

权利要求书

- 1、一种安全检测设备，所述安全检测设备用于检测 IoT 网络中的 IoT 终端，所述安全检测设备包括：
- 软件无线电单元：用于监听所述 IoT 终端发出的无线信号，获取通信报文；
- 5 分析单元，用于：利用所述通信报文确定所述 IoT 终端的目标运行特征，对比所述目标运行特征和所述 IoT 终端的历史正常运行特征，确定所述 IoT 终端是否异常运行。
- 2、根据权利要求 1 所述的设备，所述目标运行特征/所述历史正常运行特征包括如下一种或多种：
- 所述 IoT 网络中 IoT 终端的数量变化特征、所述 IoT 终端的通信报文的接收方特征、
- 10 所述 IoT 终端的报文流量变化特征、所述 IoT 终端上线/下线的时间特征或所述 IoT 终端的业务特征。
- 3、根据权利要求 1 所述的设备，所述利用所述通信报文确定所述 IoT 终端的目标运行特征，包括：
- 利用预定通信协议规定的校验规则对所述通信报文中的校验码校验失败后，利用私
- 15 有规则对所述校验码解析成功，确定所述 IoT 终端的目标运行特征包括传输隐秘报文。
- 4、根据权利要求 1 所述的设备，所述目标运行特征/所述历史正常运行特征包括如下一种或多种攻击特征：
- 攻击指令特征、设定攻击行为特征或干扰信号特征。
- 5、根据权利要求 1 所述的设备，所述 IoT 终端的硬件能力/计算能力低于设定参数。
- 20 6、一种安全检测方法，所述方法包括：
- 获取 IoT 终端的通信报文，所述通信报文利用软件无线电技术监听所述 IoT 终端发出的无线信号而获取得到；
- 利用所述通信报文确定所述 IoT 终端的目标运行特征，对比所述目标运行特征和所述 IoT 终端的历史正常运行特征，确定所述 IoT 终端是否异常运行。
- 25 7、根据权利要求 1 所述的方法，所述目标运行特征/所述历史正常运行特征包括如下一种或多种：
- 所述 IoT 网络中 IoT 终端的数量变化特征、所述 IoT 终端的通信报文的接收方特征、所述 IoT 终端的报文流量变化特征、所述 IoT 终端上线/下线的时间特征或所述 IoT 终端的业务特征。
- 30 8、根据权利要求 6 所述的方法，所述利用所述通信报文确定所述 IoT 终端的目标运行特征，包括：

利用预定通信协议规定的校验规则对所述通信报文中的校验码校验失败后,利用私有规则对所述校验码进行解析成功,确定所述 IoT 终端的目标运行特征包括传输隐秘报文。

- 9、根据权利要求 6 所述的方法,所述目标运行特征/所述历史正常运行特征包括如下
5 下一种或多种攻击特征:

攻击指令特征、设定攻击行为特征或干扰信号特征。

10、根据权利要求 6 所述的方法,所述 IoT 终端的硬件能力/计算能力低于设定水平。

11、一种安全检测装置,所述装置包括:

- 获取模块,用于:获取 IoT 终端的通信报文,所述通信报文利用软件无线电技术监
10 听所述 IoT 终端发出的无线信号而获取得到;

确定模块,用于:利用所述通信报文确定所述 IoT 终端的目标运行特征,对比所述目标运行特征和所述 IoT 终端的历史正常运行特征,确定所述 IoT 终端是否异常运行。

12、一种安全检测设备,包括软件无线电处理器、存储器、主处理器及存储在存储器上并可在主处理器上运行的计算机程序,其中,所述主处理器执行所述程序时实现如

- 15 下方法:

获取 IoT 终端的通信报文,所述通信报文利用所述软件无线电处理器监听所述 IoT 终端发出的无线信号而获取得到;

利用所述通信报文确定所述 IoT 终端的目标运行特征,对比所述目标运行特征和所述 IoT 终端的历史正常运行特征,确定所述 IoT 终端是否异常运行。