(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

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

WIPO | PCT

(10) 国际公布号
WO 2020/042856 A1

(51) 国际专利分类号:
H04W 12/08 (2009.01) *H04W 12/12* (2009.01)

(21) 国际申请号: PCT/CN2019/098469

(22) 国际申请日: 2019 年 7 月 30 日 (30.07.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810980737.2 2018年8月27日 (27.08.2018) CN

(71) 申请人: 北京智芯微电子科技有限公司(**BEIJING SMARTCHIP MICROELECTRONICS TECHNOLOGY COMPANY LIMITED**) [CN/CN]; 中国北京市海淀区西小口路66号中关村东升科技园A区3号楼, Beijing 100192 (CN)。 国网信息通信产业集团有限公司(**STATE GRID INFORMATION & TELECOMMUNICATION GROUP CO., LTD**) [CN/CN]; 中国北京市昌平未来科技城北区国网智能电网研究院内C座4层, Beijing 102211 (CN)。 国家电网有限公司(**STATE GRID CORPORATION OF CHINA**) [CN/CN]; 中国北京市西城区西长安街86号, Beijing 100031 (CN)。 国网福建省电力有限公司电力科学研究院(**STATE GRID FUJIAN ELECTRIC POWER RESEARCH INSTITUTE**) [CN/CN]; 中国福建省福州市仓山区复园支路48号, Fujian 350007 (CN)。

(72) 发明人: 唐晓柯(**TANG, Xiaoke**); 中国北京市海淀区西小口路66号中关村东升科技园A区3号楼, Beijing 100192 (CN)。 崔炳荣(**CUI, Bingrong**); 中国北京市海淀区西小口路66号中关村东升科技园A区3号楼, Beijing 100192 (CN)。 闫天瑜(**YAN, Tianyu**); 中国北京市海淀区西小口路66号中关村东升科技园A区3号楼, Beijing 100192 (CN)。 甘杰(**GAN, Jie**); 中国北京市海淀区西小口路66号中关村东升科技园A区3号楼, Beijing 100192 (CN)。

(54) **Title:** SECURITY AUDITING SYSTEM AND METHOD

(54) 发明名称: 安全审计系统及方法

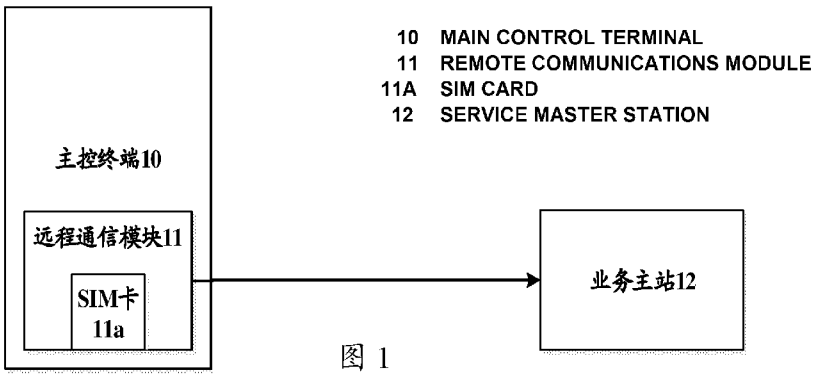

图 1

(57) **Abstract:** Disclosed in the embodiments of the present invention are a security auditing system and a method for same. The security auditing system comprises an eSIM module. The eSIM module is configured to: on the basis of pre-stored auditing rules, perform a security check on each received network connection request; if the security check is passed, determine said network connection request to be a legitimate request and allow the main control terminal that sent the network connection request to perform mobile network connection; and if the security check is not passed, determine the network connection request to be an illegitimate request and prohibit the main control terminal that sent the network connection request from performing mobile network connection.

(57) 摘要: 本申请实施例公开了一种安全审计系统及方法。其中，所述安全审计系统包括eSIM模块；eSIM模块，配置为：根据预先存储的审计规则对每次收到的网络连接请求进行安全审查；若通过安全审查，则确认该网络连接请求为合法请求，则允许发起所述网络连接请求的主控终端进行移动网络连接；若未通过安全审查，则确认该网络连接请求为非法请求，禁止发起所述网络连接请求的主控终端进行移动网络连接。

WO 2020/042856 A1

[见续页]

(74) 代理人：北京派特恩知识产权代理有限公司(CHINA PAT INTELLECTUAL PROPERTY OFFICE)；中国北京市海淀区海淀南路21号中关村知识产权大厦B座2层, Beijing 100080 (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, 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))。

安全审计系统及方法

相关申请的交叉引用

本申请基于申请号为201810980737.2、申请日为2018年08月27日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的内容在此以引入方式并入本申请。

技术领域

本申请涉及无线通信领域，具体是一种用于远程连接的安全审计系统及方法。

背景技术

随着无线网络的不断发展，无线通信技术已被广泛应用到各行各业中。这种技术使用运营商现有的无线网络资源，具有覆盖范围大，使用成本低，通信质量好等优点。在电力系统当中，无线通信技术也已成为主要的传输手段。

现有的电力采集系统中，主控终端不具有与业务主站进行直接连接的功能，当其需要与业务主站进行连接如无线连接时，主要依靠远程通信模块与业务主站进行连接。进一步的，主控终端向远程通信模块发送网络连接指令，远程通信模块无条件的连接业务主站。这种无条件的连接方式无法保证数据安全性。

公开于该背景技术部分的信息仅仅旨在增加对本申请实施例的总体背景的理解，而不应当被视为承认或以任何形式暗示该信息构成已为本领域一般技术人员所公知的现有技术。

发明内容

本申请实施例在于提供一种安全审计系统及方法，至少能够增加通信

数据的安全性。

为实现上述目的，本申请实施例提供了一种安全审计系统，包括：

嵌入式通用集成电路卡 eSIM 模块，配置为：

根据预先存储的审计规则对接收的网络连接请求进行安全审查；

若通过安全审查，则确认该网络连接请求为合法请求，则允许发起所述网络连接请求的主控终端进行移动网络连接；

若未通过安全审查，则确认该网络连接请求为非法请求，禁止发起所述网络连接请求的主控终端进行移动网络连接。

在一实施方式中，所述 eSIM 模块，配置为：对非法请求信息进行记录。

在一实施方式中，所述系统还包括：

安全服务器，与所述 eSIM 模块相耦合，配置为存储所述 eSIM 模块记录的非法请求信息。

在一实施方式中，所述安全服务器，还配置为：

配置所述审计规则以及上传规则，将所述审计规则以及所述上传规则写入所述 eSIM 模块中以供所述 eSIM 模块存储；

相应的，所述 eSIM 模块，配置为根据所述审计规则对所述网络连接请求进行安全审查；根据所述上传规则将记录的非法请求信息上传至所述安全服务器。

在一实施方式中，所述系统还包括：

主控终端，插入有远程通信模块，所述 eSIM 模块焊接在所述远程通信模块上；

所述远程通信模块，配置为接收所述主控终端发起的所述网络连接请求并将该网络连接请求发送给所述 eSIM 模块；以及

业务主站，在所述网络连接请求通过所述 eSIM 模块的安全审查并与移动网络成功连接的情况下，通过所述远程通信模块与所述主控终端建立通

信。

本申请实施例还提供了一种安全审计方法，包括:

根据预先存储的审计规则，对接收的网络连接请求进行安全审查;

若通过安全审查，则确认该网络连接请求为合法请求，则允许发起所述网络连接请求的主控终端进行移动网络连接;

若未通过安全审查，则确认该网络连接请求为非法请求，禁止发起所述网络连接请求的主控终端进行移动网络连接。

在一实施方式中，所述方法还包括:

对非法请求信息进行记录。

在一实施方式中，所述方法还包括:

将记录的非法请求信息进行上传。

在一实施方式中，所述方法还包括:

接收配置的所述审计规则和上传规则;

根据所述审计规则对所述网络连接请求进行安全审查;

根据所述上传规则将记录的非法请求信息进行上传。

在一实施方式中，所述方法还包括:

接收由远程通信模块转发的所述主控终端发起的所述网络连接请求，其中所述主控终端插入有所述远程通信模块;

在所述网络连接请求通过安全审查、所述主控终端与移动网络成功连接的情况下，所述主控终端通过所述远程通信模块与业务主站进行通信。

与现有技术相比，本申请实施例中，采用物联网（M2M）安全级别的嵌入式通用集成电路卡（eSIM）模块，基于 eSIM 模块，对主控终端发起的连接事件进行安全审查，若通过安全审查，则确认该网络连接请求为合法请求，则允许发起所述网络连接请求的主控终端进行移动网络连接；若未通过安全审查，则确认该网络连接请求为非法请求，禁止发起所述网络

连接请求的主控终端进行移动网络连接。在不改变现有主站模式和采集系统架构，不增加主控终端硬件成本的前提下，基于 eSIM 模块对主控终端发起的连接事件的安全审计，确保了数据的安全性。该安全性的提高可以进一步扩展 eSIM 模块和远程通信模块的应用，保证了与其他业务主站连接的安全，满足了业务拓展的需求。

附图说明

图 1 是现有的一种主控终端与业务主站的远程连接结构；

图 2 是根据本申请实施例一实施方式的安全审计系统的结构示意图；

图 3 是根据本申请实施例一实施方式的安全审计方法的流程图。

具体实施方式

下面结合附图，对本申请实施例的具体实施方式进行详细描述，但应当理解本申请实施例的保护范围并不受具体实施方式的限制。

除非另有其它明确表示，否则在整个说明书和权利要求书中，术语“包括”或其变换如“包含”或“包括有”等等将被理解为包括所陈述的元件或组成部分，而并未排除其它元件或其它组成部分。

相关技术中，针对现有电力采集系统中，通过远程通信模块无条件与业务主站进行连接使得主控终端与业务主站进行连接的方案具体可以如下所述：

远程通信模块具有分组无线数据包的功能。图 1 是现有的一种主控终端的远程连接示意图。在该示意图中包括 4 个组成部分：主控终端 10、远程通信模块 11、用户识别模块（SIM）卡 11a、业务主站 12。网络连接过程为：主控终端 10 发送网络连接请求指令至远程通信模块 11，远程通信模块 11 通过 SIM 卡 11a 进行移动网络连接，远程通信模块 11 再与业务主站 12 进行连接，打开数据通路。

前述方案中，远程通信模块只承担了数据通路的作用，而远程通信模块内部的 SIM 卡主要用来做网络鉴权。如果主控终端配置的 IP 地址遭到恶意篡改，数据将存在被泄露的风险。

针对现有的主控终端的远程连接过程没有安全审计而存在的泄露风险的问题，本申请实施例提供了一种安全审计系统及方法。其原理是：将可插拔的 SIM 卡升级为物联网 M2M(machine to machine)安全级别的 eSIM 模块，基于远程通信模块和 eSIM 模块，将每次连接事件（网络连接请求）进行安全审查。进一步的，当远程通信模块接收到主控终端发送的网络连接指令后，将连接事件下发到 eSIM 模块。eSIM 模块对连接事件进行分析，主要进行连接事件是合法连接事件还是非法（恶意）连接事件的分析。如果为合法连接事件，则通过安全审查，确认该网络连接请求为合法请求，则允许发起所述网络连接请求的主控终端进行移动网络连接；如果为非法连接事件，则视为未通过安全审查，确认该网络连接请求为非法请求，禁止发起所述网络连接请求的主控终端进行移动网络连接。其中，判断为恶意连接事件，eSIM 模块上报到安全服务器。其中，eSIM 模块的上报可以是实时上报、也可以是定期上报。可以是主动上报、也可以是基于一定的触发事件如应安全服务器的上报请求而上报，具体不做限定。

可以理解，本申请实施例，由于主控终端通过 eSIM 模块进行安全审计，并与远程的安全服务器进行连接，为一种用于远程连接的安全审计系统和方法。

图 2 是根据本申请实施例一实施方式的安全审计系统的结构示意图。该安全审计系统包括主控终端 20、远程通信模块 21、eSIM 模块 21a、业务主站 22、安全服务器 23。

需要说明的是，本申请实施例中的主控终端 20 为无法与其它设备如业务主站和/或安全服务器进行连接的通信实体，需要通过插入主控终端 20

的远程通信模块 21 进行连接。其中，远程通信模块 21 焊接有 eSIM 模块 21a，eSIM 模块 21a 焊接在远程通信模块 21 的底板上。远程通信模块 21 用于接收主控终端的 20 发起的网络连接请求并将该网络连接请求发送给 eSIM 模块 21a。

eSIM 模块 21a 存储审计规则，配置为：根据审计规则对每次接收到的网络连接请求进行安全审查，若通过安全审查，则确认该网络连接请求为合法请求，则允许发起所述网络连接请求的主控终端 20 进行移动网络连接，否则，确认该网络连接请求为非法请求，禁止也即不允许发起所述网络连接请求的主控终端 20 进行移动网络连接。

其中，对于远程通信模块 21 发送至 eSIM 模块 21a 的由主控终端发起的网络连接请求中携带有主控终端想要访问的业务主站的信息如业务主站 22 的标识和/或网际协议地址（IP）。eSIM 模块 21a 对主控终端 20 发起的网络连接请求进行安全审查，相当于基于业务主站 22 的标识和/或 IP 地址判断主控终端想要访问的业务主站 22 是否出现在业务主站白名单上，如果出现则认为是安全审查通过，如果未出现则认为安全审查未通过。业务主站白名单为预先设置的、记载有主控终端可访问的业务主站、及其标识和/或 IP 地址信息。

实际应用中，对于业务主站白名单上出现的业务主站，合法终端可以对其进行访问，为避免非法终端对其进行访问，可以理解，eSIM 模块 21a 对主控终端发起的网络连接请求进行安全审查，也就是对需要对业务主站进行访问且插入有焊接所述 eSIM 模块 21a 的远程通信模块 21 的主控终端的合法性进行审查，以避免非法终端对业务主站进行恶意访问。

eSIM 模块 21a 还配置为记录非法请求信息；此外，eSIM 模块 21a 还配置为记录安全审查过程中的网络信号质量信息。eSIM 模块 21a 还配置为存储上传规则。eSIM 模块 21a 根据该上传规则将记录的非法请求信息、网络

信号质量等信息上传至安全服务器 23。其中，eSIM 模块 21a 根据上传规则将记录的前述内容上传到安全服务器 23 可以这样理解：在记录的非法请求级别高于预设级别阈值也即非法请求级别较高的情况下，即刻将记录的较高非法请求上传至安全服务器 23；eSIM 模块 21a 应安全服务器 23 的上传请求将记录的内容上传至安全服务器 23；在 eSIM 模块 21a 的用于记录的空间容量低于预设容量阈值的情况下也即 eSIM 模块 21a 记录的内容较多的情况下主动上传记录的内容至安全服务器 23。其中，对于 eSIM 模块 21a 记录的不同内容可以同时进行上传，也可以按照一定的顺序如记录的先后顺序进行上传，具体不做限定。

可以理解，对于 eSIM 模块 21a 上传的非法连接请求信息，安全服务器 23 通过该非法连接请求信息进行分析，如对非法连接请求的数量进行统计和/或对发起非法连接请求的主控终端的标识进行统计，以避免同一非法终端多次访问。对于 eSIM 模块 21a 上传的网络信号质量信息，安全服务器 23 对当前所处的网络环境进行评估，得到评估结果。其中，上传规则可根据评估结果进行灵活调整，如在评估结果表征主控终端 20 当前所处的网络环境较好的情况下，允许上传至安全服务器 23 的记录内容多些；如在评估结果表征主控终端 20 当前所处的网络环境较差的情况下，允许上传至安全服务器 23 的记录内容少些。以避免在网络环境差的情况下由于上传过多而导致的上传失败的问题。

在网络连接请求通过 eSIM 模块 21a 的安全审查并成功连接至移动网络的情况下，主控终端 20 通过远程通信模块 21 与业务主站 22 建立通信。

eSIM 模块 21a 内存储的这些数据无法进行外部读写，只可由自己及可信任的安全服务器 23 进行更新从而保证了 eSIM 模块 21a 的数据的安全性。

其中，eSIM 模块 21a 可由可信任的安全服务器 23 进行更改、维护、删除等操作之前，还需要执行以下的验证过程：在主控终端 20 通过 eSIM

模块 21a 入网后，通过远程通信模块 21 与安全服务器 23 进行通信。进一步的，主控终端 20 通过远程通信模块 21 向安全服务器 23 发送自身的身份标识信息和上行安全认证信息，安全服务器 23 依据该身份标识信息和接收到的上行安全认证信息，对主控终端 20 进行身份认证和上行安全验证。在身份认证和上行安全验证均通过的情况下，安全服务器 23 向主控终端 20、具体是远程通信模块 21 发送下行安全认证信息，远程通信模块 21、具体是 eSIM 模块 21a 对下行安全认证信息进行认证，认证通过，允许安全服务器 23 对其进行更改、删除、写入等更新操作。可以理解，以上验证过程为 eSIM 模块 21a 和安全服务器 23 双方均需要通过对方验证，该验证过程为一种双向验证，双向验证后允许执行更改、维护、删除等更新操作。

安全服务器 23 配置为存储 eSIM 模块 21a 上传的信息，还配置为配置审计规则以及上传规则，并将审计规则以及上传规则写入 eSIM 模块 21a 中，以供 eSIM 模块 21a 存储与使用。安全服务器 23 可以根据主控终端在各地的不同分布情况、eSIM 模块 21a 的读写次数和/或自身的处理能力等因素，合理配置上传规则，也即本申请实施例中的上传规则可根据实际情况而灵活配置的。例如，在安全服务器 23 与主控终端 20 之间连接的网络环境较差的情况下，允许主控终端 20 通过远程通信模块 21 上传至安全服务器 23 的记录内容少些，可视为对上传规则的一种根据实际网络环境进行灵活配置的方案。考虑到一个 eSIM 模块 21a 的用于记录的空间容量较为有限，可以设置上传规则可以为在可记录的空间容量低于预设容量阈值的情况下也即用于记录的空间容量较少的情况下，触发 eSIM 模块 21a 进行记录信息的上传，从而使 eSIM 模块 21a 达到智能上传的效果。

本领域技术人员可以理解，eSIM 模块 21a 除了能够进行以上信息的上传之外，还可以对主控终端 20 的地理位置数据、安全攻击数据、网络情况如网络信号质量信息等进行上传。可见，eSIM 模块 21a 能够实现对多种业

务数据的上传，相当于 eSIM 模块 21a 的功能被扩展，体现了 eSIM 模块 21a 的功能多样性。其中，安全攻击数据可以理解为存在有哪些非法安全服务器想要对其访问。

上述的安全审计系统和方法，相对于现有技术加入了 eSIM 模块和安全服务器，并结合审计机制（审计规则）和上传机制（上传规则）使得主控终端与业务主站的通信环境更加的安全，在此系统的安全保障下，可以进一步增加业务主站从而灵活进行业务扩展。

基于上述实施例的安全审计系统，图 2 是该实施方式的安全审计的具体方法。该安全审计方法包括步骤 S1-S3。

在 S1 中主控终端发送网络连接请求：主控终端 20 向远程通信模块 21 发送网络连接请求。

在 S2 中远程通信模块转发网络连接请求：远程通信模块 21 将该网络连接请求发送给 eSIM 模块 21a。

在 S3 中对网络连接请求进行安全审查：eSIM 模块 21a 根据审计规则对该网络连接请求进行安全审查，若通过安全审查，则将该网络连接请求确认为合法请求，且返回相应提示至远程通信模块 21，远程通信模块 21 正常进行入网连接，并与业务主站 22 建立通信。若未通过安全审查，则该网络连接请求确认为非法请求，且将返回相应提示至远程通信模块 21，远程通信模块 21 不进行移动网络连接也即不进行入网连接。根据上传规则，eSIM 模块 21a 应安全服务器 23 的上传请求、该记录的非法请求级别高或用于记录的空间容量剩余较少的情况下，将该非法请求的信息上传至安全服务器 23。

其中，主控终端 20 与业务主站 22 之间的数据通信的具体实现过程参见现有相关说明，不做赘述。

综上，本申请实施例的安全审计系统及方法，采用物联网 M2M 安全级

别的 eSIM 模块，一方面可保证数据的安全性，另一方面通过对 eSIM 模块的功能的扩展，使其实现对多种业务数据的上传。其中，基于 eSIM 模块，对主控终端发起的网络连接事件进行安全审查，若通过安全审查，则确认该网络连接请求为合法请求，则允许发起所述网络连接请求的主控终端进行移动网络连接；若未通过安全审查，则确认该网络连接请求为非法请求，禁止发起所述网络连接请求的主控终端进行移动网络连接。在不改变现有主站模式和采集系统架构，不增加主控终端硬件成本的前提下，基于 eSIM 模块对主控终端发起的连接事件的安全审查，确保了数据的安全性。该安全性的提高可以进一步扩展 eSIM 模块和远程通信模块的应用，保证了与其他业务主站连接的安全，满足了业务拓展的需求。其中，如果判断为恶意连接事件，eSIM 模块将其上报安全服务器。

本申请实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时至少用于执行前述实施例的安全审计方法的步骤。所述计算机可读存储介质具体可以为存储器。

本申请实施例还提供一种安全审计系统，包括处理器和用于存储能够在处理器上运行的计算机程序的存储器；所述处理器在运行前述的计算机程序时执行前述的安全审计方法的步骤。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流

程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

最后应当说明的是：以上实施例仅用于说明本申请实施例的技术方案而非对其保护范围的限制,尽管参照上述实施例对本申请进行了详细的说明,所属领域的普通技术人员应当理解：本领域技术人员阅读本申请后依然可对申请的具体实施方式进行种种变更、修改或者等同替换，但这些变更、修改或者等同替换，均在申请待批的权利要求保护范围之内。

工业实用性

本申请实施例中，采用物联网 M2M 安全级别的 eSIM 模块，对于主控终端而言，基于 eSIM 模块，对主控终端发起的网络连接事件进行安全审查，如果判断为非恶意连接事件如正常连接事件，则允许主控终端进行网络连接。如果判断为恶意连接事件，则禁止也即不允许主控终端进行网络连接，

且 eSIM 模块将恶意连接事件上报至安全服务器。本申请实施例，不增加主控终端硬件成本的前提下，基于 eSIM 模块对主控终端发起的连接事件的安全审查，确保了数据的安全性。

权利要求书

1. 一种安全审计系统，包括:

嵌入式通用集成电路卡 eSIM 模块，配置为:

根据存储的审计规则对接收的网络连接请求进行安全审查;

若通过安全审查，则确认该网络连接请求为合法请求，则允许发起所述网络连接请求的主控终端进行移动网络连接;

若未通过安全审查，则确认该网络连接请求为非法请求，禁止发起所述网络连接请求的主控终端进行移动网络连接。

2. 如权利要求 1 所述的安全审计系统，其中，所述 eSIM 模块，配置为: 对非法请求信息进行记录。

3. 如权利要求 2 所述的安全审计系统，其中，所述系统还包括:

安全服务器，配置为存储所述 eSIM 模块记录的非法请求信息。

4. 如权利要求 3 所述的安全审计系统，其中，

所述安全服务器，还配置为:

配置所述审计规则以及上传规则，将所述审计规则以及所述上传规则写入所述 eSIM 模块中以供所述 eSIM 模块存储;

相应的，所述 eSIM 模块，配置为:

根据所述审计规则对所述网络连接请求进行安全审查; 根据所述上传规则将记录的非法请求信息上传至所述安全服务器。

5. 如权利要求 1 所述的安全审计系统，其中，所述系统还包括:

主控终端，插入有远程通信模块，所述 eSIM 模块焊接在所述远程通信模块上;

所述远程通信模块，配置为接收所述主控终端发起的所述网络连接请求并将该网络连接请求发送给所述 eSIM 模块; 以及

业务主站，在所述网络连接请求通过所述 eSIM 模块的安全审查并与移动网络成功连接的情况下，通过所述远程通信模块与所述主控终端建立通

信。

6. 一种安全审计方法，包括:

根据预先存储的审计规则，对接收的网络连接请求进行安全审查;

若通过安全审查，则确认该网络连接请求为合法请求，则允许发起所述网络连接请求的主控终端进行移动网络连接;

若未通过安全审查，则确认该网络连接请求为非法请求，禁止发起所述网络连接请求的主控终端进行移动网络连接。

7. 如权利要求 6 所述的安全审计方法，其中，所述方法还包括:

对非法请求信息进行记录。

8. 如权利要求 7 所述的安全审计方法，其中，所述方法还包括:

将记录的非法请求信息进行上传。

9. 如权利要求 8 所述的安全审计方法，其中，所述方法还包括:

接收配置的所述审计规则和上传规则;

根据所述审计规则对所述网络连接请求进行安全审查;

根据所述上传规则将记录的非法请求信息进行上传。

10. 如权利要求 6 所述的安全审计方法，其中，所述方法还包括:

接收由远程通信模块转发的所述主控终端发起的所述网络连接请求，其中所述主控终端插入有所述远程通信模块;

在所述网络连接请求通过安全审查、所述主控终端与移动网络成功连接的情况下，所述主控终端通过所述远程通信模块与业务主站进行通信。

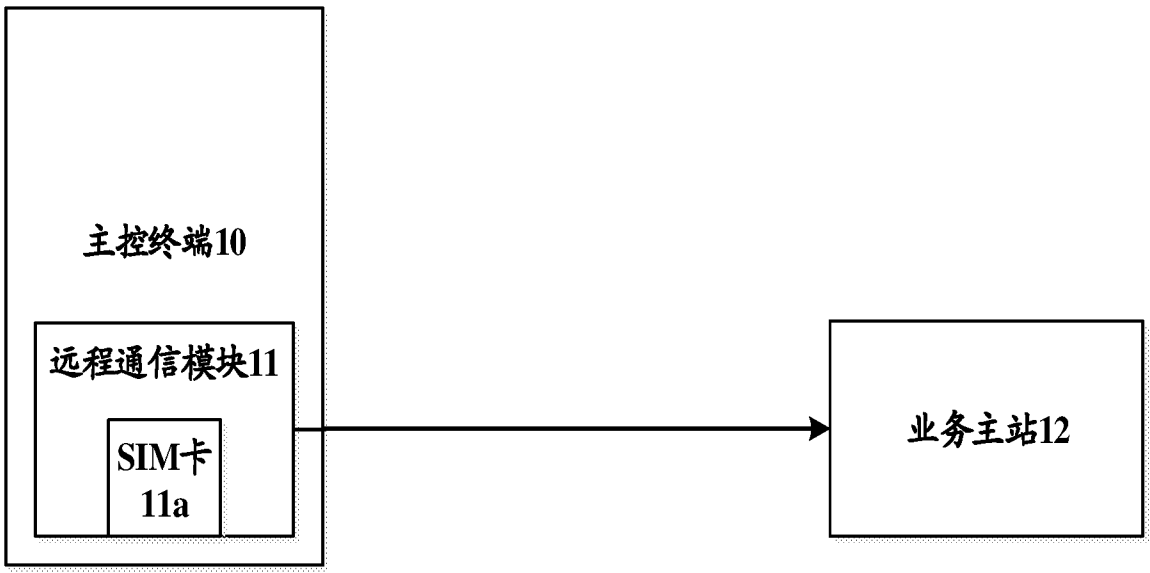

图 1

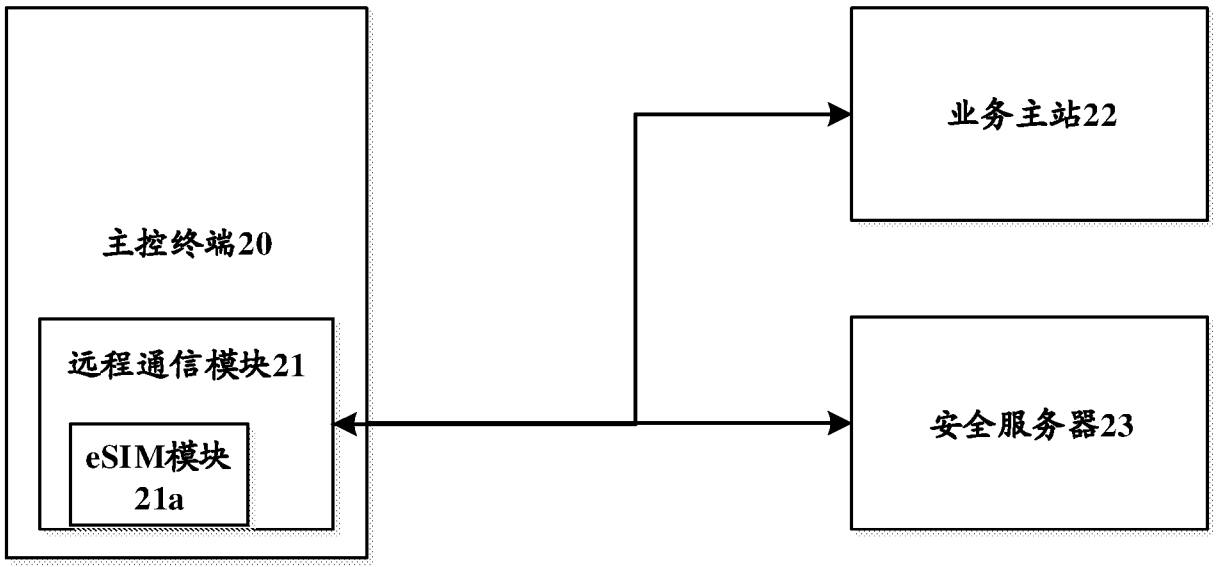

图 2

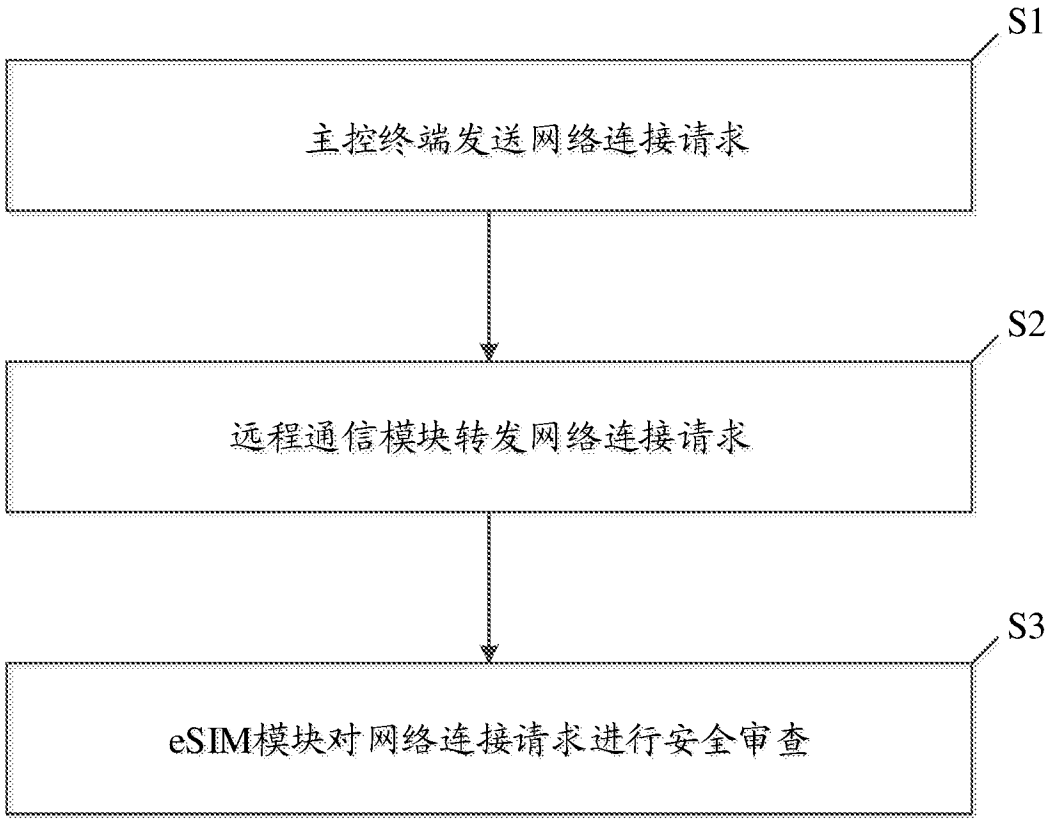
S1
主控终端发送网络连接请求
S2
远程通信模块转发网络连接请求
S3
eSIM模块对网络连接请求进行安全审查

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/098469

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/08(2009.01)i; H04W 12/12(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; VEN; USTXT; EPTXT; WOTXT; CNKI: 嵌入式, 用户识别卡, 通用集成电路卡, 安全, 审计, 访问, 网络, 连接, 请求, 网络地址, 白名单, 篡改, embedded SIM, eUICC, network, connection, request, address, IP, white list, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109246704 A (BEIJING SMARTCHIP MICROELECTRONICS TECHNOLOGY COMPANY LIMITED ET AL.) 18 January 2019 (2019-01-18) claims 1-10	1-10
X	CN 108024243 A (HENGBAO CO., LTD.) 11 May 2018 (2018-05-11) description, paragraphs [0059]-[0079] and [0107]-[0115], and figures 1-4	1-10
X	CN 105141621 A (BEIJING STAR-NET RUIJIE NETWORKS TECHNOLOGY CO., LTD.) 09 December 2015 (2015-12-09) description, paragraphs [0061]-[0085], and figures 1 and 2	6-10
A	CN 106131090 A (BEIJING LEADINGSOFT TECHNOLOGY CO., LTD. ET AL.) 16 November 2016 (2016-11-16) entire document	1-10
A	US 9949113 B1 (APPLE INC.) 17 April 2018 (2018-04-17)	1-10

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 September 2019	**26 September 2019**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/098469

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109246704 A	18 January 2019	None	
CN 108024243 A	11 May 2018	CN 108024243 B	21 June 2019
CN 105141621 A	09 December 2015	None	
CN 106131090 A	16 November 2016	None	
US 9949113 B1	17 April 2018	US 10149150 B1	04 December 2018
		US 2018352425 A1	06 December 2018
		KR 20180132519 A	12 December 2018
		JP 2018207479 A	27 December 2018
		DE 102018208578 A1	06 December 2018
		JP 6503494 B2	17 April 2019
		CN 108990020 A	11 December 2018
		IN 201814020337 A	07 December 2018

国际检索报告

国际申请号
PCT/CN2019/098469

A. 主题的分类

H04W 12/08(2009.01)i; H04W 12/12(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;VEN;USTXT;EPTXT;WOTXT;CNKI：嵌入式，用户识别卡，通用集成电路卡，安全，审计，访问，网络，连接，请求，网络地址，白名单，篡改，embedded SIM，eUICC，network，connection，request，address，IP，white list，security

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 109246704 A (北京智芯微电子科技有限公司等) 2019年 1月 18日 (2019-01-18) 权利要求1-10	1-10
X	CN 108024243 A (恒宝股份有限公司) 2018年 5月 11日 (2018-05-11) 说明书第[0059]-[0079]，[0107]-[0115]段，图1-4	1-10
X	CN 105141621 A (北京星网锐捷网络技术有限公司) 2015年 12月 9日 (2015-12-09) 说明书第[0061]-[0085]段，图1-2	6-10
A	CN 106131090 A (北京力鼎创软科技有限公司等) 2016年 11月 16日 (2016-11-16) 全文	1-10
A	US 9949113 B1 (APPLE INC) 2018年 4月 17日 (2018-04-17)	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 9月 11日	2019年 9月 26日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 李灿灿 电话号码 86-(20)-28950754

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/098469

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	109246704	A	2019年 1月 18日	无			
CN	108024243	A	2018年 5月 11日	CN	108024243	B	2019年 6月 21日
CN	105141621	A	2015年 12月 9日	无			
CN	106131090	A	2016年 11月 16日	无			
US	9949113	B1	2018年 4月 17日	US	10149150	B1	2018年 12月 4日
				US	2018352425	A1	2018年 12月 6日
				KR	20180132519	A	2018年 12月 12日
				JP	2018207479	A	2018年 12月 27日
				DE	102018208578	A1	2018年 12月 6日
				JP	6503494	B2	2019年 4月 17日
				CN	108990020	A	2018年 12月 11日
				IN	201814020337	A	2018年 12月 7日