

文章编号: 1671-251X(2023)03-0131-06

DOI: [10.13272/j.issn.1671-251x.18043](https://doi.org/10.13272/j.issn.1671-251x.18043)

# 井下人员精确定位系统无线终端 同步升级方法

张立峰<sup>1,2</sup>, 包建军<sup>1,2</sup>, 金业勇<sup>1,2</sup>

(1. 中煤科工集团常州研究院有限公司, 江苏 常州 213015;  
2. 天地(常州)自动化股份有限公司, 江苏 常州 213015)

**摘要:** 针对井下人员定位系统采用无线应用内编程(IAP)方式进行固件升级存在的升级期间标志卡无法正常使用、升级效率较低、安全性不高等问题, 提出了一种井下人员精确定位系统无线终端同步升级方法。给出了井下人员精确定位系统架构和无线终端同步升级方法流程, 重点介绍了无线终端同步升级的安全性设计和高并发技术实现。安全性设计: 为提升空中数据传输的安全性, 针对读卡器与标志卡之间的数据传输方式, 采用高级加密标准(AES)加密器进行针对性加密; 为确保标志卡无线升级后运行正常, 在标志卡完成接收即将切换时引入信息摘要算法 MD5 进行完整性校验。高并发技术实现: 利用矿井全覆盖的超宽带(UWB)无线通信网络扩展并兼容无线升级协议, 实现井下所有标志卡分布式多节点同步升级; 通过断点续传方式, 解决运动状态下多节点之间数据切换的问题; 基于时隙 ALOHA 算法, 提出一种动态时隙分配机制, 以保证人员精确定位系统的容量及响应效率。测试结果表明, 该方法可以在井下人员精确定位系统内兼容运行, 在不影响系统性能指标的情况下, 实现所有无线终端定位标志卡嵌入式固件的无线升级, 升级成功率为 100%, 且升级过程高效、可靠、安全。

**关键词:** 井下人员精确定位; 无线终端; 固件升级; 无线升级; 同步升级; 混合加密; 断点续传; 动态时隙分配机制

中图分类号: TD655.3

文献标志码: A

Synchronous upgrade method for the wireless terminal of  
underground personnel precise positioning system

ZHANG Lifeng<sup>1,2</sup>, BAO Jianjun<sup>1,2</sup>, JIN Yeyong<sup>1,2</sup>

(1. CCTEG Changzhou Research Institute, Changzhou 213015, China;  
2. Tiandi (Changzhou) Automation Co., Ltd., Changzhou 213015, China)

**Abstract:** When the underground personnel positioning system's firmware is upgraded using the wireless in-application programming (IAP) mode, the mark card can not be used normally, the upgrade efficiency is low and the security is not high. In order to solve the above problems, a synchronous upgrade method for the wireless terminal of the underground personnel precise positioning system is proposed. The architecture of underground personnel precise positioning system and the process of wireless terminal synchronous upgrade method are pointed out. The security design and high concurrency technology implementation of the wireless terminal synchronous upgrade are mainly introduced. Security design: in order to improve the security of air data transmission, advanced encryption standard (AES) encryptor is used to encrypt the data transmission between the card reader and the identification card. In order to ensure the normal operation of the identification card after the wireless upgrade, the message digest algorithm MD5 is introduced to perform integrity verification when the

收稿日期: 2022-10-13; 修回日期: 2023-02-22; 责任编辑: 胡娟。

基金项目: 天地科技股份有限公司科技创新创业资金专项项目(2020-TD-ZD004); 天地(常州)自动化股份有限公司科研项目(2021-GY-2013)。

作者简介: 张立峰(1990—), 男, 江苏常州人, 研究实习员, 研究方向为煤矿井下定位及通信技术, E-mail: zhanglifeng0339@126.com。

引用格式: 张立峰, 包建军, 金业勇. 井下人员精确定位系统无线终端同步升级方法[J]. 工矿自动化, 2023, 49(3): 131-136.

ZHANG Lifeng, BAO Jianjun, JIN Yeyong. Synchronous upgrade method for the wireless terminal of underground personnel precise positioning system[J]. Journal of Mine Automation, 2023, 49(3): 131-136.



扫码移动阅读

identification card completes receiving and is about to switch. High concurrency technology: the ultra wide band (UWB) wireless communication network with full coverage in the mine is used to extend and compatible the wireless upgrade protocol. The distributed multi-node synchronous upgrade of all underground identification cards is realized. The problem of data switching between nodes in motion is solved by the way of breakpoint continuous transmission. Based on the slotted ALOHA algorithm, a dynamic slot allocation mechanism is proposed to ensure the capacity and response efficiency of the personnel precise positioning system. The test results show that the method can be compatible with the underground personnel precise positioning system. The method can realize the wireless upgrade of the embedded firmware of all wireless terminal positioning identification cards without affecting the system performance indicators. The upgrade success rate is 100%, and the upgrade process is efficient, reliable and safe.

**Key words:** precise positioning of underground personnel; wireless terminal; firmware upgrade; wireless upgrade; synchronous upgrade; mixed encryption; breakpoint resume; dynamic slot allocation mechanism

## 0 引言

矿井人员定位系统作为煤矿井下安全避险“六大系统”<sup>[1]</sup>之一,目前已在全国各大煤矿安装普及,提高了煤矿安全保障能力。在提供定位服务的基础上,人员定位系统可逐步增加考勤、调度、门禁等功能。在扩展这类应用时,需要对系统配套的标志卡、矿灯等无线终端设备进行固件升级。由于无线终端设备具有基数大、分布广、难拆卸等特点,需要研究一种可靠、高效的方法满足固件升级需求<sup>[2-4]</sup>。

传统的固件升级主要采用在线系统编程(In-System Programming, ISP)方式。该方式不需要编程器就可以进行单片机实验和开发,便于调试,但仍然需要外部电路辅助实现,而标志卡为本质安全设计,不具备易拆卸或引脚外露的条件,因此维护成本极高。目前,针对井下人员定位应用场景,较为高效的固件升级方式是基于标志卡本身通信技术的无线应用内编程(In Application Programming, IAP)方式。采用该方式时,维护人员先将升级程序存入定制的升级设备,再在灯房、下井口等人员集中处启动升级功能,循环广播发送升级数据,升级设备覆盖范围内的标志卡会被触发进入长接收状态,直到升级完成。这种方式通过合理嵌入式软件架构,采用无线传输方式解决 ISP 方式需要拆卸的问题,可实现标志卡批量无线升级。然而在实际应用场景中, IAP 方式仍然存在以下缺点:升级期间标志卡无法正常使用,影响井下人员正常生产作业;信号只能覆盖一个特定范围,而下井人员在时间和空间上都不集中,实际并发数和升级效率有待提高;采用广播方式循环发送升级信息,意味着传输过程中空中消息公开,存在被扫描侦听窃取的风险,安全性不高<sup>[5-7]</sup>。

针对上述问题,提出了一种井下人员精确定位系统无线终端同步升级方法。采用点对点通信、断

点续传的方式,应用混合高级加密标准(Advanced Encryption Standard, AES)加密传输和 MD5 完整性校验保证安全性,采用动态时隙分配机制,在定位系统信号覆盖范围内,实现无线终端设备在正常使用过程中的固件升级<sup>[8-9]</sup>。

## 1 井下人员精确定位系统架构

井下人员精确定位系统主要包括上位机、读卡器和标志卡 3 个部分,如图 1 所示。上位机通过以太网接入井下环网交换机,与读卡器通信,读卡器与标志卡之间采用超宽带(Ultra Wide Band, UWB)通信方式进行数据交互<sup>[10-12]</sup>。

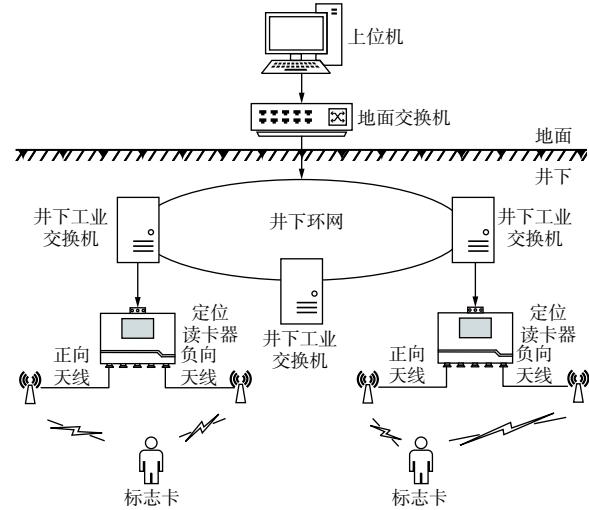


图 1 井下人员精确定位系统架构

Fig. 1 Structure of underground personnel precise positioning system

## 2 无线终端同步升级方法流程

一次完整的无线终端同步升级分为启动、传输、完成 3 个阶段,上位机、读卡器与标志卡在不同阶段的交互协作流程如图 2 所示。

升级启动阶段:维护人员远程加载升级文件至

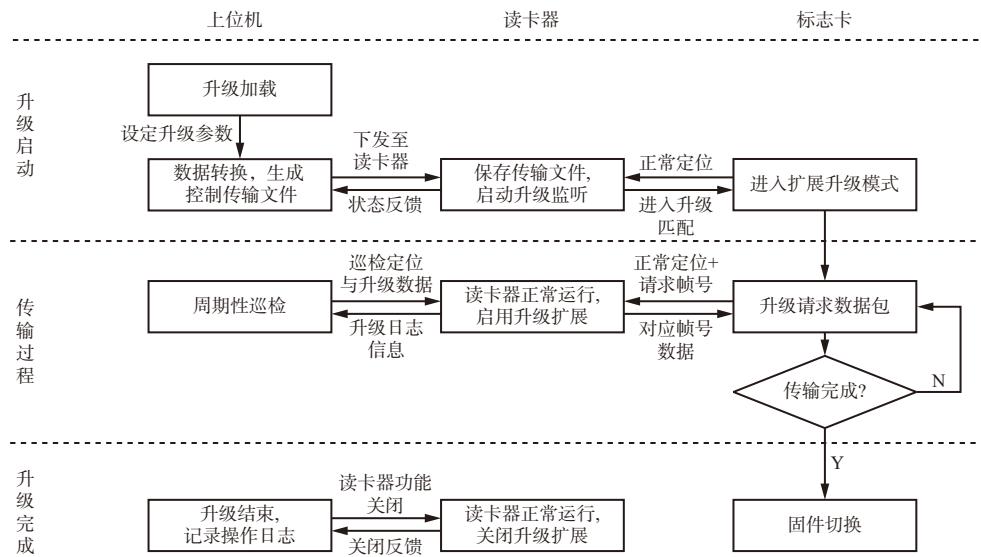


Fig. 2 Wireless terminal synchronization upgrade process

定位系统上位机；上位机对升级文件进行处理转换后生成控制传输文件，并通过网络下发给读卡器；读卡器收到文件后保存在本地并启动升级过程；标志卡进入读卡器覆盖范围后被触发进入扩展升级模式，在周期性定位中主动定向请求升级数据。

**升级传输阶段：**标志卡定位时，在扩展字节中附带具体请求数据帧号；读卡器以点对点通信方式向指定标志卡发送对应的数据帧；上位机定期巡检读卡器，收集标志卡升级日志信息。

**升级完成阶段：**维护人员通过操作上位机结束升级过程，结合读卡器日志，生成本次升级日志；读卡器收到上位机结束升级命令后，停止触发新的标志卡进入扩展升级模式；标志卡在数据包传输完成并校验通过后进行固件切换。

### 3 安全性设计

#### 3.1 AES 混合加密传输

当前无线终端升级方法主要采用广播方式循环传输升级数据，升级数据在空域中为公开状态，通过扫频接收等技术手段很容易获取完整的升级文件包，并进行逆向破解和复制。对于厂家，存在核心技术泄密风险；对于矿方，存在安全生产方面的隐患。

为了提升空中数据传输的安全性，针对读卡器与标志卡之间的数据传输方式，采用AES加密器进行针对性加密。标志卡在首次接入读卡器时，会上传自己的ID与私钥，读卡器校验后将ID和私钥绑定并存入升级链表，结合读卡器私钥形成一个混合密钥回复标志卡。读卡器收到某一标志卡的升级数据帧请求时，先去升级链表中找到对应标志卡的私钥，然后将帧明文数据用对应混合密钥进行加密后

发送；标志卡收到回复帧数据后用对应密钥进行解密存储，然后按这种传输方式依次请求指定数据，直至所有数据接收完成<sup>[13-14]</sup>。

应用这种加密方式的安全性体现在3个方面：  
①采用AES-128算法加密空中传输的升级数据，在确保安全性的同时兼顾运算效率。  
②基于标志卡主动请求的机制，在多标志卡情况下，接收端如果没有密钥，将无法确认空中数据包的目标及数据包序号。  
③读卡器基于标志卡唯一私钥进行针对性混合加密，保证不同标志卡和读卡器之间升级数据包的差异性，第三方即使捕获到数据包也无法破解。

#### 3.2 MD5 完整性校验

基于UWB技术的特性，无法完全避免空中数据干扰。为了提高数据无线传输的可靠性，确保标志卡无线升级后运行正常，在标志卡完成接收即将切换时引入信息摘要算法MD5<sup>[15-17]</sup>。标志卡完成升级数据接收后，向读卡器请求本次升级文件的MD5码，然后与本地文件的MD5码进行比对，如果一致则可确认传输无误，标志卡可切换到新的程序，否则重新接收升级数据。

### 4 高并发技术实现

#### 4.1 多节点同步升级

为了提高系统升级并发量，摆脱广播方式只能覆盖一定范围区域的限制，利用矿井全覆盖的UWB无线通信网络扩展并兼容无线升级协议。当需要进行无线升级时，上位机将升级固件在井下环网内发布，环网内所有读卡器通过网络下载后保存在本地，由上位机综合调度，井下所有读卡器作为升级节点触发覆盖范围内标志卡进行扩展升级，实现

井下所有标志卡分布式多节点同步升级。

#### 4.2 断点续传

基于标志卡的移动特性,以及混合 AES 加密设计下不同读卡器节点的空中数据不一致的情况,井下标志卡同步升级需要解决运动状态下多节点之间数据切换的问题。

标志卡逻辑处理流程如图 3 所示。标志卡采用主动请求方式,多节点之间通过握手切换,升级数据

采用断点续传方式。标志卡触发进入升级模式后,在 Flash 中开辟一个升级数据记录表,按照表中的记录顺序依次请求节点对应的升级数据。当移动中标志卡需要切换接入陌生节点时,采用握手验证的交互方式记录节点密钥,并从升级数据记录表的断点处继续接收,直至升级数据接收完成并通过 MD5 完整性校验。

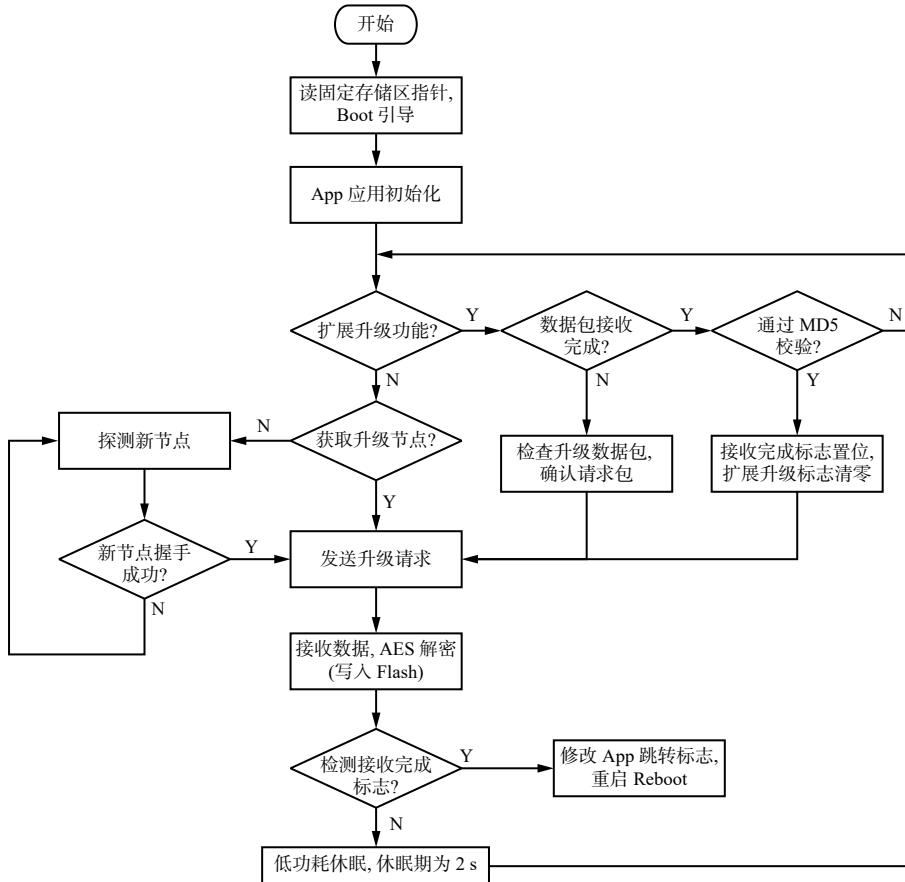


图 3 标志卡逻辑处理流程

Fig. 3 Logic processing flow of identification card

#### 4.3 动态时隙分配机制

基于随机竞争的纯 ALOHA 算法信道利用率较低,基本只在 RFID, ZigBee 等井下区域人员定位系统中应用<sup>[18-19]</sup>。基于 UWB 的人员精确定位系统由于通信模式相对复杂且单次定位周期较长,更容易发生空中碰撞导致测距失败,普遍应用的算法为时隙 ALOHA。该算法是将时间分成若干个相同的时间片,所有标志卡在分配的时间片内进行定位及数据交互,避免发送数据的随意性,提高信道的利用率和吞吐量<sup>[20-21]</sup>。

标志卡通过扩展字节实现升级传输,而定位字节扩展会导致定位时间延长,在采用时隙 ALOHA 算法的系统中,意味着单个标志卡的分配时隙需要拉长,如果时隙数不变,则系统响应效率会下降。为了

保证人员精确定位系统的容量及响应效率,提出了一种应用于无线升级过程中的动态时隙分配机制。在该机制下,读卡器存在 2 种时隙,分别用于正常定位和无线升级,并可根据读卡器覆盖范围内标志卡数量自适应切换负载模式,动态调整 2 种时隙的数量分配。

动态时隙分配机制如图 4 所示,  $T$  为时隙分配周期,  $S_1$  为正常定位时间片,  $S_2$  为扩展升级时间片,  $N_1$  为  $S_1$  时隙最大容量,  $N_2$  为  $S_2$  时隙最大容量,  $x$  为忙碌状态  $S_1$  时隙数量,  $y$  为忙碌状态  $S_2$  时隙数量。在实际应用中,假设读卡器的实际负载数量为  $n$ ,当  $n < N_2$  时,空中消息空闲,给所有标志卡分配  $S_2$  时隙;当  $N_1 < n < N_2$  时,空中消息忙碌,  $S_2$  时隙数  $y = (n - N_1)S_1 / (S_2 - S_1)$ ,  $x = n - y$ ;当  $n > N_1$  时,系统满载,

不再分配  $S_2$  时隙,当前读卡器覆盖范围内的标志卡无线升级将停止,等待空闲时再进行升级。

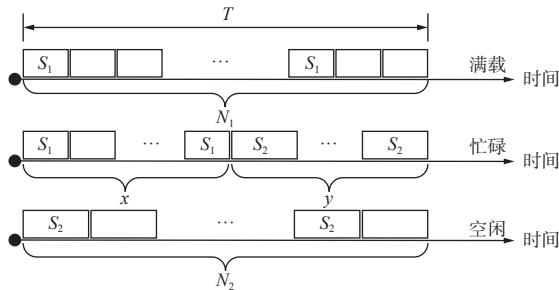


图 4 动态时隙分配机制

Fig. 4 Dynamic slot allocation mechanism

## 5 测试分析

选取长 60 m、宽 20 m 的长方形模拟巷道进行测试,如图 5 所示。在模拟巷道内部搭建基于 UWB 的人员精确定位系统,测试设备为 1 台上位机、4 台读卡器和若干张标志卡。

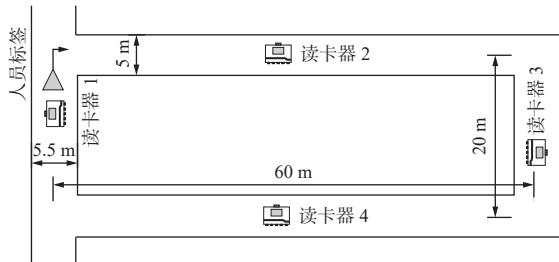


图 5 无线终端同步升级测试环境

Fig. 5 Test environment of wireless terminal synchronization upgrade

标志卡定位周期为 2 s,升级程序大小为 36 Kibit,单次定位传输数据量为 64 B,理论最快完成时间为  $36 \times 1024 \times 2 / (8 \times 64) = 144$  s。测试时人员携带标志卡以 1.5 m/s 的速度绕圈,针对空闲、忙碌、满载 3 种负载情况,分别投入 40, 100, 200 张标志卡进行升级测试。在进行标志卡固件无线升级的同时,验证人员定位相关功能,最后从上位机中调取升级记录日志,整理得到测试结果,如图 6 所示。

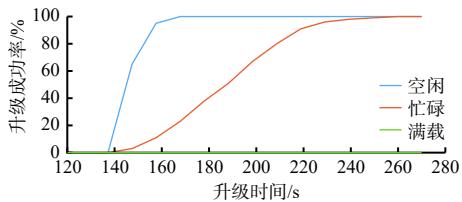


图 6 无线终端同步升级测试结果

Fig. 6 Test result of wireless terminal synchronization upgrade

从图 6 可看出,无线终端同步升级方法整体可靠,在空闲和忙碌 2 种状态下,标志卡升级成功率都为 100%。不同状态主要影响标志卡升级的时间期望,在满载状态下,为了保证井下人员精确定位系统

功能,读卡器不会分配升级时隙,符合动态时隙分配机制设计预期。

## 6 结论

1) 提出了一种井下人员精确定位系统无线终端同步升级方法,详细论述了实现思路及关键技术。关键技术包括安全性设计和高并发技术实现 2 个方面。安全性设计通过 AES 加密器和 MD5 算法实现,高并发技术通过矿井全覆盖的 UWB 无线通信网络、断点续传方式、动态时隙分配机制实现。

2) 测试结果表明,该方法可以在井下人员精确定位系统内兼容运行,在不影响系统性能指标的情况下,实现所有无线终端定位标志卡嵌入式固件的无线升级,升级成功率为 100%。

3) 该方法排除了基于广播方式的无线 IAP 升级方法的安全隐患,为数量大、分布广、工作时间不固定的标志卡提供了一种高效、可靠、安全的固件升级方法。需要说明的是,该方法本身并不依赖特定系统或通信技术,可以研究移植扩展至其他系统,如煤矿安全监测监控系统、矿用广播系统等。该方法的高安全、全覆盖、强校验设计可满足煤矿井下无线终端的定制化需求,为全矿井无线终端产品的固件无线升级提供参考。

## 参考文献(References):

- [1] 国家安全监管总局国家煤矿安监局关于建设完善煤矿井下安全避险“六大系统”的通知[EB/OL]. [2022-09-13]. [http://www.gov.cn/govweb/gzdt/2010-08/26/content\\_1688935.htm](http://www.gov.cn/govweb/gzdt/2010-08/26/content_1688935.htm). Notice of the State Administration of Coal Mine Safety, State Administration of Safety Supervision on the construction and improvement of the "six systems" for safety avoidance in underground coal mines[EB/OL]. [2022-09-13]. [http://www.gov.cn/govweb/gzdt/2010-08/26/content\\_1688935.htm](http://www.gov.cn/govweb/gzdt/2010-08/26/content_1688935.htm).
- [2] 刘夏,李国良,张灵峰,等.一种井下人员无线定位算法研究[J].工矿自动化,2020,46(4):38-45.  
LIU Xia, LI Guoliang, ZHANG Lingfeng, et al. Research on a wireless positioning algorithm for underground personnel[J]. Industry and Mine Automation, 2020, 46(4): 38-45.
- [3] 张吉同.基于人员定位-虹膜-矿灯的煤矿井下综合考勤系统[J].煤矿安全,2018,49(7):102-105.  
ZHANG Jitong. Coal mine underground comprehensive attendance system based on personnel location, iris and miner's lamp[J]. Safety in Coal Mines, 2018, 49(7): 102-105.
- [4] 陈晨.井下无线通讯及人员定位考勤系统的应用分析[J].中国机械,2014,12:188-189.  
CHEN Chen. Application analysis of underground

- wireless communication and personnel location and attendance system[J]. China Machinery, 2014, 12: 188-189.
- [5] 张立峰, 金业勇, 陈康, 等. 一种矿井定位设备的无线软件升级方法 [J]. 工矿自动化, 2019, 45(11): 14-18, 23.  
ZHANG Lifeng, JIN Yeyong, CHEN Kang, et al. Wireless software upgrade method for mine positioning equipments[J]. Industry and Mine Automation, 2019, 45(11): 14-18, 23.
- [6] 陈贤, 金业勇, 陈康. 一种矿用人员便携设备的无线程序升级方法 [J]. 煤矿安全, 2021, 52(3): 170-174.  
CHEN Xian, JIN Yeyong, CHEN Kang. A wireless program upgrade method for mine personnel portable equipment[J]. Safety in Coal Mines, 2021, 52(3) : 170-174.
- [7] 信金龙, 王超超, 刘少军, 等. 基于UWB通信的定位标签无线升级的研究与实现 [J]. 电子质量, 2021(8): 50-53.  
XIN Jinlong, WANG Chaochao, LIU Shaojun, et al. Research and implementation of wireless upgrade of positioning label based on UWB communication[J]. Electronics Quality, 2021(8): 50-53.
- [8] 黄飞龙, 谭晗凌, 陈冰怀. 基于无线分包传输的气象站固件无感升级方法 [J]. 计算机测量与控制, 2020, 28(1): 166-169, 174.  
HUANG Feilong, TAN Hanling, CHEN Binghuai. Non-feelable upgrade of automatic weather station based on wireless packet transmission[J]. Computer Measurement & Control, 2020, 28(1): 166-169, 174.
- [9] 彭亮, 沈安文, 张宁, 等. 基于无线IAP的工业嵌入式系统升级技术应用 [J]. 仪表技术与传感器, 2013(12): 36-38.  
PENG Liang, SHEN Anwen, ZHANG Ning, et al. Application of industrial embedded system upgrade technology based on wireless IAP[J]. Instrument Technique and Sensor, 2013(12): 36-38.
- [10] 刘世森. 基于UWB的矿井人员精准定位技术 [J]. 煤矿安全, 2019, 50(6): 118-120.  
LIU Shisen. Accurate positioning technology for mine workers based on UWB[J]. Safety in Coal Mines, 2019, 50(6): 118-120.
- [11] 霍振龙. 矿井定位技术现状和发展趋势 [J]. 工矿自动化, 2018, 44(2): 51-55.  
HUO Zhenlong. Status and development trend of mine positioning technology[J]. Industry and Mine Automation, 2018, 44(2): 51-55.
- [12] 张海军, 孙学成, 赵小虎, 等. 煤矿井下UWB人员定位系统研究 [J]. 工矿自动化, 2022, 48(2): 29-34, 41.  
ZHANG Haijun, SUN Xuecheng, ZHAO Xiaohu, et al. Research on UWB personnel positioning system in coal mine[J]. Industry and Mine Automation, 2022, 48(2): 29-34, 41.
- [13] 潘锋. 基于混合加密算法的测发控系统无线通讯加密研究 [J]. 自动化技术与应用, 2019, 38(11): 72-78.  
PAN Feng. Encryption research of wireless communication in missile launch control system based on hybrid algorithm[J]. Techniques of Automation and Applications, 2019, 38(11): 72-78.
- [14] 孙顺远, 赵亚亚. 基于AES算法的远程水质监控系统设计 [J]. 测控技术, 2019, 38(6): 59-63.  
SUN Shunyuan, ZHAO Yaya. Design of remote water quality monitoring system based on AES algorithm[J]. Measurement & Control Technology, 2019, 38(6) : 59-63.
- [15] 汪金龙, 曾艳阳, 侯桂云, 等. 低占空比无线传感器网络中节点自适应休眠机制 [J]. 沈阳工业大学学报, 2019, 41(4): 412-416.  
WANG Jinlong, ZENG Yanyang, HOU Guiyun, et al. A node self-adaptive sleeping mechanism in low-duty-cycle wireless sensor networks[J]. Journal of Shenyang University of Technology, 2019, 41(4): 412-416.
- [16] 李强, 陈登峰. 改进MD5加密算法在系统密码存储中的研究及应用 [J]. 信息记录材料, 2021, 22(10): 157-159.  
LI Qiang, CHEN Dengfeng. Research and application of improved MD5 encryption algorithm in system password storage[J]. Information Recording Materials, 2021, 22(10): 157-159.
- [17] 斯燕. 基于MD5算法的文件完整性检测系统分析及设计 [J]. 网络安全技术与应用, 2019(11): 36-38.  
JIN Yan. Analysis and design of file integrity detection system based on MD5 algorithm[J]. Network Security Technology & Application, 2019(11): 36-38.
- [18] 张长森, 李赓, 王筱超, 等. 基于RFID的矿井人员定位系统设计 [J]. 河南理工大学学报(自然科学版), 2009, 28(6): 742-746.  
ZHANG Changsen, LI Geng, WANG Xiaochao, et al. Design of personnel orientation system in mine based on RFID[J]. Journal of Henan Polytechnic University (Natural Science), 2009, 28(6): 742-746.
- [19] 张晋, 龙廉骏. 锦界煤矿中ZigBee人员定位系统的研究与应用 [J]. 煤矿机械, 2017, 38(9): 184-186.  
ZHANG Jin, LONG Lianjun. Research and application of ZigBee personnel positioning system in Jinjie Coal Mine[J]. Coal Mine Machinery, 2017, 38(9): 184-186.
- [20] 孙若凡, 冯勇华, 杨奇, 等. 一种帧长优化的动态时隙ALOHA算法 [J]. 光通信研究, 2017(1): 54-56.  
SUN Ruofan, FENG Yonghua, YANG Qi, et al. Frame size optimized dynamic framed slotted ALOHA algorithm[J]. Study on Optical Communications, 2017(1): 54-56.
- [21] 崔可嘉, 孙昕. 基于TDMA的无冲突动态时隙分配算法 [J]. 计算机工程, 2014, 40(10): 122-126.  
CUI Kejia, SUN Xin. Dynamic slot assignment algorithm of contention-avoid based on TDMA[J]. Computer Engineering, 2014, 40(10): 122-126.