说　明　书　附　图

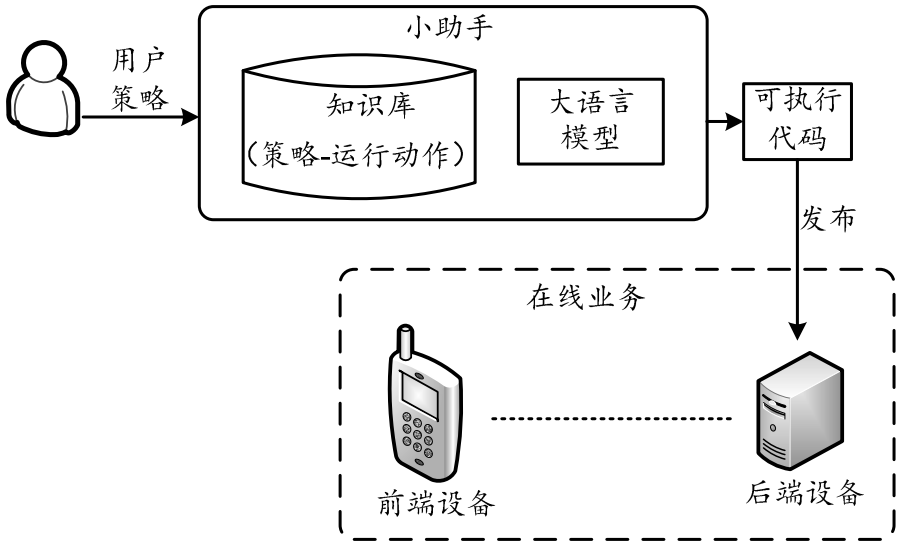

小助手
用户
策略
知识库
（策略-运行动作）
大语言
模型
可执行
代码
发布
在线业务
前端设备
后端设备

图 1

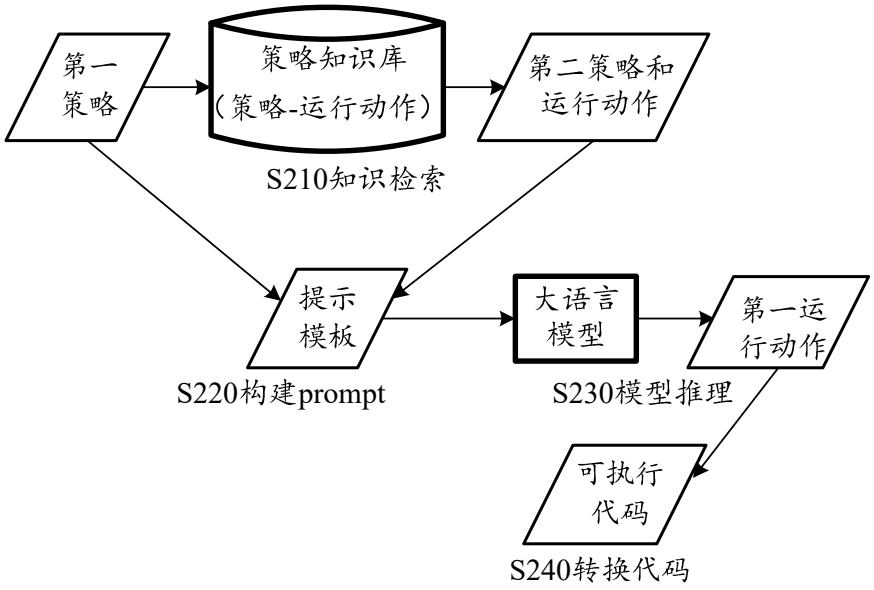

第一
策略
策略知识库
（策略-运行动作）
第二策略和
运行动作
S210知识检索
提示
模板
大语言
模型
第一运
行动作
S220构建prompt
S230模型推理
可执行
代码
S240转换代码

图 2

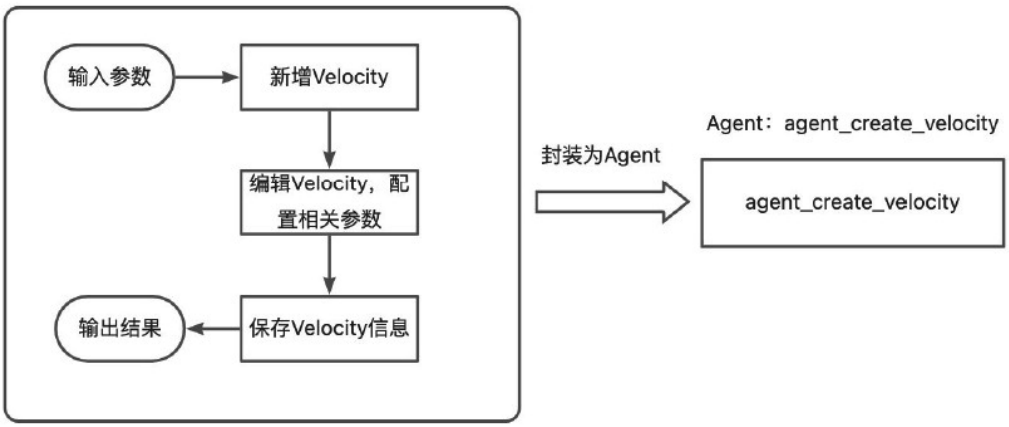

输入参数
新增Velocity
编辑Velocity，配置相关参数
输出结果
保存Velocity信息
封装为Agent
Agent：agent_create_velocity
agent_create_velocity

图 3

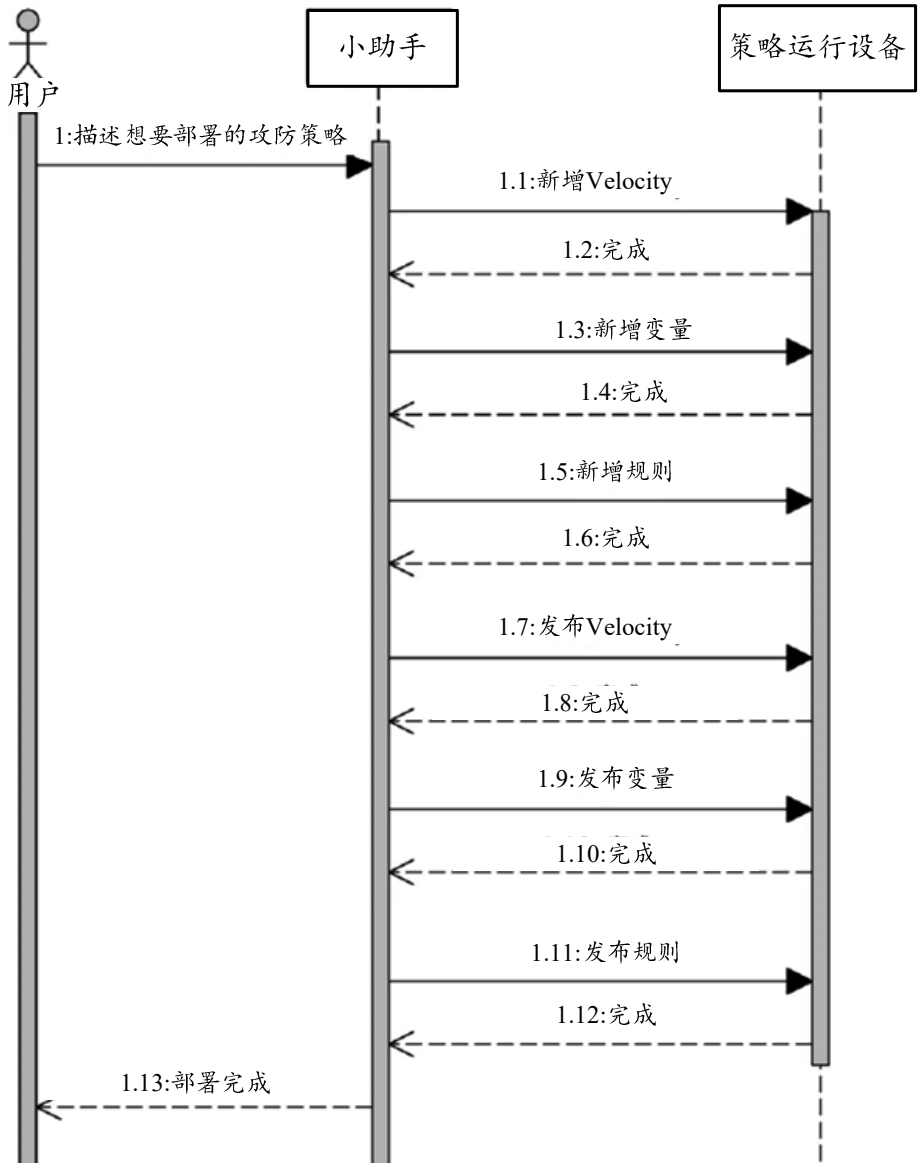

用户
小助手
策略运行设备
1:描述想要部署的攻防策略
1.1:新增Velocity
1.2:完成
1.3:新增变量
1.4:完成
1.5:新增规则
1.6:完成
1.7:发布Velocity
1.8:完成
1.9:发布变量
1.10:完成
1.11:发布规则
1.12:完成
1.13:部署完成

图 4

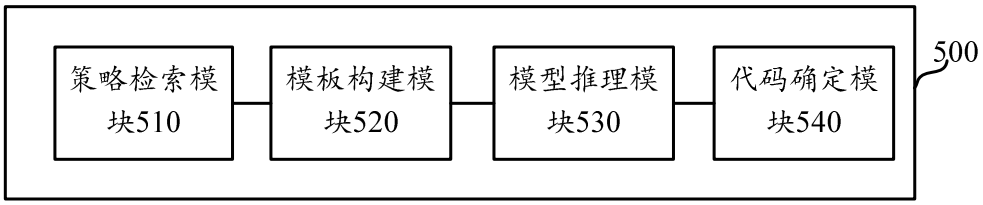

策略检索模块510
模板构建模块520
模型推理模块530
代码确定模块540
500

图 5

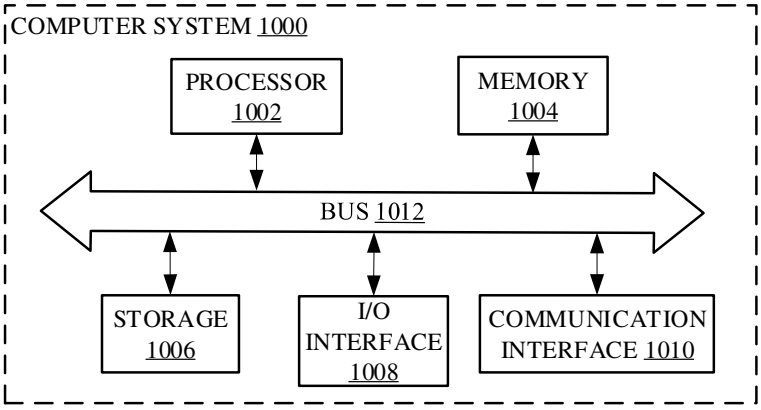

COMPUTER SYSTEM 1000
PROCESSOR 1002
MEMORY 1004
BUS 1012
STORAGE 1006
I/O INTERFACE 1008
COMMUNICATION INTERFACE 1010

图 6