 $(r_{x_1 1}\cdot G,r_{x_2 2}\cdot G,\cdots,r_{x_v v}\cdot G)$。任何认知节点通过公开的公钥种子矩阵均可计算出用户 U 的公钥为：

$$P_k(U)=(r_{x_1 1}\cdot G+r_{x_2 2}\cdot G+\cdots+r_{x_v v}\cdot G)$$

由于椭圆曲线 E 上点的加法计算复杂度很低，因此计算 $v-1$ 次点的加法成本很低。

(2)密钥分发

1)密钥管理机构生成密钥。密钥管理机构收到身份认证机构发送的认知节点 U 的请求报文后，立刻计算该认知节点的唯一标识符，并从种子矩阵中查找管理机构将信息该认知节点的私钥 $S_k(U)$，为该私钥附上有效期 L_t，得到消息 $M=(S_k(U),L_t,\omega_2)$，其中 ω_2 为功能代码，表示此为密钥分发消息。密钥管理机构将信息传送给身份认证机构。

2)身份认证机构转发密钥信息。身份认证机构收到密钥管理机构发送的密钥信息后，加密消息 M 得密文 C：$C=EC(M,ID_U,K_U)$，并用身份认证机构的私钥签名得 $SIGs_{id}(hash(M),K_U,K_{id},ID_{id})$，并通过密文与签名得：

$\{EC(M,ID_U,K_U),SIGs_{id}(hash(C),K_U,K_{id},ID_{id})\}$

身份认证机构将信息发送给认知节点 U。

(3)密钥接收。认知节点 U 收到消息后，验证身份认证机构的签名，并用自己与认证中心之间通信的私钥 s_u 对其解密，以获得自己在认知节点之间通信的私钥 $S_k(U)$ 以及该私钥的有效期 $(S_k(U),L_t)=DC(C,s_u,K_U)$。

私钥的有效期 L_t 表示发放给该认知节点私钥的使用期限。使用到期后，密钥管理机构会自动更换所有可信用户的私钥。

2.3 密钥定期更换

密钥分发过程可以实现用户私钥的安全分发，但是为了确保私钥的绝对安全性，需要定期更换密钥。主要原因如下：

(1)椭圆曲线中，密钥的长度与密码的安全性成正比，但是与加解密、签名等操作时间成反比，即密钥越长越安全，但是时间复杂度越高，所以往往牺牲一定的安全性换取效率。

(2)密钥种子矩阵无法抵制合谋攻击，域内恶意用户越多，则私钥种子矩阵越可能暴露。

(3)随着时间的推移，敌手通过反复尝试，破解认知用户和系统私钥的可能性增加。

为此，引入密钥定时更换机制来确保密钥的绝对安全。密钥定时更换机制与密钥分发过程一致，即认证中心生成系统密钥，并生成相应的公/私钥种子矩阵，通过现有仍然有效的认知用户公钥加密，并附上系统签名，来安全地分发密钥。密钥定时更换流程如图 2 所示。

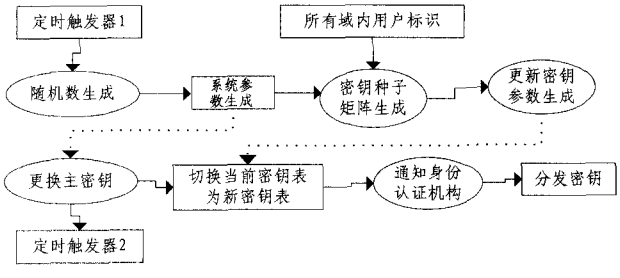

图 2 密钥定时更换流程

具体过程如下：

(1)密钥管理中心生成系统参数，即完成系统初始化过程。设椭圆曲线密码系统参数为：$T'=(p,a,b,G,K'_{pub},K'_{id},K'_{pr},q,n)$。

(2)认证管理中心生成新的密钥种子矩阵，即完成密钥种子矩阵初始化。设私钥种子矩阵为 SK'，公钥种子矩阵为 PK'，式中：

$$SK'=\begin{bmatrix} r'_{1,1} & \cdots & r'_{1,v} \\ \vdots & \ddots & \vdots \\ r'_{u,1} & \cdots & r'_{u,v} \end{bmatrix}$$

其中，$r'_{i,j}$ 在 Z_q^* 内随机选取。

$$PK'=\begin{bmatrix} r'_{1,1}\cdot G & \cdots & r'_{1,v}\cdot G \\ \vdots & \ddots & \vdots \\ r'_{u,1}\cdot G & \cdots & r'_{u,v}\cdot G \end{bmatrix}$$

(3)当产生触发时，密钥管理机构生成更新密钥参数(以认知节点 U 为例)$F=(T',s'_u,K'_U,S_k(U)',P_k(U)',\omega_2,L'_t,D_{new})$，其中 T' 为新的系统参数；K'_U 和 s'_u 为认知节点 U 与系统之间的通信公私钥对；$P_k(U)'$、$S_k(U)'$ 分别为认知节点在域内通信用的公私钥对；ω_3 为功能代码，表示此为密钥更新消息；L'_t 表示新发放私钥的使用期限；D_{new} 表示新密钥生效时间。

(4)密钥管理结构通知身份认证中心，由身份认证中心给域内所有用户发送广播消息申请更换私钥。身份认证机构使用认知用户 U 现用的公钥 K'_U 对更新密钥参数 F 进行加密，并使用机构现用的私钥 s_{id} 进行签名，之后，将其分别发送给域内用户。

(5)域内用户收到信息后，使用现用系统公钥 K_{id} 验证签名，使用与系统之间的通信私钥 s_u 进行解密，以获得新的密钥对，并发送应答信息，在规定的新密钥启动时间 D_{new} 准时使用新密钥来通信。

2.4 域内通信过程

公钥密码体制使用方便，但是其密钥长、计算复杂度高，加解密、签名等过程需要耗费较多能量，故通常用公钥密码体制完成身份认证和握手过程，并建立用于双方通信的会话密钥(对称密钥)。在大数据量的通信过程中，使用对称密码体制进行加密。假设认知节点 A 与 B 进行通信。

(1)A 生成随机数 k_{ab} 作为认知节点之间的会话密钥，通过认知节点 B 的唯一标识符计算出其公钥 $P_k(B)$，并加密 k_{ab}，加盖时间戳，再使用自己的私钥 $S_k(A)$ 进行签名，之后，将握手信息发送给 B。

(2)B 通过 A 的唯一标识符计算其公钥，验证身份，解密获得 k_{ab}，发送确认信息，该信息可用会话密钥 k_{ab} 加密。

2.5 跨域通信

本方案是以域为单位进行身份认证的，当域间用户相互通信时，需要跨域认证，认证过程如下：

(1)假设认知节点 A 与 B 分别为不同域的用户，认知节点 A 提交接收节点 B 的唯一标识符 ID_B 给本域的权限管理机构 $V_A(ID_{pw})$；

(2)$V_A(ID_{pw})$ 向 B 所在域的权限管理机构 $V_B(ID_{pw})$ 发送身份认证信息；

(3)$V_B(ID_{pw})$ 验证 B 身份后，向 $V_A(ID_{pw})$ 发送确认信息，并附上 B 的公钥信息；

(4)$V_A(ID_{pw})$ 转发该信息给用户 A。

同理，B 可验证 A 的身份并获得其公钥，从而实现跨域通信。

3 方案安全性分析

方案的安全性分析主要可分为两个部分，一是密码方案本身可能存在的安全问题，二是可靠的密码方案在实际应用过程中，因安全方案的完备性导致的协议安全问题。

3.1 密码方案的安全性分析

(1)椭圆曲线密码体制安全性

在本文中，密码方案采用椭圆曲线密码体制，椭圆曲线密码体制于 1987 年由 N. Koblitz 和 Miller 提出。椭圆曲线密码体制的安全性由椭圆曲线决定，而椭圆曲线的安全性是由 ECDLP(即椭圆曲线上的离散对数问题)求解难题决定的。ECDLP 由椭圆曲线上点形成的 Abel 加法群构造，是比因子分解问题更难的问题，为指数级的难度。实验证明，椭圆曲线加密算法中，当密钥选取为 160bits 时，可实现与 RSA 算法中 1024bits 密钥相当的安全性，且随着模数的增大，两种密码体制的安全性差距猛烈增加。安全的椭圆曲线能有效地抵抗各种已有攻击算法。只要为椭圆曲线选择合适的参数(a,b)，使相应 Weierstrass 方程满足非超奇异椭圆曲线的要求，且选取合适的有限域 F_p，椭圆曲线就能有效抵抗各种已有攻击算法。由于专门针对椭圆曲线密码体制安全性讨论的文献很多，且均经过严格的推理和验证，因此本文不再对其进行讨论。

(2)基于密钥种子矩阵 IBE 密码体制的安全性

文中密码体制还涉及基于密钥种子矩阵的 IBE 密码体制安全性问题。基于密钥种子矩阵的 IBE 密码体制的安全性也有较多讨论，其中，文献[16,17]分别基于种子矩阵提出了两种可证明安全的 IBE 方案，在随机预言机(Random Oracle，RO)模型下证明了基于种子矩阵 IBE 方案具有可证明的 IND-ID-CCA 安全性，即在 RO 模型下有效地实现了 CDH 问题到该基于种子矩阵 IBE 方案的 IND-ID-CCA 攻击者的归约。本安全方案中采用的基于种子矩阵的 IBE 方案是基于文献[17]提出的一种适用于多跳认知无线电网络的高效 IBE 方案，该方案具有标准模型下可证明的 IND-sID-CPA 安全性，即能有效实现标准模型下 DDH 问题到本文 IBE 方案的 IND-sID-CPA 攻击者的归约。由于种子矩阵本身的特点，基于种子矩阵的 IBE 系统在抵抗合谋攻击方面具有一定的局限性，即如果所有用户合谋攻击，则私钥种子矩阵无法确保安全性。但本系统的前提假设中，经过身份认证机构验证的认知节点均为合法节点，而在敌手攻击的情况下，发生大规模私钥泄露的可能性较小，且本系统设置了密钥定期更新机制，故基于密钥种子矩阵密码体制的安全性满足本系统应用环境的要求。

3.2 能抵抗的部分攻击

本安全方案是针对认知无线电网络的特征设计的。一个成功的方案必须能有效抵抗认知无线电网络已有的攻击方式，下面针对认知无线电网络中存在的常见攻击方式，分别讨论本方案的安全性。

定理 1 本文提出的 Yu-IBE 安全解决方案可抵抗模仿主用户攻击。

证明：模仿主用户攻击为攻击者利用认知无线电网络对主用户感知的特性，发送模拟主用户特征信号造成其他认知用户退出使用该信道的攻击方式。在本文提出的 Yu-IBE 安全解决方案中，所有用户均经过身份认证，当认知节点收到模仿主用户信号特征的无线电信号消息时，通过计算合法主用户的唯一标识符计算出其公钥，对该消息进行签名验证。模仿主用户的非法节点由于无主用户的私钥，因此签名验证失败，认知节点确认该消息为模仿主用户攻击，并发送广播信息告知相关节点。定理 1 得证。

定理 2 本文提出的 Yu-IBE 安全解决方案可抵抗拒绝服务攻击。

证明：拒绝服务攻击即攻击者阻止合法用户接入系统的攻击方式。在本文提出的 Yu-IBE 安全解决方案中，域内所有节点均经过身份认证，且为合法节点，认知节点发送信息的目的节点以及所有转发路径均为经过身份认证的合法节点，非法节点因无法参与通信过程，所以无法产生拒绝服务攻击的后果。定理 2 得证。

定理 3 本文提出的 Yu-IBE 安全解决方案可抵抗自私行为攻击。

证明：自私行为攻击即攻击者为了改善自身性能，不惜牺牲网络整体性能的攻击方式，如发送欺骗性的信道可用信息帧。本系统中所有域内用户均通过身份认证，在每一次通信过程中，均可确认通信方身份，非法用户一旦使用自私行为攻击，就无法通过签名验证，攻击失败。定理 3 得证。

定理 4 本文提出的 Yu-IBE 安全解决方案可抵抗窃听攻击。

证明：由于本方案中所有发送的信息均经过公钥加密体制(握手过程)或对称密码体制(大数据报通信过程)加密，因此即便敌手窃取该信息，也会因为没有解密的私钥而无法解密该信息，从而达到抵抗窃听攻击的目的。定理 4 得证。

定理 5 本文提出的 Yu-IBE 安全解决方案可抵抗数据伪造攻击。

证明：数据伪造攻击指攻击者发送虚假的频谱感知数据，使认知节点做出错误的频谱感知决策，广义上来说，也包括仿冒主用户攻击等，本方案中，由于域内所有认知用户均经过身份认证机构认证身份，为可信节点。由于攻击者无法获取用户的公/私钥对，则无法进行加密和签名，一旦发送数据伪造攻击信息，接收者就无法通过签名验证，该数据包即被丢弃，从而抵抗数据伪造攻击。定理 5 得证。

定理 6 本文提出的 Yu-IBE 安全解决方案可定位恶意节点。

证明：认知无线电网络中，由于认知的特性以及缺乏物理基础设施的保护，容易产生各种攻击，攻击者发动攻击后，往往难以确定恶意节点。在本方案中，由于所有合法节点均通过身份认证，一旦敌手发动攻击，数据包在签名验证失败后，就可认定该数据包为敌手发动，并立即定位敌手。定理 6 得证。

3.3 安全解决方案性能仿真

在认知无线电网络中，各认知节点在频谱感知阶段通常采用分布式合作感知手段，每个节点均接收其他次用户的感知报告，并通过数据融合技术进行数据处理，做出频谱决策。本文通过将提出的 Yu-IBE 安全方案与目前知名的 Bayesian 检测、加权序列概率比测试 (Weighted Sequential Probability

Ratio Test，WSPRT）安全感知方案进行对比仿真，在类似文献[18]的环境模型下，得出3种方案在数据融合过程中的性能指标，并对其进行了结果分析。仿真环境及参数设置如表1所列。

表1 仿真环境及参数设置

内容	参数
仿真环境	CPU：Intel(R) Core(TM)2 Duo T6400@ 2.00ghz；内存：2GB
操作系统	Windows XP sp3
仿真平台	cgywin+ns-allinone-2.29+mobiwan2.26
结果分析工具	Gnuplot AWK
攻击类型	always-false、always-busy、always-free
网络范围	$2000*2000m^2$ 的几何区域
主用户个数	1
次用户个数	x=500（包含恶意攻击节点）
恶意攻击节点	y=0，10，20…200（步长为10）
主用户到网络中心距离	D(S)=2000m
主用户带宽频道	6MHz
信道数	z=30
每条信道忙/闲比	20%（即主用户20%的时间占用信道）

假设次用户随机分布，信号覆盖范围为300m，节点运动速度最大为15m/s，攻击节点包括always-false、always-busy、always-free 3种类型。假设中心节点可准确掌握忙/闲比，恶意节点数从0以步长10递增到200。图中的每个数据点均为运行50次所取得的平均值，本文主要对认知节点的正确感知率进行仿真，从而分析认知无线电网络在遭受不同种攻击类型时的性能指标。

当为always-false攻击时，认知节点正确感知率如图3所示。

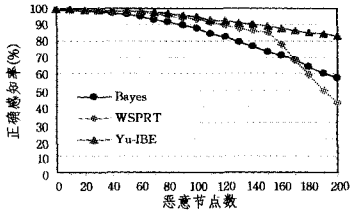

图3 always-false攻击时性能指标

当为always-busy攻击时，认知节点正确感知率如图4所示。

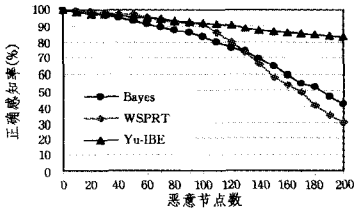

图4 always-busy攻击时性能指标

当为always-free攻击时，认知节点正确感知率如图5所示。

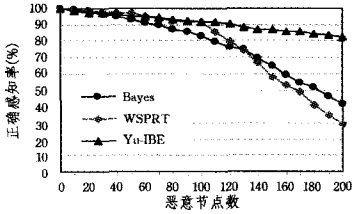

图5 always-free攻击时性能指标

影响认知网络正确感知率的因素主要包括几个方面：一是各种类型的攻击，二是节点原始数据采集的准确率，三是传输环境的影响。

在always-busy攻击中，恶意节点在感知报告中发送的可用信道数始终为0；而在always-free攻击中，恶意节点在感知报告中发送的可用信道数始终为 z，即所有信道均为空闲。

由图3—图5可知，当恶意节点数为50个以下时，3种攻击类型下，Bayesian检测、WSPRT以及本文提出的Yu-IBE方案数据融合性能指标基本相当，感知正确率均在90%以上。随着恶意节点的增加，Bayesian检测的正确感知率下降较快；WSPRT在恶意节点较少时，始终保持较为稳定的感知正确率，当恶意节点较多（超过30%后）时，WSPRT的正确感知率下降速度增加，其正确感知率低于Bayesian检测和Yu-IBE方案。Yu-IBE方案始终保持较稳定的正确感知率，在3种攻击下正确感知率均超过80%，但是随着恶意节点的增加，正确感知率仍然在下降。从理论上说，由于通过身份认证，恶意节点均因验证失败而确认其攻击行为，但是随着恶意节点的增加，部分节点周围均布满恶意节点，合法认知节点无法收集正确的感知信息，又由于感知环境差异、各种干扰等的存在，即便是合法节点，所感知的信息与真实情况也具有一定的差异，导致在数据融合过程中做出错误的决策。

结束语 本文对认知无线电网络中的安全性进行了深入研究，对存在的安全问题、已有的攻击方式和现有的解决方案均进行了阐述；并针对存在的安全问题，结合认知无线电网络的特点，提出了一种基于身份的安全解决方案，即Yu-IBE方案。该方案无需在线可信第三方即可实现认知节点的身份认证，其功能与PKI类似，但是认证链却简单很多。该安全解决方案基础设施较少，只有一个可离线的认证中心。该认证中心由身份认证机构、密钥管理机构、权限管理机构3个分机构组成，能实现系统密钥的分发、密钥定期更换、域内及跨域通信等功能。本文系统阐述了方案的工作原理，并分别针对密码方案的安全性和方案能抵抗的部分攻击进行了安全性分析。在此基础上，分别对Yu-IBE安全解决方案中的密码方案和总体方案的性能指标进行了仿真。密码方案部分仿真结果显示，本文密码方案的计算时间复杂度、私钥长度和密文长度均较低，密钥对生成和加解密时间开销均较小，能适应认知无线电网络的需求；将Yu-IBE总体安全解决方案与已有的两种知名数据融合方案进行了对比仿真，仿真结果显示，本文所提方案在所列攻击类型下均具有较好的稳定性，认知正确率始终保持较高水平。

参 考 文 献

[1] Chen R，Park J. Ensuring trustworthy spectrum sensing in cognitive radio networks[C]// IEEE Workshop on Networking Technologies for Software Defined Radio Networks. 2006：147-152

[2] Johnston D. 802.22 security sublayer proposal[S]. IEEE 802.22-07/0054r0，January 2007：246-255

[3] Mishra S M，Tandra R，Sahai A. Coexistence with primary users of different scales[C]// IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks. 2007：373-379

[4] Zhao J，Zheng H，Yang G H. Distributed coordination in dynamic spectrum allocation networks[C]// Proc IEEE DySPAN. 2005：

76-84

[5] Bian K G, Park J M. MAC-layer misbehaviors in multi-hop cognitive radio networks[C]// US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006). 2006:65-73

[6] Sethi A, Brown T X. Potential cognitive radio denial-of-service vulnerabilities and countermeasures[C]// International Symposium on Advanced Radio Technologies. February 2007:236-242

[7] Raya M, Hubaux J P, Aad I. DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots[C]// Proc of MobiSys. 2004:42-50

[8] Radosavac S, Baras J S, Koutsopoulos I. A framework for MACprotocol misbehavior detection in wireless networks[C]// Proc of the 4th ACM Workshop on Wireless Security (WiSE' 05). 2005:98-105

[9] Shamir A. Identity-based cryptosystems and signature schemes [C]// Blakley G R, Chaum D C, eds. Advances in Cryptology-Proceedings of CRYPTO' 84. California: Springer-Verlag, LNCS, 1985, 196:48-53

[10] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing[C]// Kilian J, eds. Advances in Cryptology-Crypto 2001, LNCS 2139. California: Springer-Verlag, 2001:231-229

[11] Boneh D, Boyen X. Efficient Selective-ID Identity Based Encryption Without Random Oracles[C]// Cachin C, Camenisch J, eds. Advances in Cryptology-EUROCRYPT' 2004, LNCS 3027. Switzerland: Springer-Verlag, 2004:223-238

[12] Boneh D, Boyen X. Secure Identity Based Encryption Without Random Oracles[C]// Franklin M K, eds. Advances in Cryptology-Crypto 2004, LNCS 3152. California: Springer-Verlag, 2004: 443-459

[13] Waters B. Efficient Identity-Based Encryption Without Random Oracles[C]// Cramer R, eds. Advances in Cryptology-EUROCRYPT' 2005, LNCS 3494. Denmark: Springer-Verlag, 2005: 114-127

[14] Gentry C. Practical Ientity-Based ENcyrption Without Random Oracles[C]// Vaudenay S, eds. Advances in Cryptology-EUROCRYPT'2006, LNCS 4004. Russia: Springer-Verlag, 2006: 445-464

[15] 南相浩,唐文,余嘉宁. ECC 组合公钥[C]//中国计算机学会信息保密专业委员会论文集. 2001

[16] 徐鹏,崔国华,雷凤宇. 非双线性映射下一种实用的和可证明安全的 IBE 方案[J]. 计算机研究与发展,2008,45(10):1687-1695

[17] 徐鹏,崔国华,雷凤宇,等. 标准模型下一种实用的和可证明安全的 IBE 方案[J]. 计算机学报,2010,33(2):335-344

[18] Chen R, Park J M, Bian K. Robust distributed spectrum sensing in cognitive radio networks[C]// Proceedings of The 27th Conference on Computer Communications, INFOCOM 2008. IEEE, Apr. 2008:1876-188

(上接第 52 页)

[2] Ahmed A, Mohamed Y. A survey on clustering algorithms for wireless sensor networks[J]. Comput. Commun., 2007, 30(14/15):2826-2841

[3] 黄河清,沈杰,姚道远,等. 无线传感网自适应能量驱动簇头轮换算法研究[J]. 电子与信息学报,2009,31(5):1040-1044

[4] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks[C]// Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. Hawaii, 2000:10-15

[5] Younis O, Fahmy S. HEED: A hybrid, energy-efficient, distributed clustering approach for Ad hoc sensor networks[J]. IEEE Trans. on Mobile Computing, 2004, 3(4):366-379

[6] Chan H, Perrig A. ACE: An Emergent Algorithm for Highly Uniform Cluster Formation in Wireless Sensor Networks[C]// First European Workshop, EWSN 2004. Berlin, 2004

[7] Wang Y, Zhao Q, Zheng D. Energy-driven adaptive clustering data collection protocol in wireless sensor networks[C]// International Conference on Intelligent Mechatronics and Automation. Chengdu, 2004:599-604

[8] Gamwarige S, Kulasekere E. An algorithm for energy driven cluster head rotation in a distributed wireless sensor network [C]// Proceedings of the International Conference on Information and Automation(ICIA2005). Hong Kong, 2005:354-359

[9] 刘志,裘正定. 基于分环多跳的无线传感网分簇路由算法[J]. 通信学报,2008,29(3):104-113

[10] Tatiana B, Nirupama B, Sanjay J. SASHA: Toward a self-healing hybrid sensor network architecture[C]// The Second IEEE Workshop on Embedded Networked Sensors. 2005:71-78

[11] Amir J, Walter L. Advanced Bio-Inspired Plausibility Checking in a Wireless Sensor Network Using Neuro-Immune Systems [C]// The Fourth International Conference on Sensor Technologies and Applications. 2010:108-114

[12] Chen Y J, Yuan S F, Wu J, et al. Performance optimization for wireless sensor networks based on immune system [J]. Systems Engineering and Electronics, 2010, 32(5):1065-1069

[13] Teng Rui, Leibnitz K, Zhang Bing. Immune System Inspired Reliable Query Dissemination in Wireless Sensor Networks[C]// 10th International Conference on Artificial Immune Systems. 2011:282-293

[14] Baris A, Ozgür B A. Immune system based distributed node and rate selection in wireless sensor networks [C]// 1st Bio-Inspired Models of Network, Information and Computing Systems. 2006

[15] Li H B, Yu C B, Quan X L, et al. Fault-Tolerant Vascular Routing Algorithm for Wireless Sensor Networks [J]. Telecommunication Engineering, 2011, 51(2):56-61

[16] Kao Yu-cheng, Lee S-Y. Combining K-means and Particle Swarm Optimization for Dynamic Data Clustering Problems[C]// IEEE International Conference on Intelligent Computing and Intelligent Systems(ICIS 2009). 2009:757-761

[17] Li H B, Yu C B, Yan J H, et al. Clustering strategy for energy balance of wireless sensor networks based on improved particle swarm optimization clustering algorithm [J]. Application Research of Computers, 2011, 28(2):657-660

[18] Goh K-I, Salvi G, Kahng B, et al. Skeleton and Fractal Scaling in Complex Networks [J]. Phys. Rev. Lett., 2006, 96(1):1-4