doi:10.3969/j.issn.1000-436x.2012.z2.013

认知无线电网络主用户模仿攻击下次用户通信性能分析

王珊珊[1,2]，罗兴国[1]，李鹏[3]
（1. 国家数字交换系统工程技术研究中心，河南 郑州 450000；2. 解放军 61580 部队，北京 100000；3. 解放军 95949 部队，河北 沧州 061000）

摘 要：随着认知无线电网络（CRN）技术的不断发展，安全问题日益受到重视。模仿主用户（PUE）是一种典型的易于实现且对 CRN 影响巨大的攻击行为，根据产生的原因、目的和过程的差异，可以分为恶意不端次用户 PUE 和自私不端次用户 PUE 2 类攻击。已有文献大多针对前者进行了分析，而对后者分析极少。重点对两者进行了区分，提出了四维连续时间马尔科夫链分析模型，详细地分析了自私不端次用户 PUE 攻击对正常次用户通信性能的影响，并对比了几类典型的 PUE 攻击检测技术。通过仿真结果可以看出：PUE 攻击检测技术引入自私不端次用户检测机制极为必要，可以有效地改进检测效果。

关键词：认知无线电网络；频谱感知；通信性能；次用户；仿冒主用户
中图分类号：TN918.91 **文献标识码**：A **文章编号**：1000-436X(2012)Z2-0104-07

Communication performance analysis of secondary users in cognitive radio networks under primary user emulation attacks

WANG Shan-shan[1,2], LUO Xing-guo[1], LI Peng[3]
(1. National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450000, China;
2. 61580 Troop, Beijing 100000, China; 3. 95949 Troop, Cangzhou 061000, China)

Abstract: Cognitive radio network (CRN) is an effective technology and a hot research direction which could solve the problem of deficient resource and revolutionize utilization. And its safety technology attracted more and more researches. Primary user emulation (PUE) is a typically easily and largely affecting attack. PUE attacked come from both malicious misbehavior secondary users (MMU) and selfish misbehavior secondary users (SMU). The former was studied much more deeply than the later one. Distinguishing MMU and SMU, a four dimensional continuous time markov chain model to analyze the communication performance of normal secondary users under PUE attacks, and typically affected by SMUs was proposed. Furthermore, several PUE detection technologies were compared. The emulation results indicate that the SMU detection mechanism is essential for the PUE attack detection technology, which can improve the detection effects largely.

Key words: cognition radio networks (CRN); spectrum sensing; communication performance; secondary user; primary user emulation (PUE)

1 引言

认知无线电（CR, cognition radio）技术是解决当前无线电频谱资源紧张和利用率低下的有效技术[1, 2]。在 CR 网络中，未授权的认知用户作为次用户（SU, secondary user）可以动态地使用空闲的授权频谱资源，而不对授权主用户（PU, primary user）产生干扰。为此，SU 需要遵循 2 项基本规则[3]：一

收稿日期：2012-05-04
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2009AA012201）；上海市科委重大科技攻关基金资助项目（08DZ501600）
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2009AA012201) The Committee of Science and Technology of Shanghai Municipality (08DZ501600)

是持续感知目标频带或信道的使用状态，当空闲时方可使用；二是使用过程中要持续监测，一旦发现 PU 使用该频段或信道时，立即退出，防止对 PU 的通信产生影响。规则 2 保证了授权用户的权益，有助于推动 CR 技术向更多的授权频谱资源辐射，但是该规则可能会被不端次用户（MU, misbehavior secondary user）利用来发起拒绝服务（DoS, denial of service）攻击，即仿冒主用户（primary user emulation）攻击[4]。

为了实现 PUE 攻击，通常一组 MU 发送具有与 PU 信号相似特征的仿冒信号，SU 收到仿冒信号之后，误认为 PU 将要通信，故立即退出正在使用的频段，切换到其他可用空闲频段，如果此时无可用空闲频段，则该 SU 中断通信，退出 CR 系统。

目前 PUE 攻击已成为一个热点研究领域，但大部分文献[5,6]研究的是检测和消除技术，针对 PUE 攻击对 CR 系统性能影响的分析比较少，文献[7]将 SU、MU、PU 三者的数目作为主要参量模拟信道占用情况，首次分析了在受到 PUE 攻击条件下 CR 系统的通信阻塞率和中断率的变化情况，该方法为对比 PUE 攻击检测技术的性能提供了有效方法。

由于 MU 分为恶意不端用户（MMU, malicious misbehavior user）和自私不端用户（SMU, selfish misbehavior user）2 大类，前者对 CR 系统破坏性较大，其目的是破坏 CR 系统的正常通信，它通过持续欺骗的手段使 SU 无法使用可用频段，最终不得不频繁切换或离开系统；后者的目的是使得通信效益最大化，首先通过欺骗的手段获得高优先级通信优势后，进行正常通信，然后释放所占用频段，其产生的影响主要是增加了 SU 的阻塞率和中断率。由于 MMU 和 SMU 两者的攻击原因和表现不同，因此，实际系统中需要针对两者的差异分别设计应对措施，目前大多数文献是针对 MMU 的 PUE 攻击设计检测算法，而针对 SMU 的研究较少。

文献[7]和文献[8]提出了 PUE 攻击对 CR 系统性能影响的分析方法，但是均未对 MU 进行详细区分，只笼统地认为 MU 即 MMU，导致该分析方法对 SMU 的适用性打了折扣。本文针对这个问题，把 MU 细化为 2 部分，分别对 2 部分的不同机理进行了研究，提出了四维连续时间马尔可夫链（FDMC, four dimensional continuous time markov chain）分析模型。

2　模型建立

2.1　假定与符号描述

本文在建立模型的过程中，做了以下基本假定。

1) CR 系统中共有 N_C 个可用信道。

2) 每次通信过程都需要占用 1 个信道；CR 系统无等待队列，当新的通信请求到达时，若系统中无可用信道，则该用户发生阻塞（block），不进入系统。

3) SU 检测到 PU 信号或遭受 PUE 攻击时，立即退出当前占用的信道，切换到其他可用信道，如果无可用信道供其切换，则该用户发生中断（drop），离开系统。

4) SU 能够精确检测到 PU。

5) PUE 攻击成功率为 100%。

6) PU、SU 发起通信请求的过程均是 Poisson 过程，到达率分别为 λ_{p}、λ_{s}，占用信道的时间分别服从均值为 μ_{p}、μ_{s} 的负指数分布。

7) MMU、SMU 发起 PUE 攻击的过程是 Poisson 过程，到达率分别为 λ_{mm}、λ_{sm}，占用信道的时间分别服从均值为 μ_{mm}、μ_{sm} 的负指数分布。

8) $N_{\mathrm{s}}(t)$、$N_{\mathrm{mm}}(t)$、$N_{\mathrm{sm}}(t)$ 和 $N_{\mathrm{p}}(t)$ 分别表示 SU、MMU、SMU 和 PU 在时刻 t 所占用的信道数量（在不发生混淆的情况下，为简洁表达，分别用 N_{s}、N_{mm}、N_{sm} 和 N_{p} 代替）。

2.2　模型分析

为了清晰构造 CR 系统通信性能分析模型，下文分别对 SU、MMU、SMU、PU 4 个参量的状态变化情况以及其他需要注意的情况进行分析。

1) SU

①进入系统。由于 SU 是否进入系统只与自身通信需求有关，而与系统中信道占用情况无关，因此 SU 进入系统进行通信的概率是 λ_{s}。

②离开系统。有 3 种情况：一是为避让 PU 而退出；二是因被 MU 欺骗而退出；三是通信结束，自动退出。前两者属于强制意外中断，其发生的概率与 PU、MU 出现的概率有关；第 3 种情况的概率为 $N_{\mathrm{s}}\mu_{\mathrm{s}}$。

2) MMU

①进入系统。MMU 发动 PUE 攻击有 2 类：一是在空闲信道发送仿冒 PU 信号，阻止潜在的 SU 使用；二是向 SU、SMU 正在占用的信道发送仿冒 PU 信号，欺骗 SU、SMU 退出信道。只有当系统

中的信道全被 PU 占用（即 $N_{\mathrm{p}}=N_C$）时，MMU 不发动 PUE 攻击。另外，为了影响 SU 正常通信，一般采取多个 MMU 同时针对不同信道发动 PUE 攻击，为了提高效率，它们之间一般会有某种协同机制，所以不考虑不同 MMU 之间发生欺骗和抢占信道的情况。因此，MMU 进入系统进行通信的概率是 $(N_C-N_{\mathrm{p}}-N_{\mathrm{mm}})\lambda_{\mathrm{mm}}$。

② 离开系统。有 2 种情况：一是为避让 PU 而退出；二是通信结束，自动退出。前者发生的概率与 PU 出现的概率有关；后者发生的概率为 $N_{\mathrm{mm}}\mu_{\mathrm{mm}}$。

3) SMU

①进入系统。分为 3 种情况：一是系统中有可用空闲信道（即 $N_{\mathrm{s}}+N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}<N_C$），则 SMU 直接进行通信；二是系统中没有空闲信道，且不存在 SU 和其他 SMU（即 $N_{\mathrm{mm}}+N_{\mathrm{p}}=N_C$），则 SMU 不进入系统；三是系统中没有空闲信道、但存在 SU 或 SMU（即 $N_{\mathrm{s}}+N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}=N_C$，$N_{\mathrm{s}}\geqslant 1$ 或 $N_{\mathrm{sm}}\geqslant 1$），则 SMU 首先发动 PUE 攻击，一旦抢占 SU 或其他 SMU 的信道后，将停止 PUE 攻击，转而进行 SU 式正常通信。由于 SMU 的目的是为了满足“自私”需求、实现个体利益的最大化，所以不同 SMU 之间一般不会采取协同行动，自然不会知道彼此的身份，从而导致它们之间也会发生欺骗和抢占的情况。因此，SMU 进入系统进行通信的概率是 $(N_C-N_{\mathrm{p}}-N_{\mathrm{mm}})\lambda_{\mathrm{sm}}$。

②离开系统。有 3 种情况：一是为避让 PU 而退出；二是在进行 SU 式通信过程中，因被 MMU 或其他 SMU 欺骗而退出；三是通信结束，自动退出。前两者属于强制意外中断，其发生概率与 PU、MU 出现的概率有关；第 3 种情况发生概率为 $N_{\mathrm{sm}}\mu_{\mathrm{sm}}$。

4) PU

①进入系统。有 2 种情况：一是系统中的信道已经全被 PU 占用（即 $N_{\mathrm{p}}=N_C$），则不进入系统；二是系统中的信道未完全被 PU 所占用（即 $N_{\mathrm{p}}<N_C$），则进入系统，其概率为 $(N_C-N_{\mathrm{p}})\lambda_{\mathrm{p}}$。

②离开系统。只有当通信结束时，PU 才会退出所占用的信道[注]，其概率为 $N_{\mathrm{p}}\mu_{\mathrm{p}}$。

5）其他

①信道切换。有 2 种情况：一是当 SU、MMU、SMU 检测到 PU 出现时，会立即退出当前信道，尝试切换到其他信道；二是当 SU 被 MMU 和 SMU 欺骗、SMU 被 MMU 欺骗时，会尝试切换信道。信道切换能否成功，取决于是否存在可用空闲信道或是否存在可被欺骗用户。

②过程等效。对于当前用户（SU 或 SMU）退出信道 Ch_1，成功切换到信道 Ch_2 的情形，为方便处理，假定切换时间忽略不计，因此可以将此情形等同于当前用户占用 Ch_1、PU 或 MU 直接占用 Ch_2 的情形。当 $N_{\mathrm{s}}+N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}=N_C$，且 $N_{\mathrm{s}}\geqslant 1$、$N_{\mathrm{sm}}\geqslant 1$ 时，如 PU 或 MMU 占用了 SMU 信道而非 SU 信道，则 SMU 会立即切换到 SU 的信道，该 SU 离开系统，此过程在状态分析中等效于 PU 或 MMU 直接占用了 SU 的信道。

3 性能分析

3.1 模型特征分析

经过分析，得到以下结论。

定理 1 令 $X(t)=(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})$，则随机过程 $\{X(t),t\geqslant 0\}$ 为连续时间齐次马尔可夫链。

证明 ①因为 N_{s}、N_{mm}、N_{sm}、$N_{\mathrm{p}}\in[0,N_C]$，N_C 为常数，所以对于任意正整数 $n\geqslant 0$，$\{X(t),t\geqslant 0\}$ 的状态集 $I=\{i_n=X(t_n),n\geqslant 0,t_n\geqslant 0\}$ 为可数集。

② 对于任意 $0\leqslant t_n<t_{n+1}$，有 $X(t_{n+1})=X(t_n)+(t_n,t_{n+1}]$ 表示进入系统的用户数，$-(t_n,t_{n+1}]$ 表示离开系统的用户数，因此 t_{n+1} 时刻系统中的用户数仅与 t_n 时刻系统中的用户数有关，而与 t_n 以前的时刻无关，故马氏性成立。

③ 记 $p_{ij}(s,t)=P\{X(s+t)=j|X(s)=i\}$，其中，$i,j\in I$，$s,t\geqslant 0$，易知转移概率只与初始状态 i、目标状态 j 以及所用时间 t 有关，而与初始时刻 s 无关，即 $p_{ij}(s,t)=p_{ij}(t)$，故齐次性成立。

综上，随机过程 $\{X(t),t\geqslant 0\}$ 为连续时间齐次马尔可夫链。

定理 2 $\{X(t),t\geqslant 0\}$ 为正常返，存在平稳分布 $\{P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}}),(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})\in I\}$。

证明 系统中有可用空闲信道，即 $N_{\mathrm{s}}+N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}<N_C$；系统中无可用空闲信道，分为 2

注：因受到干扰或信道条件发生较大变化而导致 PU 退出系统的情况不属于本文的研究范畴。

种情况：一是存在 SU，即 $N_{\mathrm{s}}+N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}=N_C$ 且 $N_{\mathrm{s}}\geqslant 1$，此时 MMU、SMU、PU 皆可正常进入系统；二是不存在 SU，即 $N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}=N_C$，此时 MMU 可占用 SMU 信道、PU 可占用 MMU 和 SMU 信道。根据第 2 节对各参量和切换、等效等事项的分析，可以得到模型在以上 3 种条件下的状态转移图，如图 1~图 3 所示。从中可以看出，$\{X(t),t\geqslant 0\}$ 各状态皆为正常返，故存在平稳分布。

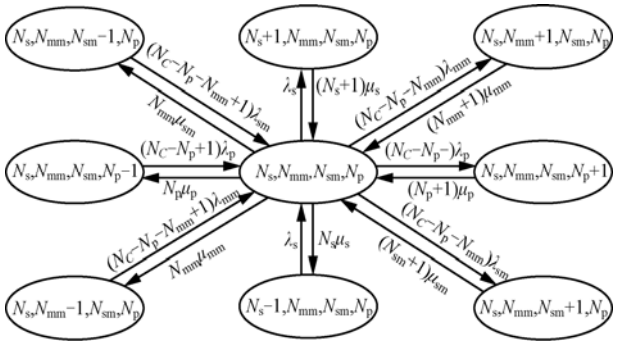

图 1　在 $N_{\mathrm{s}}+N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}<N_C$ 条件的一步状态转移

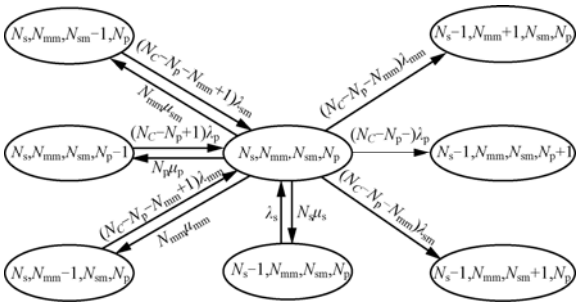

图 2　在 $N_{\mathrm{s}}+N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}=N_C$ 且 $N_{\mathrm{s}}\geqslant 1$ 条件的一步状态转移

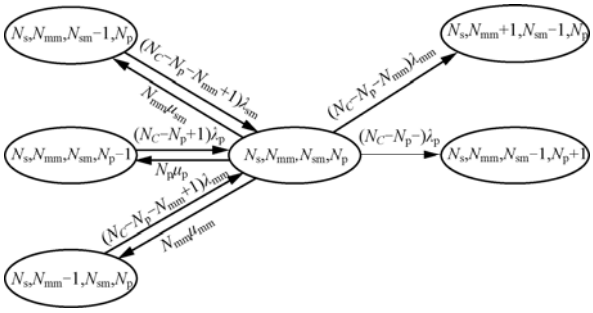

图 3　在 $N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}=N_C$ 条件的一步状态转移

根据图 1~图 3 给出的原则，做出了 $N_C=2$ 的完整状态转移示例，如图 4 所示。

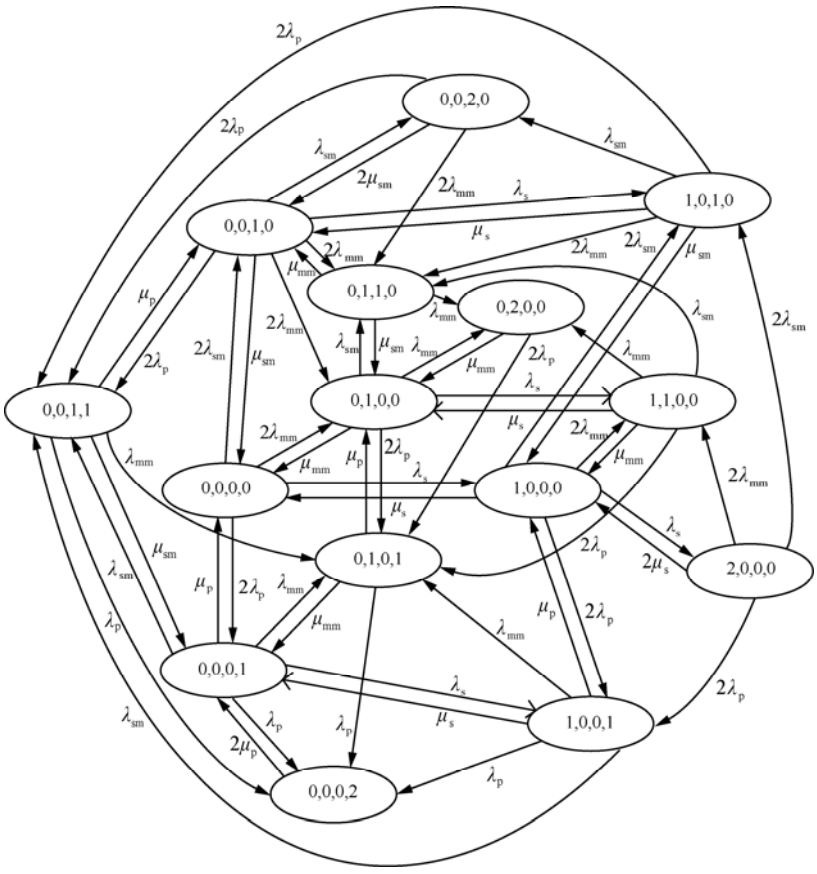

图 4　$N_C=2$ 时状态转移

对于该齐次马尔可夫链，显然存在以下结论：

①对于图 1 情况有

$$\begin{aligned}&P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})=\\&\lambda_{\mathrm{s}}P(N_{\mathrm{s}}-1,N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})+\\&(N_C-N_{\mathrm{p}}-N_{\mathrm{mm}}+1)\lambda_{\mathrm{mm}}P(N_{\mathrm{s}},N_{\mathrm{mm}}-1,N_{\mathrm{sm}},N_{\mathrm{p}})+\\&(N_C-N_{\mathrm{p}}-N_{\mathrm{mm}}+1)\lambda_{\mathrm{sm}}P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}}-1,N_{\mathrm{p}})+\\&(N_C-N_{\mathrm{p}}+1)\lambda_{\mathrm{p}}P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}}-1)+\\&(N_{\mathrm{s}}+1)\mu_{\mathrm{s}}P(N_{\mathrm{s}}+1,N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})+\\&(N_{\mathrm{mm}}+1)\mu_{\mathrm{mm}}P(N_{\mathrm{s}},N_{\mathrm{mm}}+1,N_{\mathrm{sm}},N_{\mathrm{p}})+\\&(N_{\mathrm{sm}}+1)\mu_{\mathrm{sm}}P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}}+1,N_{\mathrm{p}})+\\&(N_{\mathrm{p}}+1)\mu_{\mathrm{p}}P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}}+1)\end{aligned}\tag{1}$$

②对于图 2 情况有

$$\begin{aligned}&P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})=\\&\lambda_{\mathrm{s}}P(N_{\mathrm{s}}-1,N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})+\\&(N_C-N_{\mathrm{p}}-N_{\mathrm{mm}}+1)\lambda_{\mathrm{mm}}P(N_{\mathrm{s}},N_{\mathrm{mm}}-1,N_{\mathrm{sm}},N_{\mathrm{p}})+\\&(N_C-N_{\mathrm{p}}-N_{\mathrm{mm}}+1)\lambda_{\mathrm{sm}}P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}}-1,N_{\mathrm{p}})+\\&(N_C-N_{\mathrm{p}}+1)\lambda_{\mathrm{p}}P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}}-1)\end{aligned}\tag{2}$$

③对于图 3 情况有

$$\begin{aligned}&P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})+\\&(N_C-N_{\mathrm{p}}-N_{\mathrm{mm}}+1)\lambda_{\mathrm{mm}}P(N_{\mathrm{s}},N_{\mathrm{mm}}-1,N_{\mathrm{sm}},N_{\mathrm{p}})+\\&(N_C-N_{\mathrm{p}}-N_{\mathrm{mm}}+1)\lambda_{\mathrm{sm}}P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}}-1,N_{\mathrm{p}})+\\&(N_C-N_{\mathrm{p}}+1)\lambda_{\mathrm{p}}P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}}-1)\end{aligned}\tag{3}$$

④所有情况均满足

$$\sum_{(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})\in I}P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})\tag{4}$$

可以看出，对于任意 $(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})\in I$，$P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})$ 均可由式(1)~式(4)求得。

3.2 SU 通信性能评估

为了对各种检测 PUE 攻击机制的性能进行有效的评估分析，引入以下 2 个性能指标。

1) SU 阻塞率（p_{b}）。当 SU 到达系统时，系统内无可用空闲信道，则 SU 不进入系统，发生通信阻塞，可由下式求得

$$\begin{aligned}p_{\mathrm{b}}=&\sum_{N_{\mathrm{s}}=0}^{N_C}\sum_{N_{\mathrm{mm}}=0}^{N_C}\sum_{N_{\mathrm{sm}}=0}^{N_C}\sum_{N_{\mathrm{p}}=0}^{N_C}[P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})\cdot\\&\gamma(N_{\mathrm{s}}+N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}=N_C)]\end{aligned}\tag{5}$$

其中，$\gamma(N_{\mathrm{s}}+N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}=N_C)$ 满足

$$\gamma=\begin{cases}1, & N_{\mathrm{s}}+N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}=N_C\\0, & N_{\mathrm{s}}+N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}<N_C\end{cases}\tag{6}$$

2) SU 中断率（p_{d}）。正在通信的 SU 因避让 PU 或被 MMU、SMU 欺骗而退出所占信道，但又无其他空闲信道可供切换，则该 SU 离开系统，发生通信中断，可由下式求得

$$\begin{aligned}p_{\mathrm{d}}=&\frac{(N_C-N_{\mathrm{p}})\lambda_{\mathrm{p}}+(N_C-N_{\mathrm{p}}-N_{\mathrm{mm}})(\lambda_{\mathrm{mm}}+\lambda_{\mathrm{sm}})}{\lambda_{\mathrm{s}}+(N_C-N_{\mathrm{p}})\lambda_{\mathrm{p}}+(N_C-N_{\mathrm{p}}-N_{\mathrm{mm}})(\lambda_{\mathrm{mm}}+\lambda_{\mathrm{sm}})}\cdot\\&\sum_{N_{\mathrm{s}}=1}^{N_C}\sum_{N_{\mathrm{mm}}=0}^{N_C}\sum_{N_{\mathrm{sm}}=0}^{N_C}\sum_{N_{\mathrm{p}}=0}^{N_C}[P(N_{\mathrm{s}},N_{\mathrm{mm}},N_{\mathrm{sm}},N_{\mathrm{p}})\gamma(N_{\mathrm{s}}+\\&N_{\mathrm{mm}}+N_{\mathrm{sm}}+N_{\mathrm{p}}=N_C)]\end{aligned}\tag{7}$$

3) 检测因子（p_{detect}）、攻击成功率因子（p_{PUE}）。在实际系统中，SU 对 PU 的检测可能会受到各种因素的影响，无法达到 100%，即 2.1 节中的假定 4) 将不成立。针对这种情况，设置一个新的参量——检测因子 p_{detect}，在计算 SU 阻塞率和中断率时只需要将式(5)、式(7)中 PU 到达率由 λ_{p} 换为 $P_{\mathrm{detect}}\lambda_{\mathrm{p}}$ 即可，P_{detect} 的大小根据实际情况进行设置。同样地，实际中 PUE 攻击也不会全部成功，尤其是系统增加了检测 PUE 攻击的机制之后，2.1 节中的假定 5) 失效，引入 PUE 攻击成功率因子 P_{PUE}，将式(5)、式(7)中的 λ_{mm} 换为 $P_{\mathrm{PUE}}\lambda_{\mathrm{mm}}$、$\lambda_{\mathrm{sm}}$ 换为 $P_{\mathrm{PUE}}\lambda_{\mathrm{sm}}$ 即可，由于不同的 PUE 攻击检测机制的性能各异，因此 p_{PUE} 的大小需要根据系统实际情况进行设置。在相同条件下，可以用 $(1-p_{\mathrm{PUE}})$ 的大小来作为衡量 PUE 攻击检测技术的参考指标之一。当系统未受到 PUE 攻击，即 $\lambda_{\mathrm{mm}}=\lambda_{\mathrm{sm}}=0$、$\mu_{\mathrm{mm}}=\mu_{\mathrm{sm}}=0$ 时，$p_{\mathrm{detect}}=p_{\mathrm{PUE}}=0$。

4) SMU 对 SU 性能的影响因子（μ_{sm}）。SMU 攻击发起的前提是 CR 网络中不存在空闲信道，即 $\gamma=1$，而当网络中存在空闲信道时，不会发生 SMU 攻击，因此 SU 因 SMU 攻击发生阻塞的概率 $p_{\mathrm{b}}^{\mathrm{sm}}$ 为

$$p_{\mathrm{b}}^{\mathrm{sm}}=p_{\mathrm{b}}\frac{N_{\mathrm{sm}}}{N_{\mathrm{mm}}+N_{\mathrm{sm}}}\tag{8}$$

同理，SU 因 SMU 攻击发生中断的概率 $p_{\mathrm{d}}^{\mathrm{sm}}$ 为

$$p_{\mathrm{d}}^{\mathrm{sm}}=p_{\mathrm{d}}\frac{N_{\mathrm{sm}}}{N_{\mathrm{mm}}+N_{\mathrm{sm}}}\tag{9}$$

令

$$\zeta_{\mathrm{sm}}=\frac{N_{\mathrm{sm}}}{N_{\mathrm{mm}}+N_{\mathrm{sm}}}\tag{10}$$

4 仿真分析

在仿真时，假定 $\lambda_{\mathrm{p}}=1$ 次/h、$\lambda_{\mathrm{s}}=600$ 次/h、

$1/\mu_p$=24 s、$1/\mu_s$=36 s、N_{mm}=30、ζ_{sm}=0.4、$\lambda_m=\lambda_{mm}+\lambda_{sm}$=150 次/h、$1/\mu_{mm}$=80 s、$\mu_{sm}=\mu_s$。

对不存在 PUE 攻击、存在 MMU 而不存在 SMU、存在 MMU 和 SMU 3 种情况分别进行仿真，得到了 SU 的阻塞率和中断率随信道数量变化的曲线，如图 5 和图 6 所示。在 N_C=10 的条件下，对比了无 PUE 攻击、存在 PUE 攻击但无检测技术、独立 PUE 攻击检测技术[9]、具有 SMU 检测功能的独立 PUE 攻击检测技术[9,10]、协同 PUE 攻击检测技术[11]、具有 SMU 检测功能的协同 PUE 攻击检测技术[10, 11]6 种情况下的 SU 中断率随 PUE 攻击到达率的变化趋势，得到了图 7 所示的结果。

从图 5 中可以看出：1) 本文所提原理得到的理论值与蒙特卡洛仿真计算的仿真值比较符合，验证了本文所提阻塞率计算方法的有效性；2) 不存在 PUE 攻击时也会有一定的阻塞率，这是由于 PU、SU 已将可用信道占满，后续 SU 就被阻塞了；3) 当可用信道数量较少时，PUE 攻击对阻塞率影响较大，随着信道数量的增加，阻塞率逐渐降低，当 N_C>12 时，p_b 趋近于 0；4) 信道数量较少时，SMU 对 p_b 影响较大，存在 SMU 的情况与只存在 MMU 的情况相比，p_b 增幅接近 80%。

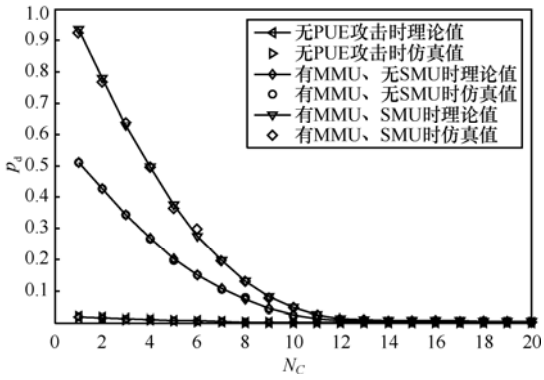

图 5　在 3 种条件下阻塞率随信道数量的变化情况

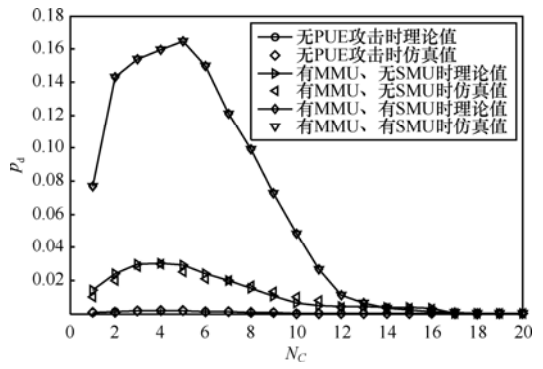

图 6　在 3 种条件下中断率随信道数量的变化情况

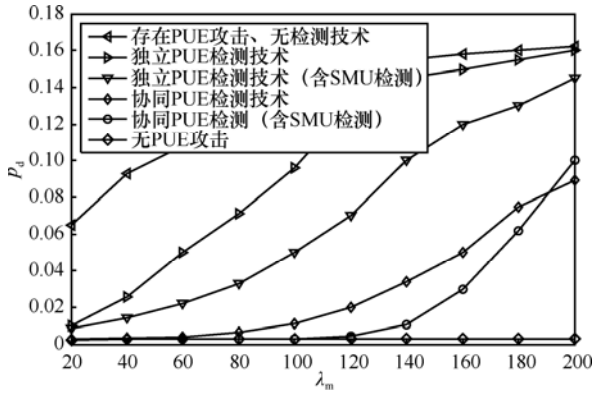

图 7　不同 PUE 检测技术的性能比较

从图 6 中可以看出：1) 理论值与仿真值相符，中断率计算方法是有效的；2) 在信道占满的情况下，若再有 PU 出现，则正在通信的部分 SU 中断数据传输退出信道，这就导致即使不存在 PUE 攻击时仍会存在一定的中断率；3) 当可用信道数量较少（N_C<5）时，中断率随信道数量的增加而增加，这是由于信道数量少导致 SU 阻塞率比较高，信道数量的小幅增加并不能满足 SU 通信的需求，新增的信道会立即被涌入的 SU 所占用，此时 PUE 的出现会迫使更多的 SU 退出所占信道，而此时又无可供切换的空闲信道，从而产生大量的中断情况；4) 当信道数量逐步增加到可以满足 SU 切换需求（N_C>5）时，中断率呈现出下降趋势，当 N_C>16 时，p_d 趋近于 0；5) SMU 对 SU 的影响比较大，尤其是当信道数量有限时，SMU 的自私行为会严重干扰其他 SU 的正常通信，因此对 SMU 的检测很有必要。

从图 7 中可以看出：1) 不同的 PUE 攻击检测技术的性能大不相同；2) 随着 λ_m 的增加，SU 中断率迅速提高；3) 协作检测机制能够有效降低 PUE 攻击的影响；4) 包含 SMU 检测机制的算法比不含该机制的算法性能优化很多；5) 在 PUE 低强度攻击（λ_m＜160）时，SMU 检测机制能够有效地提高 PUE 检测算法的性能，最高能够提高 40% 左右，这与 ζ_{sm}=0.4 相符；当 PUE 高强度攻击时，SMU 检测机制的效果逐渐变得不再明显。

5　结束语

本文针对认知无线电网络 PUE 攻击下的 SU 通信性能分析进行了建模，提出 FDMC 分析模型。该模型考虑了 PU、SU、MMU 和 SMU 4 个参量，分别对各参量的状态和变化趋势进行了详细分析，并重点对 SMU 的工作原理进行了研究，得到了 SU

在 PUE 攻击下的阻塞率和中断率。本文对比了多种 PUE 检测技术的优劣，并通过数据说明了 PUE 检测技术引入 SMU 检测机制的必要性。

参考文献：

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

[2] Federal Communications Commission. Notice of Proposed Rule Making and Order: Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies[R]. ET Docket NO.03-108. 2005.

[3] BALDO N, ASTERJADHI A, GIUPPONI L, *et al*. A scalable dynamic spectrum access solution for large wireless networks[A]. ISWPC 5th IEEE International Symposium on Wireless Pervasive Computing[C]. Modena, Italy, 2010. 430-435.

[4] BALDINI G, STURMAN T, BISWAS A, *et al*. Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead[J]. IEEE Communications Surveys & Tutorials, 2011, 14(2):1-25.

[5] JIN Z, ANAND S, SUBBALAKSHMI K P. Detecting primary user emulation attacks in dynamic spectrum access networks[A]. ICC IEEE International Conference on Communications[C]. Dresden, Germany, 2009. 1-5.

[6] LIU Y, NING P, DAI H. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures[A]. IEEE Symposium on Security and Privacy (SP)[C]. San Francisco, USA, 2010. 286-301.

[7] JIN Z, ANAND S, SUBBALAKSHMI K P. Performance analysis of dynamic spectrum access networks under primary user emulation attacks[A]. Proceedings of IEEE Globecom 2010[C]. Miami, USA, 2010. 1-5.

[8] ANAND S, JIN Z, SUBBALAKSHMI K P. An analytical model for primary user emulation attacks in cognitive radio networks[A]. Proceedings IEEE DySPAN 2008[C]. Chicago, USA, 2008. 1-6.

[9] JIN Z, ANAND S, SUBBALAKSHMI K. Detecting primary user emulation attacks in dynamic spectrum access networks[A]. IEEE International Conf Commun[C]. Dresden, Germany, 2009. 1-5.

[10] WANG W K, LI H S, SUN Y, *et al*. Research article securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks[J]. EURASIP Journal on Advances in Signal Processing, 2010, 2010(2010):1-15.

[11] CHEN C, CHENG H B, YAO Y D. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack[J]. IEEE Transactions on Wireless Communications, 2011, 10(7):2135-2141.

作者简介：

王珊珊（1983-），女，河北邢台人，国家数字交换系统工程技术研究中心博士生，解放军 61580 部队助理工程师，主要研究方向为移动通信安全。

罗兴国（1951-），男，重庆人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为无线通信、高性能计算机。

李鹏（1983-），男，河北邢台人，硕士，解放军 95949 部队助理工程师，主要研究方向为移动通信技术。