



ICCBot: 高效的Android ICC 解析工具

ICCBot: Fragment-Aware and Context-Sensitive ICC Resolution for Android Applications. ICSE 2022, Demo Track.

燕季薇(yanjw@ios.ac.cn), 张世新, 刘烨庞, 严俊, 张健

软件工程技术研究开发中心

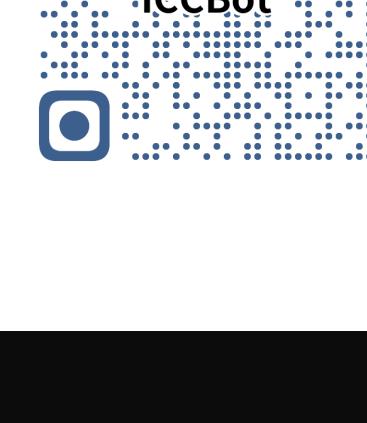
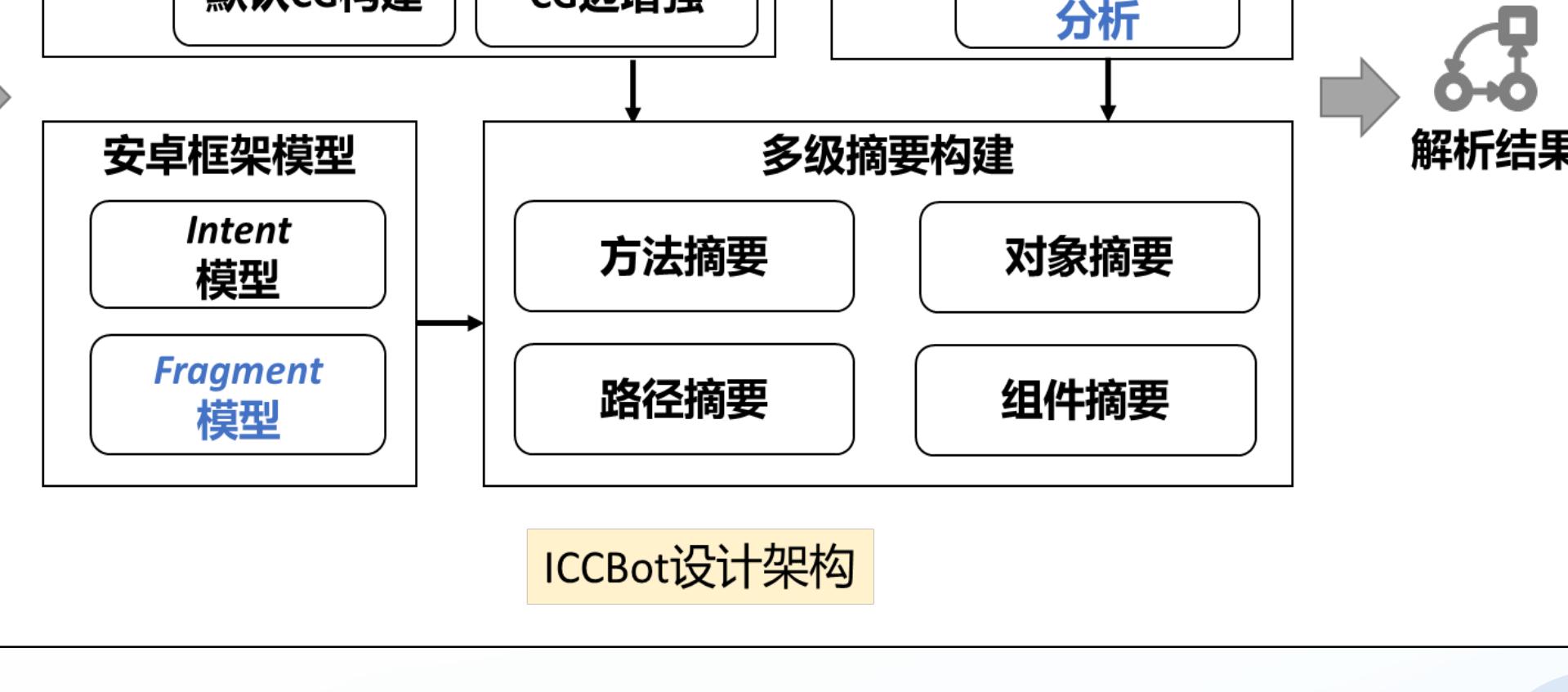
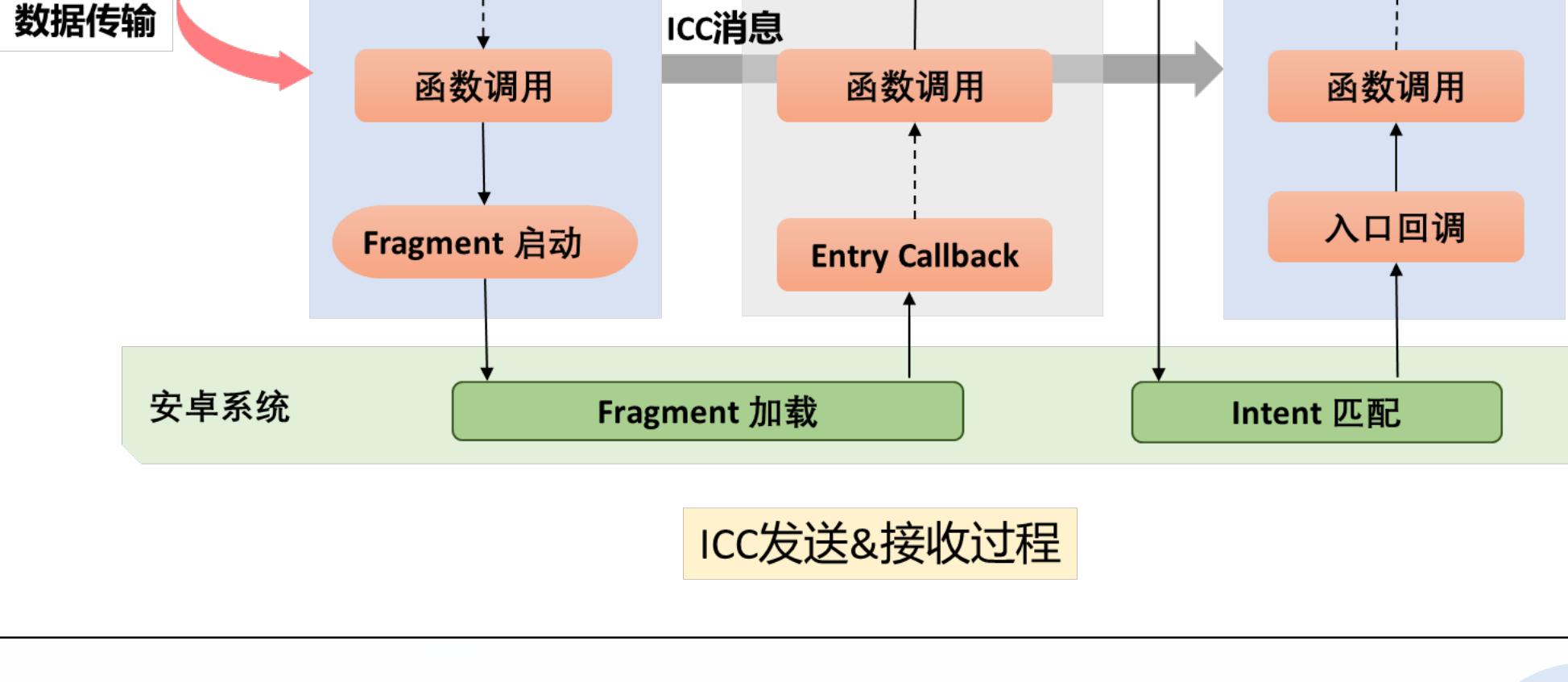
很多大型框架都提供了组件/模块化的设计，组件负责单一职责。



不同组件通过收发满足特定规范消息实现组件间通讯(ICC)，框架层隐藏了真实的函数调用行为。



ICC消息的建模和提取是安卓框架下应用控制流、数据流恢复的重要一环，对上层应用的分析和测试具有重要意义。



```
PS C:\Users\Y9910\Desktop> java -jar \ICCBot.jar -h
usage: java -jar [jarFile] [options] [apkPath] [-client] [-clientDir]
- andriodDir -apkPath [optional] [apkPath] [-client] [-clientDir]
- callgraphAlgorithm <arg> [-callgraphAlgorithm [default:SPARK]]: Set the path of andriod Dir
- client <arg> [-client CallGraphClient: Output call graph files.
- IntentClient: Output intent files.
- IntentReceiverClient: Output intent receiver files.
- FragmentClient: Output the fragment loading results.
- CGClient: Resolve the ICC and generate CG.
- ICCSpecificationClient: Resolve the ICC specification for each component.
-h [-help] [-helpForComponent] [-helpForClient]
-maxFunctionExpandNumber <arg> [-maxFunctionExpandNumber [default:10]]: Set the max number of expanded functions when
perform inter-procedural analysis.
-maxObjectSummarySize <arg> [-maxObjectSummarySize [default:1000]]: Set the max number of units in an object
summary.
-maxPathNumber <arg> [-maxPathNumber [default:100]]: Set the max number of paths.
-name <arg> [-name Set the name of the apk under analysis.
-nodagger <arg> [-nodagger: exclude dagger module]
-nosyncMethod <arg> [-nosyncMethod: exclude sync method call edge]
-noCallBackEntry <arg> [-noCallBackEntry: exclude the call back methods]
-noDynamicBC <arg> [-noDynamicBC: exclude dynamic broadcast receiver matching]
-noImplicit <arg> [-noImplicit: exclude implicit matching]
-noImplicitClient <arg> [-noImplicitClient: exclude the activities declared in app's package]
-noLocalCode <arg> [-noLocalCode: exclude local code matching]
-noStaticField <arg> [-noStaticField: exclude static field analysis]
-noStringOp <arg> [-noStringOp: exclude string operation model]
-noTypeOp <arg> [-noTypeOp: exclude type operation model]
-noTypeOpMain <arg> [-noTypeOpMain: limit the entry scope]
-outputDir <arg> [-outputDir: Set the output folder of the apk.
-path: Set the path to the apk under analysis.
-seedOutput <arg> [-seedOutput [default:10]]: Set the max running time (min)
-l <arg> [-l: Set the log level]
```

ICCBot 运行界面

工具

Fragment 加载图示例

组件迁移图示例

正确的ICC数量
最多，误报最少

实验验证

- 在三个手工构造的Benchmark上的准确性比较

Benchmark	#Ground-Truth	IC3		IC3-DialDroid		Gator		ICCBot	
		#TP	#FP	#TP	#FP	#TP	#FP	#TP	#FP
DroidBench	12	8	0	8	0	7	1	10	0
ICC-Bench	26	10	0	23	0	4	0	26	0
ICCBotBench	11	7	3	10	24	7	3	11	0
Sum	49	25	3	41	24	18	4	47	0

- 在2,000个真实应用上的识别数量比较

Tool	#Success	Time _{succ}	#ICC
IC3	1,719	57s	10,860
IC3-DialDroid	1,851	115s	8,601
Gator	1,882	20s	27,297
ICCBot	2,000	54s	28,584

两种策略辅助
ICC识别的效果

