文章编号：2095-4980(2018)04-0625-06

基于 AD9361 的智能屏蔽系统设计与实现

杨　勇，夏文龙，史晓荻，郭庆功

(四川大学 电子信息学院，四川 成都 610065)

摘　要：针对传统压制式干扰仪对采用扩频技术的宽带码分多址(WCDMA)干扰不理想，以及 WCDMA 欺骗式干扰仪实现复杂的问题，基于 PicoZed SOM 软件定义无线电平台设计出一套新型智能干扰系统。实验测量表明，该系统发射功率仅为 23 dBm 时，能有效管控半径 10 m 范围的 WCDMA 通信信号。整个设计的实现分为 4 个步骤：第 1 步基于 WCDMA 的小区搜索过程，设计出一种带有 WCDMA 小区同步特征的干扰信号；第 2 步使用 MATLAB 仿真验证该方法的有效性；第 3 步设计 WCDMA 干扰模块和 WCDMA 数字上变频模块，实现在 FPGA 上产生带有同步信息的干扰信号；第 4 步基于 ADI 提供的 PicoZed SOM 参考工程，实现在空口发射 WCDMA 干扰信号。

关键词：智能干扰；AD9361；软件无线电；宽带码分多址；小区搜索

中图分类号：TN972^{+}.31　　**文献标志码：**A　　**doi：**10.11805/TKYDA201804.0625

Design and implementation of intelligent shielding system based on AD9361

YANG Yong，XIA Wenlong，SHI Xiaodi，GUO Qinggong

(School of Electronic and Information，Sichuan University，Chengdu Sichuan 610065，China)

Abstract：The jamming effect of traditional blocking jammer on Wideband Code Division Multiple Access(WCDMA) by using spread spectrum technology is not good, and the implementation of WCDMA deceptive jammer is complex. An intelligent jamming system is designed based on the PicoZed SOM. Experiments show that when transmitted power is set at 23 dBm, this system can effectively block a range of ten meters WCDMA communication signal. The whole design is divided into four steps: firstly, a kind of jamming signal with the cell synchronization characteristics of WCDMA is designed based on WCDMA cell search process; secondly, MATLAB is adopted to verify the effectiveness of the method; thirdly, WCDMA jamming module and WCDMA DUC(Digital Up Converter) module are designed to generate the jamming signal on FPGA; lastly, the system is implemented based on the PicoZed SOM reference project provided by ADI to transmit WCDMA jamming signal to the air.

Keywords：intelligent interference；AD9361；software defined radio；Wideband Code Division Multiple Access(WCDMA)；cell search

移动通信的快速发展给人们的生活带来了极大方便，但是在某些特殊场合(如大型考试、保密会议等)需要使用干扰设备对通信进行管制。干扰仪根据干扰信号的作用机理可以分为压制式干扰仪和欺骗式干扰仪[1]。传统的压制式干扰仪发射噪声或类似噪声的干扰信号淹没特定频段的有用信号，使接收机的信噪比大大下降，进而导致解调出错[2-3]。然而，采用码分多址和扩频技术的宽带码分多址(WCDMA)解调所需的信噪比极低，使得压制式干扰极难产生效果，或者是要付出相当大的功率代价才能换取微弱的干扰效果。而过高的发射功率又会产生电磁辐射，对人类的健康造成影响[4-5]。

针对以上问题，提出了一种产生带有小区同步特征干扰信号的干扰方法。通过理论分析和仿真，验证了该方法的有效性，并基于 PicoZed SOM 软件无线电平台(该平台将 Xilinx ZYNQ 与 AD9361 集成在一起：AD9361 是一款高性能、高度集成的射频收发器，设计用于射频应用，如 3G 和 4G 基站以及测试设备、软件定义无线电等；ZYNQ 是一款组合了 FPGA 和 ARM 的芯片)设计实现了一套智能干扰系统。实验测量表明，该系统发射功率仅为 23 dBm 时，达到了良好的干扰效果。

收稿日期：2017-10-06；修回日期：2017-11-22

1 干扰信号设计

WCDMA 与小区搜索相关的下行信道有主同步信道(P-SCH)、辅同步信道(S-SCH)和主导频信道(P-CPICH)[6-7]，干扰信号通过包含这些信道使其带有小区的同步特征信息。该信号与 WCDMA 的帧结构类似，每 10 ms 的无线帧包含 15 个时隙,每个时隙包含 2 560 个码片。在每个时隙的前 256 个码片发送 P-SCH 和 S-SCH，该信道相对于基站的同步信道有一定的偏移量，使得干扰信号与基站信号叠加时可以破坏 SCH 检测。在每个时隙的后 2 304 个码片发送 P-CCPCH，生成特定的扩频码和扰码对其进行扩频和加扰，与同步信道叠加组成完整的帧。在每个时隙都发送 P-CPICH 信道，同样生成规定的扩频码和扰码对其进行扩频和加扰，该信道相对于基站的导频信道有一定的偏移量且发射功率可调，因此移动终端即使已经保存了当前基站的主扰码(再次开机时不再检测 P-SCH 和 S-SCH 而是直接利用主扰码直接检测 P-CPICH)，也能使终端设备切换到干扰导频上。最后将这些信号码字叠加在一起，组成带有 WCDMA 同步信息的干扰信号，如图 1 所示。

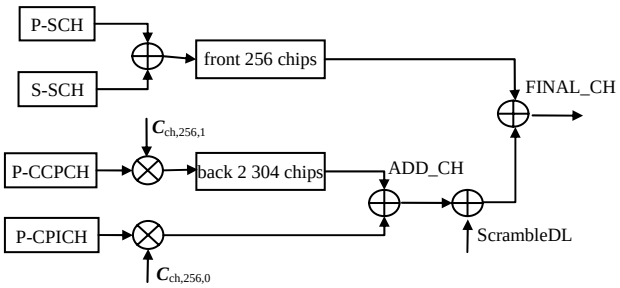

Fig.1 Composition of the jamming signal
图 1 干扰信号组成

2 干扰信号仿真验证

文献[8]中对带有小区同步特征的干扰方法进行了初步的探索分析，为了进一步验证该方法的有效性，使用 Matlab 在无干扰和有干扰 2 种情形下对 P-SCH 检测进行了仿真。图 2 是无干扰时对 5 个空口无线帧的 P-SCH 的峰值检测结果，每一帧中 P-SCH 的相关峰值有 15 个，并且分布均匀。图 3 是干扰后的检测结果，每一帧中 P-SCH 的相关峰值不再是 15 个，这会导致接收机在进行 P-SCH 信道检测时失败，进而 S-SCH 和 P-CPICH 的检测也会失败。

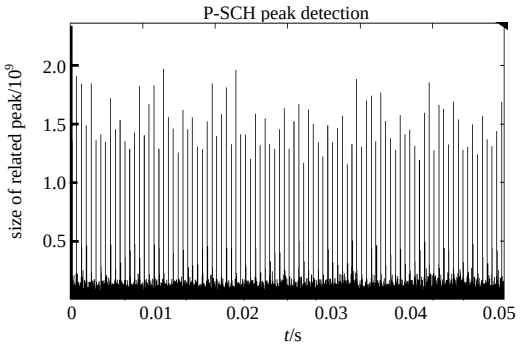

Fig.2 Result of P-SCH peak detection(no jamming)
图 2 P-SCH 峰值检测结果(无干扰)

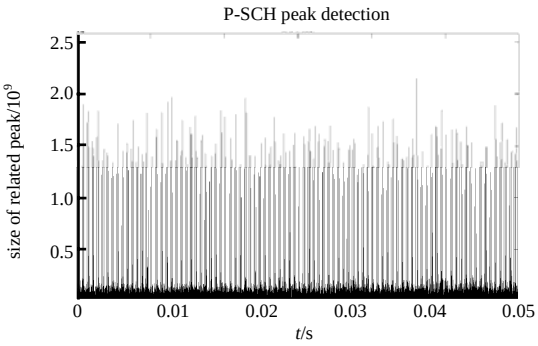

Fig.3 Result of P-SCH peak detection (jamming)
图 3 P-SCH 峰值检测结果(干扰)

3 干扰信号 FPGA 实现

3.1 WCDMA 干扰模块设计

至此已经通过理论分析和仿真验证了该方法的有效性，接下来将使用 FPGA 生成干扰信号。依据协议标准，使用 VHDL 编写 WCDMA 干扰模块：输入 CLK 为 61.44 MHz，输出信号 CH_I 和 CH_Q 的速率为 3.84 Msps，数据有效时 valid 输出高电平。顶层模块主要包含 SCH 模块、P_CCPCH 模块、ScrambleDL 模块和 Scrambling 模块。使用 Vivado 工具对 WCDMA 干扰模块进行综合后仿真，图 4 是仿真结果的部分截取。

Fig.4 Simulation of jamming module
图 4 干扰模块仿真时序图

3.2 WCDMA 数字上变频模块设计

WCDMA 在工作频带内包含 3 个信道,因此要实现有效干扰,还需设计 WCDMA 数字上变频模块对 WCDMA 干扰模块生成的信号做进一步处理，使输出也包含 3 个信道。文献[9]中设计的单载波的 WCDMA 数字上变频模型，使用的软件版本和硬件平台不满足本文设计要求，需要移植到 ZYNQ 平台。同时根据协议规定的 WCDMA 下行发射路径指标进行设计[10]。并修改了混频部分，实现了 3 载波的数字上变频模块。

图 5 是在 Xilinx System Generator 中实现的 WCDMA 数字上变频模型，I 路和 Q 路使用相同的硬件结构，工作时钟为 61.44 MHz。整个设计由 2 部分组成：滤波器模块和混频器模块。滤波器模块功能框图如图 6 所示，由 4 级滤波器组成，使用 FIR 滤波器实现。第一级为根升余弦(Root Raised Cosine，RRC)滤波器，实现 2 倍的插值，使用 44 阶的 Chebyshev 窗，旁瓣衰减为 27 dB，截止频率 1.92 MHz，过采样率为 7.68 MHz，成形因子为 0.22；后面 3 级是半带(Half Band，HB)滤波器，每级的插值系数都为 2，表 1 是半带滤波器的参数设置。输入数据速率为 3.84 Msps，总共实现了 16 倍的插值，最后输出速率为 61.44 Msps。

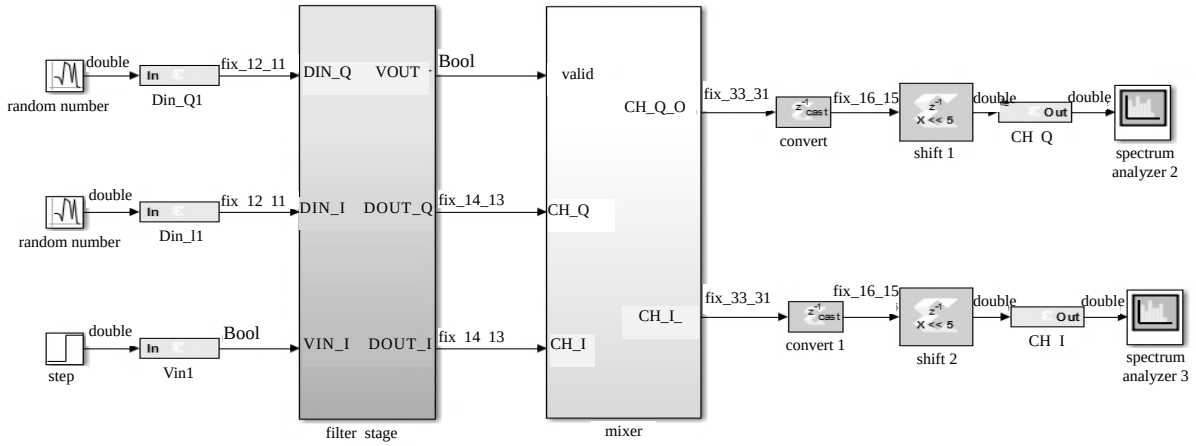

Fig.5 WCDMA DUC model
图 5 WCDMA 数字上变频模型

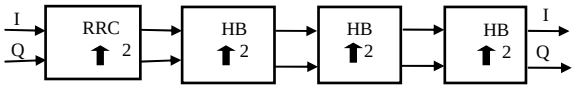

Fig.6 Filter module
图 6 滤波器模块

表 1 半带滤波器的参数
Table1 Parameters of half band filter

parameter	first stage	second stage	third stage
passband frequency/MHz	2.340	2.340	2.340
oversampling frequency/MHz	15.360	30.720	61.440
ripple voltage/dB	0.002	0.002	0.001
filter order	22	10	10
stopband attenuation/dB	80	80	10

混频器的功能框图如图 7 所示,使用 2 个 Xilinx DDS IP 核产生 2 路复数正弦信号,频率分别为 5 MHz 和 10 MHz，与滤波器模块输出的信号进行复数乘法。通过加法器将 3 路信号叠加在一起，再通过一个通带为 13 MHz，阻带为 15 MHz 的低通滤波器，最后输出中频信号的 I 路和 Q 路。

对 WCDMA 上变频模块进行软硬件协同仿真，使用随机数作为输入。图 8 是信号经过成形、插值和混频之后输出信号的频谱，该频谱是双边谱。只看正频率部分，刚好为 3 个载波。

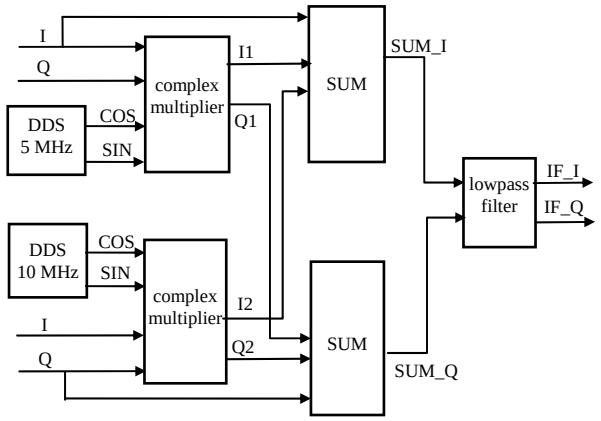

Fig.7 Mixer module
图 7 混频模块

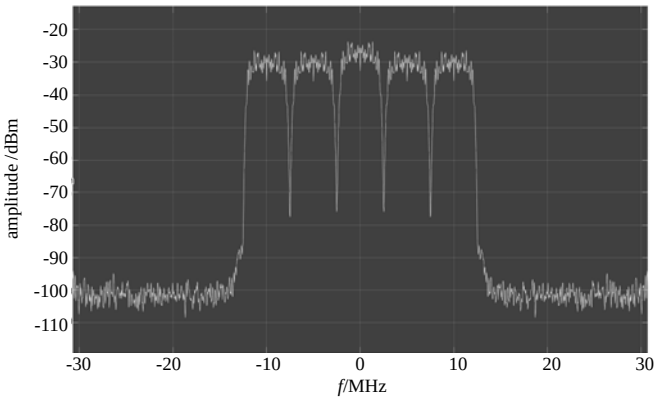

Fig.8 Simulation of DUC module
图 8 上变频模块仿真

4 智能干扰系统搭建

基于 ADI 官网提供的 PicoZed SOM 工程，在 FPGA 部分使用设计的 WCDMA 干扰模块和 WCDMA 数字上变频(DUC)模块修改信号发射路径，使发射的信号变成带有同步信息的干扰信号；在 ARM 部分修改程序完成对 AD9361 的配置:设置数字接口的数据速率为 61.44 MHz,设置发射本振(Local Oscillator,LO)的频率为 2 132.6 MHz。调节 AD9361 的衰减器的衰减值和宽带射频功放的增益来控制输出信号的功率。最后用天线发射信号到空口。实现信号发射的框图如图 9 所示。

智能干扰系统实物如图 10 所示，由 PicoZed SOM、宽带射频放大器和全向天线 3 部分组成。放大器工作频率范围为 800~2 400 MHz，最大增益 35 dB(可设置衰减值改变增益值)，饱和功率 37 dBm。天线的阻抗带宽为 800~3 000 MHz，增益 2 dBi。将修改后的工程用 Xilinx SDK 工具生成 BOOT.BIN 文件，拷贝到 SD 卡中，配置软件无线电平台从 SD 卡启动，就可以产生带有 WCDMA 同步信息的干扰信号。使用 Protek7830 频谱仪观察未接放大器时发射信号频谱，如图 11 所示：干扰信号成功覆盖了 WCDMA 的 3 个频点(f_1=2 132.6 MHz, f_2=2 137.6 MHz, f_3=2 142.6 MHz)。

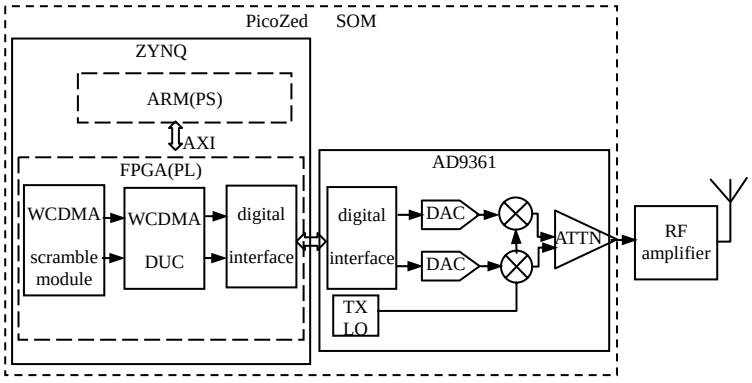

Fig.9 Block diagram of intelligent jamming system
图 9 智能干扰系统结构框图

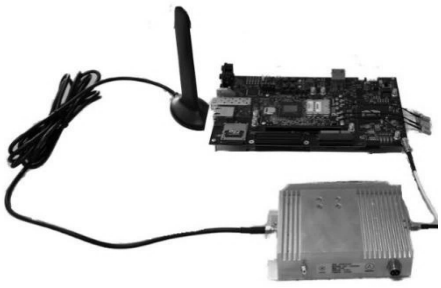

Fig.10 Intelligent jamming system
图 10 智能干扰系统实物

Fig.11 Spectrum of jamming signal
图 11 干扰信号频谱

5　系统测试

对系统进行干扰效果测试，测试框图如图 12 所示，使用 2 部联通手机放置在距离智能干扰系统 10 m 处，测试时关闭 4G，打开市面上某款通用干扰仪屏蔽 2G，打开智能干扰系统产生一定功率的 WCDMA 干扰信号，干扰 1 min 之后，拨打未干扰区域的手机，通过能否打通电话来验证干扰的有效性。进行新的一次测量时，先关闭智能干扰系统，待被干扰手机恢复 3G 信号后，再打开智能干扰系统，干扰成功后再拨打第 2 次电话。测试结果见表 2，屏蔽效果一栏 10/0，10 表示拨打电话的次数，0 表示打通的次数。从表 2 中可以看到，发射功率仅为 23 dBm 时，系统对 WCDMA 具有稳定的干扰效果。

采用同样的方法测量通用干扰仪对 WCDMA 的干扰效果，测量距离仍为 10 m，关闭待测手机 4G 功能，打开该干扰仪屏蔽 2G 和 3G。此时 WCDMA 所在频段的发射功率为 31.22 dBm，且该干扰仪使用的定向天线会产生较强的电磁污染。测量结果为：安卓手机拨打 10 次接通 3 次，苹果手机拨打 10 次接通 2 次。结果显示该压制式干扰仪满功率发射，也未能实现稳定的干扰。

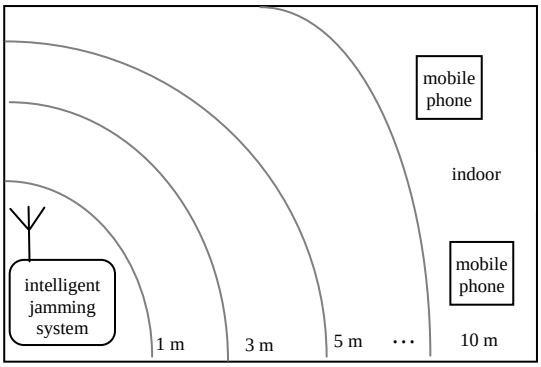

Fig.12 Schematic map of jamming effect test
图 12　干扰效果测试图

表 2　智能干扰系统 10 m 测试结果
Table2 Test results of intelligent jamming system at 10 m

transmit power/dBm	Android	iPhone
27.02	10/0	10/0
26.03	10/0	10/0
25.04	10/0	10/0
23.03	10/0	10/0
20.01		

6　结论

基于 PicoZed SOM 软件无线电平台设计实现了一套智能干扰系统，该系统能产生带有 WCDMA 小区同步信息的干扰信号来破坏手机与基站之间的同步，进而实现干扰。该系统以高集成度的 AD9361 射频芯片为核心实现了小型化。实验测量表明，系统发射信号功率为 23 dBm 时，能有效管控半径 10 m 范围的 WCDMA 通信信号，比测试时使用的通用压制式干扰仪发射功率低 8 dB。

参考文献：

[1] GROVE K,LIM A,YANG Q. Jamming and anti-jamming techniques in wireless networks:a survey[J]. International Journal of Ad Hoc and Ubiquitous Computing, 2014:197–215.

[2] NKORDEH N,LAWSON I C,IDACHABA F,et al. Design and implementation of a dual band mobile phone jammer[C]// World Congress on Engineering & Computer Science. San Francisco,USA:[s.n.], 2016.

[3] DIVYA E,ASWIN R. Design of user specific intelligent cell phone jammer[C]// International Conference on Recent Advances in Information Technology. Dhanbad,India:IEEE, 2012:312–316.

[4] LIN J C. Human exposure to RF,microwave,and millimeter-wave electromagnetic radiation[J]. IEEE Microwave Magazine, 2016,17(6):32–36.

[5] SHEKOOHI S F,MORTAZAVI S A R,JARIDEH S,et al. Short-term exposure to electromagnetic fields generated by mobile phone jammers decreases the fasting blood sugar in adult male rats[J]. Journal of Biomedical Physics & Engineering, 2016, 6(1):27–32.

[6] 3GPP. Technical Specification TS 25.211, Physical channels and mappping of transport channels[S]. 2017.

[7] 3GPP. Technical Specification TS 25. 213, Spreading and modulation[S]. 2017.

[8] 李仕超. 一种基于同步技术的 WCDMA 智能干扰仪设计与实现[D]. 成都:四川大学, 2015. (LI Shichao. Design and implementation of WCDMA smart interferometer based on synchronization technology[D]. Chengdu,China:Sichuan University, 2015.)

[9] HELEN T,KEVIN N,RAMON U,et al. Designing efficient wireless digital up and down converters leveraging core generator and system generator[EB/OL]. (2007–10–22)[2017–10–06]. http://www.xilinx.com/support/XAPP1018.

[10] 3GPP. Technical Specification TS 25.104, Radio transmission and reception[S]. 2017–06.

(下转第 644 页)