

安全检测方法、设备及装置

技术领域

[01] 本说明书涉及安全技术领域，尤其涉及安全检测方法、设备及装置。

背景技术

- 5 [02] 目前，IoT（Internet of things，物联网）设备如路由器、家用摄像头、智能手表或智能手环等，在人们工作或生活中的重要性越来越大，然而，对 IoT 终端的攻击研究和尝试也越来越火热，IoT 终端的低功耗特点等原因决定了 IoT 终端不具备复杂的安全检测功能，因此，如何保障 IoT 终端的安全成为亟待解决的技术问题。

发明内容

- 10 [03] 为克服相关技术中存在的问题，本说明书提供了安全检测方法、设备及装置。
- [04] 根据本说明书实施例的第一方面，提供一种安全检测设备，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：
- [05] 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；
- [06] 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
- 15 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。
- [07] 可选的，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：
- [08] 可选的，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。
- 20 [09] 可选的，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：
- [10] 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解析成功，确定所述 IoT 终端的目标运行特征包括传输隐私报文。
- [11] 可选的，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：
- [12] 攻击指令特征、设定攻击行为特征或干扰信号特征。

[13]可选的, 所述IoT终端的硬件能力/计算能力低于设定参数。

[14]根据本说明书实施例的第二方面, 提供一种安全检测方法, 所述方法包括:

[15]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;

- 5 [16]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。

[17]可选的, 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:

[18]可选的, 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。

[19]可选的, 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:

[20]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。

[21]可选的, 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:

- 15 [22]攻击指令特征、设定攻击行为特征或干扰信号特征。

[23]可选的, 所述IoT终端的硬件能力/计算能力低于设定参数。

[24]根据本说明书实施例的第三方面, 提供一种安全检测装置, 所述装置包括:

[25]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听所述IoT终端发出的无线信号而获取得到;

- 20 [26]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。

[27]可选的, 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:

[28]可选的, 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。

[29]可选的, 所述确定模块, 还用于:

[30]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。

[31]可选的，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：

[32]攻击指令特征、设定攻击行为特征或干扰信号特征。

[33]可选的，所述 IoT 终端的硬件能力/计算能力低于设定参数。

- 5 [34]根据本说明书实施例的第四方面，提供一种安全检测设备，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下方法：

[35]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；

- 10 [36]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。

[37]本说明书的实施例提供的技术方案可以包括以下有益效果：

[38]本说明书实施例中，安全检测设备可放置于 IoT 网络中，IoT 网络中的 IoT 终端通过无线技术传输数据，该安全检测设备中包括有软件无线电单元，因此可以监听无线覆盖范围下的所有无线信号，从而获取到 IoT 终端的通信报文。本实施例利用该安全检测设备对 IoT 网络中的 IoT 终端进行安全检测，对 IoT 终端无接触无侵入、不依赖 IoT 终端自身的检测能力；并且，通过获取 IoT 终端的目标运行特征，结合历史正常运行特征可以发现 IoT 终端是否异常运行，实现对 IoT 终端的安全检测。

- 15 [39]应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书。

附图说明

[40]此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本说明书的实施例，并与说明书一起用于解释本说明书的原理。

[41]图 1A 是本说明书根据一示例性实施例示出的一种 IoT 网络示意图。

- 25 [42]图 1B 是本说明书根据一示例性实施例示出的一种 IoT 网络系统的示意图。

[43]图 1C 是本说明书根据一示例性实施例示出的一种安全检测设备的框图。

[44]图 2 是本说明书根据一示例性实施例示出的一种安全检测方法的流程图。

[45]图 3 是本说明书实施例安全检测装置所在设备的一种硬件结构图。

[46]图 4 是本说明书根据一示例性实施例示出的一种安全检测装置的框图。

具体实施方式

5 [47]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所述的实施方式并不代表与本说明书相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书的一些方面相一致的装置和方法的例子。

[48]在本说明书使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书。
10 在本说明书和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[49]应当理解，尽管在本说明书可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在
15 不脱离本说明书范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[50]如图 1A 所示，是本说明书根据一示例性实施例示出的一种 IoT 网络示意图，包括多个 IoT 终端、IoT 网络总控和外部的攻击方设备，其中，外部的攻击方设备正在对两个
20 IoT 终端进行攻击。其中，图 1A 所示实施例以智能家居场景为例进行示意，实际应用中，IoT 网络还广泛应用于智能工控场景或无人零售等场景中。

[51]IoT 终端的厂商复杂，可能没有能力和动力进行安全相关的投入研究，一些 IoT 终端甚至不具备安全检测功能。即使具备安全检测功能，由于 IoT 终端内置的运行代码都是预先烧制的，因此也无法灵活更新攻击检测逻辑。由于 IoT 终端的低功耗特点，IoT
25 终端的计算能力通常较弱，无法承受额外复杂安全检测逻辑，因此安全检测功能通常都较弱，而 IoT 终端的攻击有很大部分是发在通信协议层面，也给安全检测带来很大困难。

[52]基于此，考虑到在 IoT 终端本身实现安全检测功能较为困难，本说明书实施例提出了在 IoT 网络配置控制设备的方案，由 IoT 控制设备实现对各个 IoT 终端的安全检测。

在 IoT 网络中，不同的 IoT 终端可能使用不同的通信协议，但大部分都是通过无线信号进行通信，大部分对 IoT 终端的攻击，也是通过无线信道进行攻击的。

[53]如图 1B 所示，是本说明书根据一示例性实施例示出的一种 IoT 网络的示意图，本实施例在 IoT 网络中额外新增一安全检测设备，该安全检测设备可以对 IoT 网络中的 IoT 终端进行安全检测，因此对 IoT 终端无接触无侵入、不需要依赖 IoT 终端自身的检测能力。当然，在其他例子中，安全检测设备也可以采用 IoT 网络中的原有的某个设备实现，但该设备可以理解为，为原有 IoT 网络的 IoT 终端额外提供了新的安全检测功能。

[54]如图 1C 所示，是本说明书根据一示例性实施例示出的一种安全检测设备的框图，包括：

10 [55]软件无线电单元 101，用于：监听所述 IoT 终端发出的无线信号，获取通信报文；

[56]分析单元 102，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。

[57]作为被攻击的 IoT 终端，一些惯用的安全检测方案是从 IoT 终端本身进行改进，使 IoT 终端提高安全防护能力。由于 IoT 终端自身的局限性，这些 IoT 终端本身的安全检测能力较弱，也可以理解为 IoT 终端的硬件能力/计算能力低于设定参数。本实施例提出的方案是新增一安全检测设备，用于检测 IoT 网络中的 IoT 终端，IoT 网络中的 IoT 终端会发出无线信号，在该安全检测设备的无线覆盖范围内，安全检测设备监听所有无线信号，通过所监听的无线信号来发现 IoT 终端是否异常。

20 [58]本实施例中，安全检测设备中包括有软件无线电单元，具体实现可以采用宽频软件无线电工具，如 USRP（Universal Software Radio Peripheral，通用软件无线电外设）、LimeSDR（Software Defined Radio，软件无线电），软件无线电单元的功能是嗅探整个安全防护区域内的所有无线频率下的无线信号，并且将嗅探到的无线信号进行拆分清洗，还原成各个 IoT 终端所使用的通信协议对应的通信报文，IoT 终端所使用的通信协议主要

25 要包括 Wi-Fi 协议、蓝牙协议或 Zigbee 协议等等。因此，IoT 网络中所有 IoT 终端的通信报文和攻击方发出的通信报文都会被该单元采集并清洗，软件无线电单元可以获取到各个不同 IoT 终端所发出的通信报文，并且还可以根据所使用的通信协议进行区分。

[59]软件无线电单元对通信报文的获取结果可以输出至分析单元，分析单元可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。可选的, 本实施例中可以预先分析 IoT 终端的历史正常运行特征, 分析的目的是为了确定 IoT 终端在什么情况下属于正常运行, 以基于历史正常运行特征监控 IoT 终端是否异常运行。

[60] 可选的, IoT 终端的历史正常运行特征可以通过多种方式实现, 作为例子, 可以是在一定时间范围内持续监听 IoT 网络中各个 IoT 终端的运行数据 (需要确保 IoT 终端处于正常运行状态), 基于这些运行数据分析 IoT 终端的正常运行特征。在另一些例子中, 5 可以获取 IoT 终端的日志进行分析; 或者, 可以进一步结合 IoT 终端的厂商提供的 IoT 终端的测试数据; 或者, 还可以是通过其他途径获取其他 IoT 终端的历史正常运行数据, 并结合需监控的 IoT 终端与该其他终端的相关性而分析得到。

10 [61] 实际应用中, 若 IoT 网络中出现攻击方, IoT 网络中 IoT 终端的数量可能出现变化, 例如有新的 IoT 终端加入作为攻击方设备, 已有的 IoT 终端被攻击后下线等等; 因此, 所述 IoT 终端的历史正常运行特征可以包括 IoT 网络中 IoT 终端的数量变化特征, 该数量变化特征指示正常情况下 IoT 网络中 IoT 终端的数量变化, 例如可以包括: 在晚上 10 点至早上 8 点, IoT 终端的数量值通常不会出现变化, 在一些时间段如白天, IoT 终端 15 的数量值通常会出现减少 (例如用户佩戴的智能手环下线导致数量减少) 等等。

[62] 在另一些例子中, 某些 IoT 终端可能有固定的上线或下线时间, 例如家居场景中, 智能手环佩戴于用户身上, 用户通常在某个时间段不在家中, 因此此类终端有固定的上线或下线时间, 因此, 所述 IoT 终端的历史正常运行特征还可以包括: 所述 IoT 终端上线/下线的特征, 通过 IoT 终端的上线或下线时间能够判断 IoT 终端是否异常运行。

20 [63] 在其他例子中, IoT 终端的通信报文可能是固定发送给某个 IoT 终端, 例如家居场景中, 摄像头的通信报文通常是发送给路由器, 智能手环的通信报文通常是发送给智能手机, 若有固定接收方的 IoT 终端将通信报文发送给某个新加入的 IoT 终端, 则该 IoT 终端有可能出现异常运行。因此, IoT 终端的历史正常运行特征还可以包括 IoT 终端的通信报文的接收方特征。

25 [64] 在其他例子中, 正常情况下, IoT 网络中 IoT 终端的报文流量也通常处于稳定状态, 例如在家居场景、智能工控或无人零售等场景中, 在晚上 10 点至早上 8 点, 各 IoT 终端的通信报文流量通常较低, 不会有频繁的通信发生; 例如某个 IoT 终端的报文流量在每天的各个时间段都较为稳定, 若被攻击后, 可能会出现频繁发送通信报文给攻击方设备的情况, 因此, 可以通过统计各个 IoT 终端之间的流量, 进而分析出报文流量变化特征。 30

[65]IoT 终端发送的通信报文中承载有数据，这些数据可能经过 IoT 终端的厂商的自定义规则（例如一些加密算法等等）处理，实际应用中可能无法获知所有 IoT 终端厂商的自定义规则，数据的实际业务含义可能无法解析，上述实施例通过 IoT 终端的历史正常运行特征，这些历史正常运行特征涉及的是通信报文的数量变化、流量变化等，不涉及数据中具体的业务含义，不需要对报文中数据进行业务层面的解析，因此能够适用于所有 IoT 终端。

[66]在已知该自定义规则的情况下（例如安全检测设备与 IoT 终端是同一厂商、与 IoT 终端的厂商合作、或者通过破解等），也可以将 IoT 终端发送的通信报文中的数据格式化为具有业务含义的数据，此种情况下可以根据通过历史运行数据分析 IoT 终端的业务数据并确定业务特征，例如，智能手环的业务特点是接收关联设备的指令后发出响应结果的报文、或者是传输手环采集的步数、心率等数据，若发现智能手环将关联设备的设备信息往外发送，则智能手环可能异常运行。

[67]实际应用中，安全检测设备也可以直接与 IoT 终端通信，一些 IoT 终端具有安全检测功能，能够检测自身是否被攻击，IoT 终端可以向安全检测设备告知攻击信息，或者传输一些数据。然而，IoT 终端在发现自身被攻击后如何告知安全检测设备则成为一个难题，因为整个 IoT 终端已经被攻击者控制，向安全检测设备传输数据就可能会被攻击者察觉。基于此，本实施例从通信协议上提供解决方案。通常，通信双方按照通信协议传输承载有数据的报文，通信协议是为保证数据通信网络中通信双方能有效、可靠通信而约定的一系列规则。这些规则包括报文格式、顺序或速率，数据传输的确认或拒收、差错检测、重传控制或询问等。

[68]通常，报文中包括一校验码字段，以用于校验报文是否错误。校验过程可以是：通信发送方利用预定通信协议规定的校验规则，针对所传输的数据计算校验码；通信接收方接收报文，利用该校验规则针对报文中的数据计算校验码后，对比计算的校验码和报文中的校验码是否一致。

[69]正常情况下，通信报文中的校验码会采用预定通信协议的校验规则生成，因此，历史正常运行特征可以包括：所述通信报文中的校验码采用预定通信协议的校验规则生成。考虑到 IoT 终端被攻击方控制后，为了实现隐秘地传输数据，本实施例中 IoT 终端可以对校验码字段进行改造，与通信协议规定的校验规则不同，本实施例采用私有规则生成校验码。其中，私有规则与通信协议规定的校验规则不同，私有规则的具体实现，实际应用中可以根据需要灵活配置，以使利用私有规则生成的校验码与利用通信协议规定的

校验规则生成的校验码不同即可；而通信报文中除校验码之外的字段则利用原有的预定通信协议生成。作为例子，私有规则可以是：利用校验规则生成校验码后进行一定的修改，例如可以是根据校验规则生成的校验码后进行其他转换，可选的，可以设定字符转换关系，将根据校验规则生成的校验码转换为其他字符。在另一些例子中，私有规则可以是利用预设密钥对所述告警数据加密，按照所述校验规则对加密数据生成校验码，本实施例中 IoT 终端与安全检测设备可以预先约定密钥（可以是对称密钥或非对称密钥），校验码的生成过程，可以先利用预设密钥对告警数据加密后（具体的加密算法可以灵活配置），再按照校验规则对加密数据生成校验码，采用此种方式，既实现了对校验码的改造，也可以供安全检测设备利用校验码校验数据是否错误。对于攻击方设备，会认为接收到一个错误的报文，而不会察觉到 IoT 终端发出告警数据。对于 IoT 控制设备来说，可以利用私有规则解析出报文中的告警数据，从而实现告警数据的隐秘传输。

[70] 因此，安全检测设备可以接收到 IoT 终端发送的各类报文，这些报文包括有正常的报文，也有前述实施例隐秘传输的报文，安全检测设备需要对报文进行识别。按照通信协议的规定，安全检测设备在接收到报文后，会利用通信协议规定的校验规则对报文中的校验码进行校验；对于用于告警的报文，由于校验码被改造，因此会出现校验失败的情况。在本实施例方案中，若校验失败，安全检测设备可以利用私有规则对所述校验码进行解析，若解析成功则可确定所述 IoT 终端发出了隐秘报文，因此确定所述 IoT 终端的目标运行特征包括传输隐秘报文，进而获取所述报文中的隐秘数据，安全检测设备可知道 IoT 终端可能被攻击，进一步的，安全检测设备可以对攻击行为进行排查和阻断。

[71] 实际应用中，若攻击方设备要对 IoT 终端进行攻击，这些攻击行为可能与正常通信行为有一些差别，因此本实施例中，还可以预先收集与攻击相关的特征。在一些例子中，攻击方设备向 IoT 终端发出的通信报文中可能包含有攻击指令，如 WiFi 协议中的 Deauth 攻击指令等，因此可以根据攻击指令确定攻击指令特征。在另一些例子中，攻击行为可以包括重放攻击、拒绝服务攻击、密码爆破攻击等，可以获取此类攻击行为在无线信号上的特征作为设定攻击行为特征。在其他例子中，攻击方设备有可能发出干扰信号对 IoT 网络中各 IoT 终端的信号传输进行干扰，干扰方式可能包括有同频率干扰、邻频道干扰、带外干扰、互调干扰和阻塞干扰等，因此可以确定干扰信号特征。

[72] 通过上述实施例可以理解，运行特征可以有多种，分析单元在对软件无线电单元的获取结果进行分析的过程中，IoT 终端可能是有一种目标运行特征与历史正常运行特征不匹配，也可以是有多种目标运行特征与历史正常运行特征不匹配，分析单元可以进行

汇总、分析和决策，最终的分析结果还可以发送给服务侧。

[73]与前述 IoT 网络系统的实施例相对应，本说明书还提供了安全检测方法的实施例，如图 2 所示，图 2 是本说明书根据一示例性实施例示出的一种安全检测方法的流程图，可应用于图 1B 所示的安全检测设备中，包括以下步骤：

- 5 [74]在步骤 202、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；

[75]在步骤 204、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。

[76]可选的，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：

- 10 [77]可选的，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。

[78]可选的，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：

[79]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。

[80]可选的，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：

[81]攻击指令特征、设定攻击行为特征或干扰信号特征。

[82]可选的，所述 IoT 终端的硬件能力/计算能力低于设定参数。

- 20 [83]与前述安全检测方法的实施例相对应，本说明书还提供了安全检测装置及其所应用的设备的实施例。

[84]本说明书安全检测装置的实施例可以应用在电子设备上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过主处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图 3 所示，为本说明书实施例安全检测装置所在设备
25 的一种硬件结构图，除了图 3 所示的软件无线电处理器 300、主处理器 310、内存 330、网络接口 320、以及非易失性存储器 340 之外，实施例中装置 331 所在的电子设备，通常根据该设备的实际功能，还可以包括其他硬件，对此不再赘述。

[85]如图 4 所示，图 4 是本说明书根据一示例性实施例示出的一种安全检测装置的框图，

所述装置包括:

[86]获取模块 41, 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听所述 IoT 终端发出的无线信号而获得;

[87]确定模块 42, 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。

[88]可选的, 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:

[89]可选的, 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。

[90]可选的, 所述确定模块, 还用于:

[91]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。

[92]可选的, 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:

[93]攻击指令特征、设定攻击行为特征或干扰信号特征。

[94]可选的, 所述 IoT 终端的硬件能力/计算能力低于设定参数。

[95]相应的, 本说明书还提供一种安全检测设备, 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下方法:

[96]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得;

[97]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。

[98]上述安全检测方法中各个步骤的实现过程、以及安全检测装置中各个模块的功能和作用的实现过程具体详见上述 IoT 网络系统的实现过程, 在此不再赘述。

[99]对于装置实施例而言, 以上所描述的装置实施例仅仅是示意性的, 其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的, 作为模块显示的部件可以是或者也可以不是物理模块, 即可以位于一个地方, 或者也可以分布到多个网络模块上。可

以根据实际的需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

5 [100] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

10 [101] 本领域技术人员在考虑说明书及实践这里申请的发明后，将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本说明书的一般性原理并包括本说明书未申请的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本说明书的真正范围和精神由下面的权利要求指出。

15 [102] 应当理解的是，本说明书并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本说明书的范围仅由所附的权利要求来限制。

[103] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。