(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 106943119 A
(43)申请公布日 2017.07.14

(21)申请号 201710139673.9

(22)申请日 2017.03.09

(71)申请人 北京大学第三医院
地址 100191 北京市海淀区花园北路49号

(72)发明人 倪诚 刘伟平 王军

(74)专利代理机构 北京国坤专利代理事务所（普通合伙）11491
代理人 姜彦

(51)Int.Cl.
A61B 5/00(2006.01)
A61B 5/0205(2006.01)
A61B 5/0476(2006.01)
A61B 5/08(2006.01)
A61B 5/083(2006.01)
H04L 29/08(2006.01)

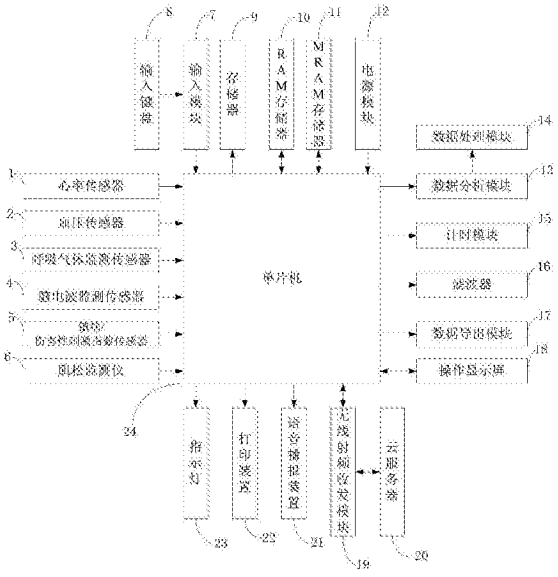
权利要求书3页 说明书8页 附图1页

(54)发明名称

一种麻醉和意识深度监测系统

(57)摘要

本发明涉及一种麻醉和意识深度监测系统，包括分别与心率传感器、血压传感器、呼吸气体监测传感器、脑电波监测传感器、镇痛/伤害性刺激指数传感器、肌松监测仪有线连接，用于对监测信号进行分析和处理的单片机；用于对监测数据进行分析的数据分析模块；用于对监测数据进行进一步处理的数据处理模块；用于消除干扰杂讯的滤波器；用于对监测信号进行显示和操作的操作显示屏；用于接收和发送无线网络信号的无线射频收发模块；与无线射频收发模块通过GPRS无线网络无线连接，用于进行数据传输与交换的云服务器。该麻醉和意识深度监测系统监测全面，数据分析精准，存储安全。



CN 106943119 A

1.一种麻醉和意识深度监测系统，其特征以及监测系统内容包括：

用于对人体心率进行监测的心率传感器；

用于对人体血压进行监测的血压传感器；

用于对人体呼吸频率、吸入氧浓度、呼气末二氧化碳、吸入麻醉气体进行监测的呼吸气体监测传感器；

用于对人体脑电波进行监测的脑电波监测传感器；

用于对人体疼痛刺激进行监测的镇痛/伤害性刺激指数传感器；

用于对人体骨骼肌松弛程度进行监测的肌松监测仪；

分别与心率传感器、血压传感器、呼吸气体监测传感器、脑电波监测传感器、镇痛/伤害性刺激指数传感器、肌松监测仪有线连接，用于对监测信号进行分析和处理的单片机；所述单片机设置有数据压缩单元，所述数据压缩单元的数据压缩方法的步骤为：

步骤一、在编码时，首先根据$E1_{n+1}=E1_n+d_{n+1}$式计算出E1值，再根据$\Delta d'_n=\frac{4\times d_n}{n}-\frac{6\times E1_n}{n(n+1)}$和$DFR_n=\Delta d_n-\lfloor\Delta d'_n\rfloor=\varepsilon$式计算出拟合残差，计算这两步时，均需要对结果进行越限判断，判断E1是否越限是为了避免其超过传感器数据总线上限而造成溢出；判断残差是否越限是为了实现分段拟合；

步骤二、当一段输入数据的拟合残差全部计算完后，构造出$\{d_n,E1_n,DFR_3,DFR_4,\cdots DFR_n\}$所示的数据包，通过S-Huffman编码方法对其进行熵编码，然后发送出去，接收端解码时，先将接收到的一组数据解码，还原出$\{d_n,E1_n,DFR_3,DFR_4,\cdots DFR_n\}$式所示的数据包，然后根据$d_{n-1}=d_n-\lfloor\Delta d'_n\rfloor-DFR_n=d_n-\left\lfloor\frac{4\times d_n}{n}-\frac{6\times E1_n}{n(n+1)}\right\rfloor-DFR_n$式计算并还原出所有原始数据；

与单片机通过输入模块有线连接，用于输入患者基本信息的输入键盘；

与单片机有线连接，用于对监测数据进行保存的存储器；

与单片机有线连接，用于对监测数据进行比对、采样和查询的RAM存储器和MRAM存储器；

与单片机有线连接，用于提供电源的电源模块；

与单片机有线连接，用于对监测数据进行分析的数据分析模块；

与数据分析模块有线连接，用于对监测数据进行进一步处理的数据处理模块；

与单片机有线连接，用于对时间进行记录的计时模块；

与单片机有线连接，用于消除干扰杂讯的滤波器；

与单片机有线连接，用于将数据进行导出的数据导出模块；

与单片机有线连接，用于对监测信号进行显示和操作的操作显示屏；

与单片机有线连接，用于接收和发送无线网络信号的无线射频收发模块；所述无线射频收发模块设置有安全接入单元，所述安全接入单元的安全接入的方法设置两种交互模式：单播模式和组播模式，单播模式和组播模式分别设有网络协调器发起握手和传感器节点发起握手两种发起方式，网络协调器和传感器节点进行增强型4-Way Handshake，得到最新的成对临时密钥，用于信息加密及认证；单播模式是无线体域网中单个传感器节点接入网络协调器；组播模式是无线体域网中多个传感器节点接入网络协调器，以实现心率、血

压、呼吸监测参数、脑电波、疼痛、骨骼肌松弛程度突然变化时，即某个或某些传感器节点的测量指标超过相应指标限制时，相应传感器节点主动发起握手过程；远距离接入时，采用多跳方式，并采用传感器节点与网络协调器之间的距离门限值，控制单跳和多跳方式之间的切换；

所述组播模式包括：主动发起方式和被动发起模式；组播模式是无线体域网中多个传感器节点接入网络协调器；

主动发起方式，是网络协调器发起握手具体实现步骤如下：

步骤一，网络协调器组播经过密钥k_i加密的信息Msg1，启动改进型4-Way Handshake；

步骤二，等待接入的第i个传感器节点接收到组播信息Msg1，根据得到信息的前缀地址从维护的密钥列表里找到相应的密钥k_i，从而得到BNC生成的随机数及ID_i，验证身份ID_i，若验证成功，则生成随机数Nonce_i，并将经过密钥k_i加密的信息Msg2发送给网络协调器，否则丢弃该信息；

步骤三，网络协调器收到Msg2，验证BNC生成的随机数，若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥PTK_i，然后在AES-CBC-MAC模式下使用密钥k_i计算出{Nonce_i，ID_i}的消息完整性认证码KMACi，并将KMACi作为Msg3发送给传感器节点BN_i，否则丢弃该信息；

步骤四，第i个传感器节点BN_i收到Msg3之后，在AES-CBC-MAC模式下使用自己的密钥k_i根据相应信息计算出KMACi'，将接收到的KMACi与计算出的KMACi'进行比对，若一致，则传感器节点BN_i用PRF函数结合随机数生成并装入成对临时密钥PTK_i，改进型的4-Way Handshake完成，否则丢弃该信息；

组播模式下被动发起方式的具体实现步骤如下：

步骤一，N个传感器节点给网络协调器发送经过密钥k_i加密的信息Msg1，启动改进型4-Way Handshake；

步骤二，网络协调器接收到信息Msg1，根据得到信息的前缀地址从维护的密钥列表里找到相应的密钥k_i，从而得到Nonce_i及ID_i，并验证身份ID_i，若验证成功，则生成随机数Nonce_BNC，并将经过密钥k_i加密的信息Msg2发送给等待接入的第i个传感器节点，否则丢弃该信息；

步骤三，传感器节点_i收到Msg2，验证Nonce_i，若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥PTK_i，然后在AES-CBC-MAC模式下使用密钥k_i计算出{Nonce_i，ID_i}的消息完整性认证码KMACi，并将KMACi作为Msg3发送给传感器节点BN_i，否则丢弃该信息；

步骤四，网络协调器收到Msg3之后，验证BNC生成的随机数，如验证成功，则用PRF函数结合随机数生成并装入成对临时密钥PTK_i，然后在AES-CBC-MAC模式下使用密钥k_i根据相应信息计算出KMACi'，将接收到的KMACi与计算出的KMACi'进行比对，若一致，则网络协调器用PRF函数结合随机数生成并装入成对临时密钥PTK_i，改进型的4-Way Handshake完成，否则丢弃该信息；

与无线射频收发模块通过GPRS无线网络无线连接，用于进行数据传输与交换的云服务器；

所述操作显示屏具体为多点触控的电容式触摸屏；

所述操作显示屏上安装有语音播报装置，语音播报装置通过数据线与单片机相连接；

所述操作显示屏上安装有打印装置，打印装置均通过数据线与单片机相连接；

所述操作显示屏上安装有多个指示灯，指示灯通过数据线与单片机相连接。

2.如权利要求1所述的麻醉和意识深度监测系统，其特征在于，所述安全接入的方法握手过程发送的所有信息封装在802.15.6帧中，由帧标识来区分握手过程中发送的信息，网络协调器和传感器节点共享密钥成对主密钥，网络协调器拥有可信任传感器节点的地址维护密钥列表{k_1,k_2...k_N}、指标门限列表{w_1,w_2...w_N}以及距离门限列表{d_1,d_2...d_N}；传感器节点拥有自己的密钥k_i加密握手过程的三个信息、指标门限值w_i、距离门限制d_i，密钥k_i是由成对主密钥及传感器节点的地址ID结合生成的，接下来网络协调器和传感器节点进行增强型4-WayHandshake，得到最新的成对临时密钥，用于以后的信息加密及认证；

单播模式具体包括：主动发起方式和被动发起方式；单播模式是无线体域网中单个传感器节点接入网络协调器。

3.如权利要求2所述的麻醉和意识深度监测系统，其特征在于，所述主动发起方式，是网络协调器发起握手具体实现步骤如下：

步骤一，网络协调器发送经过密钥k_A加密的信息Msg1给传感器节点A，Msg1中包括用于产生成对临时密钥的随机数Nonce_BNC，及传感器节点身份ID_A；

步骤二，BN_A生成的随机数收到Msg1之后，验证身份ID_A；若验证成功，则生成BN_A生成的随机数，并将经过密钥k_A加密的信息Msg2发送给网络协调器，否则丢弃该信息；

步骤三，网络协调器收到Msg2之后，验证BNC生成的随机数；若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥，然后在AES-CBC-MAC模式下使用密钥k_A计算出{BN_A生成的随机数，ID_A}的消息完整性认证码KMAC，并将KMAC作为Msg3发送给传感器节点A，否则丢弃该信息；

步骤四，传感器节点A收到Msg3之后，在AES-CBC-MAC模式下使用自己的密钥k_A根据相应信息计算出KMAC'，将接收到的KMAC与计算出的KMAC'进行比对，若一致，则传感器节点A用PRF函数结合随机数生成并装入成对临时密钥，改进型的4-Way Handshake完成，否则丢弃该信息；

某传感器节点指标超过门限值w_i时，被动发起方式，是相应传感器节点发起握手具体实现步骤如下：

步骤一，传感器节点A发送经过密钥k_A加密的信息Msg1给网络协调器，Msg1中包括用于产生成对临时密钥的随机数Nonce_BNC，及传感器节点身份ID_A；

步骤二，网络协调器收到Msg1之后，验证身份ID_A；若验证成功，则生成随机数Nonce_BNC，并将经过密钥k_A加密的信息Msg2发送给传感器节点A，否则丢弃该信息；

步骤三，传感器节点A收到Msg2之后，验证传感器节点A生成的随机数Nonce_A；若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥，然后在AES-CBC-MAC模式下使用密钥k_A计算出{BN_A生成的随机数，ID_A}的消息完整性认证码KMAC，并将KMAC作为Msg3发送给网络协调器，否则丢弃该信息；

步骤四，网络协调器收到Msg3之后，在AES-CBC-MAC模式下使用密钥k_A根据相应信息计算出KMAC'，将接收到的KMAC与计算出的KMAC'进行比对，若一致，则网络协调器用PRF函数结合随机数生成并装入成对临时密钥，改进型的4-Way Handshake完成，否则丢弃该信息。

一种麻醉和意识深度监测系统

技术领域

[0001] 本发明属于医疗设备技术领域，尤其涉及一种麻醉和意识深度监测系统。

背景技术

[0002] 麻醉在外科手术中的作用极为重要，合理的麻醉可以在患者无痛觉的情况下进行手术治疗，使患者免受痛苦，同时方便医生正常工作。但是麻醉不当，不但不能消除患者的痛苦，还会带来一系列其他的问题。麻醉过深，有损患者的神经系统功能，并可能留下神经后遗症甚至威胁生命；麻醉过浅，则不能抑制伤害性刺激，使病人疼痛不适或本能体动导致手术难以进行或出现意外，还可能引起术中知晓，造成病人留存有手术中记忆，从而可能引起严重的精神或睡眠障碍。

[0003] 随着新的肌松药和镇痛剂等药剂的联合应用，全身麻醉的麻醉深度、意识状态常被掩盖或难以识别，判断并控制合适的麻醉深度已成为临床迫切需要解决的问题，因此出现一些麻醉和意识深度监测装置，但是还存在以下缺点：一是监测手段分散，相对独立，导致数据同步性差，不能反应点时间的数据相关性，也无法整体反映患者的麻醉深度和意识状态；二是受到外界和内部电力元件的干扰，导致监测参数不精确，影响麻醉深度判断的准确性；三是监测数据存储在本地，导致数据丢失的可能性大，影响患者再次手术中的数据利用和相关参考价值，导致工作效率大大降低。

发明内容

[0004] 本发明为解决现有的监测不精准，容易受到干扰和数据存储不安全的技术问题而提供一种麻醉和意识深度监测系统。

[0005] 本发明为解决公知技术中存在的技术问题所采取的技术方案是：

[0006] 该麻醉和意识深度监测系统包括：

[0007] 用于对人体心率进行监测的心率传感器；

[0008] 用于对人体血压进行监测的血压传感器；

[0009] 用于对人体呼吸频率、吸入氧浓度、呼气末二氧化碳、吸入麻醉气体进行监测的呼吸气体监测传感器；

[0010] 用于对人体脑电波进行监测的脑电波监测传感器；

[0011] 用于对人体疼痛刺激进行监测的镇痛/伤害性刺激指数传感器；

[0012] 用于对人体骨骼肌松弛程度进行监测的肌松监测仪；

[0013] 分别与心率传感器、血压传感器、呼吸气体监测传感器、脑电波监测传感器、镇痛/伤害性刺激指数传感器、肌松监测仪有线连接，用于对监测信号进行分析和处理的单片机；

[0014] 与单片机通过输入模块有线连接，用于输入患者基本信息的输入键盘；

[0015] 与单片机有线连接，用于对监测数据进行保存的存储器；

[0016] 与单片机有线连接，用于对监测数据进行比对、采样和查询的RAM存储器和MRAM存储器；

[0017] 与单片机有线连接，用于提供电源的电源模块；

[0018] 与单片机有线连接，用于对监测数据进行分析的数据分析模块；

[0019] 与数据分析模块有线连接，用于对监测数据进行进一步处理的数据处理模块；

[0020] 与单片机有线连接，用于对时间进行记录的计时模块；

[0021] 与单片机有线连接，用于消除干扰杂讯的滤波器；

[0022] 与单片机有线连接，用于将数据进行导出的数据导出模块；

[0023] 与单片机有线连接，用于对监测信号进行显示和操作的操作显示屏；

[0024] 与单片机有线连接，用于接收和发送无线网络信号的无线射频收发模块；

[0025] 与无线射频收发模块通过GPRS无线网络无线连接，用于进行数据传输与交换的云服务器。

[0026] 进一步，所述操作显示屏具体为多点触控的电容式触摸屏。

[0027] 进一步，所述操作显示屏上安装有语音播报装置，语音播报装置通过数据线与单片机相连接。

[0028] 进一步，所述操作显示屏上安装有打印装置，打印装置均通过数据线与单片机相连接。

[0029] 进一步，所述操作显示屏上安装有多个指示灯，指示灯通过数据线与单片机相连接。

[0030] 进一步，所述单片机设置有数据压缩单元，所述数据压缩单元的数据压缩方法的步骤为：

[0031] 步骤一、在编码时，首先根据$E1_{n+1}=E1_n+d_{n+1}$式计算出E1值，再根据$\Delta d'_n=\frac{4\times d_n}{n}-\frac{6\times E1_n}{n(n+1)}$和$DFR_n=\Delta d_n-\lfloor\Delta d'_n\rfloor=\varepsilon$式计算出拟合残差，计算这两步时，均需要对结果进行越限判断，判断E1是否越限是为了避免其超过传感器数据总线上限而造成溢出；判断残差是否越限是为了实现分段拟合；

[0032] 步骤二、当一段输入数据的拟合残差全部计算完后，构造出$\{d_n,E1_n,DFR_3,DFR_4,\cdots DFR_n\}$所示的数据包，通过S-Huffman编码方法对其进行熵编码，然后发送出去，接收端解码时，先将接收到的一组数据解码，还原出$\{d_n,E1_n,DFR_3,DFR_4,\cdots DFR_n\}$式所示的数据包，然后根据$d_{n-1}=d_n-\lfloor\Delta d'_n\rfloor-DFR_n=d_n-\left\lfloor\frac{4\times d_n}{n}-\frac{6\times E1_n}{n(n+1)}\right\rfloor-DFR_n$式计算并还原出所有原始数据。

[0033] 进一步，所述无线射频收发模块设置有安全接入单元，所述安全接入单元的安全接入的方法设置两种交互模式：单播模式和组播模式，单播模式和组播模式分别设有网络协调器发起握手和传感器节点发起握手两种发起方式，网络协调器和传感器节点进行增强型4-Way Handshake，得到最新的成对临时密钥，用于信息加密及认证；单播模式是无线体域网中单个传感器节点接入网络协调器；组播模式是无线体域网中多个传感器节点接入网络协调器，以实现某个或某些传感器节点的测量指标超过相应指标限制时，相应传感器节点主动发起握手过程；远距离接入时，采用多跳方式，并采用传感器节点与网络协调器之间的距离门限值，控制单跳和多跳方式之间的切换。

[0034] 进一步，所述安全接入的方法握手过程发送的所有信息封装在802.15.6帧中，由

帧标识来区分握手过程中发送的信息，网络协调器和传感器节点共享密钥成对主密钥，网络协调器拥有可信任传感器节点的地址维护密钥列表{k_1,k_2...k_N}、指标门限列表{w_1,w_2…w_N}以及距离门限列表{d_1,d_2...d_N}；传感器节点拥有自己的密钥k_i加密握手过程的三个信息、指标门限值w_i、距离门限制d_i，密钥k_i是由成对主密钥及传感器节点的地址ID结合生成的，接下来网络协调器和传感器节点进行增强型4-Way Handshake，得到最新的成对临时密钥，用于以后的信息加密及认证；

[0035] 单播模式具体包括：主动发起方式和被动发起方式；单播模式是无线体域网中单个传感器节点接入网络协调器。

[0036] 进一步，所述主动发起方式，是网络协调器发起握手具体实现步骤如下：

[0037] 步骤一，网络协调器发送经过密钥k_A加密的信息Msg1给传感器节点A，Msg1中包括用于产生成对临时密钥的随机数Nonce_BNC，及传感器节点身份ID_A；

[0038] 步骤二，BN_A生成的随机数收到Msg1之后，验证身份ID_A；若验证成功，则生成BN_A生成的随机数，并将经过密钥k_A加密的信息Msg2发送给网络协调器，否则丢弃该信息；

[0039] 步骤三，网络协调器收到Msg2之后，验证BNC生成的随机数；若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥，然后在AES-CBC-MAC模式下使用密钥k_A计算出{BN_A生成的随机数，ID_A}的消息完整性认证码KMAC，并将KMAC作为Msg3发送给传感器节点A，否则丢弃该信息；

[0040] 步骤四，传感器节点A收到Msg3之后，在AES-CBC-MAC模式下使用自己的密钥k_A根据相应信息计算出KMAC'，将接收到的KMAC与计算出的KMAC'进行比对，若一致，则传感器节点A用PRF函数结合随机数生成并装入成对临时密钥，改进型的4-Way Handshake完成，否则丢弃该信息；

[0041] 某传感器节点指标超过门限值w_i时，被动发起方式，是相应传感器节点发起握手具体实现步骤如下：

[0042] 步骤一，传感器节点A发送经过密钥k_A加密的信息Msg1给网络协调器，Msg1中包括用于产生成对临时密钥的随机数Nonce_BNC，及传感器节点身份ID_A；

[0043] 步骤二，网络协调器收到Msg1之后，验证身份ID_A；若验证成功，则生成随机数Nonce_BNC，并将经过密钥k_A加密的信息Msg2发送给传感器节点A，否则丢弃该信息；

[0044] 步骤三，传感器节点A收到Msg2之后，验证传感器节点A生成的随机数Nonce_A；若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥，然后在AES-CBC-MAC模式下使用密钥k_A计算出{BN_A生成的随机数，ID_A}的消息完整性认证码KMAC，并将KMAC作为Msg3发送给网络协调器，否则丢弃该信息；

[0045] 步骤四，网络协调器收到Msg3之后，在AES-CBC-MAC模式下使用密钥k_A根据相应信息计算出KMAC'，将接收到的KMAC与计算出的KMAC'进行比对，若一致，则网络协调器用PRF函数结合随机数生成并装入成对临时密钥，改进型的4-Way Handshake完成，否则丢弃该信息。

[0046] 进一步，所述组播模式包括：主动发起方式和被动发起模式；组播模式是无线体域网中多个传感器节点接入网络协调器；

[0047] 主动发起方式，是网络协调器发起握手具体实现步骤如下：

[0048] 步骤一，网络协调器组播经过密钥k_i加密的信息Msg1，启动改进型4-Way

Handshake；

[0049] 步骤二，等待接入的第i个传感器节点接收到组播信息Msg1，根据得到信息的前缀地址从维护的密钥列表里找到相应的密钥k_i，从而得到BNC生成的随机数及ID_i，验证身份ID_i，若验证成功，则生成随机数Nonce_i，并将经过密钥k_i加密的信息Msg2发送给网络协调器，否则丢弃该信息；

[0050] 步骤三，网络协调器收到Msg2，验证BNC生成的随机数，若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥PTK_i，然后在AES-CBC-MAC模式下使用密钥k_i计算出{Nonce_i，ID_i}的消息完整性认证码KMACi，并将KMACi作为Msg3发送给传感器节点BN_i，否则丢弃该信息；

[0051] 步骤四，第i个传感器节点BN_i收到Msg3之后，在AES-CBC-MAC模式下使用自己的密钥k_i根据相应信息计算出KMACi'，将接收到的KMACi与计算出的KMACi'进行比对，若一致，则传感器节点BN_i用PRF函数结合随机数生成并装入成对临时密钥PTK_i，改进型的4-Way Handshake完成，否则丢弃该信息；

[0052] 组播模式下被动发起方式的具体实现步骤如下：

[0053] 步骤一，N个传感器节点给网络协调器发送经过密钥k_i加密的信息Msg1，启动改进型4-Way Handshake；

[0054] 步骤二，网络协调器接收到信息Msg1，根据得到信息的前缀地址从维护的密钥列表里找到相应的密钥k_i，从而得到Nonce_i及ID_i，并验证身份ID_i，若验证成功，则生成随机数Nonce_BNC，并将经过密钥k_i加密的信息Msg2发送给等待接入的第i个传感器节点，否则丢弃该信息；

[0055] 步骤三，传感器节点_i收到Msg2，验证Nonce_i，若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥PTK_i，然后在AES-CBC-MAC模式下使用密钥k_i计算出{Nonce_i，ID_i}的消息完整性认证码KMACi，并将KMACi作为Msg3发送给传感器节点BN_i，否则丢弃该信息；

[0056] 步骤四，网络协调器收到Msg3之后，验证BNC生成的随机数，如验证成功，则用PRF函数结合随机数生成并装入成对临时密钥PTK_i，然后在AES-CBC-MAC模式下使用密钥k_i根据相应信息计算出KMACi'，将接收到的KMACi与计算出的KMACi'进行比对，若一致，则网络协调器用PRF函数结合随机数生成并装入成对临时密钥PTK_i，改进型的4-Way Handshake完成，否则丢弃该信息。

[0057] 本发明具有的优点和积极效果是：该麻醉和意识深度监测系统监测全面，数据分析精准，存储安全；通过心率传感器、血压传感器、呼吸气体监测传感器、脑电波监测传感器、镇痛/伤害性刺激指数传感器、肌松监测仪对人体麻醉和意识深度进行全面监测，并发送到单片机中，通过滤波器消除外界和内部的干扰杂讯，确保监测数据精准化，各个数据时间相关性强，数据更符合临床实际情况，利用单片机通过无线射频收发模块将监测数据存储到云服务器中，保证数据的存储安全和提取使用，通过RAM存储器、MRAM存储器和云服务器将监测数据进行比对、采样查询和存储，方便医生判断人体麻醉和意识深度的程度，更好地进行控制和手术。

附图说明

[0058] 图1是本发明实施例提供的麻醉和意识深度监测系统的原理框图；

[0059] 图中：1、心率传感器；2、血压传感器；3、呼吸气体监测传感器；4、脑电波监测传感器；5、镇痛/伤害性刺激指数传感器；6、肌松监测仪；7、输入模块；8、输入键盘；9、存储器；10、RAM存储器；11、MRAM存储器；12、电源模块；13、数据分析模块；14、数据处理模块；15、计时模块；16、滤波器；17、数据导出模块；18、操作显示屏；19、无线射频收发模块；20、云服务器；21、语音播报装置；22、打印装置；23、指示灯；24、单片机。

具体实施方式

[0060] 为能进一步了解本发明的发明内容、特点及功效，兹例举以下实施例，并配合附图详细说明如下。

[0061] 下面结合图1对本发明的结构作详细的描述。

[0062] 该麻醉和意识深度监测系统包括：

[0063] 用于对人体心率进行监测的心率传感器1；

[0064] 用于对人体血压进行监测的血压传感器2；

[0065] 用于对人体呼吸频率、吸入氧浓度、呼气末二氧化碳、吸入麻醉气体进行监测的呼吸气体监测传感器3；

[0066] 用于对人体脑电波进行监测的脑电波监测传感器4；

[0067] 用于疼痛刺激监测的镇痛/伤害性刺激指数传感器5；

[0068] 用于对人体骨骼肌松弛程度进行监测的肌松监测仪6；

[0069] 分别与心率传感器1、血压传感器2、呼吸气体监测传感器3、脑电波监测传感器4、镇痛/伤害性刺激指数传感器5、肌松监测仪6有线连接，用于对监测信号进行分析和处理的单片机24；

[0070] 与单片机24通过输入模块7有线连接，用于输入患者基本信息的输入键盘8；

[0071] 与单片机24有线连接，用于对监测数据进行保存的存储器9；

[0072] 与单片机24有线连接，用于对监测数据进行比对、采样和查询的RAM存储器10和MRAM存储器11；

[0073] 与单片机24有线连接，用于提供电源的电源模块12；

[0074] 与单片机24有线连接，用于对监测数据进行分析的数据分析模块13；

[0075] 与数据分析模块13有线连接，用于对监测数据进行进一步处理的数据处理模块14；

[0076] 与单片机24有线连接，用于对时间进行记录的计时模块15；

[0077] 与单片机24有线连接，用于消除干扰杂讯的滤波器16；

[0078] 与单片机24有线连接，用于将数据进行导出的数据导出模块17；

[0079] 与单片机24有线连接，用于对监测信号进行显示和操作的操作显示屏18；

[0080] 与单片机24有线连接，用于接收和发送无线网络信号的无线射频收发模块19；

[0081] 与无线射频收发模块19通过GPRS无线网络无线连接，用于进行数据传输与交换的云服务器20。

[0082] 进一步，所述操作显示屏18具体为多点触控的电容式触摸屏。

[0083] 进一步，所述操作显示屏18上安装有语音播报装置21，语音播报装置21通过数据

线与单片机24相连接。

[0084] 进一步，所述操作显示屏18上安装有打印装置22，打印装置22均通过数据线与单片机24相连接。

[0085] 进一步，所述操作显示屏18上安装有多个指示灯23，指示灯23通过数据线与单片机24相连接。

[0086] 进一步，所述单片机设置有数据压缩单元，所述数据压缩单元的数据压缩方法的步骤为：

[0087] 步骤一、在编码时，首先根据$E1_{n+1}=E1_n+d_{n+1}$式计算出E1值，再根据$\Delta d'_n=\frac{4\times d_n}{n}-\frac{6\times E1_n}{n(n+1)}$和$DFR_n=\Delta d_n-\lfloor\Delta d'_n\rfloor=\varepsilon$式计算出拟合残差，计算这两步时，均需要对结果进行越限判断，判断E1是否越限是为了避免其超过传感器数据总线上限而造成溢出；判断残差是否越限是为了实现分段拟合；

[0088] 步骤二、当一段输入数据的拟合残差全部计算完后，构造出$\{d_n,E1_n,DFR_3,DFR_4,\cdots DFR_n\}$所示的数据包，通过S-Huffman编码方法对其进行熵编码，然后发送出去，接收端解码时，先将接收到的一组数据解码，还原出$\{d_n,E1_n,DFR_3,DFR_4,\cdots DFR_n\}$式所示的数据包，然后根据$d_{n-1}=d_n-\lfloor\Delta d'_n\rfloor-DFR_n=d_n-\left\lfloor\frac{4\times d_n}{n}-\frac{6\times E1_n}{n(n+1)}\right\rfloor-DFR_n$式计算并还原出所有原始数据。

[0089] 进一步，所述无线射频收发模块设置有安全接入单元，所述安全接入单元的安全接入的方法设置两种交互模式：单播模式和组播模式，单播模式和组播模式分别设有网络协调器发起握手和传感器节点发起握手两种发起方式，网络协调器和传感器节点进行增强型4-Way Handshake，得到最新的成对临时密钥，用于信息加密及认证；单播模式是无线体域网中单个传感器节点接入网络协调器；组播模式是无线体域网中多个传感器节点接入网络协调器，以实现某个或某些传感器节点的测量指标超过相应指标限制时，相应传感器节点主动发起握手过程；远距离接入时，采用多跳方式，并采用传感器节点与网络协调器之间的距离门限值，控制单跳和多跳方式之间的切换。

[0090] 进一步，所述安全接入的方法握手过程发送的所有信息封装在802.15.6帧中，由帧标识来区分握手过程中发送的信息，网络协调器和传感器节点共享密钥成对主密钥，网络协调器拥有可信任传感器节点的地址维护密钥列表$\{k_1,k_2...k_N\}$、指标门限列表$\{w_1,w_2\cdots w_N\}$以及距离门限列表$\{d_1,d_2...d_N\}$；传感器节点拥有自己的密钥k_i加密握手过程的三个信息、指标门限值w_i、距离门限制d_i，密钥k_i是由成对主密钥及传感器节点的地址ID结合生成的，接下来网络协调器和传感器节点进行增强型4-Way Handshake，得到最新的成对临时密钥，用于以后的信息加密及认证；

[0091] 单播模式具体包括：主动发起方式和被动发起方式；单播模式是无线体域网中单个传感器节点接入网络协调器。

[0092] 进一步，所述主动发起方式，是网络协调器发起握手具体实现步骤如下：

[0093] 步骤一，网络协调器发送经过密钥k_A加密的信息Msg1给传感器节点A，Msg1中包括用于产生成对临时密钥的随机数Nonce_BNC，及传感器节点身份ID_A；

[0094] 步骤二，BN_A生成的随机数收到Msg1之后，验证身份ID_A；若验证成功，则生成BN_

A生成的随机数，并将经过密钥k_A加密的信息Msg2发送给网络协调器，否则丢弃该信息；

[0095] 步骤三，网络协调器收到Msg2之后，验证BNC生成的随机数；若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥，然后在AES-CBC-MAC模式下使用密钥k_A计算出{BN_A生成的随机数，ID_A}的消息完整性认证码KMAC，并将KMAC作为Msg3发送给传感器节点A，否则丢弃该信息；

[0096] 步骤四，传感器节点A收到Msg3之后，在AES-CBC-MAC模式下使用自己的密钥k_A根据相应信息计算出KMAC'，将接收到的KMAC与计算出的KMAC'进行比对，若一致，则传感器节点A用PRF函数结合随机数生成并装入成对临时密钥，改进型的4-Way Handshake完成，否则丢弃该信息；

[0097] 某传感器节点指标超过门限值w_i时，被动发起方式，是相应传感器节点发起握手具体实现步骤如下：

[0098] 步骤一，传感器节点A发送经过密钥k_A加密的信息Msg1给网络协调器，Msg1中包括用于产生成对临时密钥的随机数Nonce_BNC，及传感器节点身份ID_A；

[0099] 步骤二，网络协调器收到Msg1之后，验证身份ID_A；若验证成功，则生成随机数Nonce_BNC，并将经过密钥k_A加密的信息Msg2发送给传感器节点A，否则丢弃该信息；

[0100] 步骤三，传感器节点A收到Msg2之后，验证传感器节点A生成的随机数Nonce_A；若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥，然后在AES-CBC-MAC模式下使用密钥k_A计算出{BN_A生成的随机数，ID_A}的消息完整性认证码KMAC，并将KMAC作为Msg3发送给网络协调器，否则丢弃该信息；

[0101] 步骤四，网络协调器收到Msg3之后，在AES-CBC-MAC模式下使用密钥k_A根据相应信息计算出KMAC'，将接收到的KMAC与计算出的KMAC'进行比对，若一致，则网络协调器用PRF函数结合随机数生成并装入成对临时密钥，改进型的4-Way Handshake完成，否则丢弃该信息。

[0102] 进一步，所述组播模式包括：主动发起方式和被动发起模式；组播模式是无线体域网中多个传感器节点接入网络协调器；

[0103] 主动发起方式，是网络协调器发起握手具体实现步骤如下：

[0104] 步骤一，网络协调器组播经过密钥k_i加密的信息Msg1，启动改进型4-Way Handshake；

[0105] 步骤二，等待接入的第i个传感器节点接收到组播信息Msg1，根据得到信息的前缀地址从维护的密钥列表里找到相应的密钥k_i，从而得到BNC生成的随机数及ID_i，验证身份ID_i，若验证成功，则生成随机数Nonce_i，并将经过密钥k_i加密的信息Msg2发送给网络协调器，否则丢弃该信息；

[0106] 步骤三，网络协调器收到Msg2，验证BNC生成的随机数，若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥PTK_i，然后在AES-CBC-MAC模式下使用密钥k_i计算出{Nonce_i，ID_i}的消息完整性认证码KMACi，并将KMACi作为Msg3发送给传感器节点BN_i，否则丢弃该信息；

[0107] 步骤四，第i个传感器节点BN_i收到Msg3之后，在AES-CBC-MAC模式下使用自己的密钥k_i根据相应信息计算出KMACi'，将接收到的KMACi与计算出的KMACi'进行比对，若一致，则传感器节点BN_i用PRF函数结合随机数生成并装入成对临时密钥PTK_i，改进型的4-

Way Handshake完成，否则丢弃该信息；

[0108] 组播模式下被动发起方式的具体实现步骤如下：

[0109] 步骤一，N个传感器节点给网络协调器发送经过密钥k_i加密的信息Msg1，启动改进型4-Way Handshake；

[0110] 步骤二，网络协调器接收到信息Msg1，根据得到信息的前缀地址从维护的密钥列表里找到相应的密钥k_i，从而得到Nonce_i及ID_i，并验证身份ID_i，若验证成功，则生成随机数Nonce_BNC，并将经过密钥k_i加密的信息Msg2发送给等待接入的第i个传感器节点，否则丢弃该信息；

[0111] 步骤三，传感器节点_i收到Msg2，验证Nonce_i，若验证成功，则用PRF函数结合随机数生成并装入成对临时密钥PTK_i，然后在AES-CBC-MAC模式下使用密钥k_i计算出{Nonce_i，ID_i}的消息完整性认证码KMACi，并将KMACi作为Msg3发送给传感器节点BN_i，否则丢弃该信息；

[0112] 步骤四，网络协调器收到Msg3之后，验证BNC生成的随机数，如验证成功，则用PRF函数结合随机数生成并装入成对临时密钥PTK_i，然后在AES-CBC-MAC模式下使用密钥k_i根据相应信息计算出KMACi'，将接收到的KMACi与计算出的KMACi'进行比对，若一致，则网络协调器用PRF函数结合随机数生成并装入成对临时密钥PTK_i，改进型的4-Way Handshake完成，否则丢弃该信息。

[0113] 下面结合工作原理对本发明的结构作进一步的描述。

[0114] 通过心率传感器1、血压传感器2、呼吸气体监测传感器3、脑电波监测传感器4、镇痛/伤害性刺激指数传感器5、肌松监测仪6对人体麻醉和意识深度进行全面监测，并发送到单片机24中，通过滤波器16消除外界和内部的干扰杂讯，确保监测数据精准化，利用单片机24通过无线射频收发模块19将监测数据存储到云服务器20中，保证数据的存储安全和提取使用，通过RAM存储器10、MRAM存储器11和云服务器20将监测数据进行比对、采样、查询和存储，方便医生判断人体麻醉和意识深度的程度，更好地进行控制和手术，利用输入键盘8将患者的基本信息通过输入模块7输入到单片机24中，通过单片机24将监测数据和基本信息通过数据分析模块13和数据处理模块14进行分析处理，判断患者的麻醉和意识深度，电源模块12提供电源，利用数据导出模块17可将监测数据进行导出，通过操作显示屏18显示出来，也可通过语音播报装置21播放出来，亦可通过打印装置22打印出来进行保存，计时模块15用于计时。

[0115] 以上所述仅是对本发明的较佳实施例而已，并非对本发明作任何形式上的限制，凡是依据本发明的技术实质对以上实施例所做的任何简单修改，等同变化与修饰，均属于本发明技术方案的范围内。

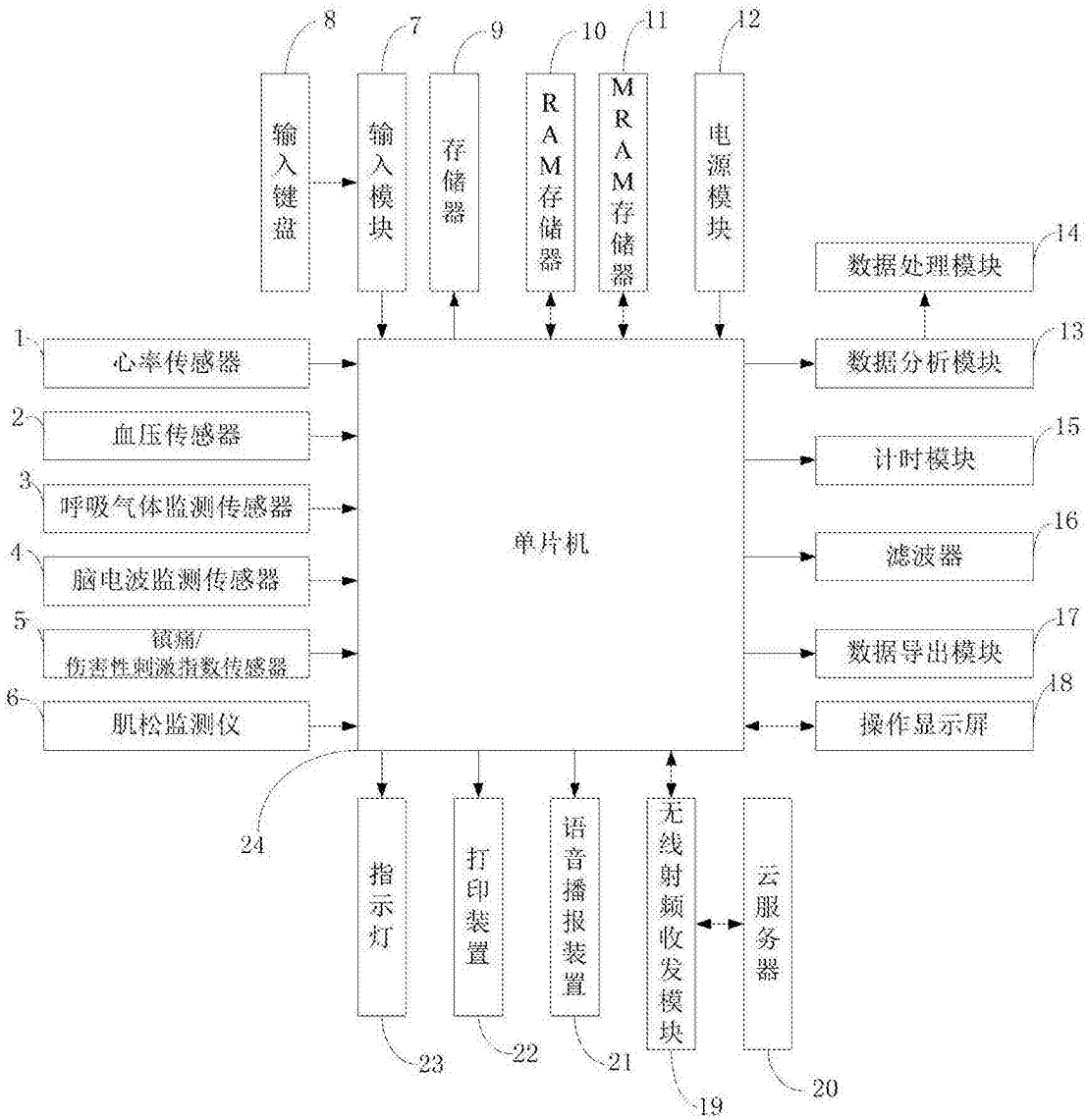

8
7
9
10
11
12
输入键盘
输入模块
存储器
RAM存储器
MRAM存储器
电源模块
14
数据处理模块
1
心率传感器
13
数据分析模块
2
血压传感器
15
计时模块
3
呼吸气体监测传感器
单片机
16
滤波器
4
脑电波监测传感器
5
颌痛/
伤害性刺激指数传感器
17
数据导出模块
6
肌松监测仪
18
操作显示屏
24
指示灯
打印装置
语音播报装置
无线射频收发模块
云服务器
23
22
21
19
20

图1

专利名称(译)	一种麻醉和意识深度监测系统		
公开(公告)号	CN106943119A	公开(公告)日	2017-07-14
申请号	CN201710139673.9	申请日	2017-03-09
[标]申请(专利权)人(译)	北京大学第三医院		
申请(专利权)人(译)	北京大学第三医院		
当前申请(专利权)人(译)	北京大学第三医院		
[标]发明人	倪诚 刘伟平 王军		
发明人	倪诚 刘伟平 王军		
IPC分类号	A61B5/00 A61B5/0205 A61B5/0476 A61B5/08 A61B5/083 H04L29/08		
CPC分类号	A61B5/4821 A61B5/0048 A61B5/0205 A61B5/021 A61B5/024 A61B5/0476 A61B5/08 A61B5/0816 A61B5/083 A61B5/0836 A61B5/4519 A61B5/72 H04L67/10 H04L67/1095 H04L67/12		
代理人(译)	姜彦		
外部链接	Espacenet SIPO		

摘要(译)

本发明涉及一种麻醉和意识深度监测系统，包括分别与心率传感器、血压传感器、呼吸气体监测传感器、脑电波监测传感器、镇痛/伤害性刺激指数传感器、肌松监测仪有线连接，用于对监测信号进行分析和处理的单片机；用于对监测数据进行分析的数据分析模块；用于对监测数据进行进一步处理的数据处理模块；用于消除干扰杂讯的滤波器；用于对监测信号进行显示和操作的操作显示屏；用于接收和发送无线网络信号的无线射频收发模块；与无线射频收发模块通过GPRS无线网络无线连接，用于进行数据传输与交换的云服务器。该麻醉和意识深度监测系统监测全面，数据分析精准，存储安全。