基于自认证的认知无线电密钥交换协议研究

周 健[1,2] 周贤伟[1] 孙丽艳[2]
(北京科技大学信息工程学院 北京 100081)[1] (安徽财经大学信息工程学院 蚌埠 233041)[2]

摘 要 开放频谱策略使得认知无线电网络面临比传统网络更为复杂的安全威胁。频谱切换引发时延,降低认知无线电网络密钥交换协议的性能。为解决这一问题,提出一种适合认知无线电网络的密钥交换协议,在分簇基础上根据切换时延使用旅行商问题和组播路由树提高簇内和簇间路径选择效率。簇间和簇内使用基于自认证的多方密钥交换协议,不仅可以防止被动攻击,也可以阻止主动攻击,保证认证和密钥协商同步进行,其运行效率为 $O(2m)$,m 为簇中节点数量。

关键词 认知无线电,安全,密钥交换,分簇,Ad hoc,自认证
中图法分类号 TP3931.04 **文献标识码** A

Key-exchange Protocols of Cognitive Radio Based on Self-certified

ZHOU Jian[1,2] ZHOU Xian-wei[1] SUN Li-yan[2]
(Department of Communication Engineering, University of Science and Technology Beijing, Beijing 100081, China)[1]
(Department of Computer Engineering, Anhui University of Finance and Economics, Bengbu 233041, China)[2]

Abstract There are more security threats in cognitive radio networks than traditional wireless networks due to the strategy of opening spectrum. Switching spectrum brings time delay and interferes with network efficiency. The question also adversely effects on key-exchange protocol which is an important part of key agreement, and gives malicious nodes the attack chance. So this paper put forward a new method, firstly cognitive radio network was divided into multiple clusters, secondly used protocol the time delay of switching channel to select the optimal path with traveling salesman problem in cluster and built the optimal multicast routing tree among clusters; at last different key-exchange protocols based on self-certified were used in cluster and among clusters, which can prevent active attack and passive attack, authentication and key agreement can also simultaneously carried out. The efficiency of protocol is $O(2m)$, m is the number of cluster.

Keywords Cognitive radio, Security, Key exchange, Cluster, Ad hoc, Self-certified

自 1999 年 Joseph Mitola 博士首次在其博士论文中提出认知无线电[1]概念以来,该技术已成为下一代网络研究[2]的关键。其动态频谱选择策略改善了频谱资源短缺的问题。然而传统无线协议无法满足非固定频谱策略[3-6],一方面频谱切换没有被考虑,另一方面也没有考虑到认知无线电特有的安全问题,通过破坏信道传输,达到增加传输延迟,降低网络性能的攻击尤为突出,如密钥耗损攻击利用链路层的频繁更换信道带来的时延,攻击传输层的会话密钥[7,8]。密钥交换协议是密钥管理的重要组成部分,频谱切换通过影响节点交互效率,进而影响密钥交换协议,因此设计安全高效的密钥交换协议是 Ad hoc 认知无线电网络安全的重要内容。现有 Ad hoc 网络安全协议[9-12]由于没有考虑到频谱选择的效率问题,因此不适合 Ad hoc 认知无线电网络。本文通过分析认知无线电信道选择效率问题,在分簇基础上设计一种适合认知无线电网络的自认证密钥交换协议,使其在保证安全的基础上,减少由于频谱切换带来的负面影响。

1 网络分簇

在非结构化的认知无线电网络中使用单一的密钥交换协议,不仅面临由多轮的交互过程导致效率低下的问题,而且也会面临因使用广播信道,增加网络负载的问题。因此通过网络分簇,如图 1 所示,通过簇间和簇内使用不同的密钥交换协议,既可以降低网络负载,也可以提高交换密钥的成功率,提高其效率。而簇内和簇间的路径选择也直接影响认知无线电密钥交换协议的性能。

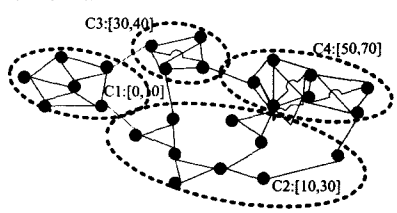

图 1 网络分簇

到稿日期:2009-07-02 返修日期:2009-09-30 本文受国家自然科学基金资助项目(60773074),国家 863 计划项目(2007AA01Z213,2009AA01Z209),安徽省高等学校自然科学研究项目(KJ2009B127Z),安徽省高校优秀青年人才基金项目(2009SQRZ084)资助。
周 健(1979—),男,博士生,讲师,主要研究方向为认知无线电、网络安全,E-mail:yewanfeng12@sina.com;周贤伟(1962—),男,教授,博士生导师,主要研究方向为下一代网络技术、光通讯等。

假设每个认知用户所使用的频段是非重叠的，信道带宽为 ω，通过实验发现，当认知节点在一定范围内自由选择频段时，其平均每跳的时延和冲突率和频谱范围相关，而和网络的规模及节点密度无关，如图 2 所示。

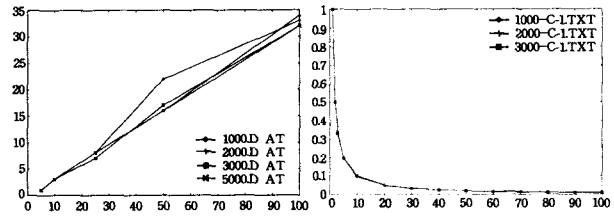

图 2 (a)不同网络规模的平均时延 (b)冲突检测

因此通过将网络分成多个簇，每个簇运行在不同频谱范围内，在保持较低的冲突率的情况下，使其具有较少的频谱切换时延。每个簇内的路径时延和簇内的冲突率只和簇所选择的频谱区间的数量相关，$t_{delay}=|f_{\max}-f_{\min}|/3\omega$，$r_{collision}=(|f_{\max}-f_{\min}|)^{-1}\omega$。假设每个簇簇头已知簇内的最大直径 R，可以得到网络每个簇的冲突和延迟指数 $Rr_{collision}$ 和 Rt_{delay}，后者是选择簇间路径的重要参数。

2 密钥交换协议

该协议包括 3 个部分，分别为初始化、簇内密钥交换、簇间密钥交换，网络在密钥交换时间内是拓扑不变的。

2.1 初始化

由于 Ad hoc 认知无线电无可信基础设施，因此通过自认证的方式[13]，帮助认知节点确认身份。每个认知节点 $node_i$ 在加入网络前，通过向离线的可信中心申请自证明公钥 pub_i。设 p,q,p_1,q_1 为大素数，$p=2p_1+1$，$q=2q_1+1$，g 是 Z_n^* 中阶为 $2p_1q_1$ 的一个元素，选择一个 RSA 加密指数 e，其解密指数为 $d=e^{-1} \bmod \varphi(n)$，其 $\varphi(n)=(p-1)(q-1)$，可信中心将 p,q,p_1,q_1,d 秘密保存，将 n,g,e 公开。设每个认知节点的身份信息分别为 $ID_i(1\leqslant i\leqslant n)$，步骤如下：

1)节点 $node_i$ 选择秘密指数 x_i，计算 $y_i=g^{x_i} \bmod n$；

2)将(x_i,y_i)提交给可信中心；

3)可信中心计算 $pub_i=(y_i-ID_i)^d \bmod n$。

2.2 簇内密钥交换

簇内成员较少，并且簇头可以作为可信第三方节点，因此使用 Diffie-Hellman 密钥交换协议，由簇头指定交换顺序，簇成员提供共享密钥成分。然而由于节点间并不是一定直接可达的，因此由簇头指定的不同连接次序，具有不同的交换效率，该问题可以归结为一个哈密顿圈问题，如图 2 中的 3 个簇，上方 3 个簇具有哈密顿圈，通过簇头选择其中一个哈密顿圈即可，而下方的簇中显然没有哈密顿圈，可以使用旅行商问题(TSP)解决该问题，每条边上权重 $w=\lambda|f_{node_i}-f_{node_j}|^{-1}$ 代表信道切换次数，λ 为时延系数，显然切换的次数越少越好。

$$\min\sum_{i=1}^{n}\sum_{j=1}^{n}c_{ij}x_{ij},x_{ij}=\begin{cases}1, & \text{信息访问节点 } i \text{ 后紧接访问 } j\\ 0, & \text{否则}\end{cases}$$

虽然旅行商问题是一个 NP 问题，然而簇内节点较少，因此簇头可以在时间内得到旅行商问题的最优解，以簇 i 为例，通过簇头 C_i 计算得到以簇头为开始节点和尾节点，通过网络所有节点最少一次，且其边权重和为最小的路径 $Path_i$。由每个参与方各选择一个秘密指数 k_{ij}，最后构造一个秘密值 K_i，m 为簇内成员数量，令 G 是一个阶数为素数 q 的乘法循环群，g 为其任一生成元，则群成员 $node_{i1},node_{i2},\cdots,node_{im}$ 的共享密钥协商过程如下：

1)簇头计算得到簇内最小路径 $Path_i$，发送给每个簇内成员，簇头作为开始节点和结束节点；

2)簇成员接收 $Path_i$，根据路径得到自己的上一跳节点和下一跳节点；

3) $\forall 1\leqslant j\leqslant m$，$node_{ij}$ 选择 $k_{ij}\in_R Z_q^*$，计算 $g^{k_{ij}}$，将 $g^{k_{ij}}$，pub_{ij}，ID_{ij} 发送给 $node_{i((j+1) \bmod m)}$；

4)第 $k=1$ 轮，节点 $node_{i(j+1 \bmod m)}$ 计算 $K_{i(j+1 \bmod m)}=g^{k_{ij}k_{i(j+1 \bmod m)}}(pub_{ij}^{x_{ij}}+ID_{ij})^{x_{i(j+1 \bmod m)}}$，$G_{ij}^1=(g^{k_{ij}})^{k_{i(j+1 \bmod m)}}$，$G_{ij}^2=(g^{x_{ij}})^{x_{i(j+1 \bmod m)}}$，将 $K_{i(j+1 \bmod m)}$，$G_{i(j+1 \bmod m)}^1$，$G_{i(j+1 \bmod m)}^2$，$g^{k_{i(j+1 \bmod m)}}$，$g^{x_{i(j+1 \bmod m)}}$，$pub_{i(j+1 \bmod m)}$，$ID_{i(j+1 \bmod m)}$ 发送给节点 $node_{i((j+2) \bmod m)}$，重新接受节点 $node_{ij}$ 的信息；

5)第 $k\in(1,m-1]$轮，节点 $node_{i((j+1) \bmod m)}$ 计算 $(\frac{K_{ij}}{G_{ij}^1})^{k_{i(j+1 \bmod m)}}(\frac{K_{ij}}{G_{ij}^2})^{x_{i(j+1 \bmod m)}}$，$G_{i(j+1 \bmod m)}^1=(G_{ij}^1)^{k_{i(j+1 \bmod m)}}$，$G_{i(j+1 \bmod m)}^2=(G_{ij}^2)^{x_{i(j+1 \bmod m)}}$ 而第一轮中的信息 $K_{i(j+1 \bmod m)}$ 已经传递给 $node_{i((j+k) \bmod m)}$，计算

$$K_{i(j+k \bmod m)}=((\frac{K_{i(j+k-1 \bmod m)}}{G_{i(j+k-1 \bmod m)}^1})^{k_{i(j+k \bmod m)}}(\frac{K_{i(j+k-1 \bmod m)}}{G_{i(j+k-1 \bmod m)}^2})^{x_{i(j+k \bmod m)}})\cdots\cdots$$

$$K_{i(j+2 \bmod m)}=((\frac{K_{i(j+1 \bmod m)}}{G_{i(j+1 \bmod m)}^1})^{k_{i(j+2 \bmod m)}}(\frac{K_{i(j+1 \bmod m)}}{G_{i(j+1 \bmod m)}^2})^{x_{i(j+2 \bmod m)}})$$

$G_{ij+k \bmod m}^1=(G_{ij}^1)_{l=1}^{\sum^k(k_{ij+l})}$，$G_{ij+k \bmod m}^2=(G_{ij}^2)_{l=1}^{\sum^k(x_{ij+l})}$ 和 $g^{k_{i(j+k \bmod m)}}$，$g^{x_{i(j+k \bmod m)}}$，$pub_{i(j+k \bmod m)}$，$ID_{i(j+k \bmod m)}$，将结果发送给 $N_{i((j+k+1) \bmod m)}$；

6)在 $m-1$ 轮之后，所有参与者可以计算得到一个共同的密钥 $K_i=g^{x_{i1}x_{i2}\cdots x_{im}+k_{i1}k_{i2}\cdots k_{im}}=g_{j=1}^{\sum^m x_{ij}+\sum_j^m k_{ij'}}$；

7)簇头节点也得到共同的密钥 $K_i=g^{x_{i1}x_{i2}\cdots x_{im}+k_{i1}k_{i2}\cdots k_{im}}$，执行簇间密钥交换协议；

8)簇成员等待簇头进行簇间密钥交换协议。

2.3 簇间密钥交换

簇头根据簇内频谱范围，计算该簇 $t_{delay}=|f_{\max}-f_{\min}|/3\omega$，据此建立组播路由树。簇头通过组播路由树执行簇间密钥交换，簇头从离线可信中心获取 $k_i^c=\prod_{j=1}^{m}x_{ij}+\prod_{j'=1}^{m}k_{ij'}$，设计如下，协议的参与者为簇头 $C_1,C_2,\cdots,C_n$，此外，令 $C_0=C_n$，$C_1=C_{n+1}$ 即 $C_i=C_{i \bmod n}$。

1)簇头节点 C_i 将 $Z_i^1=g_{j=1}^{\prod^m x_{ij}+\prod_{j'=1}^m k_{ij'}}$，$Z_i^2=g^{x_i}$ $(x_i=pub_i^{\prime}+ID_i)$，$pub_{c_i}$ 和 ID_{c_i} 组播给其他参与者簇头节点 C_{-i}；

2)C_i 计算 $X_i=(\frac{Z_i^1+1}{Z_{i-1}^1})^{k_i^c}(\frac{Z_i^2+1}{Z_{i-1}^2})^{x_i}$，将 X_i 组播给其他参与者 C_{-i}；

3)K_i 为簇间密钥，即网络共享密钥，C_i 计算 $K_i=(Z_{i-1}^1)^{nk_i^c}(Z_{i-1}^2)^{nx_i}X_i^{n-1}X_{i+1}^{n-2}\cdots X_{i+n-2}=g_{i=1}^{\sum^k((\prod_{j=1}^m x_{ij}+\prod_{j'=1}^m k_{ij'})(\prod_{h=1}^{m'}x_{i+1h}+\prod_{h'=1}^{m'}k_{ih'})+\sum_{i=1}^{k}(x_ix_{i+1})}$；

4)由簇头向簇内节点广播共享密钥，全网络共享密钥 $E(g_{i=1}^{\sum^k((\prod_{j=1}^m x_{ij}+\prod_{j'=1}^m k_{ij'})(\prod_{h=1}^{m'}x_{i+1h}+\prod_{h'=1}^{m'}k_{ih'})+\sum_{i=1}^{k}(x_ix_{i+1})})_{K_i}$；

5)簇内节点用 K_i 解密得到共享密钥，协议结束。

为了获取共享密钥，每个参与方簇头 C_i 都付出自己的贡献 $g_{j=1}^{\prod^m x_{ij}+\prod_{j'=1}^m x_{ij'}}$ 和 g^{x_i}，不同的参与者构成的群体最终协商出的密

钥也是不同的，每个参与者需要经历两轮交互，发送两个消息，最多执行 6 个模指数运算和 $O(n^4)$ 个乘法运算，n 为簇头数。

3 协议分析

3.1 安全性

在被动攻击上，该协议建立在离散对数难解问题基础上，能够有效抵御被动攻击。从簇内密钥的安全性看，被动攻击者在获取 $p,g,g^{x_{ij}}$ 时，要想获得簇内共享密钥 $g^{\prod_{j=1}^{m}x_{ij}+\prod_{j'=1}^{m}x_{ij'}}$，就需要得到 $x_{i1},x_{i2},\cdots,x_{ij-1},x_{ij+1},\cdots,x_{im},k_{i1},k_{i2},\cdots,k_{ij-1},k_{ij+1},\cdots,k_{im}$。由于这些指数是保密的，对任意指数的求解，都意味着求解离散对数问题；从簇间密钥的安全性看，被动攻击者在获取 $p,g,g^{\prod_{j=1}^{m}x_{ij}+\prod_{j'=1}^{m}x_{ij'}}$ 时，要想获取簇间共享密钥 $g^{\sum_{i=1}^{k}((\prod_{j=1}^{m}x_{ij}+\prod_{j'=1}^{m}k_{ij'})(\prod_{h=1}^{m'}x_{i+1h}+\prod_{h'=1}^{m'}k_{ih'})+\sum_{i=1}^{k}(x_ix_{i+1})}$，就需要得到指数 $x_{11}x_{12}\cdots x_{1j}\cdots x_{1n},x_{21}x_{22}\cdots x_{2j}\cdots x_{2n},\cdots,x_{i1}x_{i2}\cdots x_{ij}\cdots x_{in},x_{n1}x_{n2}\cdots x_{nj}\cdots x_{m}$，和 $k_{11}k_{12}\cdots k_{1j}\cdots k_{1n},k_{21}k_{22}\cdots k_{2j}\cdots k_{2n},\cdots,k_{i1}k_{i2}\cdots k_{ij}\cdots k_{in},k_{n1}k_{n2}\cdots k_{nj}\cdots k_{m}$。由于这些指数是保密的，对任意指数的求解，也意味着求解离散对数问题，因此可以说，该协议的簇间密钥和簇内密钥的安全性都依赖于离散对数问题的困难性。密钥交换分为两个阶段，分别运行在不同规模的网络中，首先在局部的簇内，然后在簇头间，减少了被干扰的机会，当簇内部分节点受到攻击，簇头阻断被攻击节点使其不影响整体网络的密钥管理。在主动攻击上，簇内主动攻击者 A 想假冒节点 $node_i$，可以伪造 pub_i 的值为 pub_E，从而得到一个伪造的值 y_A，但是他无法计算得到 y_A 对应的秘密指数值 x_A，而不知道这个值，他就无法计算共享密钥。

3.2 效率

密钥交换首先获取自认证信息；然后在簇内协商簇内共享密钥，具有局部性，簇间使用基于自认证的 Diffie-hellman 密钥交换，根据频谱切换次数利用旅行商模型寻找最优路径来提高密钥交换效率，其效率为 $O(m)$，m 为簇内节点数；最后通过簇头协商网络共享密钥，根据频谱切换次数建立最优组播树来提高组播路径效率，其过程不需要广播，不会产生广播风暴而增加网络负载，其效率为 O(2)。其总体效率比 Diffie-hellman($O(n)$，n 网络节点数)有较大提高。密钥交换的成功率高，冲突较少。

3.3 可行性

该密钥交换协议在第一阶段可以应用多种分簇协议，不需要特定的分簇协议支持；在第二阶段，通过簇节点获取簇内的局部拓扑图，指定交换次序，簇内节点较少，不会影响效率；在第三阶段，簇间的密钥交换可以运行于现有 Ad hoc 组播路由协议之上，不需要重新设计新的协议。

结束语 本文分析了 Ad hoc 认知无线电网络中密钥交换出现的问题，当网络规模较大时，由于信道切换延迟和动态频谱选择，使得单一的密钥交换协议都不能保障 Ad hoc 认知无线电网络快速协商共享密钥。因此在分簇的基础上，结合多方密钥交换协议的优点，设计了适合 Ad hoc 认知无线电网络的密钥交换协议，利用自认证在不降低效率的同时防止了主动攻击，通过旅行商问题解决了信道切换延迟的最优路径选择问题，提高了簇内密钥交换的效率，避免了密钥交换协议运行所带来的广播风暴，减小了网络的负载，簇间通过频段范围改善了组播路由树。从安全性、效率、可行性 3 个方面分析该协议的性能，证明了该协议适合 Ad hoc 认知无线电网络。在下一步的工作中，通过仿真模拟实验进一步验证其可靠性和可行性。

参 考 文 献

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

[2] Akyildiz I F, Lee W, Vuran M C, et al. NeXt generation /dynamic spectrum access/cognitive radio wireless networks: a survey[J]. Computer Networks J, 2006, 50(13): 2127-2159

[3] Cormiob C, Chowdhurya K R. A survey on MAC protocols for cognitive radio network[J]. Ad Hoc Networks. Elsevier B. V, 2009, 7(7): 1315-1329

[4] Zhao Q, Tong L, Swami A, et al. Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: A POMPD framework[J]. IEEE Journal on Selected Areas in Communications(JSAC), 2007, 25(11): 589-600

[5] Su H, Zhang X. Opportunistic MAC protocols for cognitive radio based wireless networks[A]// Proceedings of the 41st IEEE CISS Conference, 2007[C]. Baltimore, MD: IEEE Information Sciences and Systems, 2007: 363-368

[6] Brodersen R W, Wolisz A, Cabric D, et al. Corvus: a cognitive radio approach for usage of virtual unlicensed spectrum[R]. Berkeley: Wireless Research Center (BWRC) White paper, 2004

[7] Aad I, Hubaux J-P, Knightly E W. Denial of service resilience in ad hoc networks[A]// Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom'04), 2004[C]. Philadelphia, PA, USA: ACM New York, NY, USA, 2004: 202-215

[8] Mathur C N, Subbalakshmi K P. Security Issues in Cognitive Radio Networks[C]// Kwang-Cheng Chen, Ramjee Prasad. Cognitive Networks. Oxford: Wiley, 2007: 272-290

[9] Joux A. An One Round Protocol for Tripartite Diffie-Hellman [A]// Algorithmic Number Theory-proceedings of ANTS, 2000 [C]. Heidelberg: Springer-Verlag, 2000: 385-394

[10] Menzes A, Qu M, Vanstone S. Some New Key Agreement Protocols Providing Mutual Implicit Authentication[A]// Selected Area in Cryptography-proceedings of SAC, 1995[C]. Nashville, TN, 1995: 22-32

[11] Bresson E, Chevassut O, Pointcheval D. Provably authenticated group Diffie-Hellman key exchange-the dynamic case[A]// Advances in Crytology-Proceedings of AsiaCrypt, 2001[C]. Heidelberg: Springer-Verlag, 2001: 290-309

[12] Burmester M, Desmedt Y. A secure and efficient conference key distribution system [A] // Advances in Cryptology-EUROCRYPT'94, 1994[C]. Heidelberg: Springer-Verlag, 1995: 275-286

[13] Girault M. Self-certified public keys [C]// Advances in cryptology: Proc. Eurocrypt'91, LNCS 434. Springer, 1991: 490-497

(上接第 90 页)

[18] Pretschner A, Hilty M, Casati F, et al. Usage control in service-oriented architecture[C]// Proc. of the 4th Intl. Conf. on Trust, Privacy & Security in Digital Business. 2007

[19] Chen L, Zhang H G, Zhang L G, et al. A Peer-to-Peer Resource Sharing Scheme Using Trusted Computing Technology[J]. 2008, 13(5): 523-527

[20] 张宏，贺也平，石志国. 基于周期时间限制的自主访问控制委托模型[J]. 计算机学报，2006，29(8)：1427-1437

[21] 李军，孙玉方. 计算级安全和安全模型[J]. 计算机研究与发展，1996，33(4)：312-320

[22] 黄建，卿斯汉，温红子. 带时间特性的角色访问控制[J]. 软件学报，2003，14(11)：1944-1954

[23] 徐震，李斓，冯登国. 基于角色的受限委托模型[J]. 软件学报，2005，16(5)：970-978

[24] 洪帆，等. 多域安全互操作的可管理使用控制模型研究[J]. 计算机科学，2006，33(3)：283-286