一种 Ad Hoc 认知无线电安全频谱管理方案①

孙丽艳[1]，周　健[2]

[1](安徽财经大学 信息工程学院，蚌埠 233041)
[2](北京科技大学 信息工程学院，北京 100083)

摘　要：针对认知无线电频谱管理主要安全威胁，利用零知识证明、群密钥管理、比特承诺和安全多方计算分别解决频谱感知中的主用户识别、频谱决策中的安全信道、频谱共享中信息共享和频谱迁移中的信道协商四个主要安全问题，不仅保证频谱管理的安全性，而且提高了安全管理效率。提供了比传统的物理方法更为灵活和完整的安全频谱管理的方案。

关键词：Ad Hoc；认知无线电；频谱管理；信道；安全；半诚实

Security Spectrum Management Scheme in Ad Hoc Cognitive Radio Networks

SUN Li-Yan[1], ZHOU Jian[2]

[1](Department of Computer Engineering, Anhui University of Finance and Economics, Bengbu 233041, China)
[2](Department of Communication Engineering, Beijing University of Science and Technology, Beijing 100083, China)

Abstract: Point to the security of four sub modules in spectrum management, with the cryptographic protocols that include zero-knowledge proof, group key management, bit commitment proof and security multi computation design a novel scheme to protect the network security, which has the four substantial problems of primary identity, secure channels, information share and shared channels. This scheme not only protects the security of spectrum management, but also improves the efficiency of security management, which is more complete and flexible than the physics scheme.

Keywords: Ad Hoc; cognitive radio; spectrum management; channel; security; half honest

认知无线电的动态频谱策略虽然提高了频谱资源的利用率和灵活性，却使得认知无线电网络面临比传统无线网络更为复杂的安全威胁[1]。在频谱感知子模块中，由于主用户具有传输优势，因此成为自私和恶意用户的侵占对象，模仿主用户攻击成为该模块主要安全威胁；在频谱决策子模块中，安全合作模型和安全信道成为频谱决策安全的前提；在频谱分享子模块中，自私节点或恶意节点获取其他认知用户的频谱信息后，通过否认破坏协商过程，从而达到利己目的；在频谱移动子模块中，交互明文信息为半诚实者提供了窥探机会。频谱管理中四个子模块的安全威胁具有不同特点，单一安全体制无法满足频谱管理的整体安全性。

1　安全频谱管理

安全频谱管理包括四个方面：主用户识别、安全信道、频谱信息承诺和频谱安全计算。

1.1 基于零知识证明的主用户身份识别

提出基于零知识[4]的主用户识别方案，该协议包含两个阶段：初始化阶段和使用阶段。初始化阶段如下：

Step1:频谱服务器为某一类主用户选择秘密值 $x \in_R Z_n$，且满足 $y = g^x$，频谱服务器随机选择序列 $l = c_n c_{n-1} ... c_1$，$c_i \in \{0,1\}$；

Step2:主用户加入到网络中时，从频谱服务器获取信息 $< x, y, l, H >$，其中 x，l，H 为秘密哈希函数，y 为公开值；

① 基金项目:安徽省高校自然科学研究项目(KJ2010B005);安徽省高校优秀青年基金(2009SQRZ084)
收稿时间:2010-07-13;收到修改稿时间:2010-09-18

Step3: 认知用户从频谱服务器中获取公开值 $< y, l, H >$，秘密保存值 l 和 H；

网络使用阶段（协议执行前初始化 $i=1$，$suc=0$）：

Step1: 主用户使用注册频段前，选择秘密值 $u \in_R Z_n$，计算承诺 $a=g^u$，在信号中加入 a；

Step2: 主用户和认知用户根据 $l^{'}=H^T(l)$ 计算验证值，T 为当前时间，$l^{'}=c_1^{'}c_2^{'}c_3^{'}...c_n^{'}, c_i^{'} \in \{0,1\}$，显然如果主用户和认知用户的 T 值相同，则它们计算得到的 $l^{'}$ 也相同；

Step3: 主用户根据 $l^{'}$ 计算验证值，发布验证值 $r=u+c_i^{'}x$，$c_i^{'}$ 为 $l^{'}$ 其中一位；

Step4: 认知用户根据 $r=u+c_i^{'}x$，验证，如果 $c_i^{'}=0$，验证 $g^r=a$，如果 $c_i^{'}=1$，验证 $g^r=ay$；

Step4: 如果验证失败则退出，如果验证成功且 $suc<n$，则 $i=i+1$，$suc=suc+1$，返回 step1；如果 $suc=n$ 则执行 step5；

Step5: 主用户身份证明成功。

1.2 基于信道属性的密钥管理

在执行密钥交互[2]前，需要寻找最优路径。具体步骤：

Step1: 节点发布频谱信息 F 和拓扑结构 G；

Step2: 合作节点依据频谱信息 F，建立节点间的信道属性，为信道赋予权重 w_i；

Step3: 合作节点依据拓扑结构 G，建立优化结构 S，使得满足 $\sum_{i \in S} w_i = Max\{\sum_{j \in G} w_j\}$ 或 $\sum_{i \in S} w_i = Min\{\sum_{j \in G} w_j\}$；

Step3: 合作节点依据最优结构 S，选择路径，发布共享密钥资料 k_i；

Step4: 节点执行密钥共享协议，协商共享密钥 K；

Step5：网络运行中，如果发生群密钥管理操作，即加入、退出、合并和分裂，执行 Step1。

1.3 基于比特承诺[5]协议的频谱共享

协议由多个参与者 $U_i(1 \le i \le n)$ 共同参与，协商信道数量为 $F=\{f_i \mid 1 \le i \le m\}$，协议分为承诺阶段(Step1-Step3)和打开阶段(Step4)，每个认知用户具有哈希函数 H。具体步骤如下：

Step1:每个认知用户根据感知的结果确定信道状况 $F_{U_i}=\{f_j^{U_i} \mid 1 \le i \le n, 1 \le i \le m\}$，将其表示为二进制形式，即 $\{f_1, f_2, ..., f_m\}_i, f_i \in \{0,1\}$，然后，认知用户 U_i 为每一个信道 $f_j^{U_i}$ 计算承诺 $c_j^{U_i}$，使用 $c_j^{U_i}=H(f_j^{U_i}, r_j^{U_i})$；$R_i=\{r_j^{U_i}\}$ 为随机数集合；

Step2:当认知用户接受到所有节点在每个信道的承诺信息 $\{c_j^{U_i} \mid 1 \le i \le n, 1 \le j \le m\}$ 后，发送广播消息确认完成；

Step3:认知节点在收到所有节点的确认消息后，满足打开条件，认知节点将自己的承诺 $R_i=\{r_1^{U_i}, r_2^{U_i}, ..., r_m^{U_i}\}$ 公开；

Step3:每个认知节点接受到所有参与频谱共享的节点承诺中的随机值 $\{R_i\}$；

Step4:从 $j=1$ 到 $j=m$ 执行如下的步骤，每个认知节点计算 $H(1, c_j^{U_i})=H(f_j^i, c_j^{U_i}), 1 \le i \le n, 1 \le j \le m$，如果成立则说明 $f_j^i=1$，当所有的用户在该频段都为 1 时，说明该信道可作为共享信道，将其加入备选的共享信道集合；

Step5: 节点从备选共享信道中选择某信道作为共享信道。

1.4 频谱安全多方计算

频谱的安全计算[3]分为两个部分，首先从离线频谱服务器获取计算门电路和逻辑与表，然后对输入值计算。

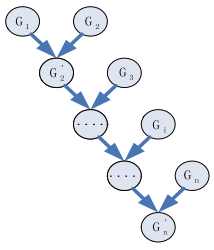

图 1 共享信道门电路函数表示图

在组建认知网络之前，由离线可信第三方协商共享信道计算的函数 f_c，该函数可用一个由若干个门电路组成的单向图 C_f 来表示，如图 1 所示，该门电路

为倒状树结构。当认知用户的数量为 n 时，门电路的数量也为 $n-1$，记做 $G_2^{'},G_3^{'},\ldots,\ G_n^{'}$，$G_1,G_2\ldots,\ G_n$ 为输入，每个门电路 $G_{i+1}^{'}$ 都比 $G_i^{'}$ 深$(i\geq 2)$，$G_n^{'}$ 的输出是整个电路 C_f 的输出，除了 $G_2^{'}$ 是 G_1 和 G_2 的输入结果外，$G_{i+1}^{'}$ 为 G_i 和 $G_{i-1}^{'}$ 的逻辑运算结果。所有的门电路都只有两个输入，一个输出值，且输入和输入值都可以用一位来表示。协议运行前使用 EL-Gamal (n,t) 协议为每个信道建立一个公钥 y_i（每个信道的公钥不同），每个节点获取 y_i 和与之对应的私钥碎片 x_i^j，t 为门限值。

使用 $B_j=\left(b_1^j,b_2^j,\ldots,b_m^j\right)=(G_j^1,G_j^2,\ldots,G_j^m)$ 表示认知用户 p_j 在信道 $i\in[1,m]$ 的输入，使用安全多方计算中 Mix-Match（MN）的目标就是正确的计算 $f(B_1,B_2,\ldots,B_n)$，同时保证 p_j 输入 B_j 的保密性。在共享信道协商过程中，对共享信道的选择是逻辑操作与，因此每个门电路都是一个 AND 门，用逻辑表 T_i 来表示信道 i 的 C_f 中的门电路 $G_i^{'}$，如表所示 T_i 为一个四行三列表，当输入的两者都为 1 是，结果为 1。换句话说，就是当 G_n^i 的结果为 1 时，得到一个共享信道 i，而如果 G_n^i 结果为 0 时，则该信道不能作为共享信道。

表 1 逻辑与表

左输入	右输入	输出
0	0	0
0	1	0
1	0	0
1	1	1

$T_i[u,v]$ 表示逻辑表 T_i 的 u 行和 v 列的值，$\overline{T}$ 表示经过 MN 混合网络解密、隐藏和随即排列后的逻辑表，行顺序随机排列，列的顺序不变。

输入值的计算步骤如下：

Step1: 输入阶段 每个认知用户 p_j 将自己的输入 b_i^j 使用 y_i 加密，然后广播自己的加密结果 G_i，因为 0 在 El-Gamal 加密方案中其加密结果是平凡的，所以可以不失一般性的使用 g^{-1} 带包 0，g 代表 1。p_j 同时也广播自己已知明文的证明或者承诺。

Step2: 混合阶段，p_j 以此使用 MN 对 $\{\{T_i\}_j\}$ 进行混合，再次加密，加密的密钥为 y_i。经过 MN 作用后，$\{T_i\}$ 变成混合的盲表 $\{\overline{T_i}\}$；

Step3: 匹配阶段，对于信道 i 的门电路 C_f，认知节点获取加密后的输入 $\{G_j^i\}$，协议的每个参与者独立的进行如下的计算，假设 l_j 和 r_j 分别表示 $G_j^{'}$ 的输入的左右秘文，当 $j=1$ 时，$l_1=G_1^i$ 和 $r_1=G_2^{'}$，当 $j\in[2,n]$ 时，$l_j=G_j^{i'}$ 和 $r_j=G_{j+1}^i$。p_j 使用 PET 协议对二元组 (l_j,r_j) 和 $\overline{T}_j$ 中的前两项进行比较。如果 $PET(l_j,\overline{T}[u,1])=1$ 且 $PET(r_j,\overline{T}[u,2])=1$ 则 $G_{j+1}^{i'}$ 对应的输出应该为 $T_i[u,3]$。p_j 在对 $G_{j+1}^{i'}$ 和 G_{j+2}^i 替换 l_j 和 r_j 进行如上的操作，直到得到结果 $G_n^{i'}$。重复上述 Step1 到 Step3 步骤，最后得到每个信道计算的结果 $\{G_n^i\}$。

Step4: 输出阶段，计算完 $\{G_n^i\}$，p_j 得到输出结果，这个结果也为 f_c 的输出结果，所有参与者参与 $\{G_n^i\}$ 的共同解密，得到二进制比特串 $b_1b_2\ldots b_n$，如 $b_i=1$ 说明信道 i 可以作为共享信道，如果 $b_i=0$ 说明信道 i 不能作为共享信道。

2 性能分析

2.1 协议安全

频谱感知中，主用户持有秘密值 $<x,l,H>$，且每次利用 $l^{'}=H^T(l)$ 给出身份证明消息，攻击者不知道 $<x,u,H>$，因此无法猜测主用户下一次的发送值是 g^{x+u} 或 g^u，因此无法模仿真实的主用户身份。 频谱决策中，共享密钥协商是建立在数学难解问题，保证共享密钥的安全性，同时信道优化降低了信道耗损攻击的威胁。频谱共享中，节点在发布共享信息前，利用哈希函数和秘密值 $r_j^{U_i}$ 隐藏频谱信息 $f_j^{U_i}$，恶意节点在没有 $r_j^{U_i}$ 的情况下是无法破解对 $f_j^{U_i}$ 的承诺，保证共享前的私密性和绑定性，满足打开条件，节点发布承诺。频谱迁移中，对输入信息，对 $\{\{T_i\}_j\}$ 进行保密，保护中间计算结果，如果恶意攻击者破解这些信息需要攻克门限值数量的认知节点。利用混合网络将逻辑表的顺序打乱，PUE 协议保证在不泄露输入和

输出的前提下保证计算的正确性，上述措施使得攻击者无法对逻辑表的内容进行猜测，进而防止对中间计算结果的分析，计算的最后结果通过多个节点的合作进行解密，在协商结果中，如果信道i可以作为共享信道，则所有节点给出的信息是可用的，而如果信道i不能作为可用信道，则说明至少由一个节的$b_i=0$，则成功猜测信道i在每个节点的状态的概率为$2^{-(n-1)}$，显然n值越大，则可能性越小。

2.2 协议效率

在频谱感知中，主用户识别需要离线服务器的支持，通过离线服务器进行分类，认知用户无需保存主用户全部信息，只需保存公开值y和秘密值$<l,H>$，提高了存储效率，识别过程中，无需交互，认知节点执行suc次指数和乘法运算，一次哈希运算，相对于复杂的物理信号识别过程具有较高的计算效率，因此该方法比传统的主用户识别方法具有非交互、低存储、低计算的优势，同时该协议也可以扩展，利用$\sum$协议为合作识别主用户，提高主用户识别的可信度，提高主用户识别效率。频谱决策中，选择优势信道提高协商效率，通过选择最优路径，进一步优化密钥协商协议的性能。频谱共享中，协议的执行效率比传统的共享方式增加了一倍，每个节点都需要向所有的节点发送一次信息，其协议复杂度为$O(2n)$，同时该方案使得认知节点可以有选择的打开承诺。频谱迁移中，以单节点单信道为例，包括密钥的建立(协议复杂度为$O(n)$)，计算过程为$O(n)$，结果解密效率为$O(t)$，在全部信道上的协议的效率为$O(m(2n+t))$，协议中使用 PUE 的匹配运算，对输入加密，对逻辑表的加密和结果的解密过程，因此协议性能依赖于网路规模和信道的数量。

2.3 整体性

该方案能够满足频谱管理在诚实、半诚实和非诚实的环境中的安全执行，为上层安全协议提供基础安全协议的支持，对频谱的每步操作，都具有相应的安全措施，操作中的得到的安全信息和频谱信息为下一步的频谱操作做好准备。

3 总结

在分析频谱管理面临的主要安全威胁后，给出一种认知无线电安全频谱管理方案，不仅丰富了主用户识别方法和保护信道安全，而且提供共享频谱信息和节点身份绑定和半诚实环境下的频谱计算。弥补现有安全方案没有从密钥学考虑的缺陷，而且是从整体上给予频谱管理安全性。然而针对频谱管理的安全性研究刚刚起步，还需要进一步研究。

参考文献

1 Akyildiz IF, Lee W, Vuran MC, et al. NeXt generation /dynamic spectrum access/cognitive radio wireless networks: a survey. Computer Networks J, 2006,50(13):2127－2159.

2 Bresson E, Chevassut O, Pointcheval D. Provably authent icated group Diffie-Hellman key exchange-the dynamic case. Advances in Cryptology-Proceedings of Asia Crypt 2001, Springer-Verlag LNCS, 2001,2248:290－309.

3 Nishitan Y, Igarashi Y. Secure multi-party computation overnetworks. IEICE Transactions on Information and Systems, March 2000, E83-D(2):561－570.

4 Rosen A. Concurrent zero-knowledge. New York, Springer, 2006,1-10.

5 Abe M, Suzuki K. Receipt-free sealed-bid auction. Proc. of ISC 2002. Heidelberg. Public Key cryptography 2000. Heidelberg: Springer-Verlag, 2000: 35－39.