(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109246704 A
(43)申请公布日 2019.01.18

(21)申请号 201810980737.2

(22)申请日 2018.08.27

(71)申请人 北京智芯微电子科技有限公司
地址 100192 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
申请人 国网信息通信产业集团有限公司
国家电网有限公司
国网福建省电力有限公司电力科学研究院

(72)发明人 唐晓柯 崔炳荣 闫天瑜 顿中强 甘杰 高琛 林华

(74)专利代理机构 北京中誉威圣知识产权代理有限公司 11279
代理人 王芊雨 张静轩

(51)Int.Cl.
H04W 12/08(2009.01)
H04W 12/12(2009.01)

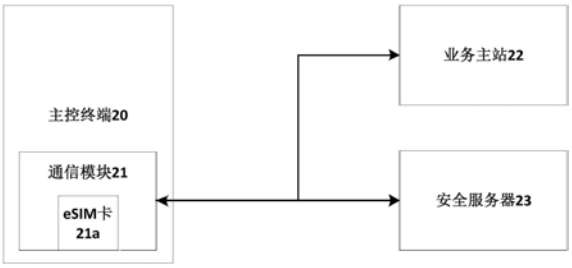
权利要求书2页 说明书4页 附图2页

(54)发明名称

用于远程连接的安全审计系统及方法

(57)摘要

本发明公开了一种用于远程连接的安全审计系统及方法。该安全审计系统包括eSIM模块。eSIM模块内部存储有审计规则，用于根据所述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，则该网络连接请求为合法请求，则进行移动网络连接，否则，该网络连接请求为非法请求，不进行移动网络连接。所述用于远程连接的安全审计系统及方法能够不增加主控终端硬件成本的前提下，增加通信数据的安全性。



CN 109246704 A

1.一种用于远程连接的安全审计系统,其特征在于,包括:

eSIM模块,内部存储有审计规则,用于根据所述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,则该网络连接请求为合法请求,则进行移动网络连接,否则,该网络连接请求为非法请求,不进行移动网络连接。

2.如权利要求1所述的用于远程连接的安全审计系统,其特征在于,所述eSIM模块内部记录所述非法请求的信息或网络信号质量的信息。

3.如权利要求2所述的用于远程连接的安全审计系统,其特征在于,所述安全审计系统还包括:

安全服务器,与所述eSIM模块相耦合,所述eSIM模块将记录的非法请求的信息或网络信号质量的信息上传至所述安全服务器进行最终存储。

4.如权利要求3所述的用于远程连接的安全审计系统,其特征在于,所述安全服务器还用于设置所述审计规则以及上传规则,并将所述审计规则以及所述上传规则写入所述eSIM模块中,所述eSIM模块根据所述审计规则对所述连接请求进行安全审查,所述eSIM根据所述上传规则将内部记录的信息上传至所述安全服务器。

5.如权利要求1所述的用于远程连接的安全审计系统,其特征在于,所述安全审计系统还包括:

主控终端,内置远程通信模块,所述远程通信模块与所述eSIM相耦合,所述远程通信模块用于接收所述主控终端的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,当所述网络连接请求通过所述eSIM模块的安全审查后且所述移动网络已成功连接后,所述业务主站通过所述远程通信模块与所述主控终端建立通信。

6.一种用于远程连接的安全审计方法,其特征在于,包括:

eSIM模块对收到的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,且进行移动网络连接,否则,该网络连接请求确认为非法请求,不进行移动网络连接。

7.如权利要求6所述的用于远程连接的安全审计方法,其特征在于,该安全审计方法还包括:

eSIM模块定期记录网络信号质量的信息并将其上传至安全服务器。

8.如权利要求7所述的用于远程连接的安全审计方法,其特征在于,该网络连接请求确认为非法请求,不进行移动网络连接后还包括:

eSIM模块记录该非法请求的信息并将其上传至安全服务器。

9.如权利要求8所述的用于远程连接的安全审计方法,其特征在于,所述安全审计方法还包括:

所述安全服务器设置审计规则和上传规则并写入所述eSIM模块中;以及

所述eSIM模块根据所述审计规则对所述连接请求进行安全审查并根据所述上传规则将内部记录的信息上传至所述安全服务器。

10.如权利要求6所述的用于远程连接的安全审计方法,其特征在于,所述安全审计方法还包括:

主控终端向远程通信模块发送网络连接请求;

所述远程通信模块将该网络连接请求发送给所述eSIM模块进行安全审查,以及

当网络连接请求通过所述eSIM模块的安全审查，且所述移动网络已成功连接后，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。

用于远程连接的安全审计系统及方法

技术领域

[0001] 本发明是关于无线通信领域,特别是关于一种用于远程连接的安全审计系统及方法。

背景技术

[0002] 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。

[0003] 现有的电力采集系统中,主控终端与业务主站的无线连接,主要依靠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服务器。其中的远程通信模块具有提供GPRS数据包的功能。图1是现有的一种主控终端的远程连接结构。该远程连接结构包括4个组成部分:主控终端10、远程通信模块11、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进行服务器连接,并打开数据通路。

[0004] 配置主控终端的方式有两种:一种是通过弱口令的密码保护,通过人工修改主控终端的配置,另外一种是在通路链接建立后,通过业务主站下发命令修改主控终端的配置。现有技术方案中,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,不具备安全审计和数据上报的能力。如果主控终端配置的IP地址遭到恶意篡改,数据存在被泄露风险。

[0005] 公开于该背景技术部分的信息仅仅旨在增加对本发明的总体背景的理解,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

[0006] 本发明的目的在于提供一种用于远程连接的安全审计系统及方法,其能够不增加主控终端硬件成本的前提下,增加通信数据的安全性。

[0007] 为实现上述目的,本发明提供了一种用于远程连接的安全审计系统,该安全审计系统包括eSIM模块。eSIM模块内部存储有审计规则,用于根据所述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,则该网络连接请求为合法请求,则进行移动网络连接,否则,该网络连接请求为非法请求,不进行移动网络连接。

[0008] 在一优选的实施方式中,所述eSIM模块内部记录所述非法请求的信息或网络信号质量的信息。

[0009] 在一优选的实施方式中,所述安全审计系统还包括安全服务器。所述安全服务器与所述eSIM模块相耦合,所述eSIM模块将记录的非法请求的信息或网络信号质量的信息上传至所述安全服务器进行最终存储。

[0010] 在一优选的实施方式中,所述安全服务器还用于设置所述审计规则以及上传规则,并将所述审计规则以及所述上传规则写入所述eSIM模块中,所述eSIM模块根据所述审

计规则对所述连接请求进行安全审查，所述eSIM根据所述上传规则将内部记录的信息上传至所述安全服务器。

[0011] 在一优选的实施方式中，所述安全审计系统还包括：主控终端和业务主站。所述主控终端内置远程通信模块，所述远程通信模块与所述eSIM相耦合，所述远程通信模块用于接收所述主控终端的网络连接请求并将该网络连接请求发送给所述eSIM模块。当所述网络连接请求通过所述eSIM模块的安全审查后且所述移动网络已成功连接后，所述业务主站通过所述远程通信模块与所述主控终端建立通信。

[0012] 本发明还提供了一种用于远程连接的安全审计方法，其包括：eSIM模块对收到的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，且进行移动网络连接，否则，该网络连接请求确认为非法请求，不进行移动网络连接。

[0013] 在一优选的实施方式中，该安全审计方法还包括：eSIM模块定期记录网络信号质量的信息并将其上传至安全服务器。

[0014] 在一优选的实施方式中，该网络连接请求确认为非法请求，不进行移动网络连接之后还包括：eSIM模块记录该非法请求的信息并将其上传至安全服务器。

[0015] 在一优选的实施方式中，所述安全审计方法还包括：所述安全服务器设置审计规则和上传规则并写入所述eSIM模块中；所述eSIM模块根据所述审计规则对所述连接请求进行安全审查并根据所述上传规则将内部记录的信息上传至所述安全服务器。

[0016] 在一优选的实施方式中，所述安全审计方法还包括：主控终端向远程通信模块发送网络连接请求；所述远程通信模块将该网络连接请求发送给所述eSIM模块进行安全审查，当网络连接请求通过所述eSIM模块的安全审查，且所述移动网络已成功连接后，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。

[0017] 与现有技术相比，根据本发明的所述用于远程连接的安全审计系统及方法将可插拔的SIM卡升级为物联网M2M安全级别的eSIM模块，基于远程通信模组和eSIM模块，将每次连接事件进行安全审计，如果判断为恶意连接事件，还要求eSIM主动上报到安全服务器。该用于远程连接的安全审计系统及方法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，增加了数据的安全性。该安全性的提高可以进一步扩展eSIM和远程通信模组的应用，保证了与其他的业务主站连接的安全，满足了业务拓展的需求。

附图说明

[0018] 图1是现有的一种主控终端与业务主站的远程连接结构；

[0019] 图2是根据本发明一实施方式的用于远程连接的安全审计系统的结构示意图；

[0020] 图3是根据本发明一实施方式的用于远程连接的安全审计方法的流程图。

具体实施方式

[0021] 下面结合附图，对本发明的具体实施方式进行详细描述，但应当理解本发明的保护范围并不受具体实施方式的限制。

[0022] 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。

[0023] 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，本发明提供了一种用于远程连接的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，基于远程通信模组和eSIM模块，将每次连接事件进行安全审计。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。eSIM对连接事件进行分析、存储，判定。如果判断为恶意连接事件，还要求eSIM主动上报到安全服务器。

[0024] 图2是根据本发明一实施方式的用于远程连接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。

[0025] 主控终端20内置远程通信模块21。远程通信模块21用于接收主控终端的20网络连接请求并将该网络连接请求发送给eSIM模块21a。

[0026] eSIM模块21a内部存储审计规则，用于根据所述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，则该网络连接请求为合法请求，则进行移动网络连接，否则，该网络连接请求为非法请求，不进行移动网络连接。eSIM模块21a还用于记录非法请求信息以及网络信号质量信息。eSIM模块21a还用于存储审计规则以及上传规则。eSIM模块21a根据该上传规则将内部记录的非法请求信息或网络信号质量等信息上传至安全服务器23。其中，eSIM模块21a会在不影响安全审查过程的前提下，在另外的逻辑通道记录非法请求信息以及网络信号质量信息。

[0027] 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进行更改、维护、删除从而保证了eSIM模块21a的数据的安全性。

[0028] 业务主站22在当所述网络连接请求通过eSIM模块21a的安全审查后且所述移动网络已成功连接后，通过远程通信模块21与主控终端20建立通信。

[0029] 安全服务器23用于存储eSIM模块21a上传的信息，还用于设置所述审计规则以及上传规则，并将所述审计规则以及所述上传规则写入eSIM模块21a中。安全服务器23可以根据各地情况、eSIM模块21a的读写次数以及安全服务器的处理能力等因素，合理配置上传规则，使eSIM模块21a达到智能上传的效果。

[0030] 在上述的用于远程连接的安全审计系统中相对与现有技术加入了eSIM和安全服务器以及安全审计机制、上传预警机制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。

[0031] 基于上述实施例的用于远程连接的安全审计系统，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。

[0032] 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。

[0033] 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所述eSIM模块21a。

[0034] 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，和业务主站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，并且根据上传规则，eSIM模块21a审查当前的网络环境，在适当时机，将该非法请求的信息上传至安全服务器23。

[0035] 综上，所述用于远程连接的安全审计系统及方法将可插拔的SIM卡升级为物联网M2M安全级别的eSIM模块，基于远程通信模组和eSIM模块，将每次连接事件进行安全审计，如果判断为恶意连接事件，还要求eSIM主动上报到安全服务器。该用于远程连接的安全审计系统及方法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，增加了数据的安全性。该安全性的提高可以进一步扩展eSIM和远程通信模组的应用，保证了与其他的业务主站连接的安全，满足了业务拓展的需求。

[0036] 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。

[0037] 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。

[0038] 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。

[0039] 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。

[0040] 最后应当说明的是：以上实施例仅用于说明本发明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。

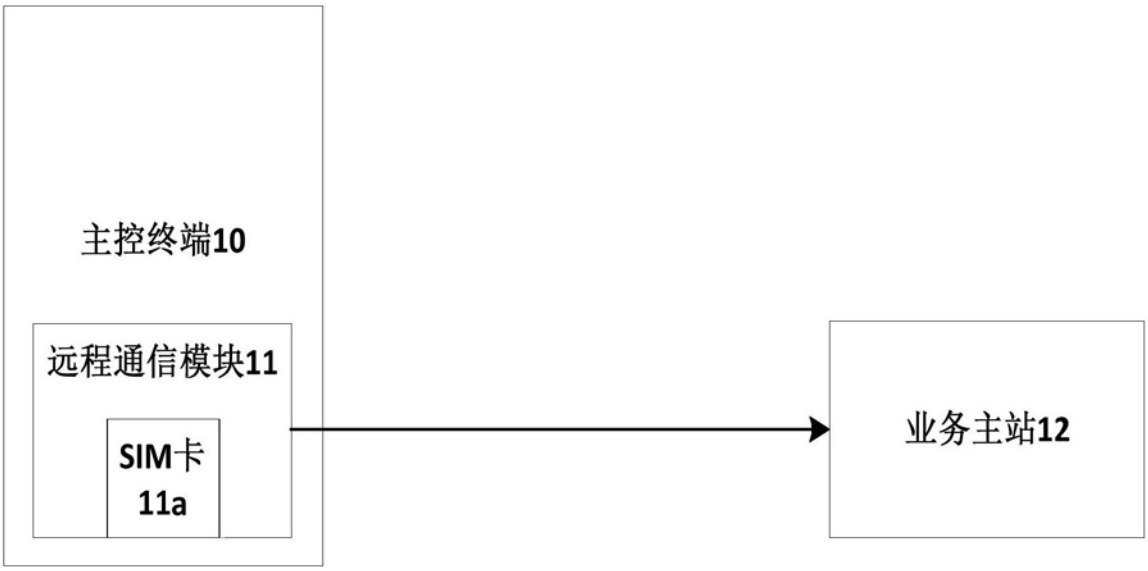

主控终端10
远程通信模块11
SIM卡
11a
业务主站12

图1

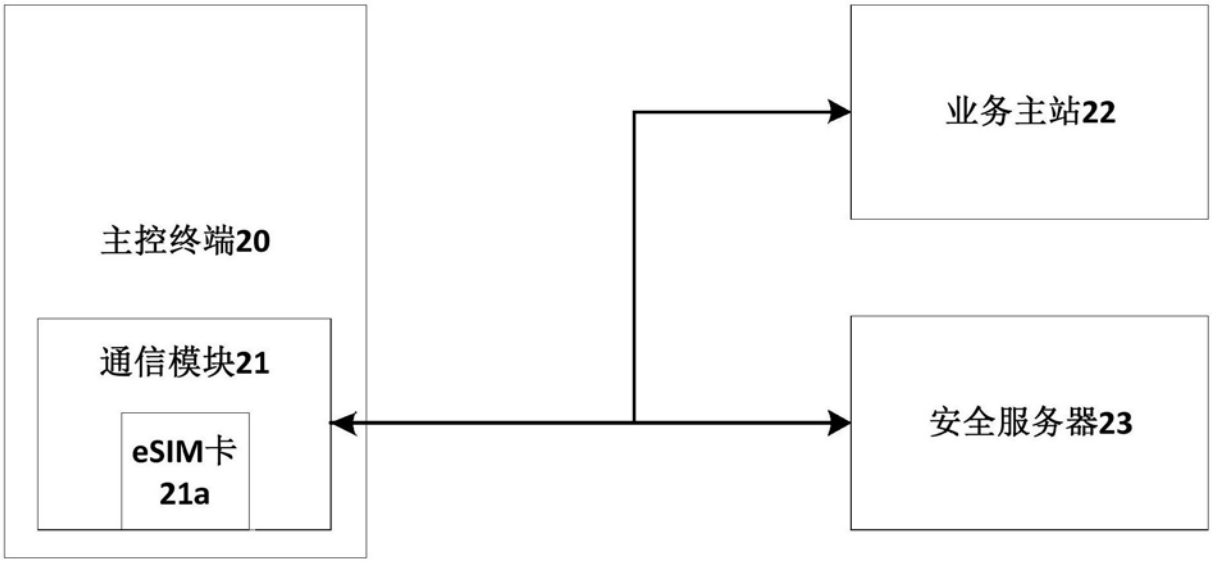

主控终端20
通信模块21
eSIM卡
21a
业务主站22
安全服务器23

图2

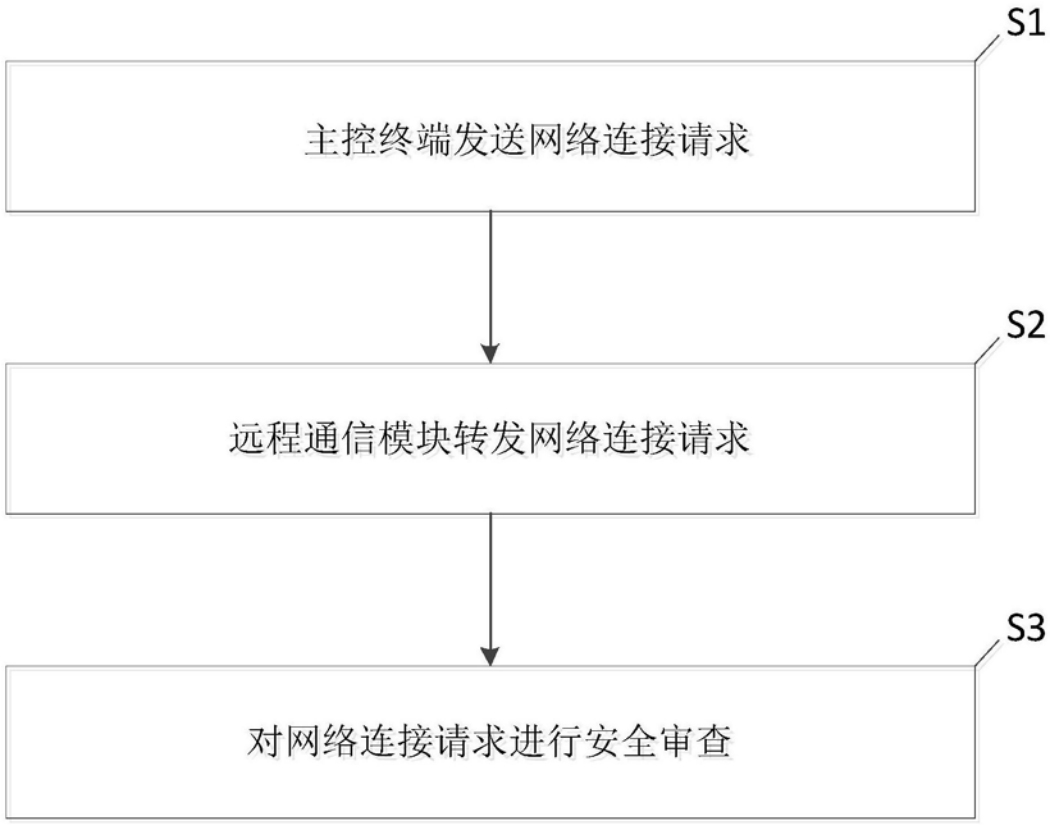


图3