|  |  |  |  |
| --- | --- | --- | --- |
| 项目编号 |  | 文档编号 |  |
| 版本号 |  | 保密级别 |  |
| 编制人 | 陈秀鹏 | 编制日期 | 2012-7-25 |
| 审核人 |  | 审核日期 |  |
| 阅读权限 |  | | |

设备通信协议调研报告

# 版本历史

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 版本日期 | 修改人 | 变更描述 |
| 1.0 | 2012-7-25 | 陈秀鹏 | 创建文档 |
| 2.0 | 2012-9-11 | 王宏飞 | 修改协议内容 |
| 2.1 | 2013-1-5 | 安勇 | GPS位置信息格式由8字节增加为10字节 |
| 2.2 | 2013-3-8 | 安勇 | 2.1终端编号增加无线基站、护工胸牌、智能药箱 |
| 2.3 | 2013-3-14 | 吴杰影 | 修改设备编号 |
| 2.4 | 2013-04-01 | 安勇 | 去掉“帧中0x1A替换” |
| 2.5 | 2013-5-21 | 赵伟光 | 针对床垫设备增加猝死功能，增加报警类型，修改问询回复帧结构 |
| 2.6 | 2013-7-16 | 赵伟光 | 增加了“无线门灯0x0D”  “LED显示屏0x0E”和“尿湿感应终端0x0F” |
| 2.7 | 2014-1-8 | 陈秀鹏 | 修改协议，以保证室内网关和园区一卡通在丢包情况下仍能正常报警 |
| 2.8 | 2014-4-1 | 赵伟光 | 增加“电子看板0x10”“腕带0x11” |
| 2.9 | 2014-5-13 | 赵伟光 | 增加“红外0x12” |
| 2.10 | 2014-10-16 | 赵伟光 | 明确红外设备与服务器的通信 |
| 2.11 | 2015-06-10 | 倪志斌 | 增加烟雾报警终端 |

# 当前协议评估

* 1. **协议统一**

当前协议分两个版本，床垫及床垫报警器单独采用“Sensor Pad报警终端通信流程及帧结构”文档协议，其他设备（如温湿度、园区内老人终端、园区外老人终端等）采用“终端数据类型及格式”文档，和“HS-10-01项目终端分类规则”文档，和“福利院项目MCU与Zigbee通信说明VA”文档。两者采用的终端ID及帧格式不一致，造成了信息解析上的混乱。所以，急需重新修订统一协议，及其相关命名规则。

* 1. **安全隐患**
     1. **Zigbee侧**
     2. **网络侧**

攻击方在获取到目标机监听的IP地址和端口后，可以发起对话请求，目标机会接受该请求，并与攻击方建立会话。攻击方若产生大量链接，将影响合法设备的接入。所以，协议中需要引入身份认证功能，即目标机要验证客户端的身份合法性。

攻击方通过抓包工具，可完全获取到明文信息。所以，协议中需要引入加密功能，防止网络窃听。

攻击方可对网络数据进行部分拦截、仿冒。所以，协议中需要引入完整性校验，保证数据的完整性，确保信息在传递过程中未被篡改。

推荐采用TLS协议。

# 明文协议

这次修正包括以下几点：

1. 帧格式统一为【目的终端编号+源终端编号+帧序列号+消息类型+参数个数+参数内容（参数类型+参数值）+奇偶校验】。其中目的终端编号为4字节，源终端编号4字节，帧序列号2字节，消息类型1字节，参数个数1字节，参数内容（参数类型1字节+参数值），奇偶校验1字节。
2. 帧进行0xC0封装。具体方法：数据中的0xC0替换为0xDB 0xDC，数据中的0xDB替换为0xDB 0xDD；
3. 终端编号由2字节扩充到4字节，设备种类编号也发生变化。
4. 上行通道中，引入帧序列号。
5. 温湿度设备原有协议中，“温度”字段不仅用来表明温度值，也用来表明“低电压告警帧”和“错误帧”；现将功能分离，引入新字段“报警数据”单独表示。
   1. **终端编号**

唯一标识一个设备终端，由4个字节构成，第一个字节代表终端种类，后三个字节为该种类唯一序号（需要定义规则）。该系统最多有255种设备构成（0不可用），每类最多有16,777,215个设备。

终端标识号：4 bytes

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| + | Byte +0 | Byte +1 | Byte +2 | Byte +3 |
| Byte 0 | 终端种类编号 | 终端序号 | | |

终端种类编号

|  |  |  |
| --- | --- | --- |
| 序号 | 字节 | 代表意义 |
| 1 | 0x01 | 上层控制中心 |
| 2 | 0x02 | 床垫报警终端 |
| 3 | 0x03 | 床压力采集垫 |
| 4 | 0x04 | 温湿度设备 |
| 5 | 0x05 | 园区内老人终端 |
| 6 | 0x06 | 园区内定位辅助终端 |
| 7 | 0x07 | 园区外老人终端 |
| 8 | 0x08 | 一键报警终端 |
| 9 | 0x09 | 无线门磁终端 |
| 10 | 0x0A | 无线基站 |
| 11 | 0x0B | 护工胸牌 |
| 12 | 0x0C | 智能药箱 |
| 13 | 0x0D | 无线门灯 |
| 14 | 0x0E | LED显示屏 |
| 15 | 0x0F | 尿湿检测终端 |
| 16 | 0x10 | 电子看板 |
| 17 | 0x11 | 腕带 |
| 18 | 0x12 | 红外报警终端 |
| 19 | 0x13 | 烟雾报警终端 |

* 1. **床垫设备通信协议**

修改内容为：

1. 在问询帧中加入“帧序列号”，2字节，在“源终端ID”和“消息类型”之间，表示当前帧序号，每次重置时随机生成，此后递增加一。
2. 在应用帧中加入“帧序列号”，2字节，在“源终端ID”和“消息类型”之间，表示当前帧序号，每次重置时随机生成，此后递增加一。
3. 在应用回复帧中加入“帧序列号”，2字节，在“源终端ID”和“消息类型”之间，表示当前帧服务端已收到，并进行了相应处理。
4. 修改应用帧中“报警数据”。原有“报警数据”的参数类型为0x05，值为设备ID+【0x01，0x02，0x03，0x04，0x05】；现修改为只有设备ID+【b0=1有人,b0=0无人，b1=1预警,b2=1报警】。增加“设备报警”，参数类型为0x06，值为设备ID+【b0=1设备故障】。
5. 修改问询回复帧中的“配置信息（9Byte）”为“配置信息（10Byte）”，其中原Byte[1]~Byte[8]变更为Byte[2]~Byte[9]，内容不变。原Byte[0]变更为Byte[1]，并当Byte[1]的值为0xff时，关闭离床报警功能，增加Byte[0]，内容为猝死预警和报警的时间间隔，单位分钟，Byte[0]的值为0xff时，关闭离猝死报警功能。
6. 修改“报警数据”。原有“报警数据”Byte[0]中，bit[0]=1有人, bit[0]=0无人，bit[1]=1预警, bit[2]=1报警。修改为bit[0]=1有人, bit[0]=0无人，bit[1]=1离床预警, bit[2]=1离床报警bit[3]=1猝死报警。
7. 其他内容不变，详见“***Sensor Pad报警终端通信流程及帧结构v1.2.docx***”文档。

通信流程如下：

1. 设备每隔300秒发送一次问询帧，接收问询回复帧。问询帧中包含“报警器状态数据”一种参数。问询回复帧中包含“系统时间”，“配置信息”两种参数。
2. 设备检测到“报警数据”发生变化时，发送应用帧，接收应用回复帧。应用帧中包含“系统时间”，“报警数据”两种参数。应用回复帧中不含参数。
3. 设备检测到“设备报警”发生变化时，发送应用帧，接收应用回复帧。应用帧中包含“系统时间”，“设备报警”两种参数。应用回复帧中不含参数。
   1. **温湿度设备通信协议**

修改内容为：

1. 帧格式重新定义为【目的终端编号+源终端编号+帧序列号+消息类型+参数个数+参数内容（参数类型+参数值）+奇偶校验】。其中目的终端编号为4字节，源终端编号4字节，帧序列号2字节，消息类型1字节，参数个数1字节，参数内容（参数类型1字节+参数值），奇偶校验1字节。
2. 目的终端编号为4字节，值为0x01000000-0x01FFFFFF。
3. 源终端编号为4字节，值为0x04000000-0x04FFFFFF。
4. 帧序列号为2字节，值为0x0000-0xFFFF，表示当前帧序号，递增加一。
5. 消息类型为1字节，值为0x09，表示为“应用帧”。
6. 参数个数为1字节，值为0x00-0xFF，表示帧中参数个数。
7. 参数类型为1字节，值为0x40，表示为“温度值”；参数值为2字节，定义不变。
8. 参数类型为1字节，值为0x41，表示为“湿度值”；参数值为2字节，定义不变。
9. 参数类型为1字节，值为0x42，表示为“设备报警”；参数值为1字节，【b0=1低压】。
10. 奇偶校验为1字节，值为该帧中所有字节依次按位异或运算的结果。

通信流程如下：

1. 设备每隔3600秒发送一次应用帧。应用帧中包含“温度值”，“湿度值”，“设备报警”三种参数。
2. 设备检测到“设备报警”发生变化时，发送一次应用帧。应用帧中包含“设备报警”一种参数。
   1. **园区内老人终端设备通信协议**

修改内容为：

1. 帧格式重新定义为【目的终端编号+源终端编号+帧序列号+消息类型+参数个数+参数内容（参数类型+参数值）+奇偶校验】。其中目的终端编号为4字节，源终端编号4字节，帧序列号2字节，消息类型1字节，参数个数1字节，参数内容（参数类型1字节+参数值），奇偶校验1字节。
2. 目的终端编号为4字节，值为0x01000000-0x01FFFFFF。
3. 源终端编号为4字节，值为0x05000000-0x05FFFFFF。
4. 帧序列号为2字节，值为0x0000-0xFFFF，表示当前帧序号，递增加一。
5. 消息类型为1字节，值为0x09，表示为“定位应用帧”；值为0x0A，表示为“状态应用帧”；。
6. 参数个数为1字节，值为0x00-0xFF，表示帧中参数个数。
7. 参数类型为1字节，值为0x50，表示为“身体状态”；参数值为1字节，【b0=1摔倒，b1=1手动报警】。（删除）
8. 参数类型为1字节，值为0x50，表示为“身体状态”；参数值为1字节，b0=1摔倒，b0=0摔倒取消，b1-b3为摔倒序列号，每次重置时随机生成，此后在摔倒状态变化时递增1，b4=1手动报警，b4=0手动报警取消，b5-b7为序列号，每次重置时随机生成，此后在状态变化时递增1。（增加）
9. 参数类型为1字节，值为0x51，表示为“位置信息”；参数值为5字节，园区内定位辅助终端编号+能量值。其中园区内定位辅助终端编号值为0x06000000- 0x06FFFFFF。
10. 参数类型为1字节，值为0x52，表示为“设备报警”；参数值为1字节，【b0=1低压；b1=1人卡分离】。（删除）
11. 参数类型为1字节，值为0x52，表示为“设备报警”；参数值为1字节，b0=1低电压报警，b0=1低电压报警取消，b1-b3为低电压报警序列号，每次重置时随机生成，此后在状态变化时递增1，b4=1人卡分离报警，b4=1人卡分离报警取消，b5-b7为人卡分离报警序列号，每次重置时随机生成，此后在状态变化时递增1。（增加）
12. 奇偶校验为1字节，值为该帧中所有字节依次按位异或运算的结果。

通信流程如下：

1. 设备每隔一定时间（动态周期，10秒-正无穷）发送一次定位应用帧。定位应用帧中包含“位置信息”一种参数。
2. 当“身体状态”正常时，设备每隔300秒发送一次状态应用帧。状态应用帧中包含“身体状态”，“设备报警”两种参数。
3. 当“身体状态”不正常时，设备每隔10秒发送一次状态应用帧。状态应用帧中包含“身体状态”，“设备报警”两种参数。
4. “身体状态”由正常状态变化为不正常状态时，发送一次状态应用帧。
5. “身体状态”由不正常状态变化为正常状态时，连续发送三次状态应用帧，时间间隔为10s，第四次及以后发送状态应用帧的时间间隔增长到300s。
6. 设备检测到“身体状态”发生变化时，发送一次应用帧。应用帧中包含“身体状态”一种参数。
7. 设备检测到“设备报警”发生变化时，发送一次应用帧。应用帧中包含“设备报警”一种参数。
   1. **园区外老人终端设备通信协议**

修改内容为：

1. 帧格式重新定义为【目的终端编号+源终端编号+帧序列号+消息类型+参数个数+参数内容（参数类型+参数值）+奇偶校验】。其中目的终端编号为4字节，源终端编号4字节，帧序列号2字节，消息类型1字节，参数个数1字节，参数内容（参数类型1字节+参数值），奇偶校验1字节。
2. 目的终端编号为4字节，值为0x01000000-0x01FFFFFF。
3. 源终端编号为4字节，值为0x07000000-0x07FFFFFF。
4. 帧序列号为2字节，值为0x0000-0xFFFF，表示当前帧序号，递增加一。
5. 消息类型为1字节，值为0x09，表示为“应用帧”。
6. 参数个数为1字节，值为0x00-0xFF，表示帧中参数个数。
7. 参数类型为1字节，值为0x70，表示为“身体状态”；参数值为1字节，【b0=1摔倒，b1=1手动报警】。（删除）
8. 参数类型为1字节，值为0x71，表示为“GPS位置信息”；参数值为10字节，定义不变。
9. 参数类型为1字节，值为0x72，表示为“设备报警”；参数值为1字节，【b0=1低压；b1=1人卡分离】。（删除）
10. 奇偶校验为1字节，值为该帧中所有字节依次按位异或运算的结果。

通信流程如下：

1. 当“身体状态”正常时，设备每隔300秒发送一次应用帧。应用帧中包含“GPS位置信息”（可选项），“身体状态”，“设备报警”三种参数。
2. 当“身体状态”不正常时，设备每隔10秒发送一次应用帧。应用帧中包含“GPS位置信息”（可选项），“身体状态”，“设备报警”三种参数。
3. “身体状态”由不正常状态变化为正常状态时，连续发送三次状态应用帧，时间间隔为10s，第四次及以后发送状态应用帧的时间间隔增长到300s。
4. 设备检测到“身体状态”发生变化时，发送一次应用帧。应用帧中包含“GPS位置信息”（可选项），“身体状态”，“设备报警”三种参数。
5. 设备检测到“设备报警”发生变化时，发送一次应用帧。应用帧中包含“GPS位置信息”（可选项），“身体状态”，“设备报警”三种参数。
   1. **腕带协议**

腕带协议总体上与一键报警一致，但有如下区别：

1. 终端大类编号为0x11.
2. 腕带不属于任何一个“室内网关”设备，及在“问询回复帧”中不可包含相关内容。
3. 室内网关从来不会发送腕带设备故障和取消腕带设备报警的信息。
   1. **红外协议**

红外设备总体上和智能感应垫一致，但有如下区别：

1. 终端大类编号为0x12
2. 报警阈值字段单位为小时，而非分钟
3. 红外设备从来不会发送无人数据给室内网关。
4. 红外设备自带电量检测功能，更改心跳帧中的原状态数据字段为设备状态字段表明设备是否低电量（室内网关端暂不解析该字段，与服务器的协议暂不添加此功能）
   1. **烟雾报警终端协议**

烟雾报警终端设备总体上和一键报警一致，但有如下区别：

1）终端大类编号为0x13

2）无报警阈值字段和报警时间段