非诚实环境下认知无线电共享信道安全协商①

孙丽艳[1]，张 海[1]，周 健[1,2]

[1](安徽财经大学 管理科学与工程学院，蚌埠 233030)
[2](北京科技大学 信息工程学院，北京 100083)

摘 要：由于认知无线电网络中节点工作在不同频段，因此需要在通信前进行共享信道的协商过程。在 Ad hoc 认知无线电网络中，现有协商方式是协商节点暴露自身频段的使用信息计算出共享信道，然而该方法过度的泄漏节点的频谱使用信息，从而有利于恶意节点的攻击。针对这一问题，提出基于安全多方计算的认知无线电共享信道的协商方法，通过将该问题建模为百万富翁问题，利用安全多方计算协议在无需可信第三方的支持下，通过共享秘密信息，计算出正确的共享信道，且该方法不会暴露协商节点的信道使用信息，防止了恶意节点利用共享频谱信息的攻击。

关键词：Ad hoc 认知无线电；安全多方计算；共享信道；频谱

Acquiring the Shared Channel in the Non-Honest CR Networks

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

[1](Department of Management Science and Engineering, Anhui University of Finance and Economics, Bengbu 233041, China)
[2](Department of Communication Engineering, University of Science and Technology Beijing, Beijing 100081, China)

Abstract: As every node could work on different frequencies in cognitive radio networks, cognitive nodes must consult a shared channel with other ones to communicate before sending the data. The method of negotiating the shared channel in Ad hoc cognitive radio network is that cognitive nodes give the plaintext on using frequencies, in other words, neighbor nodes knows the all information about this node' frequencies. However, compromise nodes make good use of the information of using frequencies to attack cognitive nods. To solve the problem, this paper the method based on secure multi-party computation, firstly the question is modeled with Millionaires' Problem, secondly the protocol of shared channel securely is designed. The method not only compute the accurate shared channel without revealing the information of using frequencies and the support of trust third party, but also protect the attack with the shared spectrum information.

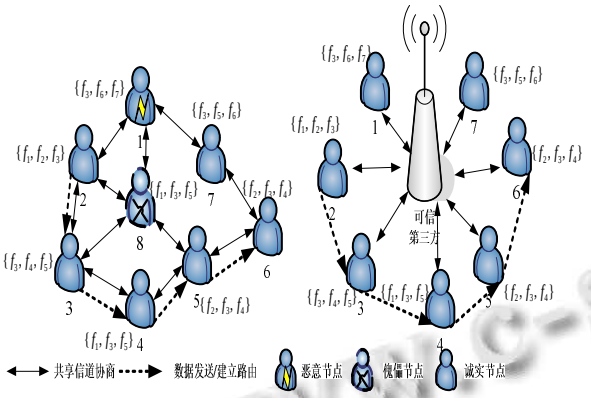
Key words: ad hoc cognitive radio; secure multi-party computation; shared channel; spectrum

自 1999 年 Joseph Mitola 博士首次在其博士论文中提出认知无线电[1,2]概念以来，该技术已成为下一代网络研究[3]的关键。尽管动态频谱选择策略改善了频谱资源短缺的问题，然而该策略也触发了一些新的安全威胁[4]，如主用户攻击[5]、密钥耗损攻击[6]、信道延迟攻击[6,7,9]、控制信道饱和攻击[6,8,10]等，其中以泄漏信道使用信息为基础的一些衍生攻击尤为突出，在 Ad hoc 认知无线电网络中，由于无可信中心，且节点工作在不同的频段，因此节点间的通讯是建立在共享信道协商基础上的，通信双发发送各自的信道使用情况，经过计算得到共享信道。然而这种以暴露自身信道使用信息的共享信道协商方式很容易遭受攻击者的破坏，既然攻击者已然知道认知节点的频谱使用情况，就可以根据频谱使用情况做出恰当的攻击方式，如拒绝服务攻击，饱和信道攻击和寄生虫攻击[11]都是建立在此基础之上，虽然在一些文献中给出了攻击方式，

① 基金项目:安徽省高校优秀青年人才基金(2009SQRZ084);安徽省教育厅自然科学研究项目(KJ2010B005);安徽财经大学青年科研项目(ACKYQ1146ZC)
收稿时间:2011-07-12;收到修改稿时间:2011-09-11

然而仍未有解决的方法。本文为解决这一问题，提出建立基于安全多方计算[12-14]的信道协商过程，不仅不会暴露协商者的信道使用状况，而且能够根据双方秘密的信道使用情况计算出正确的结果，协商过程中无需可信第三方的支持。

1 共享信道的安全问题



(a)　　(b)

图 1　Ad hoc 认知无线电共享信道协商方式

如图 1 所示，由于 Ad hoc 认知无线电网络中节点工作在不同的频段中，因此在通信前，需进行共享信道协商，该过程帮助两个邻居节点间建立可靠的通信媒介，在 Ad hoc 认知无线电网络有两种共享信道协商方式，一种是通过可靠第三方来计算得到共享信道，如图 1(a)所示，每个认知节点向可信第三方提供自身的频段使用信息，由可信第三方计算邻居节点间是否具有共享信道，计算结果传递给认知节点，优点是简单易行，而且每个认知节点的频段使用信息不会泄漏给其他节点，计算结果可信度高，节点间的交互次数较少，然而可信第三方的建立是需要花费巨大代价，在一些紧急场景中该方案并不适用；因此考虑在 Ad hoc 认知无线电网络中没有可信第三方节点，则由两节点进行协商，如图 1(b)所示，邻居节点两两协商，其过程如图 2 所示，认知节点首先在控制信道上传送各自的频谱使用情况，双方各自计算出共享信道，进而通信，由此看出共享信道协商的结果是建立在协商节点互信的基础上的，而且双发都暴露自己的全部频段信息，否则部分信息的暴露有可能会导致协商失败，或者降低效率，由此而带来的安全隐患也是严重的。

方案 2 的安全威胁是非常严重的，具体表现为如下几个方面：

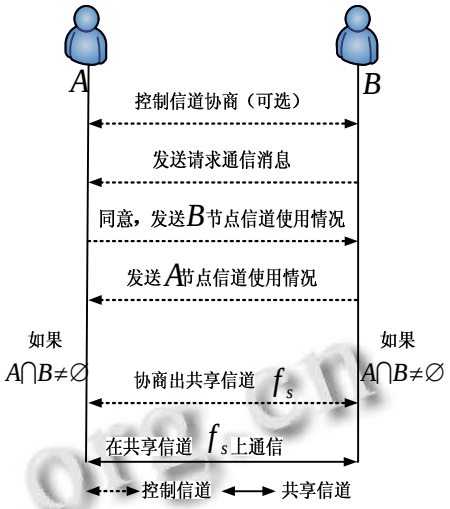


图 2　共享信道的协商过程

(1) 在一些场景中，控制信道也是共享信道协商的结果，既然暴露认知节点的所有信息，因此也包或控制信道的信息，由此很容易对控制信道进行拒绝服务攻击和饱和信道攻击，从而造成网络性能下降，甚至破坏网络运行；

(2) 由于协商的节点互相暴露自己的全部频段信息，则当某方为攻击节点的情况下，很容易通过伪造信息，达到欺骗攻击，或者通过傀儡节点搜集网络中的关键信息或发布虚假的利己信息，攻击网络；

(3) 信道的寄生虫攻击，自私节点在判断出那些频段是优势频段后，通过傀儡节点发布虚假信息，从而长期占用该优势频段，如图 1 所示，如果频段 3 是优势频段，则攻击节点 1 通过傀儡节点 8 发布频段 3 为不可用频段，不仅破坏了节点 2 和节点 6 间的正常通信，而且使得节点 1 长期占用频段 3，阻止其他节点合理的占用优势频段，破坏了频谱资源使用的均衡性；

由此提出问题，即两个节点在无可信第三方的情况下，如何在不泄漏自身频谱使用消息的情况下，协商出共享信道。该问题正是百万富翁问题，由此利用安全多方计算对这一问题建模，并给出共享信道协商的安全协议。

2　安全的控制信道协商

2.1 模型设计

协议的参与者都为半诚实参与者，也就是说参与者在频谱共享协商的执行过程中将正确的执行协议步骤，但可以保留中间计算数据以窃取他人的频谱使用

输入数据。协议的参与者为协商共享信道的两个认知节点 A 和 B，以及一个非可信的第三方 T，可以是公报板，或者是协商节点的共同邻居，它包括一个二元域上的一个算术电路。

将两个认知节点间的信道协商过程建模，设认知节点 A 掌握可用信道列表 $X=\sum_{i=1}^{n}x_i\times 2^{n-1}$，且 $X\in Z$，$x\in\{0,1\}$，认知节 B 点掌握可用信道列表 $Y=\sum_{i=1}^{n}y\times 2^{n-1}$，且 $y\in Z$，$y\in\{0,1\}$，x_i 和 y_i 中的每一位代表该编号的信道是否可用，如果为 1 则表明该节点可以使用该信道，为 0 则该节点不可以使用该信道。则认知节点 A 和 B 想要安全计算函数。

$$F(X,Y)=\begin{cases}1, x_i=1且y_i=1\\ 0, x_i\neq 1或y_i\neq 1\end{cases} \quad (1)$$

如果 $F(X,Y)=1$，说明两者间共享的信道 i，$F(X,Y)=0$ 两节点间没有共享信道。这样就将两认知节点间的共享信道协商过程建立为安全的两方安全计算问题，其中的安全性是指，在共享信道的协商过程中，节点不会泄漏各自的频谱使用情况下，保证计算结果的正确性，即得到双方都可以使用的共享信道。根据安全多方计算的方法，需将所计算的函数式表示为布尔电路或者有限域上的算术电路，根据约定 A 和 B 输入一个 n 位的二进制数，将利用函数(2)计算上式(1)，公式为某个信道是否可作为共享信道：

$$G(X,Y)=\begin{cases}(1,1), 有共享信道\\ (0,1), 无共享信道\\ (1,0), 无共享信道\end{cases} \quad (2)$$

公式(3)为共享信道的判断选择过程，返回第一个共享信道：

$$g(X,Y)=\sum_{i=n}^{1}((x_i\otimes y_i)\prod_{j=n}^{i}(x_j\oplus y_i)) \quad (3)$$

$\oplus$ 和 $\otimes$ 分别表示二元域上的加法和乘法，进一步得到公式在二元域上的算术电路。然后根据基于不经意传输协议 OT [15]的安全多方计算协议设计计算函数 $g(X,Y)$。

2.2 输入阶段

已知认知节点 A 输入可用信道列表 $X=x_nx_{n-1}x_{n-2}...x_i...x_1\in\{0,1\}^n$，认知节点 B 输入可用信道列表 $y=y_ny_{n-1}y_{n-2}...y_i...y_1\in\{0,1\}^n$，下标表示编号为 i 的信道。认知节点 A 针对在 X 上的每个比特在二元域上选择随机 x_{ia} 数，计算得到 $x_{ib}=x_i+x_{ia}$，然后将 x_{ib} 传送给认知节点 B；同理认知节点 B 针对在 Y 上的每个比特在二元域上选择随机数 y_{ia}，计算得到 $y_{ib}=y_i+y_{ia}$，将 y_{ia} 传送给 A。

输入前，认知节点 A 得到 $<x_{1a},y_{1a},...,x_{na},y_{na}>$，认知节点 B 得到 $<x_{1b},y_{1b},...,x_{nb},y_{nb}>$，且满足，,

2.3 计算阶段

根据公式(3)表示为二元域上的算术电路，将 A 和 B 的参数输入到算术电路中，由于在输入前 $<x_i,y_i>$ 以门限 $(2,2)$ 的方式在参与双方间共享，A 拥有 $\{x_{ia},y_{ia}\}$，B 拥有 $\{x_{ib},y_{ib}\}$。要求在经过每次 $x_i\oplus y_i$ 或者 $x_i\otimes y_i$ 运算后，A 和 B 分别得到 z_{ia} 和 z_{ib}，并满足 $z_{ia}+z_{ib}=x_i\oplus y_i$ 或 $z_{ia}+z_{ib}=x_i\otimes y_i$，同时该结果将作为下一步的运算输入，加法和乘法的处理如下：

●："$x\oplus y$" 由于 A 和 B 经过交互，A 和 B 分别具有 $\{x_{ia},y_{ia}\}$ 和 $\{x_{ib},y_{ib}\}$，因此 A 和 B 可以独立计算 $z_{ia}=x_{ia}\oplus y_{ia}$ 和 $z_{ib}=x_{ib}\oplus y_{ib}$，并满足关系 $z_{ia}+z_{ib}=x_i\oplus y_i$；

●："$x\otimes y$" 该操作需要借助于不经意传输协议 OT，在 A 和 B 之间执行一个 OT_4^1，A 在二元域上随机选择 z_{ia} 构建如公式(4)，A 将 $\{d_i,1\le i\le 4\}$ 发送给 B，B 根据参数 x_{ib} 和 y_{ib} 计算得到 $i=1+2x_{ib}+y_{ib}$ 且 $i\in Z$，选择消息 d_i，替换 z_b ($z_b=d_i$)，且满足 $z_{ia}+z_{ib}=xy$，即结果得到满足。

$$\begin{cases}z_{ia}=d_1+x_{ia}y_{ia}\\ z_{ia}=d_2+x_{ia}(y_{ia}+1)\\ z_{ia}=d_3+(x_{ia}+1)y_{ia}\\ z_{ia}=d_4+(x_{ia}+1)(y_{ia}+1)\end{cases} \quad (4)$$

1) 当 $i=1$，x_{ib} 与 y_{ib} 值都为，则 $z_{ia}+z_{ib}=x_{ia}y_{ia}$，等价于 $xy=(x_{ia}+0)(y_{ia}+0)=x_{ia}y_{ia}$；

2) 当 $i=4$，x_{ib} 与 y_{ib} 值分别为 0 和 1，则 $z_{ia}+z_{ib}=x_{ia}(y_{ia}+1)$，等价于 $xy=(x_{ia}+0)(y_{ia}+1)=x_{ia}(y_{ia}+1)$；

3) 当 $i=4$，x_{ib} 与 y_{ib} 值都分别为 1 和 0，则 $z_{ia}+z_{ib}=(x_{ia}+1)y_{ia}$，等价于

$xy=(x_{ia}+1)(y_{ia}+0)=(x_{ia}+1)y_{ia}$；

4) 当 $i=4$，x_{ib} 与 y_{ib} 值都为 1，则 $z_{ia}+z_{ib}=(x_{ia}+1)(y_{ia}+1)$，等价于 $xy=(x_{ia}+1)(y_{ia}+1)=(x_{ia}+1)(y_{ia}+1)$；

在共享信道的计算过程中，⊗运算为判断某个信道是否为可共享的信道，而⊕运算为得到某个共享信道后的阻止预算，也就是说该算术电路返回一个可用共享信道。

2.4 输出阶段

在计算的最后阶段，A 和 B 分别得到 z_{na} 和 z_{nb}，满足 $G(X,Y)$ 的计算要求，得到共享信道编号，实际上当出现⊕操作结果为零的情况下，则计算过程便可终止，因为已经得到共享信道。

3 协议分析总结

3.1 安全性分析

证明安全多方计算的安全性，通过对现实协议和理想模型的比较，后者蕴含了所有共享信道安全性的需求，如果两者间没有差别，则说明现实协议与理想模型具有相同的安全性。首先构建理想模型：理想模型中具有两个认知节点 A 和 B，可信第三方 T，攻击者 S，两节点可以与 T 在安全信道上进行秘密通信，S 具有和现实模型中一样的攻击，但是它不能攻陷 T，同时也不能阻止 T 与 A 和 B 间的秘密通信。协议运行中，A 和 B 把输入信息通过安全信道传送给 T，T 完成计算，并把相应的结果传送给 A 和 B。在输入阶段，S 可以收买 A 或 B，不失一般性，以 A 作为傀儡，但是另一个诚实的参与者的输入他是无法得到的；在计算阶段，如果攻击者是被动的，由于 A 发送的消息仍是自己信道使用的真实情况，因此最后的结果仍是计算正确的，如果攻击者是主动的，尽管 A 发送的消息仍是虚假信道使用的情况，然而且计算得到的结果仍是正确的，并且与上者相同，都无法得到 B 的信道使用信息。在输出阶段，T 将计算结果 y_A 和 y_B 通过安全信道传送给 A 和 B，虽然 S 可以得到 A 中所有信道信息，也可得到 B 中一个可用信道信息，然而仍然无法看到 B 中所有信道的使用信息。在现实协议运行中，输入阶段 S，得到 A 中所有信道使用信息，获取输入数据 $\{x_i=x_{ia}+x_{ib}\}$ 和 B 的消息 $\{y_{ia}\}$，由于 A 不知道 $\{y_{ib}\}$，因此 A 也无法理解 $\{y_{ia}\}$，攻击者可以输入真实消息 $\{<x_{ia},y_{ia}>\}$，也可以发送虚假消息 $\{<x'_{ia},y'_{ia}>\}$；计算阶段，如果是⊕运算，由于该运算过程中 A 和 B 间无交互过程，S 获取的消息并不比输入阶段多，如果是⊗运算，当 A 为发送方时，A 发送真实 z_{ia} 或者虚假 z_{ia}，S 没有获取更多消息，当 A 为接受方时，S 只是获取了随机比特 $\{d_i\}$，因此 S 也无法读懂；在输出阶段，A 和 B 都得到以输入信息计算后的正确结果。根据上文描述，可以看出由于每个参与者的最后输出以及攻击者得到的信息与理想模型是相同的（正确计算 $G(X,Y)$），没有差别，由此该信道的协商过程是安全的。

3.2 性能分析

在具有可信第三方的情况下，两节点和可信第三方具有两次交互的过程。当使用可信计算协议时，如果是⊗运算则无需交互的过程，而在⊗运算中，需要一次 A 和 B 的交互，根据公式，当产生第一个共享信道时，计算结束，则其运行效率为 $O(k)$，k 为协商失败的次数，也是执行 OT_4^1 的次数。

3.3 可行性分析

协议的交互过程可以在控制信道上增加信令发起交互过程，无需时间同步，同时由于该方案只在两节点间交互，且协议中无需复杂的加密解密机制，因此较为容易实现。网络运行中午特殊节点，也无需特殊设备辅助，因此适合快速部署方式。

4 总结

本文通过将认知无线网络节点间的共享信道协商过程建模为百万富翁问题，通过安全多方计算协议解决了认知节点间共享信道协商中频谱使用信息的泄漏问题，防止了恶意节点依此为基础的攻击，该方法无需可信第三方的支持，使之适用于 Ad hoc 认知电网络中，然而由于信道协商过程中，需要认知节点间多次的加法和乘法操作，以及秘密共性。导致其协商的性能较低，这也是我们下一步工作的内容。

参考文献

1 Mitola J, Maguire G. Cognitive radio: making software radios more personal. IEEE Personal Commun, 1999,6(4):13–18.

2 Haykin S. Cognitive radio:brain-empowered wireless communications. IEEE Journal on Selected Areas in Communications, 2005,23(2):201–20.

3 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.

4 Clancy TC, Goergen N. Security in cognitive radio networks: threats and mitigation, 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008), Singapore, May. 2008:5.

5 Chen RL, Jung MP, Reed JH. IEEE Journal on Selected Areas in Communications, 2008,26(1):25–37.

6 Chetan N, Mathur K, Subbalakshmi P. Security Issues in Cognitive Radio Networks. Cognitive Networks. 25 July 2007: 272–290.

7 Bian KG, Park JM. MAC-Layer Misbehaviors in Multi-Hop Cognitive Radio Networks.2006 US-Korea Conference on Science,Technology, and Entrepreneurship (UKC2006), Aug 2006.

8 Brown TX, Sethi A. Potential Cognitive Radio Denial-of-Service VulNerilIties and Protection Countermeasures: A Multi-dimensional Analysis and Assessment. Cognitive Radio Oriented Wireless Networks and Communications,2007.CrownCom 2007. 2nd International Conference on.1–3 Aug. 2007: 456–464.

9 Sampath A, Dai H, Zheng HT, Zhao BY. Multi-channel Jamming Attacks using Cognitive Radios. Computer Comm–unications and Networks, 2007. ICCCN 2007. Proc. of 16th International Conference on.13–16 Aug. 2007: 352–357.

10 Safdar GA, O'Neill M. Common control channel security framework for cognitive radio networks, 2009 IEEE 69th Vehicular Technology Conference, April 2009, Barcelona, Spain:211–217.

11 Haq A, Naveed A, Kanhere SS. Securing Channel Assignment in Multi-Radio Multi-Channel Wireless Mesh Networks, Wireless Communications and Networking Conference 2007 WCNC, Kowloon, March 2007: 3111–3116.

12 Nishitan Y, Igarashi Y. Secure multi-party computation over networks. IEICE Trans. on Information and Systems, March 2000, E83–D(2):561–570.

13 Asokan N, Ginzboorg P. Key agreement in ad hoc networks. Computer Communications, 2000,23(17):1627– 1637.

14 Yao AC. Protocols for secure computations, Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on. Chicago USA, Nov 1982: 160–164.

15 Rabin MO. How to exchange secrets with oblivious transfer, technical report TR–81. Aiken Computation Lab, Harvard University, 1981.

（上接第 35 页）

工截取同一个播音员、在不同的语音段发音的敏感词，共截取 3 个敏感词（ot/火, yarlinish/伤, olush/死），每个敏感词重复发音两次，建立训练语音语料库。然后，对同一个播音员的含有敏感词的另外一个新闻 60 分节目连续语音（不是截取训练敏感词的语音段）进行敏感词检索。

实验结果显示，一、帧长和帧移越大错识率越高，但识别速度越快、鲁棒性相当好。二、倒谱系数和分差倒谱系数越小识别的成功率越低，系统也越不稳定。三、特征矢量聚类数目越小识别率越低。

总之，帧长，帧移，倒谱系数，分差倒谱系数，码本大小，聚类数目等参数直接影响系统的识别率。所以识别率和识别速度之间取舍时，经实验来决定。

参考文献

1 哈力克·尼亚孜.基础维吾尔语.乌鲁木齐:新疆大学出版社,1997.

2 那斯尔江·吐尔逊,吾守尔·斯拉木.基于隐马尔可夫模型的维吾尔语连续语音识别系统.计算机应用,2009,29(7).

3 王炳锡,屈丹,彭煊,等.实用语音识别基础.北京:国防工业出版社,2005.

4 屈丹,王波,李弼程,等.VoIP 语音处理与识别.北京:国防工业出版社,2010.

5 Jurafsky D, Martin JH. Speech and Language Processing. Second Edition, Beijing: Posts & Telecom Press, 2010.

6 Hahn B, Valentine D. Essential Matlab for Engineers and Scientists. Fourth Edition, Canada: Academic Press, 2010.

7 张德丰,等.Matlab 概率与数理统计分析.北京:机械工业出版社,2010.