



(12)发明专利申请

(10)申请公布号 CN 107347020 A

(43)申请公布日 2017. 11. 14

(21)申请号 201710497983.8

G10L 25/60(2013.01)

(22)申请日 2017.06.27

(71)申请人 周显春

地址 572000 海南省三亚市学院路123号高知园1栋B单元702

(72)发明人 周显春

(74)专利代理机构 北京科亿知识产权代理事务所(普通合伙) 11350

代理人 汤东风

(51) Int. Cl.

H04L 12/24(2006.01)

H04L 12/26(2006.01)

H04L 29/06(2006.01)

H04W 24/02(2009.01)

H04W 24/08(2009.01)

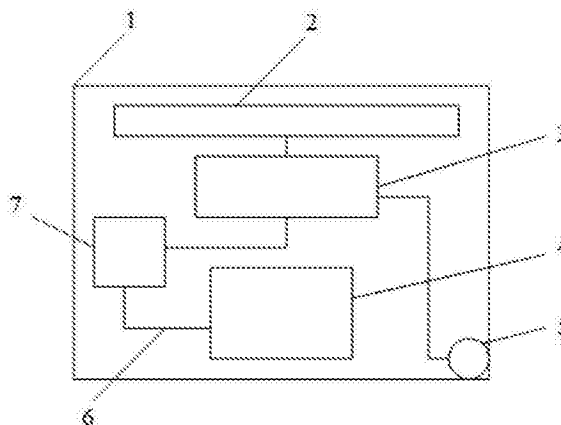
权利要求书2页 说明书7页 附图2页

(54)发明名称

一种分布式系统的智能网络安全验证控制系统

(57)摘要

本发明属于网络安全验证技术领域,公开了一种分布式系统的智能网络安全验证控制系统,设置有:网络设备;所述网络设备上端置有外设接口;所述外设接口通过导线连接安全验证装置;所述安全验证装置通过导线连接存储器;所述安全验证装置通过导线连接警示灯;所述存储器通过导线连接处理器。本发明为分布式系统的智能网络安全验证控制系统,使用该网络设备,若网络出现未知连接问题,能够通过警示灯显示该问题是安全验证问题,从而得知该数据属于未授权或病毒程度数据;更加容易排查出网络问题,处理方便,效果明显,安全机制更加完善。



1. 一种分布式系统的智能网络安全验证控制系统,其特征在于,所述分布式系统的智能网络安全验证控制系统设置有:

网络设备;

所述网络设备上端置有外设接口;

所述外设接口通过导线连接安全验证装置;

所述安全验证装置通过导线连接存储器;

所述安全验证装置通过导线连接警示灯;

所述存储器通过导线连接处理器。

2. 如权利要求1所述的分布式系统的智能网络安全验证控制系统,其特征在于,所述外设接口的电路包括:

发出控制指令的主控单元;

与主控单元电连接,用于通讯类型的切换的通讯兼容接口单元;

与通讯兼容接口单元电连接,用于接收控制指令的受控设备单元;

所述的通讯兼容接口单元包括:

在实际使用中,根据控制设备和受控设备的通讯类型,选择恰当的通讯接口类型,保证设备间的通讯链路正常的通讯类型选择单元;

在RS232TTL通讯信号到其他任意一种通讯类型切换的通讯类型切换单元;

在实际使用时,根据不同的选择,实时显示当前完成切换的两种通讯类型的通讯类型显示单元。

3. 如权利要求1所述的分布式系统的智能网络安全验证控制系统,其特征在于,所述网络设备的语音优化方法包括:

步骤一、检测当前网络状态,并判断是否为移动通信网无线网络,否则自动退出运行;是则进入步骤二;

步骤二、采集移动通信网无线网络的信令数据和语音数据,并进行信令和语音的关联;

步骤三、分析采集到的数据,并根据语音质量的分析结果判断出无线网络的状况及问题,优化无线网络的语音质量;

步骤四、对基于语音业务的最佳优化率进行分析计算,获得移动通信网无线网络语音业务最佳优化率;

所述步骤二具体为采集2G网络的Aover IP信令和BSC的语音数据,并且通过A接口的Transport AoIP IP地址、Transport AoIP Port和BSC的RTP语音数据进行数据关联;

所述步骤二具体为采集3G网络的Iucs over IP信令和RNC的语音数据,IuPS的transportLayerAddress、bindingID和RNC的语音数据进行关联;

所述步骤二具体为采集LTE网络的S1接口的VoLTE的SIP信令和语音数据,并且通过SDP信息和语音数据关联;

所述步骤二具体为采集非IP承载的A、Abis接口和Iub接口的信令和语音数据。

4. 如权利要求1所述的分布式系统的智能网络安全验证控制系统,其特征在于,所述安全验证装置包括2条边界扫描链:第一边界扫描链和第二边界扫描链;所述第一边界扫描链包括:第一SN74BCT8244A器件、第二SN74BCT8244A器件、第三SN74BCT8244A器件、第四SN74BCT8244A器件、第一SN74BCT8374A器件、第二SN74BCT8374A器件及XC4003E-PC84器

件;所述第二边界扫描链包括:第三SN74BCT8374A器件及第五SN74BCT8244A器件;

所述第一边界扫描链的连接关系为:第一SN74BCT8244A器件、第二SN74BCT8244A器件、第一SN74BCT8374A器件、第二SN74BCT8374A器件、第三SN74BCT8244A器件、第四SN74BCT8244A器件及XC4003E-PC84器件依次连接;

所述第二边界扫描链的连接关系为:第三SN74BCT8374A器件连接第五SN74BCT8244A器件。

5.如权利要求1所述的分布式系统的智能网络安全验证控制系统,其特征在于,所述存储器设置有前端装置,前端装置设置有文字识别MCU,所述文字识别MCU与光学扫描仪通过USB接口连接,第一SDRAM存储器、第一Flash存储器通过数据线连接到文字识别MCU,第二SDRAM存储器、第二Flash存储器通过数据线连接到论文分析与处理MCU。

6.如权利要求1所述的分布式系统的智能网络安全验证控制系统,其特征在于,所述警示灯包括:

主控制器模块,用于接收时钟模块输出的时钟信号,同时接收输入的警报发放指令、产生和发放警报控制信号;

时钟模块,与主控制器模块连接,用于向主控制器模块提供时钟信号;

键盘输入模块,与主控制器模块连接,用于输入信息,由六个独立键盘组成表示六种不同的工作状态,分别是预先、空袭、解除、灾警、测试、终止;

LED指示灯模块,与主控制器模块连接,用于显示无线数传模块的数据和发射信号及对应的六个独立按键状态,当按下不同按键时,相应的指示灯会点亮,指示当前警报器的警报状态;

开关电源模块,包括12V开关电源和48V开关电源,12V开关电源连接无线数传模块,12V开关电源向无线数传模块供电及经过12V-5V电平转换产生5V电压向主控制器模块供电;48V开关电源连接继电器,48V开关电源经继电器开关电源向大功率数字功放模块供电;

报警控制模块,连接主控制器模块,用于接收主控制器模块输出的警报控制信号,并对警报控制信号进行传输的通信模块;

无线数传模块,与12V开关电源连接,用于将收发端的数据通过串口通信模块传输到主控制器模块进行数据分析处理,主控制器模块执行相应的指令给报警控制模块启动音频播放模块,将警报发送出去;

串口通信模块,与PC机、无线数传模块与主控制器模块连接,用于主控制器模块通过串口通信模块接到PC机或无线数传模块数据执行相应的警报指令;

音频播放模块,与报警控制模块连接,用于接收报警控制模块输出的警报控制信号,启动音频播放模块读取事先存入SD卡里的音频文件,并将音频信号输出的功率放大模块;

功率放大模块,与音频播放模块连接,包括有大功率数字功率放大模块和小功率功放模块两部分,大功率数字功率放大模块用于将音频播放模块输出的音频信号功率放大驱动外扬声器;小功率功放模块用于将音频播放模块输出的音频信号小功率的放大驱动内扬声器。

一种分布式系统的智能网络安全验证控制系统

技术领域

[0001] 本发明属于网络安全验证技术领域,尤其涉及一种分布式系统的智能网络安全验证控制系统。

背景技术

[0002] 目前,随着网络的普及,电脑几乎进入了所有的行业,扮演着举足轻重的角色。它已经成为当今社会得以正常运行不可缺少的工具,电脑在现代人的生活中占据着如此重要的地位,人们对电脑的依赖性不断的提高。然而,现在的网络设备连接复杂,安全问题不能得到保障,信息处理繁琐,网络出现问题查询过程艰难,安全验证机制简单。

[0003] 综上所述,现在的技术存在的问题是:现在的网络设备连接复杂,安全问题不能得到保障,信息处理繁琐,网络出现问题查询过程艰难,安全验证机制简单。

发明内容

[0004] 针对现有技术存在的问题,本发明提供了分布式系统的智能网络安全验证控制系统。

[0005] 本发明是这样实现的,分布式系统的智能网络安全验证控制系统设置有:

[0006] 网络设备;

[0007] 所述网络设备上端置有外设接口;

[0008] 所述外设接口通过导线连接安全验证装置;

[0009] 所述安全验证装置通过导线连接存储器;

[0010] 所述安全验证装置通过导线连接警示灯;

[0011] 所述存储器通过导线连接处理器。

[0012] 进一步,所述外设接口的电路包括:

[0013] 发出控制指令的主控单元;

[0014] 与主控单元电连接,用于通讯类型的切换的通讯兼容接口单元;

[0015] 与通讯兼容接口单元电连接,用于接收控制指令的受控设备单元;

[0016] 所述的通讯兼容接口单元包括:

[0017] 在实际使用中,根据控制设备和受控设备的通讯类型,选择恰当的通讯接口类型,保证设备间的通讯链路正常的通讯类型选择单元;

[0018] 在RS232TTL通讯信号到其他任何一种通讯类型切换的通讯类型切换单元;

[0019] 在实际使用时,根据不同的选择,实时显示当前完成切换的两种通讯类型的通讯类型显示单元。

[0020] 进一步,所述网络设备的语音优化方法包括:

[0021] 步骤一、检测当前网络状态,并判断是否为移动通信网无线网络,否则自动退出运行;是则进入步骤二;

[0022] 步骤二、采集移动通信网无线网络的信令数据和语音数据,并进行信令和语音的

关联；

[0023] 步骤三、分析采集到的数据，并根据语音质量的分析结果判断出无线网络 的状况及问题，优化无线网络的语音质量；

[0024] 步骤四、对基于语音业务的最佳优化率进行分析计算，获得移动通信网无 线网络语音业务最佳优化率；

[0025] 所述步骤二具体为采集2G网络的Aover IP信令和BSC的语音数据，并且 通过A接口的Transport AoIP IP地址、Transport AoIP Port和BSC的RTP语 音数据进行数据关联；

[0026] 所述步骤二具体为采集3G网络的Iucs over IP信令和RNC的语音数据， IuPS的transportLayerAddress、bindingID和RNC的语音数据进行关联；

[0027] 所述步骤二具体为采集LTE网络的S1接口的VoLTE的SIP信令和语音 数据，并且通过SDP信息和语音数据关联；

[0028] 所述步骤二具体为采集非IP承载的A、Abis接口和Iub接口的信令和语 音数据。

[0029] 进一步，所述安全验证装置包括2条边界扫描链：第一边界扫描链和第二 边界扫描链；所述第一边界扫描链包括：第一SN74BCT8244A器件、第二 SN74BCT8244A器件、第三SN74BCT8244A器件、第四SN74BCT8244A器件、 第一SN74BCT8374A器件、第二SN74BCT8374A器件及XC4003E-PC84器件； 所述第二边界扫描链包括：第三SN74BCT8374A器件及第五SN74BCT8244A器 件；

[0030] 所述第一边界扫描链的连接关系为：第一SN74BCT8244A器件、第二 SN74BCT8244A器件、第一SN74BCT8374A器件、第二SN74BCT8374A器件、 第三SN74BCT8244A器件、第四SN74BCT8244A器件及XC4003E-PC84器件 依次连接；

[0031] 所述第二边界扫描链的连接关系为：第三SN74BCT8374A器件连接第五 SN74BCT8244A器件。

[0032] 进一步，所述存储器设置有前端装置，前端装置设置有文字识别MCU，所 述文字识别MCU与光学扫描仪通过USB接口连接，第一SDRAM存储器、第 一Flash存储器通过数据线连接到文字识别MCU，第二SDRAM存储器、第二 Flash存储器通过数据线连接到论文分析与处理MCU。

[0033] 进一步，所述警示灯包括：

[0034] 主控制器模块，用于接收时钟模块输出的时钟信号，同时接收输入的警报 发放指令、产生和发放警报控制信号；

[0035] 时钟模块，与主控制器模块连接，用于向主控制器模块提供时钟信号；

[0036] 键盘输入模块，与主控制器模块连接，用于输入信息，由六个独立键盘组 成表示六种不同的工作状态，分别是预先、空袭、解除、灾警、测试、终止；

[0037] LED指示灯模块，与主控制器模块连接，用于显示无线数传模块的数据和 发射信号及对应的六个独立按键状态，当按下不同按键时，相应的指示灯会点 亮，指示当前警报器的警报状态；

[0038] 开关电源模块，包括12V开关电源和48V开关电源，12V开关电源连接无 线数传模块，12V开关电源向无线数传模块供电及经过12V-5V电平转换产生5V 电压向主控制器模块供电；48V开关电源连接继电器，48V开关电源经继电器 开关电源向大功率数字功放模块供 电；

[0039] 报警控制模块,连接主控制器模块,用于接收主控制器模块输出的警报控制信号,并对警报控制信号进行传输的通信模块;

[0040] 无线数传模块,与12V开关电源连接,用于将收发端的数据通过串口通信模块传输到主控制器模块进行数据分析处理,主控制器模块执行相应的指令给报警控制模块启动音频播放模块,将警报发送出去;

[0041] 串口通信模块,与PC机、无线数传模块与主控制器模块连接,用于主控制器模块通过串口通信模块接到PC机或无线数传模块数据执行相应的警报指令;

[0042] 音频播放模块,与报警控制模块连接,用于接收报警控制模块输出的警报控制信号,启动音频播放模块读取事先存入SD卡里的音频文件,并将音频信号输出的功率放大模块;

[0043] 功率放大模块,与音频播放模块连接,包括有大功率数字功率放大模块和小功率功放模块两部分,大功率数字功率放大模块用于将音频播放模块输出的音频信号功率放大驱动外扬声器;小功率功放模块用于将音频播放模块输出的音频信号小功率的放大驱动内扬声器。

[0044] 本发明具有的优点和积极技术效果是:使用该网络设备的过程中若网络出现未知连接问题,能够通过警示灯显示该问题是安全验证问题,从而得知该数据属于未授权或病毒程度数据;更加容易排查出网络问题,处理方便,效果明显,安全机制更加完善。

附图说明

[0045] 图1是本发明实施例提供的分布式系统的智能网络安全验证控制系统结构示意图;

[0046] 图2是本发明实施例提供的分布式系统的安全验证装置的结构示意图;

[0047] 图3是本发明实施例提供的网络设备的语音优化方法流程图。

[0048] 图中:1、网络设备;2、外设接口;3、安全验证装置;4、处理器;5、警示灯;6、导线;7、存储器。

具体实施方式

[0049] 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。

[0050] 下面结合附图对本发明的结构作详细的描述。

[0051] 该分布式系统的智能网络安全验证控制系统设置有:

[0052] 网络设备1;

[0053] 所述网络设备1上端置有外设接口2;

[0054] 所述外设接口2通过导线6连接安全验证装置3;

[0055] 所述安全验证装置3通过导线6连接存储器7;

[0056] 所述安全验证装置3通过导线6连接警示灯5;

[0057] 所述存储器7通过导线6连接处理器4。

[0058] 所述外设接口2的电路包括:

[0059] 发出控制指令的主控单元;

- [0060] 与主控单元电连接,用于通讯类型的切换的通讯兼容接口单元;
- [0061] 与通讯兼容接口单元电连接,用于接收控制指令的受控设备单元;
- [0062] 所述的通讯兼容接口单元包括:
- [0063] 在实际使用中,根据控制设备和受控设备的通讯类型,选择恰当的通讯接口类型,保证设备间的通讯链路正常的通讯类型选择单元;
- [0064] 在RS232TTL通讯信号到其他任意一种通讯类型切换的通讯类型切换单元;
- [0065] 在实际使用时,根据不同的选择,实时显示当前完成切换的两种通讯类型的通讯类型显示单元。
- [0066] 通讯类型选择单元使用机械开关,可实现3个IO信号的电平切换功能。该通讯类型选择单元选择拨码开关时,包括DIP-2型的拨码开关SW1/SW2;10K电阻R1/R3/R5;1K电阻R2/R4/R6。拨码开关SW1pin4接R1,R1另一端接GND;拨码开关SW1pin1接R2,R2另一端接3.3V。IO信号从SW1pin4与R1的连接处引出,当SW1-1导通时,IO信号为3V,符合TTL高电平标准;当SW1-1断开时,IO信号为0V,符合TTL低电平标准。同理,拨码开关SW1-2,拨码开关SW2-1也能产生可切换的高低电平。该单元选用单刀双掷开关时,包括型号为SS-12D00的开关SW4/SW5/SW6,1K电阻R7/R8/R10/R11/R13/R15。单刀双掷开关的Pin2接IO信号,Pin1接R7/R10/R13的一端,Pin1接R8/R13/R15的一端,R7/R10/R13的另一端接3.3V,R8/R13/R15的另一端接GND。当开关连接Pin2和Pin1时,IO信号为3.3V高电平,当开关连接Pin2和Pin3时,IO信号为0V低电平。
- [0067] MAXIM公司的MAX3160EAP芯片,就可以实现RS232 TTL信号与RS232/RS485/RS422信号的切换,同时满足了产品元器件较少,电路板尺寸较小的要求,同时可降低产品采购备货的难度。该单元包括U1芯片MAX3160EAP,电容C1/C2/C3/C4/C5,电容容值0.1uF,耐压50V。芯片的Pin2接滤波电容C1,Pin1与Pin3接电荷泵电容C4,Pin18与Pin19接电荷泵电容C5,Pin17接电容C3,Pin20接电容C1。芯片U1的Pin16为RS232 TTL端信号输入RS232_TTL_Rx,Pin8为RS232 TTL端信号输出RS232_TTL_Tx;当切换为RS422通讯信号时,RS422_A/B/Y/Z分别为Pin13/Pin14/Pin6/Pin5;当切换为RS485通讯信号时,RS485_A/B分别为Pin6/Pin5;当切换为RS232信号时,RS232_RX/TX分别为Pin13/Pin5。切换通讯信号类型为芯片引脚Pin11/Pin12/Pin15,其信号定义分别为RS485/RS232,HDPLX,DE485,这3个引脚电平通过通讯类型选择单元的设置。IO电平类型与通讯切换的关系,其中‘0’表示低电平,‘1’表示高电平。当信号RS485/RS232,HDPLX,DE485电平组合为‘011’时,通讯类型为RS232;电平组合为‘110’时
- [0068] 所述网络设备1的语音优化方法包括:
- [0069] S101、检测当前网络状态,并判断是否为移动通信网无线网络,否则自动退出运行;是则进入S102;
- [0070] S102、采集移动通信网无线网络的信令数据和语音数据,并进行信令和语音的关联;
- [0071] S103、分析采集到的数据,并根据语音质量的分析结果判断出无线网络的状况及问题,优化无线网络的语音质量;
- [0072] S104、对基于语音业务的最佳优化率进行分析计算,获得移动通信网无线网络语音业务最佳优化率;

[0073] 所述S102具体为采集2G网络的Aover IP信令和BSC的语音数据,并且通过A接口的Transport AoIP IP地址、Transport AoIP Port和BSC的RTP语音数据进行数据关联;

[0074] 所述S102具体为采集3G网络的Iucs over IP信令和RNC的语音数据, IuPS的transportLayerAddress、bindingID和RNC的语音数据进行关联;

[0075] 所述S102具体为采集LTE网络的S1接口的VoLTE的SIP信令和语音数据,并且通过SDP信息和语音数据关联;

[0076] 所述S102具体为采集非IP承载的A、Abis接口和Iub接口的信令和语音数据。

[0077] 不仅能够监测当前网络是否为移动通信网无线网络,并且采集该移动通信网无线网络语音通话的信令数据,而且采集语音通话的语音数据,根据语音通话的信令和语音进行关联,自动判断用户在通话过程中的语音包的特征特性和语音内容的特征特性,来分析语音质量,并且根据信令定位语音质量问题的小区、用户号码、终端类型、位置等信息,发现无线网络的问题,优化无线网络,提高语音质量。

[0078] 采用基于用户偏好的多播技术,提高了频谱资源利用率。考虑用户可能请求相同视频内容的情形,根据用户的位置信息和视频请求偏好信息进行用户聚类,处于相近位置的请求偏好也相近的用户可以划分为一个多播组,在一个多播组中采用多播技术分发相同的内容,多播组内所有用户共享一个载波资源,从而提高了系统的频率资源利用率。

[0079] 实现有源天线阵列波束对用户群的精确对准,提高了功率、频率资源利用率。通过有源阵列天线波束赋形技术,为每个多播组分配一个服务的有源天线波束。每个波束指向所服务的多播组,方向性很强,波束带宽较全向天线变窄,使得能量比较集中,信号强度增大,提高了功率的利用率。另外,由于波束主瓣较窄,副瓣迅速衰减,不同方向的波束间相互干扰很小,可以实现不同波束间的用户群的频率复用,提高了频率资源利用率。

[0080] 通过对用户群分簇,实现用户群间的频率复用,提高了频谱效率。在本发明中,根据用户群波束间的干扰对用户群进行分簇,将干扰较小的用户群分为一簇。同一簇中的用户群,由于相互间干扰较小,可以共享一个频率资源,从而实现用户群间的频率复用。

[0081] 提出了针对有源天线多播系统的载波分配算法,提高了用户性能和系统容量。采用有源天线的多播系统,有源阵列波束的方向性强,带宽较窄,能量较集中,使得用户的接受信号强度增大,同时提出了基于最大化吞吐量的载波分配算法,提高了用户的性能和系统容量。本发明采用单播唤醒关联包括全新的单播Wakeup帧以及单播唤醒关联机制;多播唤醒关联包括多播Wakeup帧,地址索引号对照表以及多播唤醒关联机制。本发明减少了在关联过程中帧的传输,节省了数据传输过程中的能量损耗。本发明实现了无线域网传感节点在被安全唤醒的同时开始关联,减少了从唤醒到MK建立所需传输的帧数,减小节点等待的时间;以IEEE802.15.6标准中公钥隐藏关联为例,在整个关联过程中需要传输4480比特的数据,需要5次的帧交换。在本发明中需要传输3112比特的数据,需要3次帧交换,与公钥隐藏关联相比节省数据传输达30%并减少了2帧数据的传输。

[0082] 所述安全验证装置3包括2条边界扫描链:第一边界扫描链和第二边界扫描链;所述第一边界扫描链包括:第一SN74BCT8244A器件、第二SN74BCT8244A器件、第三SN74BCT8244A器件、第四SN74BCT8244A器件、第一SN74BCT8374A器件、第二SN74BCT8374A器件及XC4003E-PC84器件;所述第二边界扫描链包括:第三SN74BCT8374A器件及第五SN74BCT8244A器件;

[0083] 所述第一边界扫描链的连接关系为：第一SN74BCT8244A器件、第二 SN74BCT8244A器件、第一SN74BCT8374A器件、第二SN74BCT8374A器件、第三SN74BCT8244A器件、第四SN74BCT8244A器件及XC4003E-PC84器件 依次连接；

[0084] 所述第二边界扫描链的连接关系为：第三SN74BCT8374A器件连接第五SN74BCT8244A器件。

[0085] 能够对支持边界扫描测试的、符合EDIF标准的网表文件进行词法分析，语法分析，错误处理之后，提取自动测试矢量生成所需的网络器件名、物理器件名、封装、描述、网络名及网络连接关系，并将其存储在相应的数据库表格中，通过对比相应的原理图信息、提取到的信息以及数据库表格中的信息，从而有效判断验证结果的可靠性。

[0086] 进一步，所述存储器7设置有前端装置，前端装置设置有文字识别MCU，所述文字识别MCU与光学扫描仪通过USB接口连接，第一SDRAM存储器7、第一Flash存储器7通过数据线连接到文字识别MCU，第二SDRAM存储器7、第二Flash存储器7通过数据线连接到论文分析与处理MCU。

[0087] 通过自动扫描装置进行自动文字识别，提供分析并搜索、下载、打印等定制需求，同时云存储器7提供私有和共享的海量数据存储，解决了传统的检索方式所导致的效率低下、速度慢的问题，解决了不能将分析、下载、存储等功能串行化一体的等问题，通过论文文字智能识别与分析等功能，提高科研和工程人员检索、下载、存储论文工作效率40%。

[0088] 所述警示灯5包括：

[0089] 主控制器模块，用于接收时钟模块输出的时钟信号，同时接收输入的警报发放指令、产生和发放警报控制信号；

[0090] 时钟模块，与主控制器模块连接，用于向主控制器模块提供时钟信号；

[0091] 键盘输入模块，与主控制器模块连接，用于输入信息，由六个独立键盘组成表示六种不同的工作状态，分别是预先、空袭、解除、灾警、测试、终止；

[0092] LED指示灯模块，与主控制器模块连接，用于显示无线数传模块的数据和发射信号及对应的六个独立按键状态，当按下不同按键时，相应的指示灯会点亮，指示当前警报器的警报状态；

[0093] 开关电源模块，包括12V开关电源和48V开关电源，12V开关电源连接无线数传模块，12V开关电源向无线数传模块供电及经过12V-5V电平转换产生5V电压向主控制器模块供电；48V开关电源连接继电器，48V开关电源经继电器开关电源向大功率数字功放模块供电；

[0094] 报警控制模块，连接主控制器模块，用于接收主控制器模块输出的警报控制信号，并对警报控制信号进行传输的通信模块；

[0095] 无线数传模块，与12V开关电源连接，用于将收发端的数据通过串口通信模块传输到主控制器模块进行数据分析处理，主控制器模块执行相应的指令给报警控制模块启动音频播放模块，将警报发送出去；

[0096] 串口通信模块，与PC机、无线数传模块与主控制器模块连接，用于主控制器模块通过串口通信模块接到PC机或无线数传模块数据执行相应的警报指令；

[0097] 音频播放模块，与报警控制模块连接，用于接收报警控制模块输出的警报控制信号，启动音频播放模块读取事先存入SD卡里的音频文件，并将音频信号输出的功率放大模

块；

[0098] 功率放大模块,与音频播放模块连接,包括有大功率数字功率放大模块和 小功率功放模块两部分,大功率数字功率放大模块用于将音频播放模块输出的 音频信号功率放大驱动外扬声器;小功率功放模块用于将音频播放模块输出的 音频信号小功率的放大驱动内扬声器。

[0099] 接收输入的警报发放指令、产生和发放警报控制信号,通讯模块对主控模 块输出的警报控制信号进行传输,放大模块对警报控制信号进行放大并输出, 报警控制模块接收放大模块输出的放大后的警报控制信号,产生并输出报警驱 动信号,驱动模块接收警报控制模块输出的警报驱动模块,对警报器进行驱动; 该全数字人防电声警报一体机采用D类功率放大器实现数字功放,针对人防专 用频点实现数据传输,机箱整体体积小,维护人员易操作,充分考虑了电磁兼 容性,采用电源隔离技术,极大地提高了系统的可靠性,声音存储采用SD卡, 功放采用D类功率放大器,实现了全数字功放,同时在工作电源与功放的大功 率电源之间增加了开关控制,只有接收到了警报信号才通过程序把功率放大器 的电源开关打开,极大地降低了功耗,使系统更加环保,可靠性极大地提高, 线路板采用模块化设计,便于维修,实用性强,具有较强的推广与应用价值。

[0100] 当外界访问该网络设备1时,首先经过外设接口2进行连接,但是数据通 接口时,安全验证装置3会对该访问数据进行安全限制,如果未经许可的数据 将不允许数据进入设备内,若是病毒程序或没有权限的数据,安全验证装置3 会启动警示灯5,来显示当前网络问题或故障。如果该数据获得权限将通过安全 验证,并进入存储器7进行实时保存,最后处理器4进行对数据的处理操作。

[0101] 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。

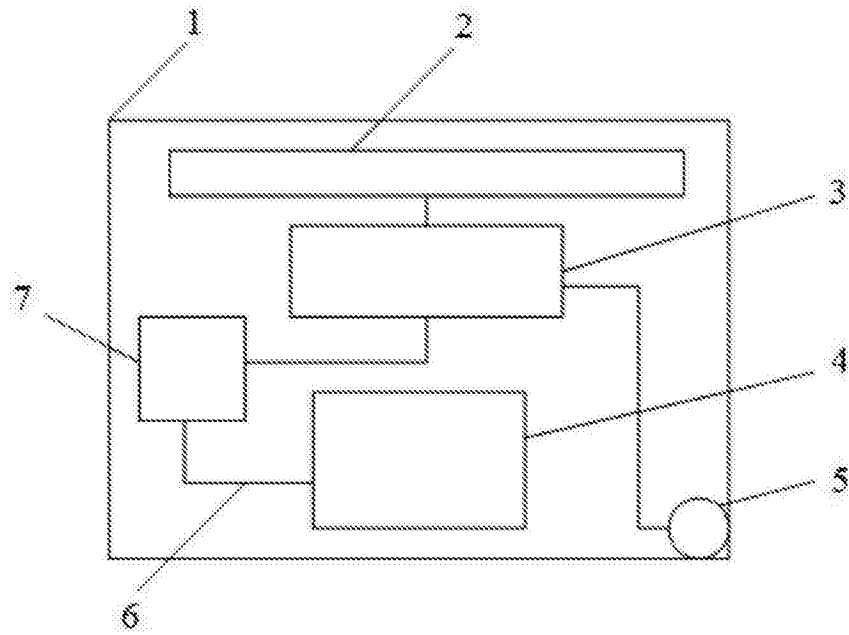


图1

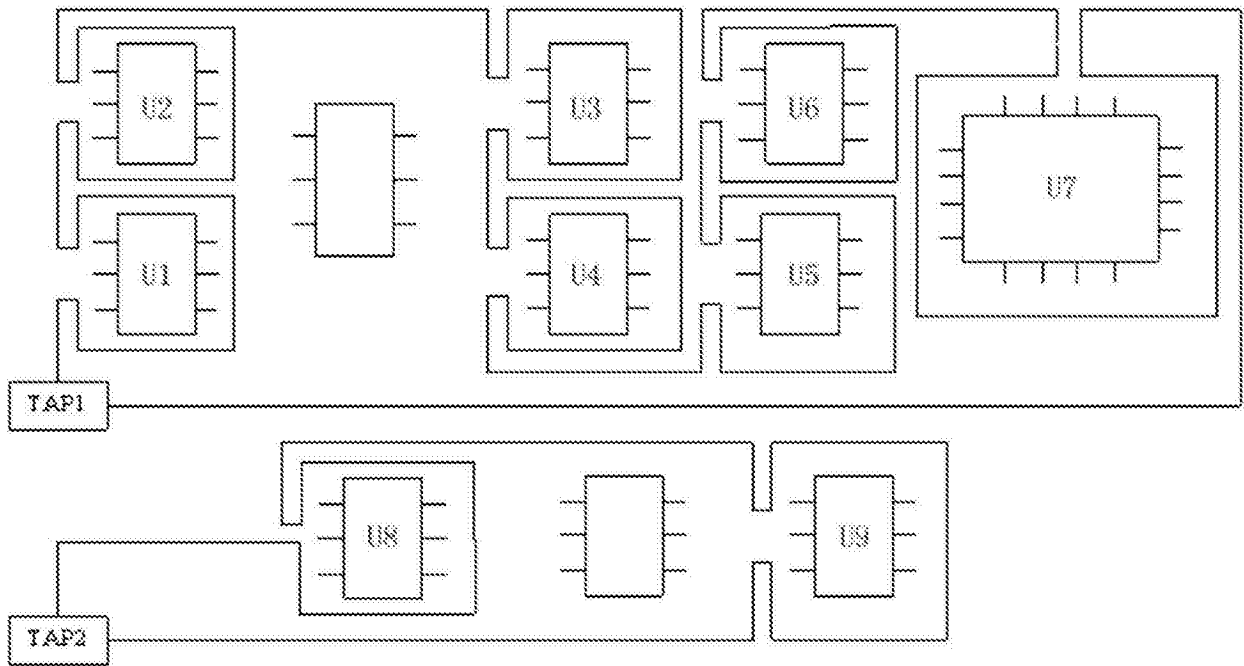


图2

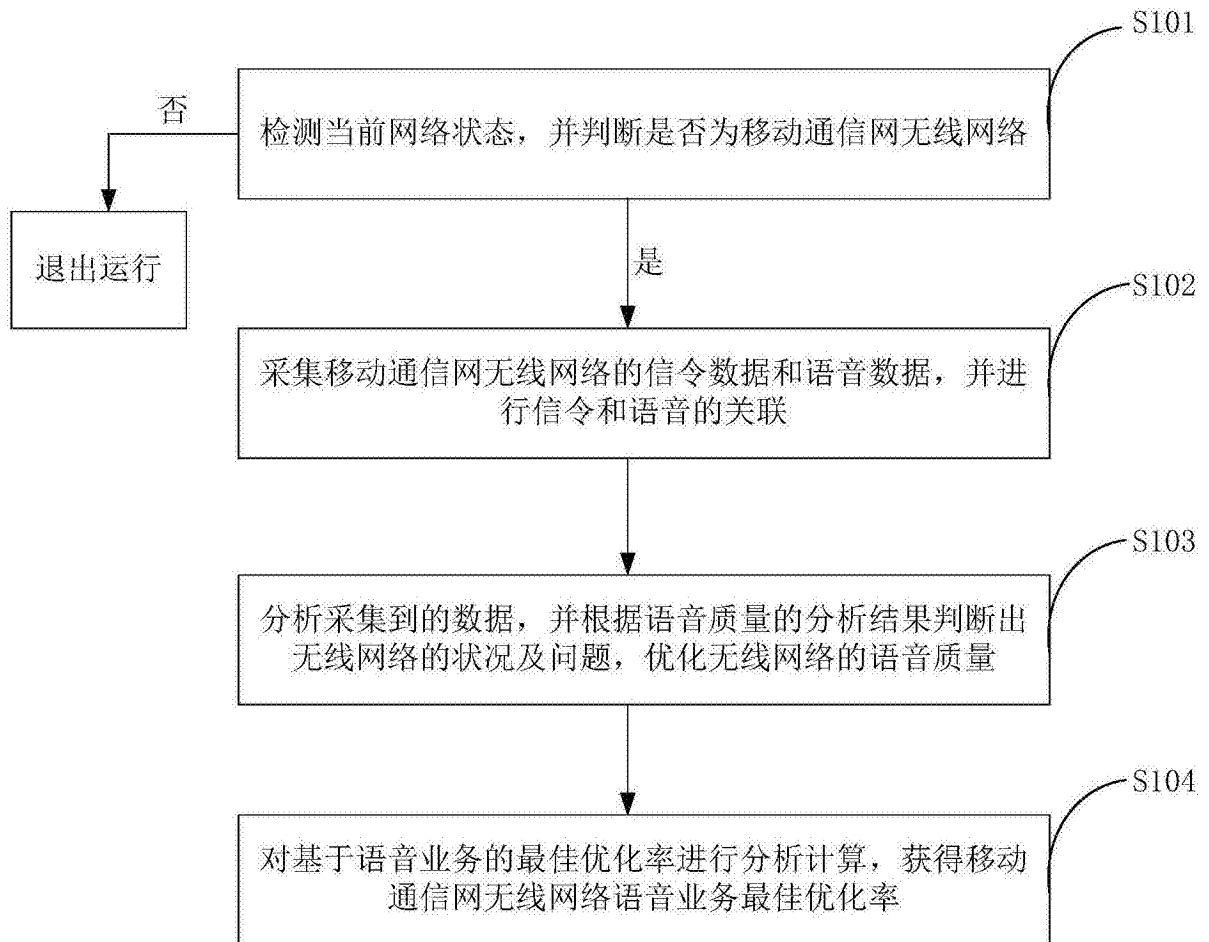


图3