International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Design and Implementation of Security Device with Dual Wireless Communication Interface for Cloud-based Framework

José Luis Mela, Edwin Cedeño Herrera, Gloris Batista Mendoza

Abstract: ***This research work is aimed at developing a low-cost security device for intrusion remote sensing, and sends alert notifications to a cloud platform. This device is basically composed of a passive infrared sensor (PIR), an MCU ESP32 microcontroller with integrated Wi-Fi interface and a SIM800L GSM modem. The proposed device incorporates fault tolerance in communication links, integrating dual wireless communication technologies, to guarantee the sending of alerts to the cloud-based framework. The algorithm that has been designed for the microcontroller are enriched with intelligence to detect when a communication service is available or not, and choice best option between the interfaces. Moreover, the device is able to notify alerts via SMS directly to the user's mobile. This solution has proven to be effective not only in the field of security, but it also has applications in scenarios where nodes are required to acquire information from remote sites via telemetry, with guarantees on information delivery.***

Keywords: Security device, communication interface, cloud platform.

I. INTRODUCTION

Today there are a variety of security devices that can be purchased at a commercial premise. However, the cost of these is a bit high, without considering the incorporation to fault tolerance in the data communication links and redundancy in the notification channels of security alerts. Also, if these integrate support or alternation to continue operating against losses in the electrical fluid. In this sense, a search of works related to this has been carried out, where safety devices have been found that implement different Arduino microcontroller technologies, however, they leave several aspects that are essential in the effective and efficient operation of a security system. Therefore, this study presents a low-cost security device. This research differs from those proposed by other authors, since it incorporates being fault-tolerant in communication links to the cloud platform, Open Energy Monitor, using dual wireless communication technology, thus guaranteeing the sending of the alerts to the cloud, addition, be sends an SMS directly the user's mobile when an alert is detected.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
José Luis Mela, Licenciatura en Ingeniería Informática, Universidad de Panamá,
Edwin Cedeño Herrera, Ph.D.*, Profesor, Facultdad de Informática, Electrónica y Comunicación, Universidad de Panamá,
Gloris Batista Mendoza, Profesora, Facultad de Informática, Electrónica y Comunicación, Universidad de Panamá,

II. LITERATURE REVIEW

In the study of [1], they develop an intelligent security device, making use of a passive infrared sensor for the detection of human movements, an Arduino Mega to control the system, a NodeMCU ESP8266 to control the home, such as doors, lamps and garage, and a GSM modem for sending SMS. However, in the study of [2], they make use of Zigbee to create a wireless network of sensors, using the PIR sensor to detect movement, implementing an ESP8266 module for sending data to a server, and a GSM modem to send alerts of user texts.

In the design and implementation of a low-cost Arduino-based smart home system proposed by [3], an Arduino Mega 2560 is used to control the system, where it is responsible for monitoring gas leaks, lighting and smoke detection, among other variables. Said system is controlled manually employing switches or automatically, using a voice recognition system.

This article differs from those previously presented in that a dual communication interface (Wi-Fi/GSM) is used to send the detected alerts to the cloud platform. Moreover, it includes sending SMS directly to the user, regardless of which communication interface is used to send the security alert to the cloud framework.

III. METHODOLOGY

A. Identification of Non-Functional Requirements

The components, both hardware, and software to develop this device are:

1. NodeMCU ESP32 Wireless Arduino.
2. GSM Module SIM800L.
3. PIR Sensor.
4. Cables Jumper.
5. Protoboard.
6. Framework Cloud (Open Energy Monitor).
7. IDE Arduino.
8. Microsoft Visio.

B. Security Device Design

The design of the security device is based on two communication interface: Wi-Fi and GSM, as shown in Fig. 1.

This device has a PIR detection sensor, which is responsible for detecting movements within a range up to seven meters [4], [5]. The ESP32 microcontroller is responsible for executing the instructions and performing the necessary orders when the device detects a movement.

The scenario used to implement this device is an office, where it has to be located in a strategic place since the PIR sensor has a vision cone of approximately 95º to 110º [6].

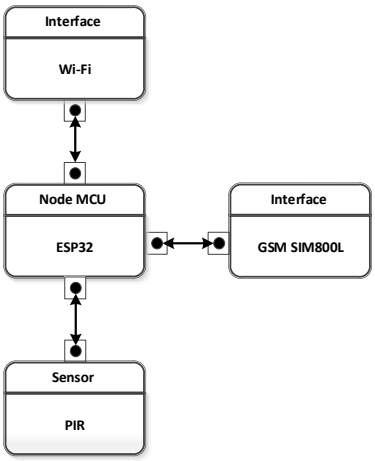

Fig. 1.Security Device Design.

The proposed security device incorporates fault tolerance in the links to the cloud platform, integrating two data communication interfaces. We present the algorithm: CSC: Communication Service Choice (Fig. 2), where you can observe the functionality of the security device as soon as an intrusion is detected, the security device is smart enough to switch between one interface and the other to send the alert to the cloud platform.

This algorithm aims to determine the communication service available to send the data, therefore the sending is agnostic to the communication service or outgoing interface. This has been designed considering that the preferred service is Wi-Fi, this has been defined for economic reasons, because GSM network services are more expensive. We assume that the devices will have an Access Point (AP) within reach and have authentication credentials. The GSM module (SIM800L) is turned off by default, due to the policy of using the Wi-Fi service by default, and will only be used on demand. Another important element that we assume is a cloud based Framework, which listens to the sending of the data.

The CSC Algorithm is executed every time the sensor detects an intrusion event (E_i), in this case the signal S is set high. A call to the sendSMS function (2) is made directly through the GSM network, which is always supposed to be available, to send a text message to the mobile phone of the guard associated to the security device, using the msg parameter. A call to PowerOff is used to turn off the GSM module (5), if it is on. Subsequently, the algorithm determines if the default service is available, calling the ConnectWifi function (4). If the result of this call is true, the notification of the alert has been sent and then makes a second call (7) to put the system in the initial state, assigning Low to S (6). In case the Wi-Fi service is not available (8), the GSM module is activated by PowerOn (9), and a call is made to ConnectGSM (10), which will try to send the information of the detected alert, if the response is correct, then proceed to make a second call (12) to put the system in initial state, assigning Low to S (11). The algorithm will keep trying to send the alert, permanently until it manages to send it through one of the interfaces.

Algorithm CSC: Communication Service Choice

```
1: ∀ E_i | E_i ∈ {Intrusion Events}
2: sendSMS(msg)
3: do
4:   if (ConnectWifi() = true)
5:     GsmModule(PowerOff)
6:     S ← Low
7:     call ConnectWifi()
8:   else
9:     GsmModule(PowerOn)
10:    if (ConnectGsm() = true)
11:      S ← Low
12:      call ConnectGsm()
13:    endif
14:  endif
15: while ((ConnectGsm() = false) ∧
          (ConnectWifi() = false))

16: Function ConnectWifi()
17:  attempt ← 0
18:  do
19:    Wifi.begin(ssid, password)
20:    db ← Wifi.Rssi()
21:    add 1 to attempt
22:  while (db = 0 ∧ attempt < K)
23:  if (¬ db = 0)
24:    if (Wifi.status() = CONNECTED)
25:      client.connect(server_ip, port)
26:      if (client.connected() = true)
27:        Sendata()
28:        client.stop()
29:        Wifi.disconnect()
30:        return true
31:      else
32:        return false
33:      endif
34:    else
35:      return false
36:    endif
37:  else
38:    return false
39:  endif
40: return false
```

Fig. 2.Communication Service Choice.

The call to the ConnectWifi function will attempt to link to the AP in its range (19), K times. Considering that this link may take a few seconds, especially if the AP is in the process of initialization, the value of K should cover these cases. The algorithm will attempt to poll (K times) on the signal power in decibels (dB - represented in the algorithm as db) (20), when it is zero we assume that it is turnoff or out of range. The algorithm repeats these instructions until K, or until db is nonzero (22). In the case of terminating the K attempts, it is not possible to connect the function will return false (35). On the contrary (23), if it is connected to the AP (24), the algorithm will try to connect to the Framework in the cloud (25), to send the data. Once the data has been sent (27), the algorithm disconnects from the server, closes the TCP connection (28) and disconnects from the Wi-Fi service (29) and returns true. This is done because TCP connections have their time out to close the connection in case not using it. Additionally, we are in a scenario where events are discrete, so we cannot maintain end-to-end connections permanently.

The SIM800L module, as far as we have researched and tested, does not have a complete library that provides support for the functionality of the proposed device. Therefore, the ConnectGSM function is developed based on low level commands. The implementation of this function has been based on commands in AT, because it has provided better results.

C. Wi-Fi Interface Based Operation

In Fig. 3, an flowchart of the security device is presented using the microcontroller with integrated Wi-Fi interface, where, after detecting an alert, we proceed to connect to the Wi-Fi network, providing a connection attempt number, therefore, if it fails to establish a connection with Wi-Fi, then the device is intelligent enough to switch to the other communication interface (Fig. 4), that is, the security device has software level intelligence to switch between one communication interface and the other.

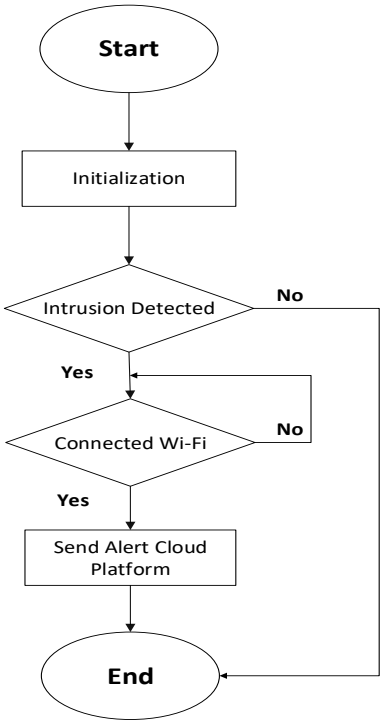

Fig. 3.ESP32 Wi-Fi connection flowchart.

If the device manages to connect to the Wi-Fi network, the alert is sent to the cloud platform, otherwise, if in three attempts it fails to connect, a message is sent indicating that the Wi-Fi connection has failed and how it been mentioned, we proceed to make use of the GSM modem.

D. Operation Based on GSM-SIM800L

The GSM SIM800l modem is used to send intrusion alerts that the security device detects for the case when the connection to the Wi-Fi network fails. In addition, it is used for sending SMS (Short Message Service) directly to the cell phone number defined in the software module of the security device. In the flowchart (Fig. 4), is presented functionality general way when an event is detected and sent to the cloud platform, using the GSM modem.

This module is used, in addition to Wi-Fi, so that the device is fault-tolerant in the communication links to the cloud. Therefore, this ensures that these alerts are sent, either by one interface or the other.

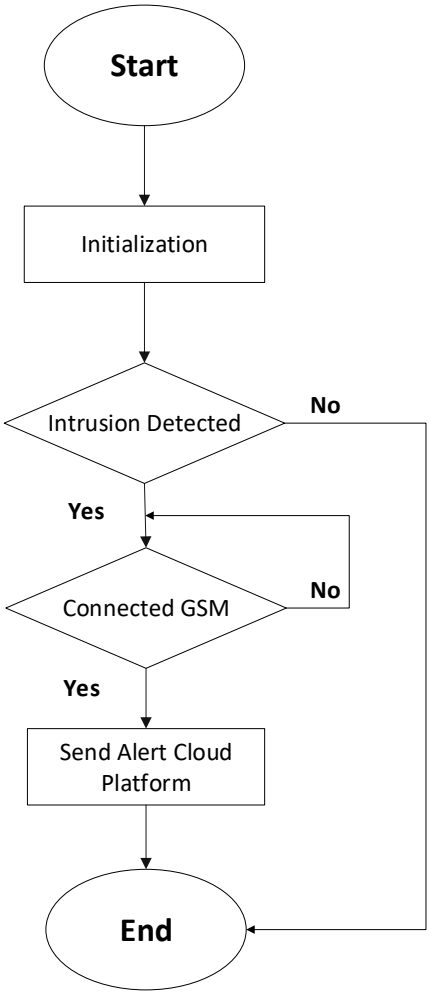

Fig. 4.GSM SIM800L connection flowchart.

IV. RESULTS AND DISCUSSION

A. General Scenario Validation

The security device is based on dual wireless communication interface (Wi-Fi/GSM) to establish links and send alerts to the cloud platform and a passive infrared sensor for motion detection.

Before continuing, it is necessary to mention that, to carry out the implementation of the proposed security device, a router of the brand TP-LINK, model TL-WR741ND has been used to create a wireless access point, to connect the microcontroller ESP32 with interface Wi-Fi integrated and for the GSM SIM800L modem a plan has been acquired that includes voice and data.

Once we have connection to the access point and acquired a plan of data, be proceed to implement the security device in offices, where its location has been strategically, since must have scope and cone of vision necessary for detection of movements.

The device works so that, when the sensor detects a movement within his detection range, the security device sends the alert to the cloud platform via Wi-Fi, due this interface has been set as the default for sending of alerts to the cloud framework, but, when an event is detected and no link to the cloud is achieved through Wi-Fi, then the GSM SIM800L modem is used to send these alerts to the cloud platform, using the GPRS network (General Packet Service Via Radio). Regardless of the interface used to send alerts to the cloud, an SMS will always be sent directly to the user's mobile, through GSM.

Further, the security device has been designed to continue operating in cases of loss or failure in the power supply. An external rechargeable battery source is used for this (Power Bank).

B. Proof of Concept with Wi-Fi ESP32

At the software level the Wi-Fi interface, be has been defined as default for sending alerts detected by the security device. Its functionality is that every time an event is detected, the device establishes a link to the wireless access point, for that east provide an IP address and then the alert can be sent to the cloud (Fig. 5), otherwise, modem is used then GSM (Fig. 6).

```
Sin Evento

Sin Evento

Sin Evento

Sin Evento
1

Evento Detectado

Intento de Conexión
Potencia de señal: -30
Intento # : 1
Conectado a Wifi

IP:
192.168.0.104


 Enviando ...
1
Envio Completo

 Enviando ...
0
Envio Completo
Desconectado ...
```

Fig. 5.Event detected and sending alert to the cloud over Wi-Fi.

C. Proof of Concept with GSM SIM800L

As said before, the device incorporates a GSM modem for the case when it is not possible to establish a link with the cloud via Wi-Fi. In this sense you can see in Fig. 6, that the security device detects an event, then tries to connect to the wireless access point, since the Wi-Fi interface has been defined by default for sending alerts to the cloud, but fails to establish connection and shows the message that has failed, therefore, the GSM modem starts.It should be noted that the alternative of the use of the GSM modem, is used for the case when there is a loss in the power supply, this means that if there is no light, there is no connection to the wireless access point. Therefore, the GSM modem is started (Fig. 6), then connection to the cloud is established and the alert is sent to the platform, using GSM trough the GPRS, but first a link is established with the cloud platform server (Fig. 7).

```
Sin Evento

Sin Evento
1

Evento Detectado

Intento de Conexión
Potencia de señal: 0
Intento # : 1
Intento de Conexión
Potencia de señal: 0
Intento # : 2
Intento de Conexión
Potencia de señal: 0
Intento # : 3
Intento de Conexión a Wifi Falló !!!

Encendiendo Modulo GSM...

AT
OK
Conectando...
```

Fig. 6.Failed Wi-Fi connection attempts.

```
Intento de conexion al Servidor ....

AT+CIPSTART="TCP","162.243.87.153","80"
OK

CONNECT OK
AT+CIPSEND=155
>
GET http://162.243.87.153/input/post.json?node=1&json={Alerta:5}
HTTP/1.1
Host:emoncms.org
Connection: close



SEND OK
AT+CIPCLOSE
CLOSE OK

Conectando...
AT+CGATT=1
OK
Conectado !!!
Intento de conexion al Servidor ....

AT+CIPSTART="TCP","162.243.87.153","80"
OK

CONNECT OK
AT+CIPSEND=155
>
GET http://162.243.87.153/input/post.json?node=1&json={Alerta:0}
HTTP/1.1
Host:emoncms.org
Connection: close
```

Fig. 7.Sending alert to the cloud over GSM SIM800L.

As mentioned in the validation part of the security device scenario, east allows sending SMS directly to the user's mobile without using the cloud platform and regardless of the interface used to send alerts to the cloud.

This process is presented in Fig. 8, where first the device detects the event, then the GSM modem is turned on, later be the text mode is established, using AT commands, be the phone number to which the SMS is sent is added and Finally, the content of the message.

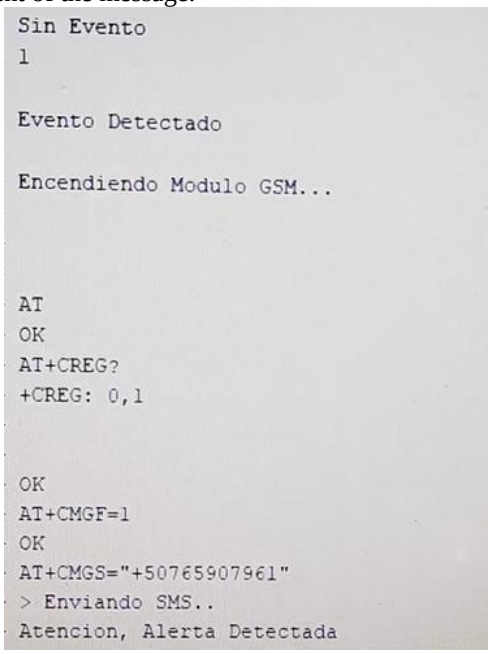

Fig. 8.Send SMS.

D. Performance test

For performance tests performed to the security device, the bandwidth of the Internet that is being used for the connection to the Wi-Fi wireless network (Access Point) must be taken into account. Therefore, these tests include timing of the time from when the sensor is activated when it detects a movement until the event is reflected or published on the cloud platform. Table I summarizes the data of the three tests performed. In Fig. 9, it can be seen that the average time it takes to send alerts to the cloud platform trough Wi-Fi is 4.0 seconds, while with GSM it takes approximately 10.35 seconds and SMS around 31.96 seconds, this means that the fastest interface or that takes less time to send alerts to the cloud framework is Wi-Fi, however, we must highlight that the device takes less than a minute to deploy the alert in the cloud platform and send the SMS.

In these times obtained we must consider the bandwidth of the Internet users and the delay that the cloud platform has to update the data when they are published or reflected in it.

V. CONCLUSIONS

The proposed security device guarantees continuity of detection, even if you do not have an access point available.

The guarantee is offered in sending security alerts to the cloud platform, commuting between one communication interface and the other (fault tolerance Wi-Fi/GSM).

The fastest interface for sending alerts detected by the security device to the cloud is Wi-Fi.

The algorithm that operates in the microcontroller is enriched with instructions that allow you to make intelligent and optimal decisions for sending the data. This program is agnostic to the communication interface. The solution presented in this research is an alternative that offers redundancy of interfaces, speed in delivery, energy saving and low cost.

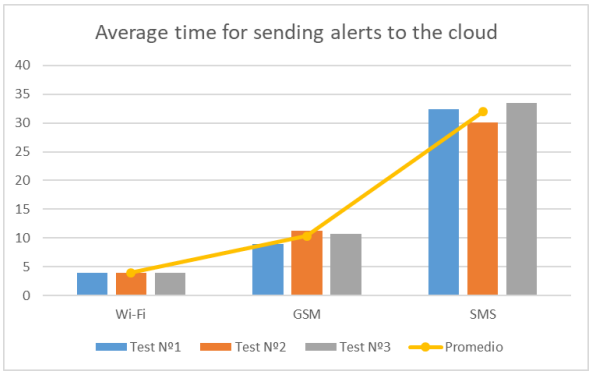

Fig. 9.Average time for sending alerts to the cloud platform and sms.

Table- I: Notification Delay Times

Interface	Test N° 1	Test N° 2	Test N° 3
Wi-Fi	4.02 s	3.98 s	4.01 s
GSM	9.02 s	11.24 s	10.78 s
SMS	32.32 s	30.12 s	33.45 s

REFERENCES

1. Munawir, I. Ahmad and M. Eka. "Wi-Fi and GSM Based Motion Detection in Smart Home Security System". 2019. IOP Conference Series: Materials Science and Engineering. pp. 2-9. DOI: 10.1088/1757-899X/536/1/012143
2. S. Khirod and P. Umesh C. "IoT based intrusion detection system using PIR sensor". 2017 9th IEEE International Conference on Communication Software and Networks. DOI: 1641-1645. 10.1109/RTEICT.2017.8256877.
3. G. Souveer, M. Anshu and O. Vishwamitra. "Design and implementation of a low-cost Arduino-based smart home system". 2017 2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT). DOI: 1491-1495. 10.1109/ICCSN.2017.8230356
4. I. Galiulina and P. Karlstén, 2018. [Online]. Available: https://kth.diva-portal.org/smash/get/diva2:1232494/FULLTEXT01.pdf
5. L. Gonzalez, "Scribd Inc., 26 August 2017. [Online]. Available: https://es.scribd.com/document/357270269/Manual-Del-Usuario-Sensor-de-Movimiento-Pir-Hc-Sr501
6. C. Platt and F. Jansson, Encyclopedia of Electronic Components, San Francisco: Maker Media, Inc., 2016.

AUTHORS PROFILE

José Luis Mela, Degree in computer engineering from the Universidad de Panamá. I have participated as an exhibitor in the national scientific congress of the Universidad de Panamá and attended conferences and workshops on methods, guidelines and methodologies for the elaboration of project proposals. In addition, I have worked on several investigations for publications. The areas of research interest focus on wireless networks, operating systems, computer architecture, robotics, internet of things, Smart city, vertical agriculture, cloud computing, quantum computing, blockchain, software engineering and artificial intelligence.

Edwin Cedeño Herrera received his Master degree in Computer Science (2009), Master degree in Network and Communications (2009), and Master degree in Distributed Systems Engineering and Communication (2011), from the Metropolitan University of Science and Technology of Panama, Technological University of Panama and Technical University of Madrid respectively. Received his Ph.D. degree in Telematics Engineering from the Technical University of Madrid in 2017.

Participates in several national and international research projects. His research interests are Service Architectures, Wireless Sensor and Actuator Networks, IoT, Delay and Disruption Tolerant Network, Distributed Systems Engineering. Since 2001 he is a professor on Informatics Engineering at the Universidad de Panamá. Currently, he is a Full-time professor, senior category II.

Gloris Batista Mendoza currently is an Assistant Professor at the Faculty Informatics, Electronics, and Communication at the Universidad de Panamá. She received her Bachelor's degree in 1998 from the Technological University of Panama and her Master's degree in Business Administration (2006), and International Relations and Foreign Trade (2013), from Latin University of Panama and Training and Employment Institute (Madrid, Spain), respectively. She has participated in several innovation and development projects sponsored by the Secretariat National of Science, Technology, and Innovation of the Republic of Panama. Since 2017 she has to work in areas related information systems and software engineering.