The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 4 || Pages || PP.83-87 || 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Control of aircraft from the base station using eog siganl transmission

[1,] L.Tamizhanban, [2,] E.Sivakumar
Embedded system technology, SRM University, Chennai, India
Assistant professor, Department of ECE, SRM University, Chennai, India

ABSTRACT
This paper proposes a system that can prevent the airplane from hijack just by sensing the IR signal from the pilot eye. The remote station which monitors the airplane will take the necessary steps like operating the flight. The EOG and IR sensor is connected to the pilot. Under normal condition the pilot can control the robot (Flight). Incase of a hijack the pilot sends the signal through the EOG and IR sensors.The microcontroller detects the input from the person using IR sensor. The microcontroller sends a digital signal which is encoded and is transmitted through a Zig-bee transmitter to the remote control station. The remote station receives the message through a Zig-bee receiver, the encoded signal is decoded and view and control through PC. Then the remote station takes the control of the airplane and lands it safely to the nearest airport.

KEY WORDS *– EOG sensor, Zig-bee, IR sensor, VB application*

Date of Submission: 26-March-2015 Date of Accepted: 15-April-2015

I. INTRODUCTIION

Aerial terrorism is gradually emerging as a potent form of terrorism capable of causing significant damage to human life and infrastructure. Aircrafts and UAVs can be easily used as guided missiles to target key locations and installations and more importantly, to communicate a political message. Dealing with such threats can be difficult as it becomes complicated to fully understand the nature and scope of unconventional acts of terrorism. There is a need to frame mechanism to assess such threats and prepare suitable responses to pre-empt the likelihood of such terror incidents.The timeline of airline security measures going back several decades shows that security has adapted to threats as they arose. But while the terrorist threat has changed over time, checkpoint security has not always kept pace and passengers have become passive subjects in the process rather than active, engaged partners.

This paper presents a basic framework of a possible mechanism that could be incorporated on the dashboard which communicates with the pilot wirelessly. The system could avoid the intervention of the hijacker as far as possible since the pilot sends the emergency signal from the bio-signal of the user [4] to the base station with less physical movements.

II. LITERARURE SURVEY

A method and system for preventing airplane hijacking provides for isolating the pilot and the cockpit from the passenger cabin of the airplane while nevertheless maintaining the necessary communication there between for assuring safety of the passengers and the airplane[2]. Physical access between the cabin and the passenger compartment is restricted by a door which can be opened only from the cockpit. Communication from the cabin to the cockpit is afforded exclusively by an electrical signalling system affording communication only of predetermined messages, specifically excluding any indication of hijacking attempts. The pilot's primary response to any emergency signalling indication is to land at the nearest airport. By assuring that all passengers are warned in advance of the installation in a plane of the system of the invention.

Aircraft have transponders[1] to assist in identifying them on air traffic control radar; and collision avoidance systems have been developed to use transponder transmissions as a means of detecting aircraft at risk of colliding with each other's) units use the term "squawk" when they are assigning an aircraft a transponder code, *e.g.*, "Squawk 7421". Squawk thus can be said to mean "select transponder code" or "squawking" to mean "I have selected transponder code xxxx"

Some potential changes to the aircraft themselves include [3]:

1. Cockpit and cabin cameras: The Federal Aviation Administration (FAA) has advocated adding video cameras to the cockpit for several years. It may also be possible to downlink these camera feeds to the ground in case of trouble allowing air traffic controllers to see who is at the controls in a hijacking attempt. In addition, cameras in the cabin would seem to be a wise addition allowing the pilots to monitor any strange behavior among the passengers.

2. Change to the FDR, CVR, and transponder: One of the clever moves made by the hijacking pilots on at least some of the aircraft was to remove the circuit breakers for the transponders. By removing the circuit breakers, these transponders were disabled and the ground controllers had greater difficulty tracking the aircraft. It has been hypothesized that the hijackers may have also disabled the Flight Data Recorder (FDR) and Cockpit Voice Recorder (CVR) in the same manner. Such an action would make it more difficult for investigators to piece together how the hijackers did what they did.

3. Impenetrable cockpit doors: Several airlines that have been subjected to repeated hijackings in the past, such as Israel's El Al, already fit thick armored cockpit doors to their planes that make it very difficult for an intruder to gain access.

4. A final interesting idea is to equip planes in flight with the ability to be flown using real-time flight simulators on the ground. If control of an aircraft is taken over by a hijacker pilot, pilots on the ground could then override his ability to fly the plane.

5. Another idea that has been tossed around is adding a system allowing the pilots to fill the passenger cabin with gas that would put all the passengers to sleep, including the terrorists, in an emergency. Although such a system would completely disable the hijackers until the plane was able to land, the gas could be circumvented simply by wearing a mask. Pilots and flight attendants are already equipped with gas masks.

III. REQUIRED COMPONENTS

A. IR Sensor

Infrared radiation exists in the electromagnetic spectrum at a wavelength that is longer than visible light. It cannot be seen but it can be detected. Objects that generate heat also generate infrared radiation and those objects include animals and the human body whose radiation is strongest at a wavelength of 9.4um. Infrared in this range will not pass through many types of material that pass visible light such as ordinary window glass and plastic. However it will pass through, with some attenuation, material that is opaque to visible light such as germanium and silicon. An unprocessed silicon wafer makes a good IR window in a weather-proof enclosure for outdoor use. It also provides additional filtering for light in the visible range. 9.4um infrared will also pass through polyethylene which is usually used to make Fresnel lenses to focus the infrared onto sensor elements.

B. EOG sensor

Electrooculogramamplifier amplifies corneal-retinal potential; the amplifier monitors the DC potential on the skin surrounding the eyes, which is proportional to the degree of eye movement in any direction. This potential difference creates an electric field around the eyeball; the orientation of this field changes during eye movements. The potential difference can be registered with electrodes placed around the eye and examined after appropriate amplification. Horizontal eye movements can be recorded with electrodes placed on the temples, while vertical movements with electrodes placed below and above the eyes. Reference electrodes are usually placed on the middle of the front or on the earlobes. This method allows the recording of eye movements up to $\pm 70^{o}$ (0^{o} corresponds to the direction straight ahead, while $\pm 90^{o}$ to the maximal horizontal or vertical deviation).Amplifier output can be switched between normal EOG output and Derivative of EOG. In derivative mode the amplifier outputs the measured velocity of the eye movement which is useful for saccade and nystagmus investigations. The amplifier permits DC coupling to electrodes for X/Y graphing of eye movements without discernible decay.

C. Zig-bee

ZigBee is an established set of specifications for wireless personal area networking (WPAN), i.e. digital radio connections between computers and related devices. WPAN Low Rate or ZigBee provides specifications for devices that have low data rates, consume very low power and are thus characterized by long battery life. ZigBee makes possible completely networked homes where all devices are able to communicate and be controlled by a single unit. There are three different ZigBee device types that operate on these layers in any self-organizing application network. These devices have 64-bit IEEE addresses, with option to enable shorter addresses to reduce packet size, and work in either of two addressing modes – star and peer-to-peer.

IV. EXPERIMENTAL WORK

A proto type for the system proposed is implemented using a microcontroller Robot model in the Place of the aircraft. The EOG sensor and IR sensor play a vital role for the detection of Hijack .under normal conditions, the IR sensor senses whether the eye is open. The pilot will now be able to controls that aircraft either through controls that are present on the cockpit of the Aircraft by moving the eyes, which is sensed by the EOG sensor.

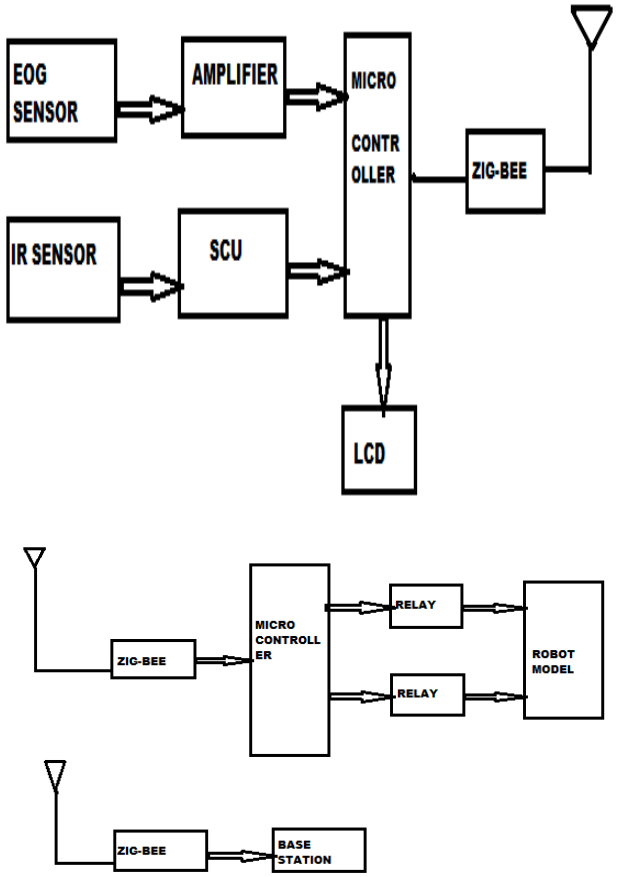

Fig. 1 Block diagram of the proposed system

This value from the EOG sensor is converted into an approximate value and the value is digitized by the PIC microcontroller. Corresponding to the variation in the ADC value the robot model moves. When the pilot controls the aircraft, the controls are transferred wirelessly across the zig-bee interface. The microcontroller that is present at the robotic end receives the signal and decodes the movement to the motor accordingly. As long as there is no hijack movement of the robot is controlled by the pilot.In the case of hijack the pilot tries to send the hijack/ emergency .For example ,say, the pilot closes the eye for particular seconds the sensor doesn't receive any signal and so the ADC value is read to be abnormal. In such a case, base station continuously monitors the signal from the aircraft. When the remote station enters an abnormal signal, the control of the aircraft is cut off from the pilot's end, and the movement of the aircraft is controlled from the remote station. The aircraft can be made to land at the nearest airport.

V. RESULTS AND DISCUSSION:

The experiment was carried out with the initial step in the Proteus simulation software. The ADC value that is digitized at the pilot's end is sent across the virtual terminal and checked whether an abnormal signal is detected at the remote station. (Fig. 2)

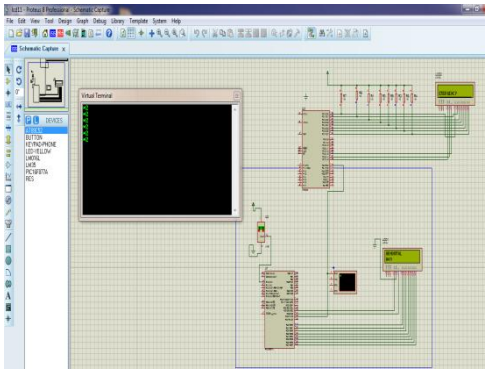

Fig.2 Proteus simulation

A VB application is developed for controlling the aircraft from the base station (Fig.3). The transceiver is connected to the COMPORT and the port number is specified in the form. From then the aircraft monitored. Under normal conditions, the status tab in the form displays "NORMAL". When the abnormal signal is received the status tab displays "ABNORMAL" (Fig.4).

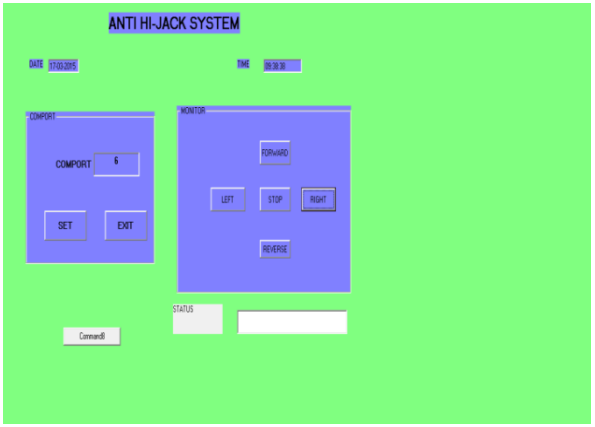

Fig.3 VB application

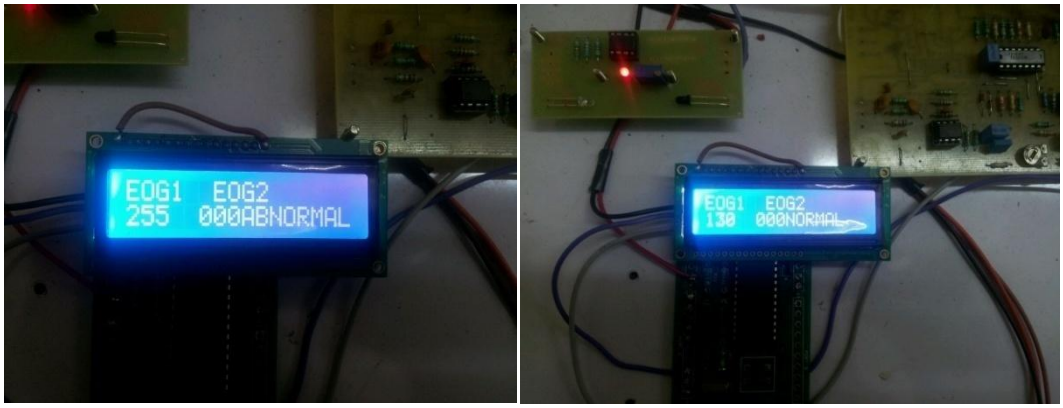

Fig.4 Normal and abnormal signal detection at the base station

Fig.5 control signals from the base station

From then the control of the aircraft is transferred to the base station. The corresponding movements are seen of the LCD display at the base station. (Fig.5)

CONCLUSION

Cockpit doors on most commercial airliners have been strengthened and are now bullet resistant. Airport security plays a major role in preventing hijackers. Screening passengers with metal detectors and luggage with x-ray machines helps prevent weapons from being taken on to an aircraft. In the United Kingdom, United States, Canada, Australia, Austria, theNetherlands and air marshals have also been added to some flights to deter and thwart hijackers. With technological advancements a transceiver to send a signal of 72MHz signal to the base station is installed onto the dash board of the aircraft. Still hijacking does happen, since the hijackers are alert before the pilot pushes the dash board button. But this proposed model could efficiently transmit the signal to the base station with less attention to the hijackers thereby increasing the security.

REFERENCES

[1] http://politicalscience.osu.edu/faculty/jmueller/stewarr2.pdf
[2] Ord Michael, us patent, US3704845 A
[3] http://www.911myths.com/images/c/c0/3610_01.pdf
[4] Liang-Hung Wang, *Member, IEEE,* Tsung-Yen Chen, Kuang-Hao Lin, *Member, IEEE, Qiang Fang, Member, IEEE,"* Implementation of a Wireless ECG Acquisition SoC for IEEE 802.15.4 (ZigBee) Applications*",* IEEE Journal of Biomedical and Health Informatics.
[5] Guoxing Zhan and Weisong Shi, Senior Member, IEEE," LOBOT: Low-Cost, Self-Contained Localization of Small-Sized Ground Robotic Vehicles", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 4, APRIL 2013.
[6] Ana Corrales, Maria Malfaz, and Miguel A. Salichs, *Member, IEEE,"* Signage system for the navigation of autonomous robots in indoor environments*".*
[7] A. Huang, C. Chen, K. Bian, X. Duan, M. Chen, H. Gao, C. Meng, Q. Zheng, Y. Zhang, B. Jiao and L .Xie, "WE-CARE: An Intelligent Mobile Telecardiology System to Enable mHealth Applications," *IEEE J. of Biomed. and Health Inf.*, vol. 18, no. 2, pp. 693-702, Mar. 2014.