



(12) 发明专利

(10) 授权公告号 CN 117041982 B

(45) 授权公告日 2024. 01. 23

(21) 申请号 202310762710.7

H04L 9/32 (2006.01)

(22) 申请日 2023.06.26

H04L 9/40 (2022.01)

(65) 同一申请的已公布的文献号

申请公布号 CN 117041982 A

(56) 对比文件

CN 101400079 A, 2009.04.01

CN 103200678 A, 2013.07.10

(43) 申请公布日 2023.11.10

CN 112954729 A, 2021.06.11

(73) 专利权人 中国软件评测中心(工业和信息化部软件与集成电路促进中心)

CN 115988468 A, 2023.04.18

US 7181081 B2, 2007.02.20

地址 100048 北京市海淀区紫竹院路66号

US 2020068166 A1, 2020.02.27

(72) 发明人 徐海波 李亚伟 罗文兵 陶新昕 崔宁宁

CN 114550450 A, 2022.05.27

CN 106535113 A, 2017.03.22

(74) 专利代理机构 北京轻创知识产权代理有限公司 11212

CN 110673169 A, 2020.01.10

CN 110673170 A, 2020.01.10

专利代理师 厉洋洋

CN 111585749 A, 2020.08.25

CN 107690133 A, 2018.02.13

(51) Int. Cl.

H04W 12/63 (2021.01)

H04W 12/69 (2021.01)

H04W 12/0431 (2021.01)

H04W 12/041 (2021.01)

H04W 12/02 (2009.01)

CN 115776396 A, 2023.03.10

CN 103024795 A, 2013.04.03

CN 106604389 A, 2017.04.26

(续)

审查员 刘慧敏

权利要求书3页 说明书8页 附图2页

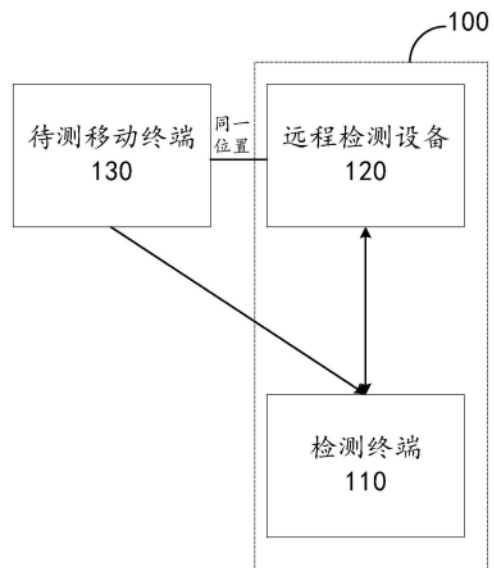
(54) 发明名称

一种空口传输数据的正确性检测系统及方法

进行快速检测的同时,还提高了检测精度。

(57) 摘要

本发明公开了一种空口传输数据的正确性检测系统及方法,包括:检测终端和远程检测设备;所述远程检测设备安装在待测移动终端上,所述检测终端与所述待测移动终端之间通过第一空口连接;所述检测终端用于:获取所述远程检测设备采集的第一当前定位数据,并利用所述第一空口,获取所述待测移动终端采集的第二当前定位数据;将所述第一当前定位数据作为标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性。本发明无需对待测移动终端内部进行程序改造和电路改造,在实现对通过空口传输的数据正确性



CN 117041982 B

[转续页]

[接上页]

**(56) 对比文件**

CN 112601230 A, 2021.04.02

CN 114765850 A, 2022.07.19

CN 101360322 B, 2011.12.14

CN 105323845 A, 2016.02.10

CN 115523861 A, 2022.12.27

JP 3731123 B2, 2006.01.05

US 4645993 A, 1987.02.24

徐冰; 刘伟; 李和平; 佟长福; 丁绍宇; 周惠;

毕立格. GPS RTK测量技术在灌区改造工程中的应用. 水资源与水工程学报. 2007, (第03期), 全文.

Shu Zhang et al. Fault Location Based on Voltage Measurement at Secondary Side of Low-Voltage Transformer in Distribution Network. 《IEEE Transactions on Instrumentation and Measurement (Volume: 71)》. 2022, 全文.

1. 一种空口传输数据的正确性检测系统,其特征在于,包括:检测终端和远程检测设备;所述远程检测设备安装在待测移动终端上,所述检测终端与所述待测移动终端之间通过第一空口连接;所述检测终端用于:

获取所述远程检测设备采集的第一当前定位数据,并利用所述第一空口,获取所述待测移动终端采集的第二当前定位数据;

将所述第一当前定位数据作为标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性;

所述检测终端还用于:

构建所述远程检测设备的设备ID,并基于SM2算法,创建所述设备ID对应的第一密钥对,并将所述设备ID和所述第一密钥对的私钥发送至所述远程检测设备;

接收所述远程检测设备发送的加密定位数据;其中,所述远程检测设备利用所述第一密钥对的私钥,对所述设备ID和所述第一当前定位数据进行加密并签名,得到所述加密定位数据;

利用所述第一密钥对的公钥,对所述加密定位数据进行解密并验签,得到所述第一当前定位数据和解密设备ID;

所述检测终端具体用于:

当所述解密设备ID与所述设备ID相同时,将所述第一当前定位数据作为所述标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性。

2. 根据权利要求1所述的空口传输数据的正确性检测系统,其特征在于,所述检测终端还用于:

基于SM2算法,创建所述设备ID对应的第二密钥对,并将所述第二密钥对的公钥发送至所述远程检测设备;

利用第二空口,接收所述远程检测设备发送的第一设备加密数据;其中,所述远程检测设备利用所述第二密钥对的公钥对所述设备ID进行加密,得到所述第一设备加密数据,并根据所述检测终端的公网地址和端口号,构建所述远程检测设备与所述检测终端之间的所述第二空口;

利用所述第二密钥对的私钥,对所述第一设备加密数据进行解密,得到第一解密设备ID;

从所述检测终端存储的所有公钥中,确定目标公钥,并利用所述目标公钥对所述第一解密设备ID进行加密,得到第二设备加密数据并发送至所述远程检测设备,以使所述远程检测设备判定所述第二设备加密数据对应的第二解密设备ID与所述设备ID是否相同;其中,所述远程检测设备利用所述目标公钥对应的私钥对所述第二设备加密数据进行解密,得到所述第二解密设备ID;

若是,则接收所述远程检测设备发送的加密定位数据。

3. 根据权利要求1或2所述的空口传输数据的正确性检测系统,其特征在于,所述检测终端具体用于:

当所述定位数据差值处于预设误差范围时,判定所述待测移动终端通过所述第一空口

所传输的数据正确;否则,判定所述待测移动终端通过所述第一空口所传输的数据已被篡改。

4. 根据权利要求3所述的空口传输数据的正确性检测系统,其特征在于,所述第一当前定位数据包括:第一当前经度数据和第一当前纬度数据,所述第二当前定位数据包括:第二当前经度数据和第二当前纬度数据,所述预设误差范围包括:经度误差范围和纬度误差范围;

所述检测终端具体用于:

当所述第一当前经度数据和所述第二当前经度数据之间的经度差值处于所述经度误差范围且所述第一当前纬度数据和所述第二当前纬度数据之间的纬度差值处于所述纬度误差范围时,判定所述待测移动终端通过所述第一空口所传输的数据正确,否则,判定所述待测移动终端通过所述第一空口所传输的数据已被篡改。

5. 根据权利要求1所述的空口传输数据的正确性检测系统,其特征在于,所述检测终端还用于:

当判定所述待测移动终端通过所述第一空口所传输的数据已被篡改时,生成预警信息并输出。

6. 根据权利要求1所述的空口传输数据的正确性检测系统,其特征在于,所述待测移动终端为:无人机、智能网联汽车或物联网设备。

7. 一种空口传输数据的正确性检测方法,其特征在于,包括:

检测终端获取远程检测设备采集的第一当前定位数据,并利用第一空口,获取待测移动终端采集的第二当前定位数据;其中,所述远程检测设备安装在待测移动终端上,所述检测终端与所述待测移动终端之间通过第一空口连接;

所述检测终端将所述第一当前定位数据作为标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性;

还包括:

所述检测终端构建所述远程检测设备的设备ID,并基于SM2算法,创建所述设备ID对应的第一密钥对,并将所述设备ID和所述第一密钥对的私钥发送至所述远程检测设备;

所述检测终端接收所述远程检测设备发送的加密定位数据;其中,所述远程检测设备利用所述第一密钥对的私钥,对所述设备ID和所述第一当前定位数据进行加密并签名,得到所述加密定位数据;

所述检测终端利用所述第一密钥对的公钥,对所述加密定位数据进行解密并验签,得到所述第一当前定位数据和解密设备ID;

所述检测终端将所述第一当前定位数据作为标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性的步骤,包括:

当所述解密设备ID与所述设备ID相同时,所述检测终端将所述第一当前定位数据作为所述标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性。

8. 根据权利要求7所述的空口传输数据的正确性检测方法,其特征在于,还包括:

所述检测终端基于SM2算法,创建所述设备ID对应的第二密钥对,并将所述第二密钥对的公钥发送至所述远程检测设备;

所述检测终端利用第二空口,接收所述远程检测设备发送的第一设备加密数据;其中,所述远程检测设备利用所述第二密钥对的公钥对所述设备ID进行加密,得到所述第一设备加密数据,并根据所述检测终端的公网地址和端口号,构建所述远程检测设备与所述检测终端之间的所述第二空口;

所述检测终端利用所述第二密钥对的私钥,对所述第一设备加密数据进行解密,得到第一解密设备ID;

所述检测终端从所述检测终端存储的所有公钥中,确定目标公钥,并利用所述目标公钥对所述第一解密设备ID进行加密,得到第二设备加密数据并发送至所述远程检测设备,以使所述远程检测设备判定所述第二设备加密数据对应的第二解密设备ID与所述设备ID是否相同;其中,所述远程检测设备利用所述目标公钥对应的私钥对所述第二设备加密数据进行解密,得到所述第二解密设备ID;

若是,所述检测终端则接收所述远程检测设备发送的加密定位数据。

## 一种空口传输数据的正确性检测系统及方法

### 技术领域

[0001] 本发明涉及数据检测技术领域,尤其涉及一种空口传输数据的正确性检测系统及方法。

### 背景技术

[0002] 随着移动终端产业的飞速发展,通过移动终端的空口进行数据传输的安全性和正确性对公共安全和国家安全构成了不容忽视的现实威胁和潜在风险。例如无人机未经登记批准的飞行活动,恶意修改位置信息,突破电子围栏,非法侵入获取图像和扰乱正常飞行秩序,极大威胁国家安全、社会稳定和经济发展;移动终端易被攻击者利用而发起信号干扰、无线网络欺骗攻击和拒绝服务攻击;移动终端安全管理系统的应用软件存在安全漏洞,可被黑客利用攻击,导致大量移动终端被控,甚至发生群体性攻击破坏的极端风险,造成重大安全隐患。

[0003] 因此,亟需提供一种技术方案解决上述问题。

### 发明内容

[0004] 为解决上述技术问题,本发明提供了一种空口传输数据的正确性检测系统及方法。

[0005] 本发明的一种空口传输数据的正确性检测系统的技术方案如下:

[0006] 包括:检测终端和远程检测设备;所述远程检测设备安装在待测移动终端上,所述检测终端与所述待测移动终端之间通过第一空口连接;所述检测终端用于:

[0007] 获取所述远程检测设备采集的第一当前定位数据,并利用所述第一空口,获取所述待测移动终端采集的第二当前定位数据;

[0008] 将所述第一当前定位数据作为标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性。

[0009] 本发明的一种空口传输数据的正确性检测系统的有益效果如下:

[0010] 本发明的系统无需对待测移动终端内部进行程序改造和电路改造,可适配所有的协议和型号;在实现对通过空口传输的数据正确性进行快速检测的同时,还提高了检测精度。

[0011] 在上述方案的基础上,本发明的一种空口传输数据的正确性检测系统还可以做如下改进。

[0012] 进一步,所述检测终端还用于:

[0013] 构建所述远程检测设备的设备ID,并基于SM2算法,创建所述设备ID对应的第一密钥对,并将所述设备ID和所述第一密钥对的私钥发送至所述远程检测设备;

[0014] 接收所述远程检测设备发送的加密定位数据;其中,所述远程检测设备利用所述第一密钥对的私钥,对所述设备ID和所述第一当前定位数据进行加密并签名,得到所述加

密定位数据；

[0015] 利用所述第一密钥对的公钥,对所述加密定位数据进行解密并验签,得到所述第一当前定位数据和解密设备ID;

[0016] 所述检测终端具体用于:

[0017] 当所述解密设备ID与所述设备ID相同时,将所述第一当前定位数据作为所述标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性。

[0018] 进一步,所述检测终端还用于:

[0019] 基于SM2算法,创建所述设备ID对应的第二密钥对,并将所述第二密钥对的公钥发送至所述远程检测设备;

[0020] 利用第二空口,接收所述远程检测设备发送的第一设备加密数据;其中,所述远程检测设备利用所述第二密钥对的公钥对所述设备ID进行加密,得到所述第一设备加密数据,并根据所述检测终端的公网地址和端口号,构建所述远程检测设备与所述检测终端之间的所述第二空口;

[0021] 利用所述第二密钥对的私钥,对所述第一设备加密数据进行解密,得到第一解密设备ID;

[0022] 从所述检测终端存储的所有公钥中,确定目标公钥,并利用所述目标公钥对所述第一解密设备ID进行加密,得到第二设备加密数据并发送至所述远程检测设备,以使所述远程检测设备判定所述第二设备加密数据对应的第二解密设备ID与所述设备ID是否相同;其中,所述远程检测设备利用所述目标公钥对应的私钥对所述第二设备加密数据进行解密,得到所述第二解密设备ID;

[0023] 若是,则接收所述远程检测设备发送的加密定位数据。

[0024] 进一步,所述检测终端具体用于:

[0025] 当所述定位数据差值处于预设误差范围时,判定所述待测移动终端通过所述第一空口所传输的数据正确;否则,判定所述待测移动终端通过所述第一空口所传输的数据已被篡改。

[0026] 进一步,所述第一当前定位数据包括:第一当前经度数据和第一当前纬度数据,所述第二当前定位数据包括:第二当前经度数据和第二当前纬度数据,所述预设误差范围包括:经度误差范围和纬度误差范围;

[0027] 所述检测终端具体用于:

[0028] 当所述第一当前经度数据和所述第二当前经度数据之间的经度差值处于所述经度误差范围且所述第一当前纬度数据和所述第二当前纬度数据之间的纬度差值处于所述纬度误差范围时,判定所述待测移动终端通过所述第一空口所传输的数据正确,否则,判定所述待测移动终端通过所述第一空口所传输的数据已被篡改。

[0029] 进一步,所述检测终端还用于:

[0030] 当判定所述待测移动终端通过所述第一空口所传输的数据已被篡改时,生成预警信息并输出。

[0031] 进一步,所述待测移动终端为:无人机、智能网联汽车或物联网设备。

[0032] 本发明的一种空口传输数据的正确性检测方法的技术方案如下:

[0033] 检测终端获取所述远程检测设备采集的第一当前定位数据,并利用所述第一空口,获取所述待测移动终端采集的第二当前定位数据;其中,所述远程检测设备安装在待测移动终端上,所述检测终端与所述待测移动终端之间通过第一空口连接;

[0034] 所述检测终端将所述第一当前定位数据作为标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性。

[0035] 本发明的一种空口传输数据的正确性检测方法的有益效果如下:

[0036] 本发明的方法无需对待测移动终端内部进行程序改造和电路改造,可适配所有的协议和型号;在实现对通过空口传输的数据正确性进行快速检测的同时,还提高了检测精度。

[0037] 在上述方案的基础上,本发明的一种空口传输数据的正确性检测方法还可以做如下改进。

[0038] 进一步,还包括:

[0039] 所述检测终端构建所述远程检测设备的设备ID,并基于SM2算法,创建所述设备ID对应的第一密钥对,并将所述设备ID和所述第一密钥对的私钥发送至所述远程检测设备;

[0040] 所述检测终端接收所述远程检测设备发送的加密定位数据;其中,所述远程检测设备利用所述第一密钥对的私钥,对所述设备ID和所述第一当前定位数据进行加密并签名,得到所述加密定位数据;

[0041] 所述检测终端利用所述第一密钥对的公钥,对所述加密定位数据进行解密并验签,得到所述第一当前定位数据和解密设备ID;

[0042] 所述检测终端将所述第一当前定位数据作为标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性的步骤,包括:

[0043] 当所述解密设备ID与所述设备ID相同时,所述检测终端将所述第一当前定位数据作为所述标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性。

[0044] 进一步,还包括:

[0045] 所述检测终端基于SM2算法,创建所述设备ID对应的第二密钥对,并将所述第二密钥对的公钥发送至所述远程检测设备;

[0046] 所述检测终端利用第二空口,接收所述远程检测设备发送的第一设备加密数据;其中,所述远程检测设备利用所述第二密钥对的公钥对所述设备ID进行加密,得到所述第一设备加密数据,并根据所述检测终端的公网地址和端口号,构建所述远程检测设备与所述检测终端之间的所述第二空口;

[0047] 所述检测终端利用所述第二密钥对的私钥,对所述第一设备加密数据进行解密,得到第一解密设备ID;

[0048] 所述检测终端从所述检测终端存储的所有公钥中,确定目标公钥,并利用所述目标公钥对所述第一解密设备ID进行加密,得到第二设备加密数据并发送至所述远程检测设备,以使所述远程检测设备判定所述第二设备加密数据对应的第二解密设备ID与所述设备ID是否相同;其中,所述远程检测设备利用所述目标公钥对应的私钥对所述第二设备加密

数据进行解密,得到所述第二解密设备ID;

[0049] 若是,所述检测终端则接收所述远程检测设备发送的加密定位数据。

### 附图说明

[0050] 图1示出了本发明提供的一种空口传输数据的正确性检测系统的实施例的结构示意图;

[0051] 图2示出了本发明提供的一种空口传输数据的正确性检测系统的实施例中的远程检测设备的结构示意图;

[0052] 图3示出了本发明提供的一种空口传输数据的正确性检测方法的实施例的流程示意图。

### 具体实施方式

[0053] 图1示出了本发明提供的一种空口传输数据的正确性检测系统的实施例的结构示意图。如图1所示,该系统100包括:检测终端110和远程检测设备120;远程检测设备120安装在待测移动终端130上,检测终端110与待测移动终端130之间通过第一空口连接。

[0054] 所述检测终端110用于:

[0055] 获取所述远程检测设备120采集的第一当前定位数据,并利用所述第一空口,获取所述待测移动终端130采集的第二当前定位数据。

[0056] 其中,①待测移动终端130为:无人机、智能网联汽车或物联网设备,也可以是其他带有GPS定位和通信功能的移动终端,在此不设限制。②第一空口为:检测终端110与待测移动终端130之间的空中接口;具体是指通过4G/5G等无线网络,实现检测终端110与待测移动终端130之间电波链接的技术规范。③第一当前定位数据为:远程检测设备120在当前时刻采集的远程检测设备120自身的定位数据。④第二当前定位数据为:待测移动终端130在当前时刻采集的待测移动终端130自身的定位数据。⑤远程检测设备120与被测移动终端130之间通过粘接、螺栓固定、磁吸、捆绑等方式连接。

[0057] 将所述第一当前定位数据作为标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端130通过所述第一空口所传输的数据的正确性。

[0058] 其中,①标准数据为:默认设置的正确定位数据,即该数据不会出现错误。②定位数据差值为:第一当前定位数据和第二当前定位数据之间的差值。

[0059] 较优地,所述检测终端110还用于:

[0060] 构建所述远程检测设备120的设备ID,并基于SM2算法,创建所述设备ID对应的第一密钥对,并将所述设备ID和所述第一密钥对的私钥发送至所述远程检测设备120。

[0061] 其中,①设备ID为远程检测设备120的唯一身份码。②第一密钥对包括:公钥(设备公钥)和私钥(设备私钥)。

[0062] 接收所述远程检测设备120发送的加密定位数据。

[0063] 其中,远程检测设备120利用第一密钥对的私钥,对设备ID和第一当前定位数据进行加密并签名,得到加密定位数据。

[0064] 利用所述第一密钥对的公钥,对所述加密定位数据进行解密并验签,得到所述第

一当前定位数据和解密设备ID。

[0065] 其中,解密设备ID为:对加密定位数据进行解密并验签所得到的设备ID。

[0066] 需要说明的是,加密签名和解密验签的过程为现有技术,在此不过多赘述。

[0067] 所述检测终端110具体用于:

[0068] 当所述解密设备ID与所述设备ID相同时,将所述第一当前定位数据作为所述标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端130通过所述第一空口所传输的数据的正确性。

[0069] 具体地,检测终端110判断解密设备ID与设备ID是否相同,若是,则将第一当前定位数据作为标准数据,并基于标准数据与第二当前定位数据之间的定位数据差值,判定待测移动终端130通过第一空口所传输的数据的正确性。

[0070] 较优地,所述检测终端110还用于:

[0071] 基于SM2算法,创建所述设备ID对应的第二密钥对,并将所述第二密钥对的公钥发送至所述远程检测设备120。

[0072] 其中,第二密钥对包括:公钥(通用公钥)和私钥(通用私钥)。

[0073] 利用第二空口,接收所述远程检测设备120发送的第一设备加密数据。

[0074] 其中,①远程检测设备120利用所述第二密钥对的公钥对所述设备ID进行加密,得到所述第一设备加密数据。②远程检测设备120根据所述检测终端的公网地址和端口号,构建所述远程检测设备120与所述检测终端110之间的所述第二空口。

[0075] 利用所述第二密钥对的私钥,对所述第一设备加密数据进行解密,得到第一解密设备ID。

[0076] 从所述检测终端110存储的所有公钥中,确定目标公钥,并利用所述目标公钥对所述第一解密设备ID进行加密,得到第二设备加密数据并发送至所述远程检测设备120,以使所述远程检测设备120判定所述第二设备加密数据对应的第二解密设备ID与所述设备ID是否相同。

[0077] 其中,①每个设备ID对应一个第一密钥对和一个第二密钥对。②远程检测设备120利用目标公钥对应的私钥对第二设备加密数据进行解密,得到第二解密设备ID。

[0078] 具体地,检测终端110利用第一密钥对的第一私钥,对第一设备加密数据进行解密,得到第一解密设备ID。检测终端110利用第一解密设备ID对应的第二密钥对的第二公钥,对第一解密设备ID进行加密,得到第二设备加密数据,并将第二设备加密数据发送至远程检测设备120,以使远程检测设备120判定第二设备加密数据对应的第二解密设备ID与设备ID是否相同。

[0079] 若是,则接收所述远程检测设备120发送的加密定位数据。

[0080] 具体地,当第二设备加密数据对应的第二解密设备ID与设备ID相同时,判定远程检测设备120与检测终端110通信握手成功,检测终端110接收远程检测设备120发送的加密定位数据。

[0081] 需要说明的是,当远程检测设备120判定第二设备加密数据对应的第二解密设备ID与设备ID不相同,返回执行远程检测设备120利用第一密钥对的公钥对所述设备ID进行加密,得到第一设备加密数据的步骤,直至远程检测设备120与检测终端110通信握手成功。

[0082] 较优地,所述检测终端110具体用于:

[0083] 当所述定位数据差值处于预设误差范围时,判定所述待测移动终端130通过所述第一空口所传输的数据正确;否则,判定所述待测移动终端130通过所述第一空口所传输的数据已被篡改。

[0084] 其中,①第一当前定位数据包括:第一当前经度数据和第一当前纬度数据。②第二当前定位数据包括:第二当前经度数据和第二当前纬度数据。③预设误差范围包括:经度误差范围和纬度误差范围。

[0085] 具体地,当所述第一当前经度数据和所述第二当前经度数据之间的经度差值处于所述经度误差范围且所述第一当前纬度数据和所述第二当前纬度数据之间的纬度差值处于所述纬度误差范围时,判定所述待测移动终端130通过所述第一空口所传输的数据正确,否则,判定所述待测移动终端130通过所述第一空口所传输的数据已被篡改。

[0086] 需要说明的是,定位数据中除包含经纬度外,还可以包括:海拔、速度、航向等,具体可根据实际需求进行设定,在此不设限制。

[0087] 较优地,所述检测终端110还用于:

[0088] 当判定所述待测移动终端130通过所述第一空口所传输的数据已被篡改时,生成预警信息并输出。

[0089] 其中,预警信息包括:文字预警信息和声音报警信息等。

[0090] 需要说明的是,当待测移动终端130通过所述第一空口所传输的数据已被篡改时,除生成预警信息并输出外,返回执行远程检测设备120采集第一当前定位数据的步骤。

[0091] 此外,图2示出了远程检测设备120的具体结构图。远程检测设备120包括:加密芯片121、控制芯片122、定位芯片123、通信芯片124、电池芯片125和天线126。其中:

[0092] 定位芯片123用于:通过天线126,实时获取当前时刻的远程检测设备120的第一当前定位数据并传输至加密芯片121。

[0093] 加密芯片121用于:接收定位芯片123输出的第一当前定位数据,并利用SM2算法进行加密签名运算,将加密后的加密定位数据传输给控制芯片122。

[0094] 控制芯片122用于:将加密定位数据通过通信芯片124发送至检测终端110。

[0095] 通信芯片124用于:建立远程检测设备120与待测移动终端130之间的空口网络(第二空口)连接。

[0096] 天线126用于:增强获取第一当前定位数据。

[0097] 电池芯片125用于:为远程检测设备120中各芯片进行供电。

[0098] 本实施例的技术方案无需对待测移动终端内部进行程序改造和电路改造,可适配所有的协议和型号;在实现对通过空口传输的数据正确性进行快速检测的同时,还提高了检测精度。

[0099] 图3示出了本发明提供的一种空口传输数据的正确性检测方法的实施例的流程示意图。如图3所示,包括如下步骤:

[0100] 步骤210:检测终端获取所述远程检测设备采集的第一当前定位数据,并利用所述第一空口,获取所述待测移动终端采集的第二当前定位数据;其中,所述远程检测设备安装在待测移动终端上,所述检测终端与所述待测移动终端之间通过第一空口连接;

[0101] 步骤220:所述检测终端将所述第一当前定位数据作为标准数据,并基于所述标准

数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性。

[0102] 较优地,还包括:

[0103] 所述检测终端构建所述远程检测设备的设备ID,并基于SM2算法,创建所述设备ID对应的第一密钥对,并将所述设备ID和所述第一密钥对的私钥发送至所述远程检测设备;

[0104] 所述检测终端接收所述远程检测设备发送的加密定位数据;其中,所述远程检测设备利用所述第一密钥对的私钥,对所述设备ID和所述第一当前定位数据进行加密并签名,得到所述加密定位数据;

[0105] 所述检测终端利用所述第一密钥对的公钥,对所述加密定位数据进行解密并验签,得到所述第一当前定位数据和解密设备ID;

[0106] 步骤220包括:

[0107] 当所述解密设备ID与所述设备ID相同时,所述检测终端将所述第一当前定位数据作为所述标准数据,并基于所述标准数据与所述第二当前定位数据之间的定位数据差值,判定所述待测移动终端通过所述第一空口所传输的数据的正确性。

[0108] 较优地,还包括:

[0109] 所述检测终端基于SM2算法,创建所述设备ID对应的第二密钥对,并将所述第二密钥对的公钥发送至所述远程检测设备;

[0110] 所述检测终端利用第二空口,接收所述远程检测设备发送的第一设备加密数据;其中,所述远程检测设备利用所述第二密钥对的公钥对所述设备ID进行加密,得到所述第一设备加密数据,并根据所述检测终端的公网地址和端口号,构建所述远程检测设备与所述检测终端之间的所述第二空口;

[0111] 所述检测终端利用所述第二密钥对的私钥,对所述第一设备加密数据进行解密,得到第一解密设备ID;

[0112] 所述检测终端从所述检测终端存储的所有公钥中,确定目标公钥,并利用所述目标公钥对所述第一解密设备ID进行加密,得到第二设备加密数据并发送至所述远程检测设备,以使所述远程检测设备判定所述第二设备加密数据对应的第二解密设备ID与所述设备ID是否相同;其中,所述远程检测设备利用所述目标公钥对应的私钥对所述第二设备加密数据进行解密,得到所述第二解密设备ID;

[0113] 若是,所述检测终端则接收所述远程检测设备发送的加密定位数据。

[0114] 本实施例的技术方案无需对待测移动终端内部进行程序改造和电路改造,可适配所有的协议和型号;在实现对通过空口传输的数据正确性进行快速检测的同时,还提高了检测精度。

[0115] 上述关于本实施例的一种空口传输数据的正确性检测方法中的各参数和各个步骤实现相应功能的步骤,可参考上文中关于一种空口传输数据的正确性检测系统的实施例中的各参数和各模块,在此不做赘述。

[0116] 在此处所提供的说明书中,说明了大量具体细节。然而能够理解,本发明的实施例可以在没有这些具体细节的情况下实践。类似地,为了精简本发明并帮助理解各个发明方面中的一个或多个,在上面对本发明的示例性实施例的描述中,本发明实施例的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。其中,遵循具体实施方式的权利要求

求书由此明确地并入该具体实施方式,其中每个权利要求本身都作为本发明的单独实施例。

[0117] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制,并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中,不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中,这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。上述实施例中的步骤,除有特殊说明外,不应理解为对执行顺序的限定。

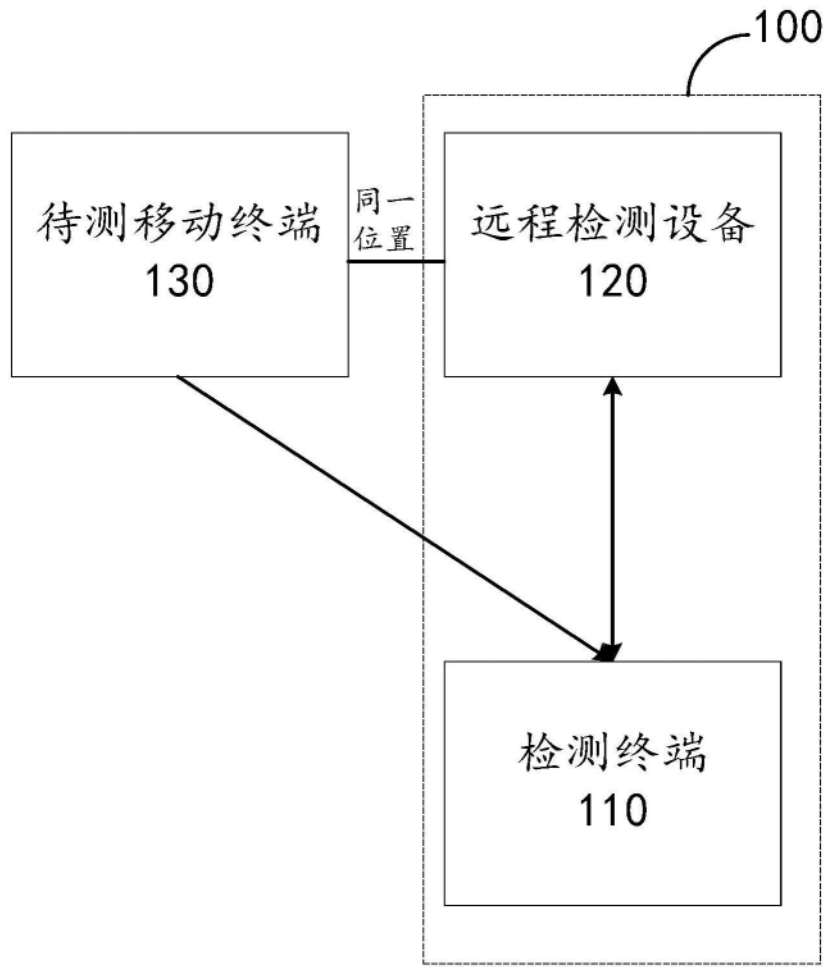


图1

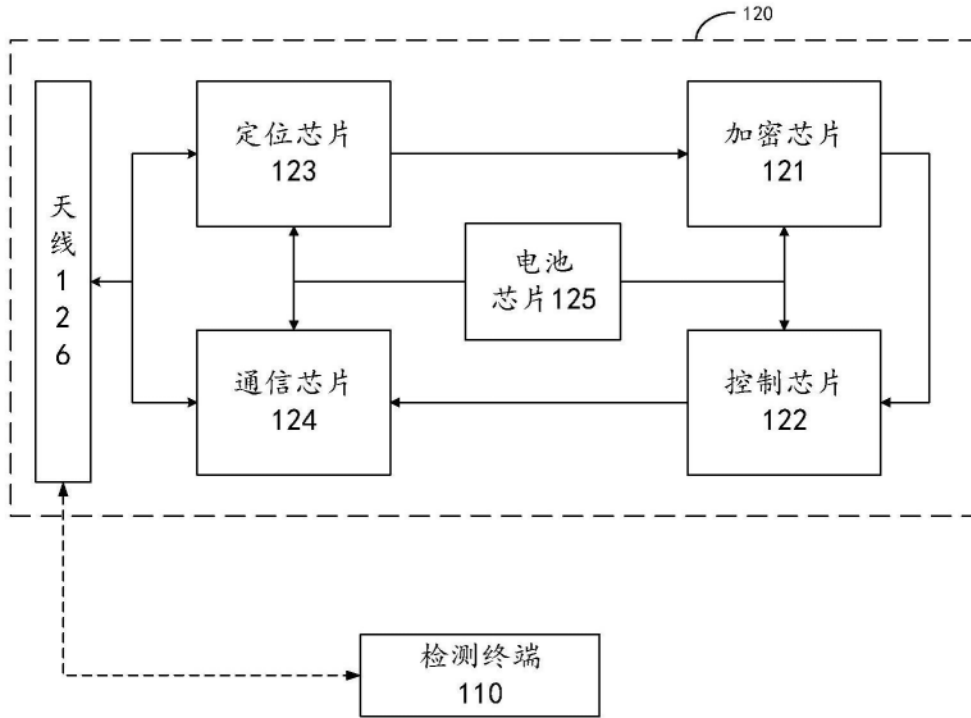


图2

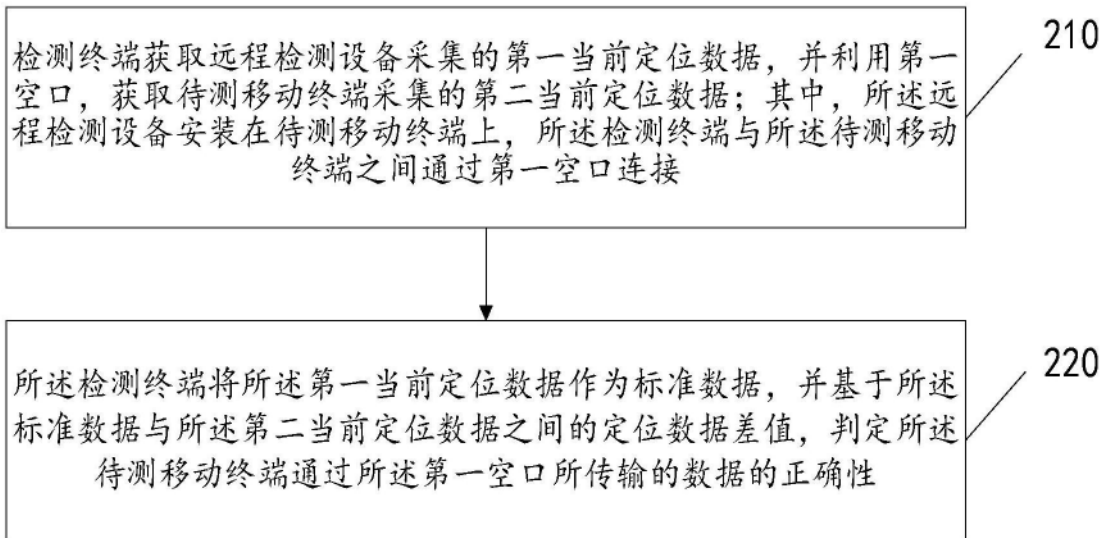


图3