**网络空间安全导论大作业（二）**

学号： 姓名：

* 移动通信网络安全实例介绍——伪基站

近年来，“伪基站”作为非法无线电台站不仅非法占用频率、扰乱正常通信，更是被犯罪分子利用，发送诈骗信息，形成了巨大的社会危害。

伪基站系统组成可分为移动终端模拟器、基站模拟器、控制系统和电源系统。移动终端模拟器，实际就是一部简易手机，其作用是对所在蜂窝小区实现扫描与检测，获取该区域基站参数代码。基站模拟器，伪装运营商基站功能，按照移动终端获取的基站数据，自动设置该蜂窝小区的基站参数，完成对正常用户终端连接请求和数据收发。控制系统主要功能是时钟同步、信号基带处理、控制信道和更新地理位置等核心功能，提供人工操作平台，用于人工参数设定和短信内容编辑等。

现在主流的伪基站仍以GSM为接入系统，这主要依赖于GSM的鉴权漏洞，即GSM只采用单向鉴权的策略。在GSM系统之下，基站和手机建立通信时，基站对MS验证，但MS检测不到基站的通信权限，无法核实基站的身份是否合法。伪基站正是利用基站的这一特性，来对MS进行攻击。

伪基站工作时，首先搜集当前蜂窝内的载频信息，然后按照该信息频率持续发射相同频率的载频，一旦MS进入该蜂窝内，伪基站将该MS强行切换到GSM伪蜂窝小区中，对原正常基站的信号进行干扰和屏蔽。通过对MSC和BSC的信令模拟，完成对目标MS的IMSI、IMEI的侦测、阻塞并强行接入。MS在伪基站信号下进行位置更新，网络登记，相关人员通过后台分析可以获得用户的IMSI、IMEI及手机号码等关键信息，进一步获取用户信息。

伪基站能够强行切换MS的GSM伪蜂窝小区的原因和MS的一个特性有关。MS有一个广播频点信息列表，该列表会列出6个周围合法的基站频点和信号强度值，根据这些参数，MS会自动接入信号强大的基站。因此，当靠近频率与目标频率相符且信号强于正常基站的伪基站时，MS便会被自动入侵，与伪基站连接，交换信令。并且由于在GSM体制下，伪基站可以直接向MS发送信令来获取IMSI码。在请求通信时，伪基站直接发送IMSI请求给手机，完成连接建立，待通信结束后，手机向伪基站返回IMSI码，伪基站收到IMSI后，释放MS。

伪基站的有以下几个特点，伪基站的识别也主要依靠这几个特点：

首先，伪基站与正常基站的C1、C2值有显著差异。伪基站会通过增大发射功 率调高C1、C2的参数，使MS顺利进入伪基站通信网络。因此可以通过检测基站的C1和C2值来辨别伪基站。

其次，MS在伪基站工作区域时，会发起位置更新、手机重选、位置再次更新等反应，致使手机在 20~30s的脱网。因此，伪基站会造成大量的位置更新，辨别伪基站也可统计手机位置更新频次。

再次，伪基站没有语音业务，并且存在大量相同长度的短信业务，因此可以检测分析基站的独立专用控制信道（SDCCH）信息。

最后，伪基站的LAI通常被设置为边界数值，因此也可以通过检测基站的LAI来识别伪基站。

对伪基站的布防，一个可行的做法是构建网格化查管一体化平台。

平台结合手机终端大数据、云计算技术、运营商“网格化”通信基础建设、无线电管理部门无线监测网络和公安部门现有卡扣等技术设施，再叠加伪基站侦测设备，实现网格化查管一体化平台。该平台的终端对人员密集区、重要路口24小时自动侦测，一旦出现伪基站信息，自动记录、报警、传输回指挥中心。从发现到查处，实现准实时性，对可疑车辆和行人的研判提供准确的情报支持，进一步缩短伪基站的案件排查时间，节约人力物力的投入，提高打击效率。

基于伪基站的巨大社会危害，我们要持续加强对伪基站的研究，完善形成行之有效的查处机制，为有力打击其犯罪活动提供有力的技术支撑。