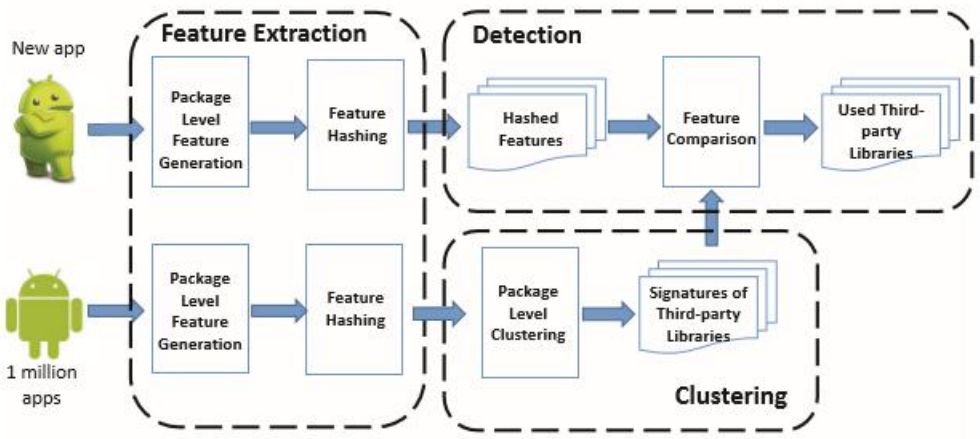
LibRadar 第三方库检测

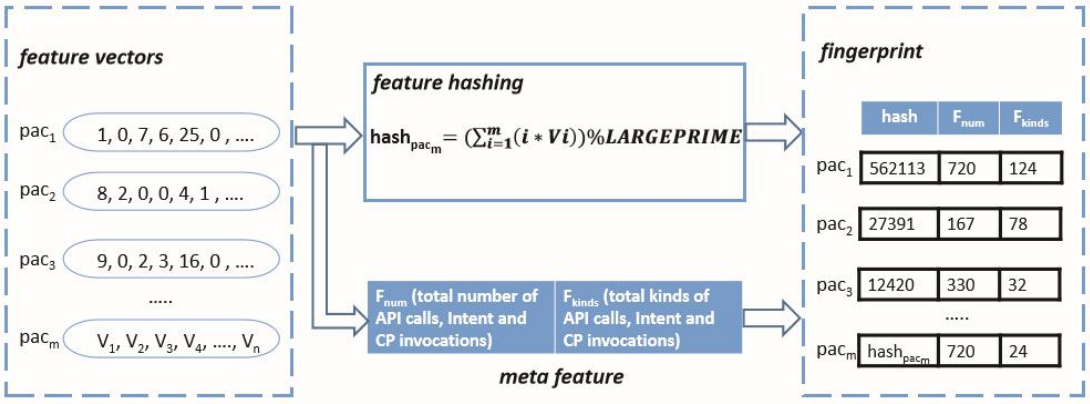
一．方法概述：



1.特征提取：

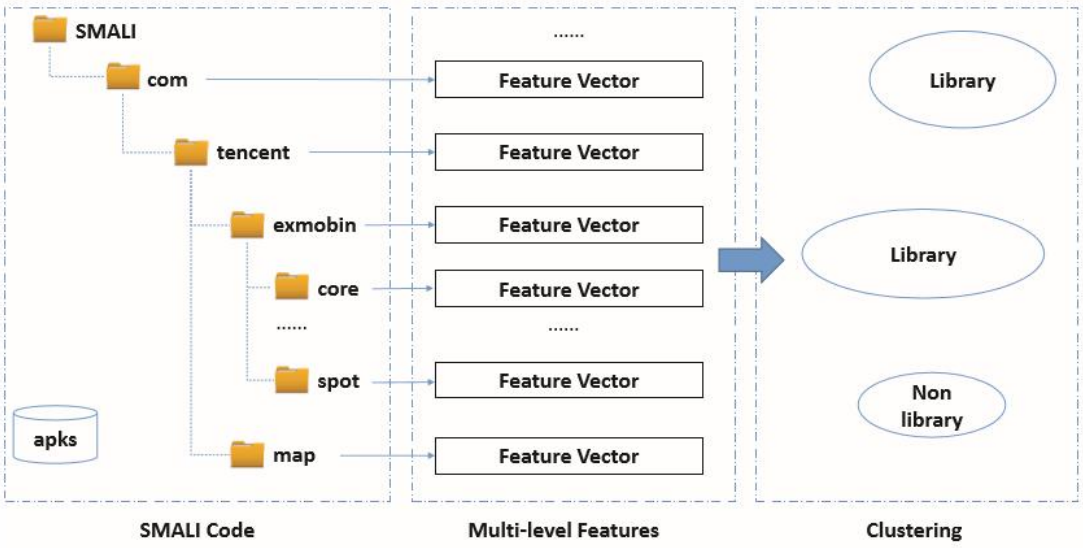
A.stable code 特征：为了抵抗包名混淆技术，LibRadar 将调用不同 Android API 的频率作为特征，这一特征的提取通过分析 smali 代码完成。

B.对特征进行 hash 计算：



按照上图方式计算每个包的 hash 值，赋予每个包独有的指纹。为了防止有些包有同样的 hash 值，再指纹中加入 API 调用总数以及 API 总种类数加以区分。

2.多级聚类



3.第三方包探测：

对于给定的 app，提取它的 stable code 特征并得到每个包的指纹与第三方指纹库比对来探测该 app 使用的第三方库。

二．运行样例（分析 B612）

```
zhouhuayu@ubuntu:~/Desktop/LiteRadar-master/LiteRadar$ python literadar.py B612.apk
[

 {
     "Library": "butterknife UI Framework",
     "Match Ratio": "5/5",
     "Package": "Lbutterknife",
     "Permission": [],
     "Popularity": 192,
     "Standard Package": "Lbutterknife",
     "Type": "GUI Component",
     "Website": "https://github.com/JakeWharton/butterknife"
 },
 {
     "Library": "Apache Common",
     "Match Ratio": "1363/1363",
     "Package": "Lorg/apache/commons",
     "Permission": [],
     "Popularity": 22,
     "Standard Package": "Lorg/apache/commons",
     "Type": "Development Aid",
     "Website": "https://commons.apache.org/"
 },
```

```
    },
    {
        "Library": "Android Support v4",
        "Match Ratio": "947/6825",
        "Package": "Landroid/support/v4",
        "Permission": [
            "android.permission.BACKUP",
            "android.permission.BLUETOOTH_ADMIN",
            "android.permission.DUMP",
            "android.permission.INTERACT_ACROSS_USERS",
            "android.permission.INTERACT_ACROSS_USERS_FULL",
            "android.permission.INTERNET",
            "android.permission.WAKE_LOCK",
            "android.permission.WRITE_SECURE_SETTINGS"
        ],
        "Popularity": "103",
        "Standard Package": "Landroid/support/v4",
        "Type": "Development Aid",
        "Website": "http://developer.android.com/reference/android/support/v4/app/packa
ge-summary.html"
    },
```

.。。。

四．优势

1.包名识别

尽管有些包名经过了包名混淆(类似 a/b/c)，但在同一聚类中存在未经过混淆的包名，利用这些包名可以还原那些被混淆的包在报告中尽量显示有意义的包名

2.提供第三方库信息

由上图运行结果图可以看出 LibRadar 不仅输出第三方库的名称还输出 permission 信息以及包使用频率和包的来源网站可以给用户更多参考信息。