International
Journal
Of Advanced Research in Engineering& Management (IJAREM)
ISSN: 2456-2033 || PP. 30-34

Radio Cheat Source Search and Localization System Design

Yang LIU[1], Meiling GAO[1]
**(School of Information Science & Electric Engineering, Shandong Jiaotong University, China)*

Abstract: With the continuous progress of society, the accelerate expansion of wireless communication technology. There are many lawless elements who use radio communication technology for examinations and cheating, which seriously affects social fairness and is aimed at the current radio cheat source monitoring vehicle antenna, etc. Due to the problem of high equipment price, the design of a search and positioning system for radio cheat sources based on signal strength was proposed. This dissertation designs a radio cheat source search and positioning system based on signal strength. The system is divided into detection end and data processing end. Among them, the detecting end is controlled by STM32F103 one-chip computer, is made up of radio receiving module, GPS module, GSM module, LCD liquid crystal display module; The data processing terminal is controlled by STC89C52 one-chip computer, make up by GSM and LCD liquid crystal display module. The detection terminal can realize the detection of the signal intensity in a specific frequency range, and calculate the distance from the detection terminal to the cheat source, and measure the GPS location information at the detection terminal, and send the GPS location and distance information to the data processing terminal; the data processing terminal it can realize the data sent by the receiving tester and calculate the cheat source GPS position through a specific algorithm. The test results show that the information detected by the modules and the positioning accuracy meet the requirements of the questions. Compared with the traditional radio monitoring vehicle equipment, the system is easy to use and inexpensive.

Keywords: GPS module, GSM module, Radio cheat source positioning, Radio receiver module

I. INTRODUCTION

Radio refers to electromagnetic waves propagating in free space. With the rapid development of radio communication technology, radio communication technology has a tremendous impact on people's lives[1]. The application fields of radio technology are also becoming more and more extensive, in broadcasting, radar, satellite. Device networks such as positioning, navigation, and mobile computers are widely used. However, many lawless elements use radio communication technology to make profits in various exam cheating. From English forty-six to postgraduate entrance examinations, from civil service examinations to national judicial examinations, the use of radio cheating has become increasingly rampant[2]. It is understood that there are two ways to cheat through the radio: First, the candidate sends the image of the test paper to the gunman outside the examination room through the micro camera, and then the gunman outside the examination room sends the answer to the candidate in the examination room by radio. Second, the gunman outside the examination room obtains the answer to the test paper through other means, and sends it directly to the candidates in the examination room by radio. The first type of cheating is relatively rare, so we directly analyze the second case. At present, the frequency of common sources of cheats in exams is mainly concentrated at 400-600MHz, and the low-frequency segment is also found at around 100-300MHz, but relatively few[3]. Moreover, the propagation distance of the radio is limited. In order to ensure the quality of information transmission, the cheaters generally hide in a residential building or hotel close to the test center.

In view of the above situation, most of the methods currently adopted in the examination room are equipped with multiple radio monitoring vehicles. Among them, radio monitoring vehicles are mainly equipped with radio scanners, direction finding antennas, etc. In addition to monitoring vehicles, fixed monitoring needs to be installed around them. Point, through these monitoring points can be used together with the monitoring vehicle to generally determine the direction of the source of radio cheats, the monitoring vehicle will continue to approach the source of cheating through the orientation, and then further positioning, and finally determine the final location of the source of cheating. The densely-equipped antenna in the radio monitoring vehicle can detect a large range of radio signals, and the antenna has a special array capable of judging the incident angle of the signal and the like, further determining the specific direction of the source of the cheating, and the positioning accuracy is high[4][5].

However, since the monitoring vehicle adopts the direction finding method based on the signal arrival angle, it is necessary to measure the incident angle of the signal, so the requirements for the antenna are relatively high and the price is relatively expensive. The design uses a signal strength-based direction finding method. This method does not have a particularly high requirement for the antenna, and does not require much hardware support. As long as the detection terminal has a radio receiving module, it is only required for a specific environment. Perform simple measurements to determine empirical values such as the attenuation factor of the signal, and obtain a more accurate positioning position by the corresponding algorithm[6].

Although domestic radio positioning technology has developed relatively late, it has developed very rapidly. Relatively well-known in these positioning systems are: WiFi or ZigBee-based positioning technology, ultra-wideband based positioning technology. Domestic positioning system applications are well-known: ZTE's CDMA mobile communication positioning technology, Kangbo's mobile positioning technology and Suzhou Industrial Park's WiFi-based real-time positioning system. In terms of the location of radio cheat sources, domestic radio monitoring vehicles are the main way to locate the source of cheating. This method generally uses the TOA-based direction finding method to complete the positioning by using the monitoring points or base stations arranged in advance. Function and determine the specific location by approximation search. In recent years, it has also been popularized throughout the country, but due to the relatively high price, the number of monitoring vehicles equipped at each test center is limited.

The research content of this subject is to find and locate the source of radio cheating. In view of the high price and complicated operation of the source of cheating source in the market, a radio cheating source localization method based on signal strength is proposed. The distance is calculated by the attenuation model of the signal. According to the distance calculated by the attenuation model and the corresponding coordinates of the device, three sets and three or more sets of data are used, and the coordinates of the source of cheating are calculated by the triangulation method. The overall system function is to detect the source of cheating in the illegal band and show the location of the source of cheating. This design mainly adopts STM32F103 and STC89C52 single-chip microcomputer which are low in price and can fully satisfy the system function as the main control chip of the detection end and the data processing end respectively. The coordinates are represented by GPS coordinates; the signal detection is realized by the wireless receiving mode; the display module is realized by the LCD liquid crystal screen. The interaction between the detection end and the data processing end data is implemented by the GSM module.

II. SYSTEM HARDWARE CIRCUIT DESIGN

The whole system is divided into a detection end and a data processing end. The function of the detection end is to collect relevant detection data required for positioning and send the data to the data processing end; the role of the data processing end is to receive data from the detection end and perform related calculations to obtain wireless cheating. The location of the source.

A. Detection circuit design

The frame of the detecting end is composed of a main control chip module, a wireless receiving module, a GPS positioning module, a GSM data transmitting module and an LCD display module. The main control chip is responsible for coordinating the transmission and reception of data of each module; the wireless receiving module is responsible for detecting the signal strength value of the specified frequency band in the surrounding environment, and transmitting the detection value to the main control chip; the GPS positioning module is responsible for detecting the GPS position of the current device, and The GPS position information is sent to the main control chip; the LCD display module is responsible for the detection value of each module and the distance value calculated by the main control chip; the GSM data transmission module transmits the received GPS position and the distance information to the value data processing end. The schematic diagram of the specific detection terminal circuit is shown in Figure 1. It includes the connection mode of each module and the single chip microcomputer and the crystal oscillator circuit.

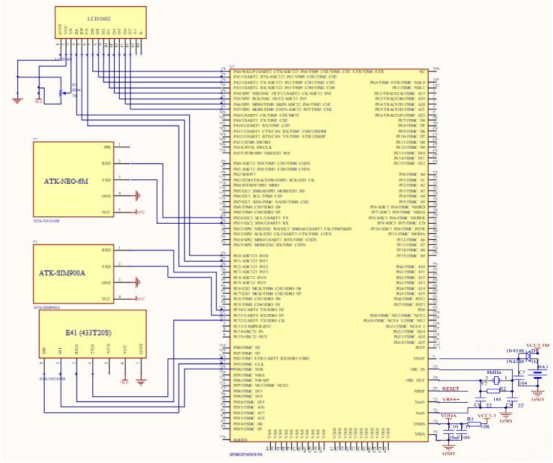

Figure 1 Detection terminal circuit schematic

B. Wireless transceiver module

The E41 (433T20S) module produced by the wireless receiving module of this design. The module is a radio communication module with a wireless transmit power of 100mW. In the case of the same frequency and co-channel, the module can detect the RSSI value of the nearby frequency. It and the MCU are connected through the serial port and operate at 425 MHz to 441 MHz. Between frequencies, compatible with 5V/3.3V microcontroller systems. The E41 (433T20S) is connected to the UART5 (PC12, PD2) pins of the STM32F103 through the serial port. The baud rate used is 9600.

C. ATK-NEO-6M module

The ATK-NEO-6M is connected to the USART3 (PB10, PB11) of the single-chip microcomputer through the serial port. The baud rate is 9600. It mainly realizes the position of the current detection terminal. Due to the slow positioning speed of the built-in ceramic antenna, I pass the SMA. An external antenna is connected to the interface to speed up the positioning of the module. The module has a working status indicator (PPS). When (PPS) is always on, it indicates that the module has been powered but has not been successfully located. When the module indicator changes from steady on to blink (900ms on for 100ms), the module has been successfully positioned. After the positioning is successful, the module outputs the positioning information through the serial port (UART). The protocol for outputting data is NME-0183 and the control protocol is UBX. There are 7 different command data formats: $GPGGA (GPS Positioning Information), $GPGSA (current satellite information), $GPGSV (visible satellite number), $GPRMC (recommended positioning information), $GPVTG (ground speed information) , $GPGLL (Target Geographic Information), $GPZDA (current time information). According to the needs of the system, the $GPRMC data format (including UTCS time, positioning state, latitude and longitude, ground rate, magnetic declination, etc.) is selected for analysis.

D. Data processing terminal circuit design

The framework of the data processing end is composed of a main control chip module, a GSM module and an LCD screen display module. The main control chip is responsible for processing and processing the data received by the GSM and calculating the location of the source of the cheat, the GSM module receives the data of the detection end; and the LCD displays the calculated GPS coordinates. The single-chip microcomputer used in the data processing end of the design is an upgraded version of the STC89C51, which can arbitrarily select the clock cycle and is fully compatible with the instruction system of the 80C51. The reason for choosing this chip is mainly because the data processing terminal is mainly responsible for data calculation, and does not need to externally connect many modules. Therefore, the serial port, SPI and other resources are less needed, only one serial port is needed, and only one serial port of the single chip microcomputer can fully satisfy the present. The system data processing side needs, so choose this microcontroller.

III. SYSTEM SOFTWARE DESIGN

The programming language of this design is C language. According to the functional requirements of the RSSI-based cheat source location system, the program detection end and the data processing end are respectively written. The detection end uses the STM32 library function to write. The advantage of using the library function is that Users need to consult the manual to configure the corresponding function registers. For example, the configuration LED needs to find the clock register first, then find the clock that needs to be enabled for the corresponding pin, and then complete the initialization through frequent shift operations, but the library function can Directly through the provided function to directly enable the clock of a certain set of pins, does not require frequent shift operations, so that the efficiency of the user to write the program is greatly improved, so I chose to use the library function to write the program; the data processing end is used The STC89C52, there is no library function similar to STM32, so it is written by configuring the register.

A. Detection program design

The detection end is mainly responsible for the data collection and transmission. The data to be collected has the GPS position of the monitoring end, the distance of the source of the cheating source from the detection end, and then the data is sent to the data processing end in a defined format.

In the ATK-NEO-6M module, the main purpose is to analyze the position information sent by the GPS. The GPS information is sent by the serial port 3. The data is continuously sent to the STM32F103 through the serial port. The program is mainly for GPS data. Initialization, reception, data analysis, and LCD position display.

In the SIM900A module, the module sends information to the data receiving end mainly through the module. First, the parameters of the module, such as the short message text mode, the character set, and the destination mobile phone number to be sent, are set first. The specific step is to receive the button. The interrupt first collects the received data and sends the data in a pre-defined format.

B. Data processing program design

The data receiving end is mainly responsible for receiving the information of the detecting end, and parsing the latitude and longitude and the distance information, thereby calculating the GPS coordinates of the source of the cheating, and displaying it on the LCD 1602.

The SIM900A module of the data processing terminal is mainly responsible for receiving the data of the detection end. Initially, the module needs to be initialized. A serial array of characters is used in the serial port interrupt receiving function to store each character received by the serial port interrupt, when the array space occupies When full, the received data will be overwritten by the previous data from the array header.

IV. SYSTEM TESTING AND VERIFICATION

The compiling software used in the design detection end is Keil 5, and the wireless receiving module, GPS module, GSM module and LCD liquid crystal display module are programmed through the library function of STM32.

During the serial assistant debugging process, when the wireless RSSI value is queried, the C5+C5+C5 hex command module is not responded. Since the three hexadecimal number transmission interval is too long, the module does not recognize the instruction, and the module returns the correct result after three hexadecimal numbers are continuously sent. During the debugging process, the serial port cannot receive the module information, and there is a problem with the timer setting of the serial port interrupt. As a result, the flag of the received message is not set, and the data can be received normally after changing the timer time.

During the serial assistant debugging process, the information cannot be sent after the command is sent. Since the information content ends with 0x1A after the module transmits the information content, the problem is solved after the addition. During program debugging, the module returned information that did not match expectations. Since the program does not recognize the module when the program is sent without the carriage return, the correct information cannot be returned, and it is restored after adding \r\n.

During the serial assistant debugging process, the screen data is garbled. Due to a problem with the data pin connection of the hardware pins, the final connection is a problem. During hardware debugging, the screen is darker and you can't see the characters. Since the screen contrast pin is grounded, the screen can be clearly displayed by adjusting the contrast pin to an external potentiometer.

The overall debugging of the physical end of the detection end is shown in Figure 2.

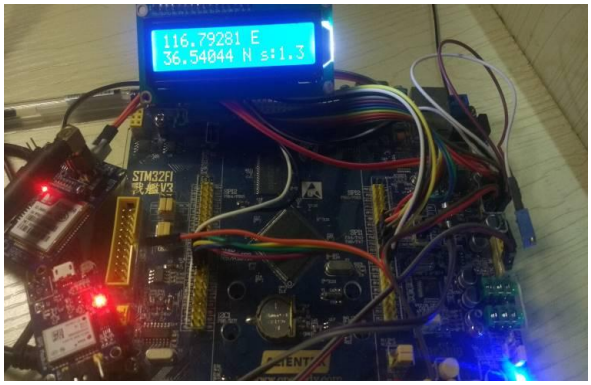

Figure 2 Detection side physical map

V. CONCLUSION

The search and positioning design of the radio cheat source studied in this design is based on the RSSI positioning principle. The whole system is low in cost and easy to use. Compared with the radio monitoring vehicle used in the current test site, the radio monitoring vehicle overcomes the disadvantages of high price and complicated functions.

This thesis designs a radio jamming source location system based on RSSI. The system is divided into detection terminal and data processing terminal. The detection terminal is controlled by STM32F103 single-chip microcomputer, and is composed of wireless receiving module, GPS module, GSM module and LCD liquid crystal display module. The utility model has the function of detecting the suspected source distance in real time, and can transmit the GPS position of the detecting end and the distance information to the data processing and processing end; the data processing end is composed of the GSM module and the LCD display module, and is mainly used for receiving the detection end data and processing. Then calculate the location of the source of the cheat and display it on the LCD. The overall system constitutes a positioning function for the source of cheating. According to the measurement results, the positioning accuracy of the system meets the accuracy requirements of the design, and the functions required by the problem are completed. It is a radio cheat source positioning system with simple operation and low price. Therefore, the system is easy to popularize, and the market has broad application prospects.

REFERENCES

[1] Fang H, Xu L, Xiao L. Secure routing and resource allocation based on game theory in cooperative cognitive radio networks [J]. *Concurrency and Computation: Practice and Experience, 28(10)*, 2016: 2958-2977.

[2] Haldorai A, Kandaswamy U. Secure Distributed Spectrum Sensing in Cognitive Radio Networks [M]// *Proc. Intelligent Spectrum Handovers in Cognitive Radio Networks*. Springer, Cham, 2019: 175-191.

[3] Liu J, Xiao L, Liu G, et al. Active authentication with reinforcement learning based on ambient radio signals[J]. *Multimedia Tools and Applications, 76(3)*, 2017: 3979-3998.

[4] Sinnreich A, Wikstrom P, DeFillippi R. Slicing the pie: The search for an equitable recorded music economy [J]. *Business Innovation and Disruption in the Music Industry*, 2016: 153-74.

[5] Cecconi B, Pruvot A, Lamy L, et al. Refurbishing Voyager 1 & 2 Planetary Radio Astronomy (PRA) data[J]. *arXiv preprint arXiv:1710.10471*, 2017.

[6] Posen H E, Keil T, Kim S, et al. Renewing research on problemistic search-A review and research agenda[J]. *Academy of Management Annals, 12(1)*, 2018: 208-251.