

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号
WO 2020/042773 A1

(43) 国际公布日
2020 年 3 月 5 日 (05.03.2020)

- (51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
- (21) 国际申请号: PCT/CN2019/095522
- (22) 国际申请日: 2019 年 7 月 11 日 (11.07.2019)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201810995418.9 2018 年 8 月 29 日 (29.08.2018) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 赵豪 (ZHAO, Hao); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。
- (74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,

(54) Title: SECURITY DETECTION METHOD, APPARATUS AND DEVICE

(54) 发明名称: 安全检测方法、设备及装置

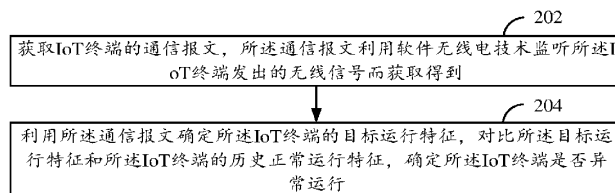


图 2

- 202 Obtain a communication message of an IoT terminal by using the software radio technology to monitor wireless signals emitted from the IoT terminal
- 204 The communication message is used to determine target operating features of the IoT terminal; the target operating features are compared with the historical normal operating feature of the IoT terminal to determine whether the IoT terminal operates normally

(57) Abstract: The present description provides a security detection method, apparatus and device. The security detection apparatus can be placed in an IoT network; an IoT terminal in the IoT network transmits data by means of wireless technology. The security detection apparatus includes a software radio unit, and thus can monitor all wireless signals within wireless coverage, thereby obtaining communication messages of the IoT terminal. According to the embodiment, the security detection apparatus is used to perform security detection on an IoT terminal in the IoT network without contacting and invading the IoT terminal or depending on the detection capability of the IoT terminal. Whether the IoT terminal operates normally can be found by obtaining target operating features of the IoT terminal in combination with historical normal operating features, and the security detection of the IoT terminal can be implemented.

(57) 摘要: 本说明书提供一种安全检测方法、设备及装置, 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。

[见续页]

WO 2020/042773 A1

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。