INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD CULHUACAN

SISTEMA CONTRA ROBO DE VEHÍCULOS

“Pisecurity car”

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

PRESENTA:

RAMÍREZ CARDONA JUAN CARLOS

ASESORES:

M. EN C. MARÍA AURORA MOLINA VILCHIS

LIC. MA. ALICIA CASTILLO GALVÁN

MÉXICO D.F. **2013**

INSTITUTO POLITECNICO NACIONAL
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESIS

Que como prueba escrita de su Examen Profesional para que obtengan el título de Ingeniero en Comunicaciones y Electrónica, deberá desarrollar el C.:

JUAN CARLOS RAMIREZ CARDONA

SISTEMA CONTRA ROBO DE VEHICULOS "PISECURITY CAR"

La actual problemática de robo de automóviles genera una necesidad de tener un sistema antirrobo eficaz.

La creación de un sistema antirrobo resulta muy útil, aunque existan sistemas similares, ninguno realiza las mismas funciones por un precio económico.

El sistema Pisecurity car utiliza una computadora Rasberry Pi como un sistema inteligente de control contra robo innovador, dicho sistema utiliza una red de sensores inalámbrica con control inteligente que permite detectar cualquier intento de acceso o encendido del automóvil, así como el bloqueo del sistema de arranque del mismo, la utilización de la tecnología inalámbrica permite al usuario el monitoreo remoto en tiempo real de su vehículo, sin importar su ubicación.

CAPITULADO

I. Panorama general de las tarjetas SBC y su aplicación en un sistema antirrobo
II. Comunicación inalámbrica entre sensores y actuadores
III. Diseño del Sistema Pisecurity car
IV. Instrumentación, integración y pruebas

Fecha: México D.F. a 24 de Septiembre de 2013

PRIMER ASESOR:

M. EN C. MARIA AURORA MOLINA VILCHIS

SEGUNDO ASESOR

LIC. MA. ALICIA CASTILLO GALVAN

Vo.Bo.

M. en C. ANTONIO ROMERO ROJANO
JEFE DE CARRERA DE I.C.E.

APROBADO

M. EN C. HECTOR BECERRIL MENDOZA
SUBDIRECTOR ACADEMICO

AGRADECIMIENTOS

Al INSTITUTO POLITÉCNICO NACIONAL y a la ESCUELA SUPERIOR DE INGENIERIA MECANICA Y ELECTRICA "Unidad Culhuacan".

Mi Alma Máter por ser una excelente institución académica y haberme dado la educación necesaria para mi desarrollo profesional.

M. en C, María Aurora Molina Vilchis.

Por brindarme su apoyo, tiempo, esfuerzo, experiencias y conocimientos para el desarrollo de esta tesis.

Lic. Ma. Alicia Castillo Galván

Por brindarme su tiempo y consejos para un buen desarrollo de esta tesis.

AGRADECIMIENTOS

A mis padres y mi hermano.

No terminaría de agradecer todo lo que han hecho por mí, todos sus sacrificios y esfuerzos. Este logro es de ustedes gracias a su cariño, confianza y apoyo incondicional hoy termino una carrera profesional.

GRACIAS! Porque sin ustedes esto no sería posible.

A mi familia.

Por su compañía, apoyo, consejos y cariño que me han brindado siempre en todas las situaciones y pese a todas las adversidades.

A Daniel C. y Enrique A.

Que me acompañaron desde mi entrada al instituto y me brindaron su amistad, apoyo y conocimientos, sin ustedes otra cosa hubiera sido. Gracias por ser mis cómplices, fueron parte esencial en el inicio de mi carrera profesional

A mis amigos.

Que estuvieron conmigo y compartimos tantas aventuras, experiencias y triunfos. Gracias a cada uno por hacer que mi estancia en ESIME fuera genial.

A Vero.

Por tu apoyo incondicional, tu paciencia, tus consejos, tu compañía y por darme esas palabras de aliento cuando más las necesitaba. Gracias totales!

"Nuestra recompensa se encuentra en el esfuerzo y no en el resultado. Un esfuerzo total es una victoria completa."

Mahatma Gandhi

Índice

Índice de figuras

Índice de Tablas

Objetivo general:

Diseñar y desarrollar un sistema de monitoreo y control remoto de un vehículo, utilizando una Raspberry Pi y una red de sensores, para detectar la intrusión a un vehículo e impedir la movilización del mismo con la finalidad de evitar el robo.

Objetivos específicos:

1. Programar en la computadora Raspberry Pi modelo B un algoritmo capaz de interpretar las variables provenientes de una red sensores.

2. Determinar los requisitos de diseño del sistema.

3. Diseñar un sistema de control capaz de reaccionar adecuadamente a partir del monitoreo de la red de sensores.

4. Integrar un módulo WiFi DWA-140 de la marca D-Link a la Raspberry Pi, para enviar los datos de los sensores vía WiFi hacia la web por medio de conexión SSH (Secured SHell).

5. Implementar el sistema en un automóvil de prueba.

6. Implementar una interfaz para el monitoreo remoto del sistema.

Justificación.

El delito de robo de vehículos en la Ciudad de México se ha incrementado de manera importante, los recursos de particulares y del sector público que destinan a la prevención y combate también se han incrementado considerablemente, sin que esto refleje una disminución en las pólizas, que deben las empresas aseguradoras.

Aunque existen diversas soluciones para impedir el robo de vehículos, hace falta un sistema inteligente que impida la movilización de unidad y que además el usuario pueda monitorear desde una computadora remota el estado de su vehículo en tiempo real, que además sea de bajo costo.

La inexistencia de un sistema que reúna todas las características antes mencionadas crea la necesidad de proponer el diseño e implementación del sistema Pisecurity car, que emplea un conjunto de sensores conectados en una red a una computadora Raspberry Pi que procesa cualquier intento de acceso o encendido no autorizado y envía por medio de un enlace WiFi información a la computadora remota del propietario.

Introducción

El robo de vehículos en la Ciudad de México es un grave problema que aqueja a la ciudadanía, este problema provoca que el patrimonio de algunas familias se vea drásticamente afectado.

De acuerdo a información del consejo ciudadano, en un lapso de máximo tres horas, se estima que un vehículo robado puede estar desvalijado o a muchos kilómetros de distancia de la ciudad de origen. Sin embargo también es el tiempo promedio que una persona puede tardar en interponer una denuncia por este delito, al considerar el traslado que puede tener una víctima a una agencia y el trámite que realiza [1].

Las autoridades intentan solventar este problema mejorando y ampliando la infraestructura de seguridad en la ciudad, una de estas mejoras es la instalación de cámaras de vigilancia en los puntos más conflictivos de la ciudad.

Pese a que las autoridades de la ciudad lograron reducir el robo de vehículos en un 26% de 2010 al 2012, las cifras de robo son alarmantes de acuerdo con la Asociación Mexicana de Instituciones de Seguros (AMIS), en el año 2012, en la Ciudad de México, se registraron 10,649 robos de autos asegurados de los cuales solo el 44% de los vehículos asegurados son recuperados por las autoridades [2].

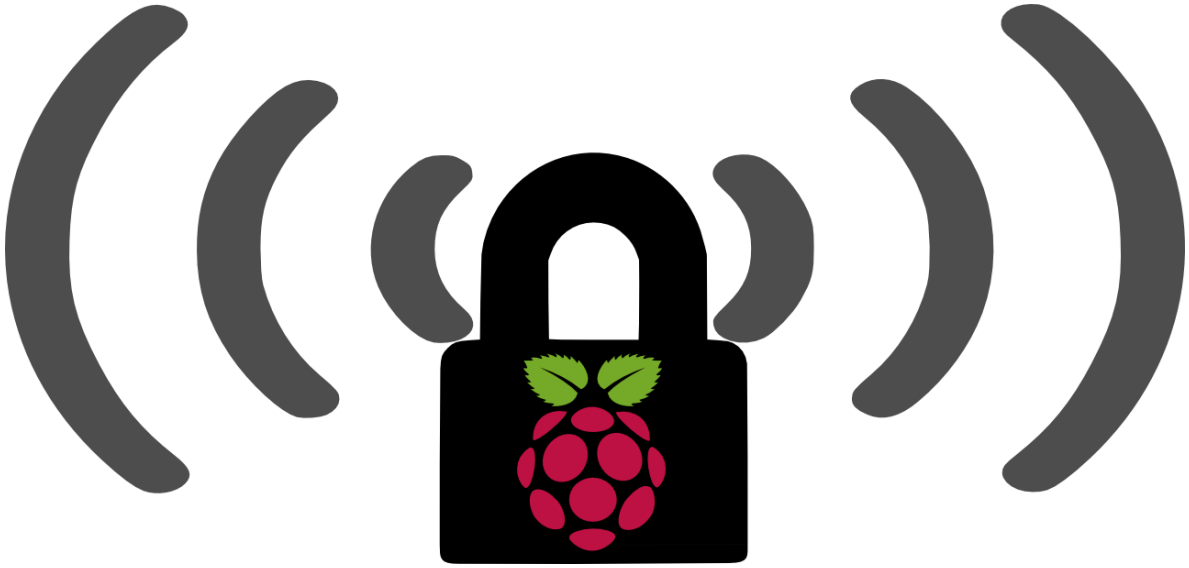
Se han propuesto mecanismos o sistemas con la finalidad de disminuir este tipo de delito, sin embargo muchas de las soluciones en el mercado no impiden que la unidad sea sustraída, es por ello que en esta investigación se propone un sistema innovador que monitorea el estado de las puertas y del volante, cuando alguno de estas variables se ve alterada el sistema activa un cortacorriente, que impide el encendido del automóvil, con el fin de mantener la integridad del mismo, además el estado de las puertas y el movimiento del volante pueden ser supervisadas por el usuario en tiempo real mediante cualquier dispositivo que permita una conexión a Internet. A este le e denominado “Pisecurity car”.

Para lograr los objetivos del sistema en esta tesis se presenta el diseño, instrumentación y pruebas del mismo. Esta tesis está organizada en cuatro capítulos, que a continuación se describen.

En el primer capítulo se presentara el problema que genera el robo de vehículos, así como la necesidad de crear un sistema innovador que impida el robo, se presentara de forma general lo referente a las SBC(por sus siglas en ingles de Single Board Computer) o computadora mono-placa desde sus antecedentes, su evolución y las ventajas de incluirlo en un sistema antirrobo. En el segundo capítulo se tratan la descripción, definición y caracterización de los elementos que componen el sistema, además de su funcionamiento y estructura. Así como la razón por la cual se eligieron dichos dispositivos. En el tercer capítulo se presentara el diseño del sistema, las cuatro etapas que la componen que son: etapa de sensado, procesamiento, comunicación y control. Se detallará el acoplamiento entre los diferentes elementos de cada etapa. En el cuarto y último capítulo se presentan las pruebas realizadas y el proceso para su implementación en un vehículo de prueba.

CAPITULO 1

PANORAMA GENERAL DE LAS TARJETAS SBC Y SU APLICACIÓN EN UN SISTEMA ANTIRROBO



CAPITULO 1. Panorama general de las tarjetas SBC y su aplicación en un sistema antirrobo

En el presente capítulo se presentará un panorama general sobre las limitantes de los sistemas antirrobo actuales, así como la importancia de dotarlos de inteligencia para que tengan la capacidad de actuar en caso de una contingencia. De acuerdo a las necesidades de un sistema antirrobo inteligente, se presenta la propuesta del sistema “Pisecurity car”, sus expectativas, los problemas a enfrentar, así como sus requerimientos tanto de hardware como de software para realizar su implementación.

1.1 Estadísticas del robo de vehículos

De acuerdo a la SSPDF (Secretaría de Seguridad Pública del Distrito Federal) en la Ciudad de México en el periodo de enero-septiembre del 2011 se registraron 14,078 robos de vehículos, es decir, un promedio de 52 casos diarios(Ver figura 1.1). Del total de robos registrados 8,964 fueron registrados sin violencia y los 5,114 restantes con violencia.

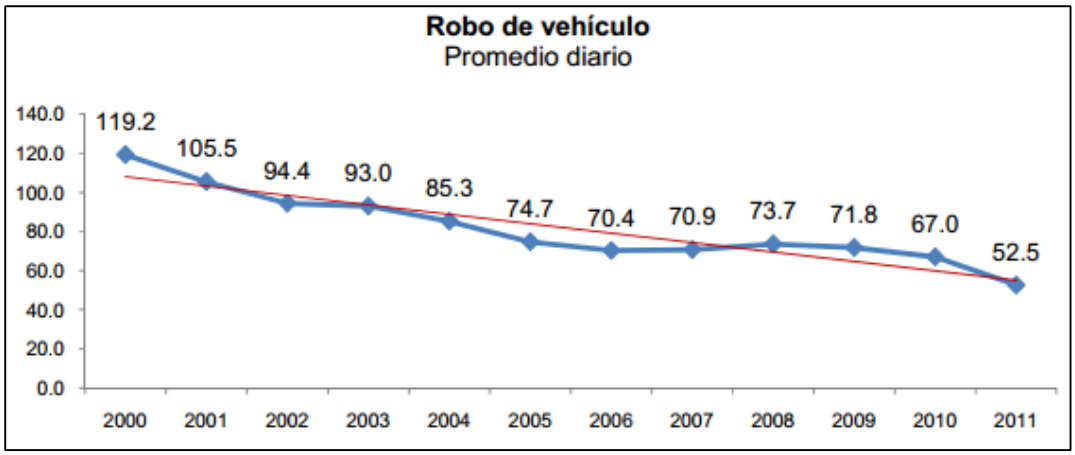


Figura. 1.1. Graficas del robo de vehículos en el D.F. periodo 2000-2011 [3].

El robo de autos sin violencia se concentra en unidades habitacionales, zonas comerciales y de oficinas, donde los autos permanecen estacionados en la calle por mucho tiempo [4].

De acuerdo a cifras de Asociación Mexicana de Instituciones de Seguros (AMIS) el robo de vehículos disminuyo un 6.8% del periodo 2010-2011 al periodo 2011-2012, también informo que solo el 30% del total de autos en el D.F. cuentan con algún tipo de seguro. En tanto, la recuperación de vehículos de julio de 2011 a junio de 2012 fue de sólo 45% de las unidades aseguradas, esto indica que el robo de vehículos es un grave problema, ya que pese que existe una disminución en el porcentaje de robo de vehículos, el parque vehicular aumenta aceleradamente y las estadísticas se modifican constantemente [5].

1.2 Sistemas antirrobo

En la actualidad los sistemas antirrobo han pasado de ser alternativa a una necesidad de seguridad, a tal grado que las empresas automotrices lo agregan a sus vehículos como un aditamento más. Hay una amplia gama sistemas antirrobo que se ajustan al poder adquisitivo de cada persona, reservando las soluciones mas completas para el mejor postor ya que su elevado costo las hace inaccesibles al presupuesto promedio del grueso de la población.

Alguno de los sistemas más comunes que vienen incluidos de serie en los vehículos o que se pueden instalar como dispositivos antirrobo para el automóvil son los siguientes:

Bloqueador del volante: Comúnmente llamado “bastón”, consiste en el bloqueo del volante mediante una barra fija que lo inmoviliza. Es un sistema muy sencillo, ya que se abre y cierra con una llave. Este es uno de los métodos más comunes ya que los usuarios suelen adquirirlo ya que son relativamente baratos, en la figura 1.2 se muestra el diseño estándar de un bastón [6].

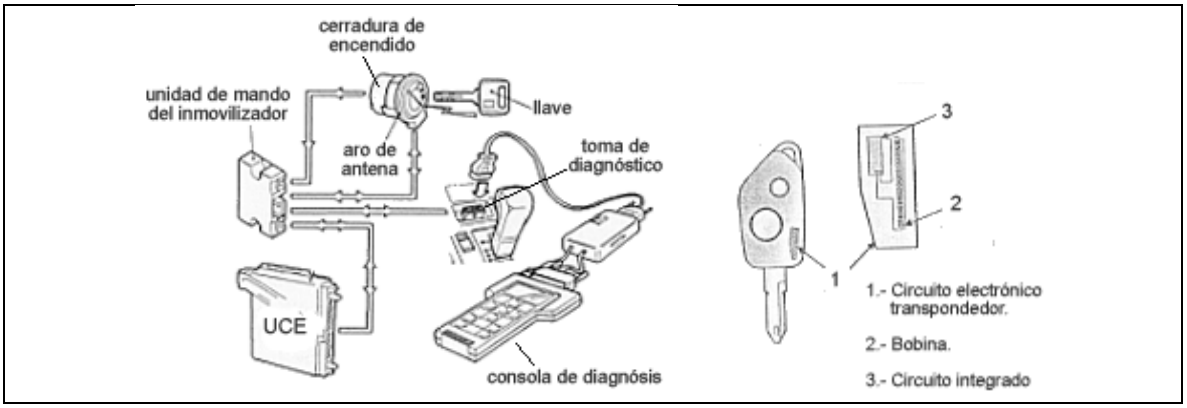
Figura. 1.2. Bastón antirrobo.

Alarma o sirena: Su funcionamiento es relativamente sencillo, ya que sirena emite una señal acústica a alta frecuencia normalmente acompañada del encendido y apagado de los focos, existen su control de activación frecuentemente se presenta en forma de llavero, en la figura 1.3 se muestran los componentes básicos de una alarma [6].

Figura. 1.3. Alarma antirrobo de vehículo con sirena.

Inmovilizador electrónico: La llave de este sistema lleva un circuito traspondedor codificado que la unidad de mando del inmovilizador puede leer a través del aro de antena. Si el código de la llave coincide con alguno de los códigos programados en la memoria de

la unidad de mando, el motor podrá arrancar. Si no hay código en la llave o no hay ningún código programado, la unidad de mando del motor bloqueará y el motor no podrá ponerse en marcha. Al girar la llave a la posición II, la unidad de mando del motor envía una señal a la unidad de mando del inmovilizador que a su vez envía corriente con una determinada frecuencia al aro de antena que hay alrededor de la cerradura de encendido. El transpondedor de la llave es activado y la frecuencia de la unidad de mando es modulada según un patrón que coincide con el código del transpondedor en caso de no coincidir bloquea el encendido del automóvil para que no pueda ser arrancado, en las figuras 1.4 a y b se puede ver los componentes principales del sistema, así con básicos de la llave [7].



a b

Figura. 1.4. Sistema inmovilizador. a) Componentes del sistema b) Componentes de la llave [7].

Existen otros sistemas que implementan mayores recursos tecnológicos por lo tanto su costo aumenta drásticamente, algunos ejemplos son los siguientes:

Kits de tele vigilancia y video vigilancia: Estos dispositivos son muy útiles cuando el vehículo se encuentra estacionado, permitiendo su visualización a través de monitores. El más popular de estos dispositivos son las llamadas “dash cameras”, son cámaras que se instalan dentro del automóvil y graban todo que esta frente de la cámara, por lo regular cuentan con una memoria interna bastante grande para tener el mayor número de horas grabadas ininterrumpidas, en la figura 1,5 se muestra una interfaz de monitoreo de una dash cam.

Figura. 1.5. Interfaz de monitoreo de dash cam .

.

GPS: Este sistema se basa en la utilización de un módulo GPS (por sus siglas en inglés: Global Positioning System) este sistema realiza una localización vía satélite del vehículo indicando su localización exacta, dependiendo de la marca y del costo serán las características adicionales que posea, tales características van desde el aviso de movimiento del vehículo hasta inmovilizadores, en la figura 1.6 se muestra esquemáticamente el funcionamiento de uno de estos sistemas.

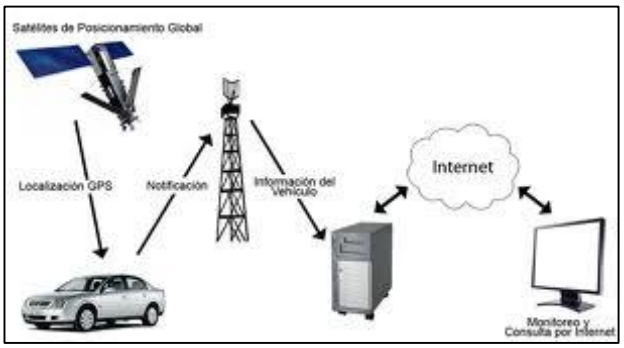


Figura.1.6. Diagrama esquemático del funcionamiento de un sistema GPS.

También existen sistemas que combinan dos o más de los dispositivos.

A continuación se describirán dos de los sistemas más populares que pueden presentar similitud con el sistema que se propone en esta tesis:

Corta corriente inalámbrico.

El cortacorriente inalámbrico [8] es un sistema ofrece el bloqueo de un automóvil por medio de un una tarjeta de proximidad, si la tarjeta de proximidad se aleja a más de 20 metros el sistema se activa.

Este sistema posee las siguientes características:

- Tarjeta de proximidad cifrada.
- Cortacorriente activado después de los 30 primeros segundos después del radio de 20 metros.
- El sistema se reestablece una vez que el sistema entra al radio de la tarjeta de proximidad.

En la figura 1.7 se puede ver la tarjeta de dicho sistema.

Figura.1.7. Tarjeta de proximidad del sistema cortacorriente inalámbrico.

Precio. 140 dólares

Sistema Goodlock.

El sistema Goodlock [9] ofrece el bloqueo de automóvil por medio de tres acciones rutinarias en un orden específico como por ejemplo:

1. Activar el encendedor.
2. Encender las luces de estacionamiento.
3. Tocar la bocina.

En la figura 1.8 se muestra un ejemplo de dichas acciones.

Figura.1.8. Combinación aleatoria de 3 acciones en un automóvil.

Desbloqueo del automóvil al instante.

Este sistema posee las siguientes características:

- Invisible: Sistema de bloqueo de motor invisible (no hay teclados ni otros dispositivos vulnerables).

- No importa que roben la llave: Aun cuando el delincuente posea una copia de la llave, el vehículo sólo arrancará con la clave correcta.

- No se desconfigura: El circuito electrónico opera en base a lógica alambrada. No emplea microcomputadores que requieren de software. En ambientes eléctricos hostiles, como en vehículos motorizados, los sistemas basados en microcomputadores suelen desconfigurarse.

- Nunca te dejará botado: Mientras el vehículo no está en uso, Goodlock no consume corriente. No existe riesgo de descarga de la batería luego de tiempo prolongado de no uso de tu automóvil.

- Seguridad aumentada: Capacidad de interrumpir hasta 4 (cuatro) circuitos que impidan la marcha del motor. Tres de ellos en base a pequeños dispositivos esclavos conectados con el circuito principal.

Precio. 220 dólares

Opiniones del autor de esta tesis con respecto a los sistemas antes descritos

Tanto el sistema de cortacorriente inalámbrico y el sistema Goodlock previamente descritos son muy eficientes, ya que reúnen diversas características que los hacen sobresalir por sobre su competencia, pese a que cada de uno de ellos pose formas de funcionamiento distintas cada uno de ellos tiene ciertas ventajas con respecto al otro, pero a la vez también tienen desventajas, una de ellas que a opinión del autor de esta tesis es la mas graves es que los dos sistemas son altamente invasivos ya que al modificar la estructura o cableado del automóvil se pierde la garantía del mismo; En el caso del sistema “Goodlock” resulta muy costoso para la mayoría de la población, es por eso que se optó por realizar un sistema antirrobo no invasivo y con un costo accesible para la mayoría de la población.

1.3 Estado del arte de las tarjetas inteligentes

Para realizar el sistema antirrobo que propone en la presente tesis, que sea eficiente, capaz de actuar de manera autónoma ante una posible amenaza, no invasivo y con un precio accesible para la mayoría de la población, se propone usar una tarjeta de nueva tecnología llamadas SBC (por sus siglas en ingles de Single Board Computer).

1.3.1. Microprocesadores

Puede definirse como un circuito integrado único que consta de millones de compuertas digitales que efectúan las funciones aritméticas, lógicas y de control de una computadora de tipo general. Es miembro de la familia de los circuitos con integración a gran escala que refleja el estado actual de una tendencia a la miniaturización que se inició con el desarrollo del transistor a finales de la década de los cuarenta. Los microprocesadores requieres circuitos externos de entrada-salida y de una memoria externa para operar funcionalmente como computadoras [10].

El primer microprocesador que se desarrolló incorporaba una unidad de 4 bits con una densidad modesta (ver figura 1.9). Otras unidades desarrolladas posteriormente han incorporado un mayor número de bits y una mayor densidad. A finales de los años setenta la mayoría de los microprocesadores utilizaban 8 bits por palabra y las unidades más recientes cuentan con 64 bits por palabra.

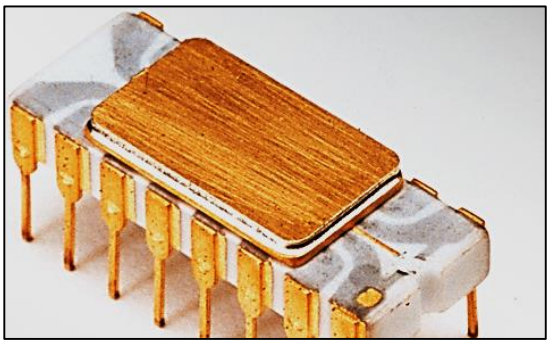


Figura.1.9. Microprocesador Intel 4004 [11].

El microprocesador o CPU(por sus siglas en ingles Central Processing Unit)se encarga básicamente de traer las instrucciones de los programas desde la memoria, interpretarlas y hacer que se ejecuten. El microprocesador también incluye los circuitos para realizar operaciones aritméticas y lógicas elementales con los datos binarios, en la denominada ALU (por sus siglas en ingles Arithmetic and Logic Unit).

Los microprocesadores se han desarrollado fundamentalmente orientados al mercado de los ordenadores personales y las estaciones de trabajo, donde se requiere una elevada potencia de cálculo, el manejo de gran cantidad de memoria y una gran velocidad de procesamiento. Un parámetro importante en los microprocesadores es el tamaño de sus registros internos (8,16,32 o 64 bits), que determina la cantidad de bits que pueden procesar simultáneamente [12].

1.3.2. Microcontroladores

En 1971 ingenieros Gary Boone y Michael Cochran de la empresa Texas Instruments lograron crear el primer microcontrolador, TMS 1000; fue comercializado en 1974. Se denomina microcontrolador a un sistema que posee varios elementos en un solo chip, dentro de este chip están incluidos la CPU(por sus siglas en ingles Central Processing Unit), memoria RAM, memoria ROM, reloj y elementos periféricos de forma que se pueda realizar todo un sistema de control solo conectando los elementos exteriores [13].

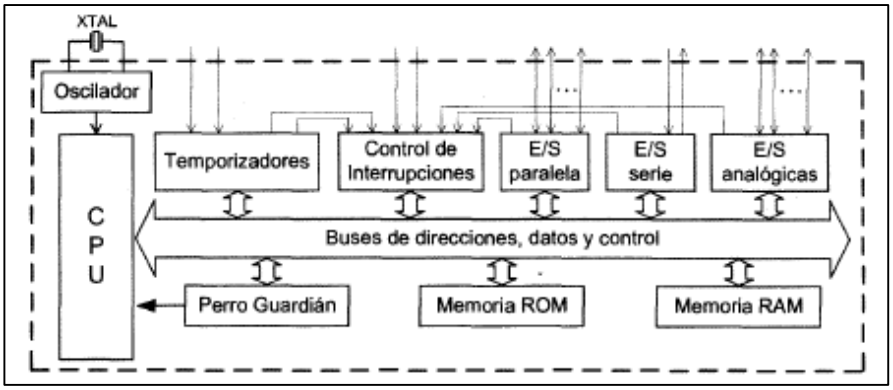


Figura.1.10 Diagrama de bloques general de un microcontrolador [12].

El microcontrolador es capaz de ejecutar órdenes grabadas en su memoria.

Los microcontroladores están concebidos fundamentalmente para ser utilizados en aplicaciones puntuales, es decir, aplicaciones donde el microcontrolador debe realizar un pequeño número de tareas, al menor costo posible. En estas aplicaciones, el microcontrolador ejecuta un programa almacenado permanentemente en su memoria, el cual trabaja con algunos datos almacenados temporalmente e interactúa con el exterior a través de las líneas de entrada y salida de que dispone. El microcontrolador es parte de la aplicación: es un controlador incrustado o embebido en la aplicación.

Los microcontroladores se han desarrollado para cubrir las más diversas aplicaciones. Se usan en automoción, en equipos de comunicaciones y de telefonía, en instrumentos electrónicos, en equipos médicos e industriales de todo tipo, en electrodomésticos, en juguetes, etc [12].

1.3.3. Sistemas mínimos

Es un sistema basado en un microprocesador o microcontrolador, es una microcomputadora de propósito específico equipada con el mínimo de componentes (memoria RAM, ROM, puertos, sensores, actuadores, etc.) para realizar sus funciones.

Los propósitos para los que puede diseñarse pueden caer en una infinidad de campos como: instrumentación, control, monitoreo, señalización, secuensiamiento, autorización, comunicaciones, procesamiento de señales, etc. En la figura 1.11 se muestran los bloques básicos de un sistema mínimo [14].

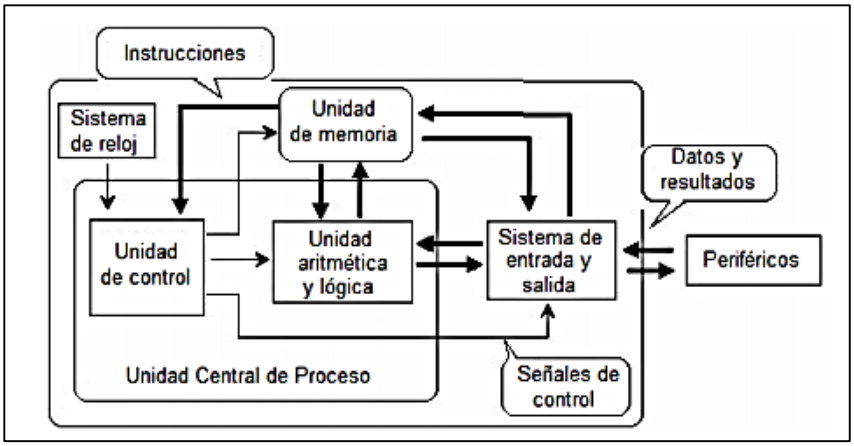


Figura.1.11. Diagrama a bloques básico de un sistema mínimo.

1.3.4. SBC

Computadora monoplaca o SBC (por sus siglas en inglés *Single Board Computer*) es una computadora completa en un sólo circuito. El diseño se centra en un sólo microprocesador con la memoria RAM, Entradas/Salidas y todas las demás características de un computador funcional en una sola tarjeta, que suele ser de tamaño reducido, y tiene todo lo que necesita en la misma placa. Originalmente las computadoras monoplaca se hicieron como sistemas de demostración o desarrollo, para los sistemas educativos, y para el uso como controladores de sistemas embebidos.

Esta arquitectura no es muy popular en los computadores personales (aunque las tendencias indican que esto puede cambiar) sino que más que todo se usan en entornos industriales o en sistemas embebidos dentro de otros que sirven como controladores e interfaces.

Con la evolución de las computadoras personales el uso de las computadoras monoplaca quedo rezagado, pero recientemente esta tendencia parece haberse revertido ya que los fabricantes cada vez ponen más características como el sonido, red, E/S e incluso gráficos en un solo circuito.

Debido a los grandes niveles de integración y reducción de componentes y conectores, los computadores en una tarjeta suelen ser más pequeños, livianos, más confiables y con un mejor manejo de la potencia eléctrica que los computadores de múltiples tarjetas.

En la tabla 1.1 se muestra una tabla con algunas de las tarjetas SBC más importantes a nivel comercial.

Tabla1.1. Lista de las principales SBC que existen en el mercado [15].

Fabricante	**Nombre**	**Fabricante de socket**	**Tipo de núcleo**	**Núcleos**	**RAM (MB)**	**Puertos USB**	**Ethernet (Mbit/s)**
Hardkernel	ODROID-XU	Samsung	Cortex-A15 + Cortex-A7	8	2048	5	100MBit/s
Boundary Devices	Nitrogen6X	Freescale	Cortex-A9	4	1024	2	1024MBit/s
Boundary Devices	SABRE Lite	Freescale	Cortex-A9	4	1024	2	1GBit/s
Hardkernel	ODROID-X2	Samsung	Cortex-A9	4	2048	6	100MBit/s
DragonBoard	DragonBoard IFC6410	Qualcomm	Krait	4	2048	2	1GBit/s
Cubieboard	Cubieboard3	Allwinner	Cortex-A7	2	2048	2	1GBit/s
Olimex	A20-OLinuXino-MICRO	Allwinner	Cortex-A7	2	1024	2	100MBit/s
PandaBoard	PandaBoard	Texas Instruments	Cortex-A9	2	1024	2	100MBit/s
CALAO Systems	SKY-S9500-ULP-C02	ST-Ericsson	Cortex-A9	2	1024	1	100MBit/s
The Raspberry Pi Foundation	Raspberry Pi, Model B	Broadcom	ARM1176JZF-S	1	512	2	100MBit/s
BeagleBoard	BeagleBoard-xM	Texas Instruments	Cortex-A8	1	512	1	100MBit/s
BeagleBoard	BeagleBone	Texas Instruments	Cortex-A8	1	256	1	100MBit/s
Boundary Devices	Nitrogen53	Freescale	Cortex-A8	1	2048	3	100MBit/s
Cubieboard	Cubieboard	Allwinner	Cortex-A8	1	1024	2	100MBit/s
Freescale	IMX53QSB	Freescale	Cortex-A8	1	1024	2	100MBit/s

Para el sistema que se propone en este tesis se optó por utilizar la SBC Raspberry Pi; La razón principal de la utilización de dicha SBC en el sistema propuesto es que debido a sus características y a su capacidad de conexión con el exterior (Ver apéndice B) sería una

opción viable para su utilización en el mejoramiento de los sistemas de seguridad antirrobo actuales, ya que dotaría de inteligencia el sistema y lo haría menos vulnerable frente a posibles escenarios de riesgo.

Otra de las razones por las cuales se eligió la Raspberry Pi es que cuando se inició este tesis (Febrero de 2012) no existía mucha diversidad de SBC en el mercado ya que la mayoría de las marcas solo presentaban prototipos de sus posibles sistemas, además el precio de la Raspberry Pi era muy bajo, ya que al ser desarrollada y financiada por una fundación (Raspberry Pi Foundation) costaba 35 dólares, debido a su gran popularidad a nivel mundial la Raspberry Pi rápidamente paso convertirse en una opción de una gran cantidad de desarrolladores alrededor del mundo.

En la actualidad el precio de la Raspberry Pi es 41 dólares más 8 dólares de impuestos ya que tiene que ser importada de Inglaterra o España.

1.4 Planteamiento del problema

De acuerdo a cifras de la AMIS (Asociación Mexicana de Instituciones de Seguros) la industria aseguradora paga 9,500 millones de pesos por siniestros de autos robados.

Y de acuerdo a ese dato se calcula que el promedio de perdida de los particulares[1] es de alrededor de 160,000 pesos en promedio por cada unidad. La industria aseguradora estima que el valor nacional del mercado de autos robados ronda alrededor de 35,000 millones de pesos [16].

Tomando en cuenta los elementos antes mencionados se hace prioritario la creación de un sistema antirrobo de bajo costo que integre nuevas tecnologías a los sistemas antirrobo actuales.

Como se mencionó en la Sección 1.1 de esta tesis el robo de vehículos es un grave problema para la sociedad, la larga estadía del vehículo en un lugar, por ejemplo fuera de la casa de propietario lo vuelve blanco perfecto para los maleantes, aunque algunos vehículos tengan instalada una alarma esto no detiene el robo ya que por diversos factores la sirena puede no ser escuchada por el dueño del vehículo, es por esa razón que hace falta una acción más contundente para evitar el robo, dicha acción es bloqueo del sistema de encendido del vehículo.

En otro escenario muy diferente existe una flotilla de vehículos de alguna empresa, como es bien sabido los choferes de dichas unidades tienen las llaves del vehículo en su posesión todo el tiempo, por lo tanto pueden dar mal uso de la unidad en cuestión si su supervisor está ausente, para evitar el mal uso del vehículo el supervisor puede bloquear y desbloquear el sistema, para así llevar un control más riguroso y tener la seguridad de que el vehículo de la empresa está estacionado a salvo.

[1] . Que afecta directamente al patrimonio familiar.

Para combatir el robo vehicular es necesario crear un sistema innovador, con la capacidad de comunicarse con el usuario aprovechando las conexiones inalámbricas existentes como el WiFi, que sea autónomo y económico.

1.5 Propuesta de solución

Para dar solución a la problemática previamente planteada se propone un sistema de seguridad para un vehículo que cumpla con las siguientes características:

- El sistema debe de almacenar y procesar dos variables del vehículo que son las puertas y el volante del mismo alertando cualquier alteración de su estado, esto lograra utilizando una red sensores conectados a una SBC que proporcione el constante monitoreo del estado de los sensores.

- El sistema debe de tener la capacidad de transmitir los datos provenientes de los sensores al usuario, para que sean monitoreados por medio de una conexión segura SSH (Secure SHell), y si el usuario lo desea anular la acción bloqueo para ello el sistema tiene que enviar los datos recabados por medio de una conexión WiFi. Para lograr que la conexión WiFi sea lo más lejana posible se instalará en el sistema una tarjeta inalámbrica de largo alcance con lo que la cobertura de la red WiFi alcanzara entre 25 y 35 metros.

- El sistema debe ser capaz de manejar los datos provenientes de los sensores de una manera óptima, procesarlos y tomar una decisión, para ello se utilizara una tarjeta inteligente programable de tipo SBC, la tarjeta debe de ser capaz de regir una acción de control que provoque el bloqueo del sistema de encendido del vehículo.

1.6 Problemas a enfrentar

Uno de los requerimientos más importantes del sistema propuesto debe ser lo menos invasivo posible, es por eso que se tienen que usar sensores pequeños(1.3cm largo X.6cm ancho X1.6cm profundidad) pero resistentes, la posición del sensor para ello se tendrá que evaluar previamente la posición de los sensores debido a que los automóviles pueden presentarse en diferentes tipos (sedan, deportivo, vagoneta, monovolumen), existe una gran diversidad de tamaño, tipo y forma de puertas laterales, una vez que la posición del sensor es la adecuada, se procederá a pegarlo a la estructura de la puerta con pegamento epóxico de alta dureza, esto garantizaría que el sensor no se mueva ni se caiga con los embates de la puerta, pero a la vez el pegamento podrá ser disuelto si ya no se desea el sistema por medio de acetona industrial. El sensor de efecto Hall que se utilizará para censar las posición del volante se colocara en la base, con diminuto tamaño será sencillo

colocarlo. Para alambrar los sensores se utilizará alambre calibre 22 que es lo suficientemente delgado como para pasar entre las uniones de las piezas o por debajo de la tapicería interior del vehículo, con ello se lograra evitar perforaciones adicionales a la estructura original del vehículo y el cableado será discreto.

Para fijar el prototipo del sistema donde estará la tarjeta inteligente, la tarjeta inalámbrica y el mecanismo de control, dicho sistema se encontrará al interior del cofre del vehículo, será necesarias abrazaderas de metal, se eligieron porque de otra forma se tendría que realizar perforaciones para fijar el sistema, las abrazaderas de metal ofrecen la suficiente fuerza para sostener el prototipo al vehículo de manera óptima.

Otro problema a enfrentar es la comunicación del sistema con el usuario, para solventarlo se dotara a la tarjeta con un módulo WiFi Range Booster (largo alcance) que tiene un alcance aproximado de ~35 metros que es la distancia promedio que se tiene que subsanar considerando los escenarios de riesgo que se describieron en la sección 1.4 de esta tesis.

Un problema menor puede ser la alimentación del sistema que será subsanada con una batería de 6 volts que podrá ser conectada al encendedor del vehículo para ser recargada aproximadamente cada 4 días para garantizar que el sistema esté disponible cuando se requiera.

1.7 Recursos y materiales

A continuación se presentan los materiales requeridos para la realización del proyecto. Los materiales fueron divididos en tres categorías que a continuación se describen.

Componentes principales.

En la tabla1.2 se pueden observas los componentes principales del sistema propuesto.

Tabla 1.2. Componentes principales del sistema.

Concepto	Descripción	Cantidad	Costo ($)
Raspberry Pi	Computadora de propósito específico, cerebro del proyecto.	1	750.00
Servomotor Futaba 3002	Servomecanismo	1	150.00
Partes de acoplamiento		Varios	
Computadora, Smartphone o Tablet	Fungirá como interfaz con el dispositivo y esto será a elección del usuario.	1	
Conexión inalámbrica a Internet	Conexión entre el sistema y el usuario	1	
Resistencias varias			
Sensores de efecto Hall	US1881KUA	4	10.00
Sensores de fin de carrera.	Matricula genérica	1	10.00
Batería de 6 volts, 1 A	Alimentación del sistema	1	90

Conector para encendedor de automóvil	Alimentación de la batería del sistema	1	25

En cuanto al software

En la tabla 1.3 se muestra todo el software utilizado para realizar esto proyecto es de distribución libre, y se puede utilizar sin problemas de licenciamiento.

Tabla 1.3. Software utilizado.

Concepto	Descripción	Costo ($)
Sistema Operativo	Raspbian Ver.7	0.00
Lenguaje de programación	Python Ver.3	0.00
Librería de conexión al hardware	RPi.GPIO Python	0.00

En cuanto a los accesorios.

Los accesorios utilizados para la realización del sistema se muestran en la tabla 1.3.

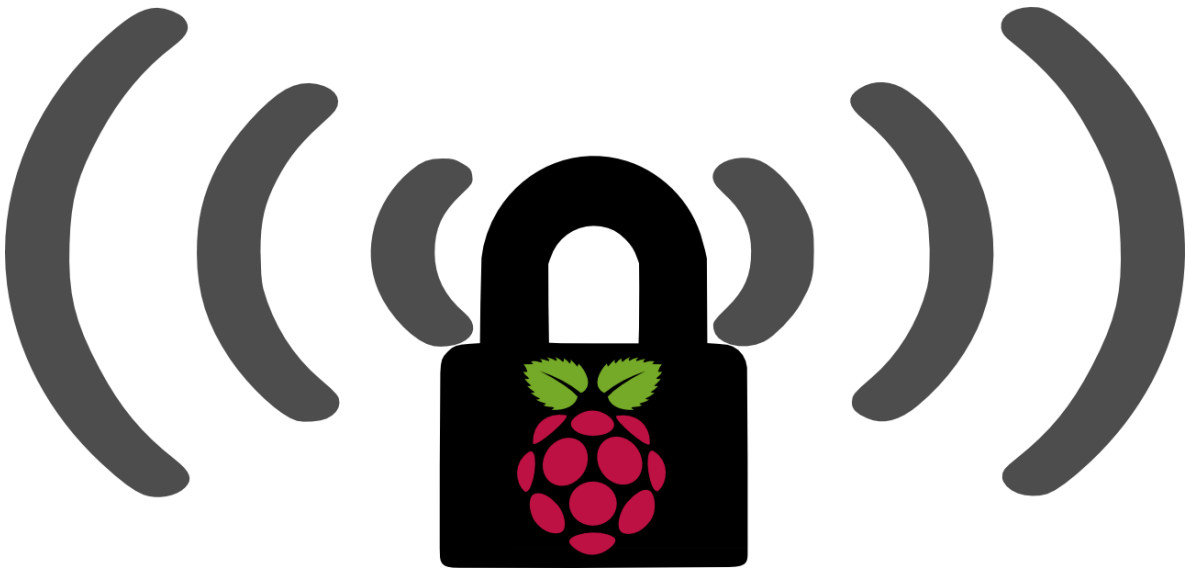
Tabla 1.4. Accesorios utilizados.

Concepto	Descripción	Cantidad	Costo ($)
Cable USB.	Cable USB Mini-B	1	45.00
Antena WiFi	D-Link DWA-140b	1	170.00
Tarjeta SD	Tarjeta SD 4Gb Marca. Kingston	1	150.00

Dando un costo total de $1400 precio que resulta mucho menor a otros sistemas ya existentes.

CAPÍTULO 2

COMUNICACIÓN INALÁMBRICA ENTRE SENSORES Y ACTUADORES



CAPÍTULO 2. Comunicación inalámbrica entre sensores y actuadores

En el presente capítulo se detallan los elementos necesarios para la realización de un sistema de monitoreo y control del encendido de un automóvil vía remota, se describirá su labor en el sistema, la interacción entre los diferentes elementos y su funcionalidad en el sistema.

2.1 Redes inalámbricas de sensores (WSN)

Tradicionalmente, las redes inalámbricas de sensores han sido usadas en aplicaciones de gama alta como lo son radiación y sistemas de detección de amenazas nucleares, aplicaciones biomédicas, sensado de viviendas y monitoreo sísmico

2.1.1 Generalidades

Las WSN (por sus siglas en inglés Wireless Sensor Networks) constan de una estación base, un nodo coordinador y nodos sensoriales los cuales se describirán a continuación. Ver Figura 2.1.

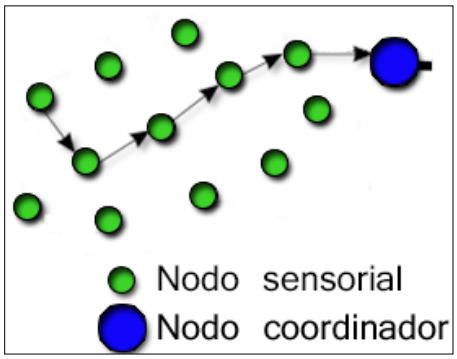


Figura. 2.1. Representación de una WSN.

Los nodos sensoriales tienen como función, registrar las variables ambientales que se encuentra a su alrededor y además se comunican de manera inalámbrica con el nodo coordinador.

Un nodo coordinador tiene como función proporcionar la configuración cuando la red se despliega, sobre todo cuando se trata de ambientes desatendidos y también instruye a los nodos sensoriales con los protocolos de comunicación independientes.

La estación base se encarga de recibir y administrar la información para lo cual fue diseñada la red.

Una desventaja con las que cuenta los nodos sensoriales es su bajo poder de procesamiento, lo cual solo permite ejecutar los protocolos propios de la comunicación entre los datos ambientales y el nodo central, otra limitante de los nodos sensoriales es que se alimentan con baterías por lo que la mayor parte del tiempo se encuentran en estado

inactivo y solo se activan para responder las preguntas de la estación base. Sin embargo unas de sus principales características es su funcionamiento autónomo, es decir actúan por sí solos y se coordinan entre sí soló para enviar información al nodo coordinador.

Debido a lo anterior los nodos sensoriales precisan de un nodo coordinador, que además de facilitar la configuración de la red, realiza las funciones de control en la transición de los nodos sensoriales y la estación base. La particularidad del nodo coordinador es que debe contar con características computacionales superiores a los nodos sensoriales, es por eso que en esta tesis se propone la integración de una computadora de uso específico a la red de sensores para que realice las funciones de coordinación y que además facilite la comunicación interactiva entre la estación base y los nodos sensoriales [17].

Para subsanar los requerimientos antes mencionados en las redes de sensores, existen en el mercado varias computadoras de uso específico llamadas “computadora mono-placa” o SBC por sus siglas en ingles que significa Single Board Computer (Véase Apéndice B).

2.2 Redes Inalámbricas de Sensores y Actuadores (WSAN)

Las WSAN (por sus siglas en inglés Wireless Sensor and Actor Networks) son un grupo de sensores y actuadores unidos por medios inalámbricos para realizar detección distribuida y tareas de accionamiento. En este tipo de red, los sensores adquieren información sobre el mundo físico, mientras que los actuadores toman decisiones y realizan acciones apropiadas sobre el medio ambiente, lo que permite la interacción remota y automatizada con el medio ambiente.

El hecho de poder tomar las acciones necesarias, hace que las WSAN tengan un dominio de problema muy distinto a las WSN, sin embargo las WSAN requieren de un mecanismo de coordinación distribuida entre los sensores y actuadores.

Las WSAN logran cubrir algunas necesidades que las WSN no pueden, una de las diferencias es la gran capacidad de procesamiento con la que cuentan los actuadores, así como la mayor potencia para la comunicación y la mayor duración de las baterías, esto convierte a las WSAN en un herramienta más completas para la manipulación del mundo físico.

2.2.1 Arquitectura

En una WSAN existen dos arquitecturas fundamentales (ver Figura. 2.2), las cuales son:

- Arquitectura Centralizada: un controlador centralizado recibe información de múltiples sensores y, una vez procesada, genera las órdenes oportunas para los actuadores.

- Arquitectura Distribuida: en este caso, no existe la figura del controlador centralizado, sino que toda la inteligencia del sistema está distribuida por todos los módulos sean sensores o actuadores.

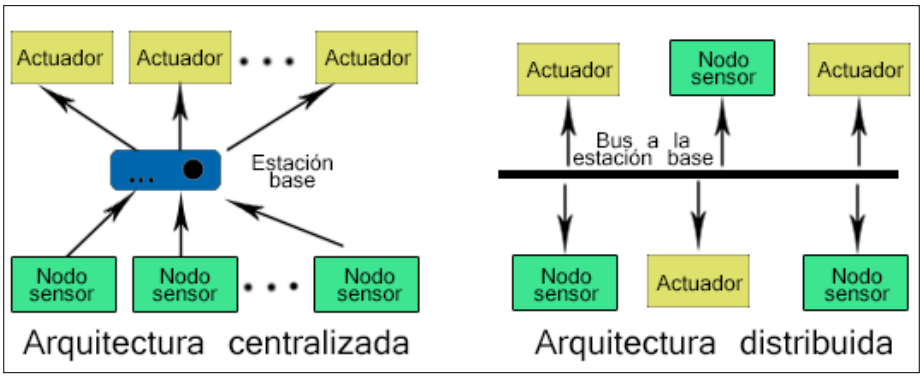


Figura.2.2. Arquitecturas de las WSAN.

2.2.2 Componentes de la WSAN

Los elementos de una WSAN son los siguientes y en la Figura. 2.3 se puede observar la forma en que los elementos interactúan entre si.

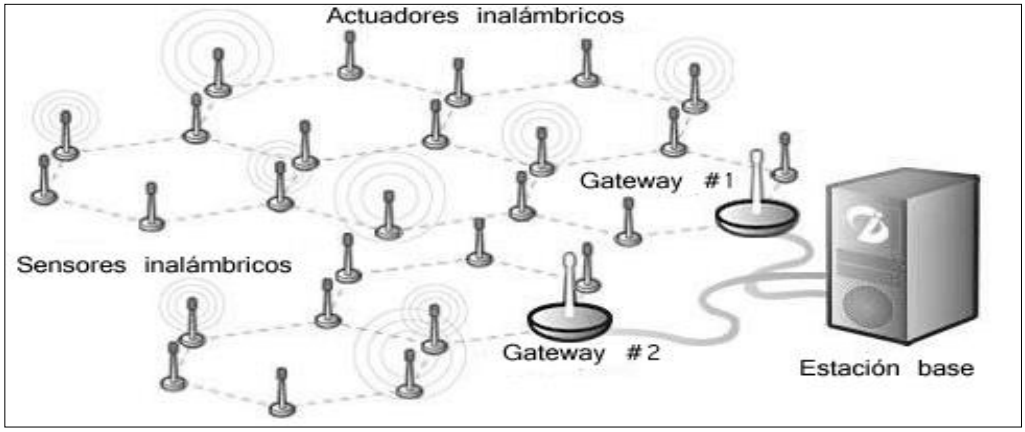


Figura.2.3. Configuración básica de la WSN.

- Sensores: Son elementos que toman del medio ambiente la información y las convierten en señales eléctricas.

- Nodos (Motas): Elementos que toman los datos del sensor y envían la información a la estación base.

- Gateway: Elementos para la interconexión entre la red de sensores y una red de datos (TCP/IP).

- Estación base: Elemento que tiene como función colectar los datos y está basado en una computadora o en un sistema embebido.

- Actuador: Es el dispositivo de salida capaz de recibir una orden del controlador y realizar una acción.

Los actuadores al ser los elementos más importantes y que diferencian las WSAN de las WSN, son los dispositivos que convierten una señal de control eléctrica a una acción física, y constituye el mecanismo por el que un agente actúa sobre el medio físico, sin embargo, un actuador, además de ser capaz de actuar sobre el medio ambiente por medio de uno o varios actuadores, también es una entidad de red que realiza acciones relacionadas con las funcionalidades de las red, como: recibir, transmitir y procesar datos [18].

Por ejemplo, un robot puede interactuar con el medio físico por medio de varios motores y servomecanismos (accionadores). Sin embargo, desde una perspectiva de red, el robot constituye una entidad única, lo que se conoce como actuador. Por lo tanto, el término actuador abarca dispositivos heterogéneos como robots, vehículos aéreos no tripulados conocidos como UAV (por sus siglas en inglés), y elementos conectados en red, tales como rociadores de agua, cámaras, brazos robóticos, etc. Las aplicaciones de sensores inalámbricos y redes de actuadores pueden percibir el entorno desde múltiples puntos de vista recogidos por una red de sensores, por ejemplo: Un sistema de aparcamiento inteligente que vuelve a dirigir a los conductores a lugares de estacionamiento disponibles, o una calefacción distribuida, sistemas basados en sensores inalámbricos.

2.3 Sensores

De acuerdo a Ivy Wigmore un sensor es un dispositivo que detecta y responde a algún tipo de entrada del medio físico [19].Estos dispositivos son diseñados para recoger datos analógicos con determinada sensibilidad dichos datos pueden ser la luz, el calor, el movimiento, la humedad, la presión, u otros fenómenos ambientales. La salida se obtiene generalmente es una señal eléctrica u óptica, esto con la finalidad de que sea procesada para su posterior análisis.

Los sensores están diseñados para trabajar de manera lineal o con una función matemática simple típicamente logarítmica, se considera un buen sensor aquel que cumple con las siguientes reglas:

- Es sensible solo a la propiedad medida.
- Es insensible a cualquier otra propiedad que se encuentren en su aplicación.
- No influye en la propiedad medida [20].

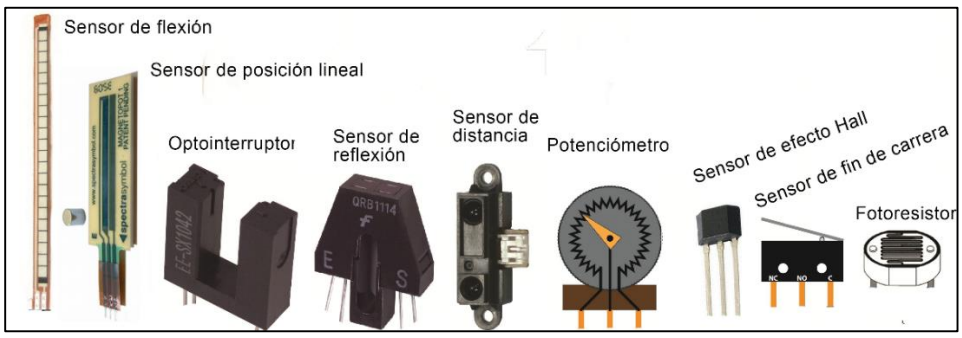


Figura.2.4. Algunos tipos de sensores.

2.3.1 Descripción de los sensores

Existen diversos tipos de sensores, su clasificación depende de su aplicación o del material de fabricación, entre otros aspectos. La Tabla 2.1 muestra una breve descripción de algunos sensores comerciales.

Tabla 2.1 Descripción general de los tipos de sensores [21].

Tipo de sensor	Descripción
Sensores de posición	Su función es medir o detectar la posición de un determinado objeto en el espacio, a este grupo, pertenecen los sensores fotoeléctricos que emplean una fuente de señal luminosa y una célula receptora, pueden estar constituidos por fotodiodos o fototransistores para la emisión y/o detección de luz. Según la forma en que realizan estas funciones se dividen en: Captadores por barrera. Estos detectan la existencia de un objeto, que interfiere la recepción de la señal luminosa. Captadores por reflexión. La señal luminosa es reflejada por el objeto, el reflejo de la luz es obtenida por el captador fotoeléctrico.
Sensores de contacto	Son interruptores que se activan o desactivan si se encuentran en contacto con un objeto.
Sensores de circuitos oscilantes	Están basados en la existencia de un circuito mismo que genera una determinada oscilación a una frecuencia prefijada, cuando en el campo de detección del sensor no existe ningún objeto, el circuito mantiene su oscilación de un manera fija. Pero cuando un objeto se encuentra dentro de la zona de detección del mismo, la oscilación deja de producirse, esto significa que el objeto es detectado.
Sensores de ultrasonidos	Se basa en el mismo funcionamiento que los de tipo fotoeléctrico, pero difiere en que éste emite una señal ultrasónica que es captada por un receptor.
Sensores de esfuerzos	Su funcionamiento está basado en el empleo de galgas extenso métricas, son dispositivos que cuando se les aplica una fuerza varía su resistencia eléctrica, de esta forma se puede medir la fuerza que se está aplicando sobre un determinado objeto.
Sensores de Movimientos	Sirven para decretar la cantidad de movimiento de un determinado objeto. Se dividen en: Sensores de deslizamiento. Se utilizan por lo regular en robots, son instalados en el órgano aprehensor (pinzas), cuando el robot decide coger el objeto, las pinzas lo agarran con una determinada fuerza y lo intentan levantar, si se produce un pequeño deslizamiento del objeto entre las pinzas, inmediatamente es incrementada la presión de las pinzas sobre el objeto, esta operación se repite hasta que el deslizamiento del objeto se ha eliminado gracias a la aplicación de la fuerza de agarre suficiente. Sensores de Velocidad. Estos sensores pueden detectar la velocidad de un objeto tanto lineal como angular. Existen también otros tipos de sensores para controlar la velocidad, basados en el corte de un haz luminoso a través de un disco perforado sujetado al eje del motor. Sensores de Aceleración. Estos sensores dan la información de la aceleración que el objeto dado experimenta.

2.3.2 Sensores de fin de carrera

Es un dispositivo electromecánico que consta de un accionador unido a una serie de contactos. Cuando un objeto entra en contacto con el accionador, el dispositivo activa (o acciona) los contactos para establecer o interrumpir una conexión eléctrica. Están compuestos por dos partes: un cuerpo donde se encuentran los contactos y una cabeza que detecta el movimiento.

Son utilizados ampliamente en ambientes industriales para censar la presencia de objetos en una posición específica. Se utilizan en diversas aplicaciones. Pueden determinar la presencia, ausencia, paso y posicionamiento de un objeto, en la figura 2.5 se puede observar los componentes básicos del sensor antes mencionado.

El sensor emite una señal de Encendido/Apagado. (Digital) basándose en la presencia o ausencia del objeto en cuestión, por lo tanto solo dan dos valores: abierto o cerrado que corresponden a una salida digital [22].

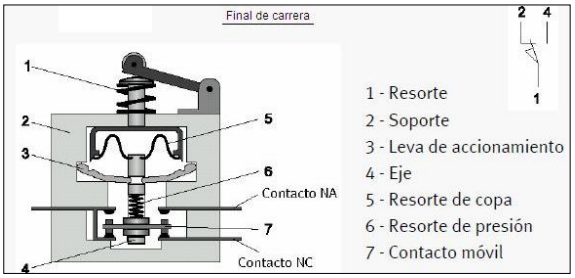


Figura. 2.5 Sensor de fin de carrera. [23]

2.3.3 Sensor de efecto Hall US1881KUA

Es un dispositivo semiconductor que genera un voltaje de salida cuando es expuesto a un campo magnético. Su construcción básica consiste en una placa de material semiconductor a través de la cual se hace pasar una corriente, como se muestra en la figura 2.6. Si se aplica un campo magnético de modo perpendicular a la dirección de la corriente (vea figura 2.6) se genera un voltaje V_h entre las dos terminales como se puede observar en la figura 2.6 [24].

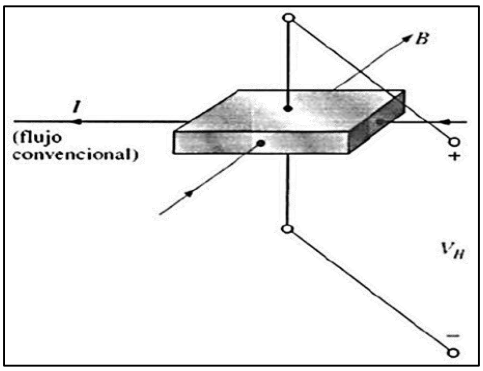


Figura.2.6. Diagrama de funcionamiento del sensor.

Cuando un objeto ferromagnético (imán) se aproxima al sensor, el campo magnético inducido por el imán provoca una corriente eléctrica dentro del sensor. Así se puede determinar la proximidad de un objeto, siempre que sea ferromagnético. Los sensores de efecto Hall se pueden utilizar como interruptores accionados por el campo magnético positivo o negativo de un imán. Ver Figura. 2.7.

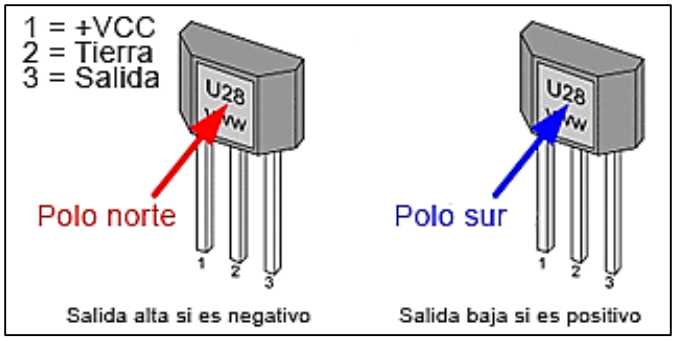


Figura.2.7. Switch de efecto Hall.

2.4 Actuadores

Un actuador es un dispositivo inherentemente mecánico cuya función es proporcionar fuerza para mover o “actuar” sobre otro dispositivo mecánico. La fuerza que provoca el actuador proviene de tres fuentes posibles: Presión neumática, presión hidráulica, y fuerza motriz eléctrica (motor eléctrico o solenoide). Dependiendo del origen de la fuerza el actuador se denomina “neumático”, “hidráulico” o “eléctrico”. En la Figura. 2.8 se presenta una clasificación de estos actuadores [25].

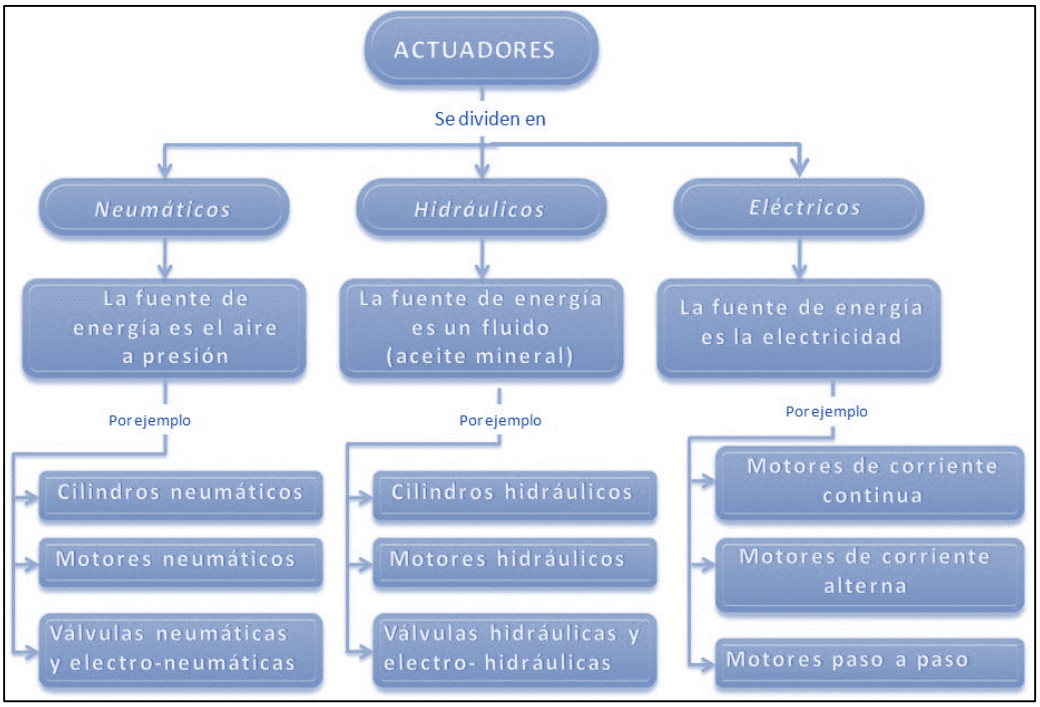


Figura. 2.8. Clasificación de actuadores.

Cada dispositivo actuador cuenta con diversas características que permiten usar sus elementos para aplicaciones específicas. La Tabla 2.2. Muestra una comparativa de las ventajas y desventajas de cada tipo de actuador.

Tabla 2.2. Comparativa de los distintos tipos de actuadores.

Tipo	**Ventajas**	**Desventajas**
Neumático	Bajo costo Rápidos Sencillos Robustos	Requieren de instalaciones especiales Ruidosos
Hidráulico	Rápidos Alta capacidad de carga Presentan estabilidad frente a cargas estáticas.	Requieren instalaciones especiales. Son de difícil mantenimiento. Resultan poco económicos.
Eléctrico	Precisos y fiables. Silenciosos. Su control es sencillo Son de una fácil instalación	Potencia limitada

2.5 Servomotores

El servomotor es un dispositivo que dispone en su interior de un motor de corriente continua con un eje de rendimiento controlado. Este puede ser llevado a posiciones angulares específicas al enviar una señal codificada. Con tal de que una señal codificada exista en la línea de entrada, el servo mantendrá la posición angular del engranaje. Cuando la señal codificada cambia, la posición angular de los piñones cambia. En la práctica, se usan servos para posicionar superficies de control como el movimiento de palancas, pequeños ascensores y timones. En la figura 2.9 se muestran los componentes principales de un servomotor.

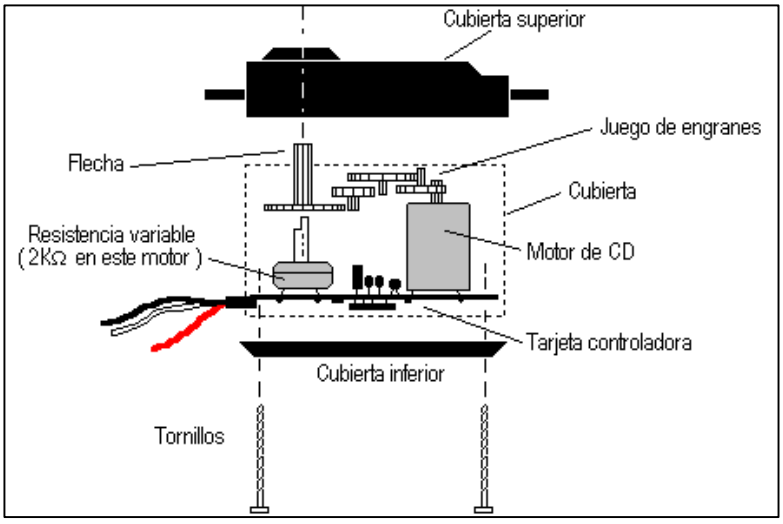


Figura.2.9. Principales componentes de un servomotor.

El servomotor tiene algunos circuitos de control y un potenciómetro (una resistencia variable) está es conectada al eje central del servomotor. Este potenciómetro permite a la circuitería de control, supervisar el ángulo actual del servomotor. Si el eje está en el ángulo correcto, entonces el motor está apagado. Si el circuito verifica que el ángulo no es el correcto, el motor girará en la dirección adecuada hasta llegar al ángulo correcto. El eje del servomotor trabaja en un movimiento angular de entre 0° y 180°.

La cantidad de voltaje aplicado al motor es proporcional a la distancia que éste necesita viajar. Así, si el eje necesita regresar una distancia grande, el motor regresará a toda velocidad. Si este necesita regresar sólo una pequeña cantidad, el motor correrá a una velocidad más lenta. A esto se le llama control proporcional [26].

2.5.1 Servomotor controlado por PWM

El servomotor es un tipo de motor pero adicionado con algunas funciones avanzadas, este tipo de motor funciona por medio de una señal demodulación por anchura de pulso, PWM (por sus siglas en ingles Pulse Width Modulation) [27]. Este sistema consiste en generar una onda cuadrada en la que se varía el tiempo que el pulso está a nivel alto, manteniendo el mismo período (normalmente), con el objetivo de modificar la posición del servomotor según se desee.

El sistema de control de un servomotor indica en qué posición se debe situar y la velocidad de movimiento que debe de tener. Esto se lleva a cabo mediante una serie de pulsos tal que la duración del pulso indica el ángulo de giro del motor. Cada servo tiene sus márgenes de operación, que se corresponden con el ancho del pulso máximo y mínimo que el servo entiende. Los valores más generales se corresponden con pulsos de entre 1 ms y 2 ms de anchura, que dejarían al motor en ambos extremos (0º y 180º). El valor 1.5 ms indicaría la posición central o neutra (90º) como se puede ver en la figura 2.10, mientras que otros valores del pulso lo dejan en posiciones intermedias. Estos valores suelen ser los recomendados, sin embargo, es posible emplear pulsos menores de 1 ms o mayores de 2 ms, pudiéndose conseguir ángulos mayores de 180°. Si se sobrepasan los límites de movimiento del servo, éste comenzará a emitir un zumbido, indicando que se debe cambiar la longitud del pulso. El factor limitante es el tope del potenciómetro y los límites mecánicos constructivos [28].

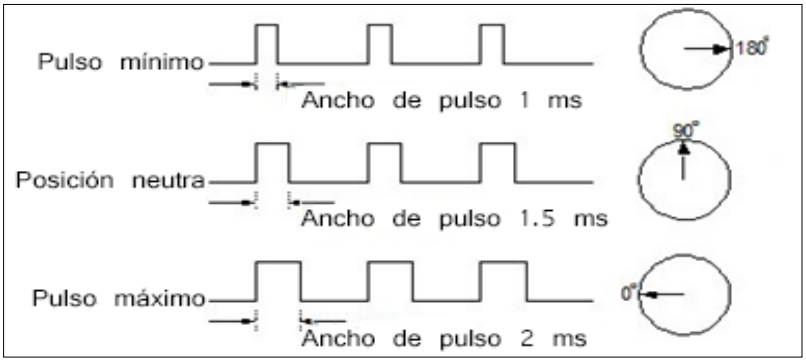


Figura.2.10 PWM Control de velocidad de un servomotor.

El período entre pulso y pulso (tiempo de apagado) no es crítico, e incluso puede ser distinto entre pulso y pulso. Se suelen emplear valores ~ 20 ms (entre 10 ms y 30 ms). Si el intervalo entre pulso y pulso es inferior al mínimo, puede interferir con la temporización interna del servomotor, causando un zumbido, y la vibración del eje de salida. Si es mayor que el máximo, entonces el servo pasará a estado dormido entre pulsos. Esto provoca que se mueva con intervalos pequeños.

Es importante destacar que para que un servo se mantenga en la misma posición durante un cierto tiempo, es necesario enviarle continuamente el pulso correspondiente. De este modo, si existe alguna fuerza que le obligue a abandonar esta posición, intentará resistirse. Si se deja de enviar pulsos (o el intervalo entre pulsos es mayor que el máximo) entonces el servo perderá fuerza y dejará de intentar mantener su posición, de modo que cualquier fuerza externa podría desplazarlo, en la figura 2.11 se puede ver de forma esquemática como un servomotor corrige constante su posición [28].

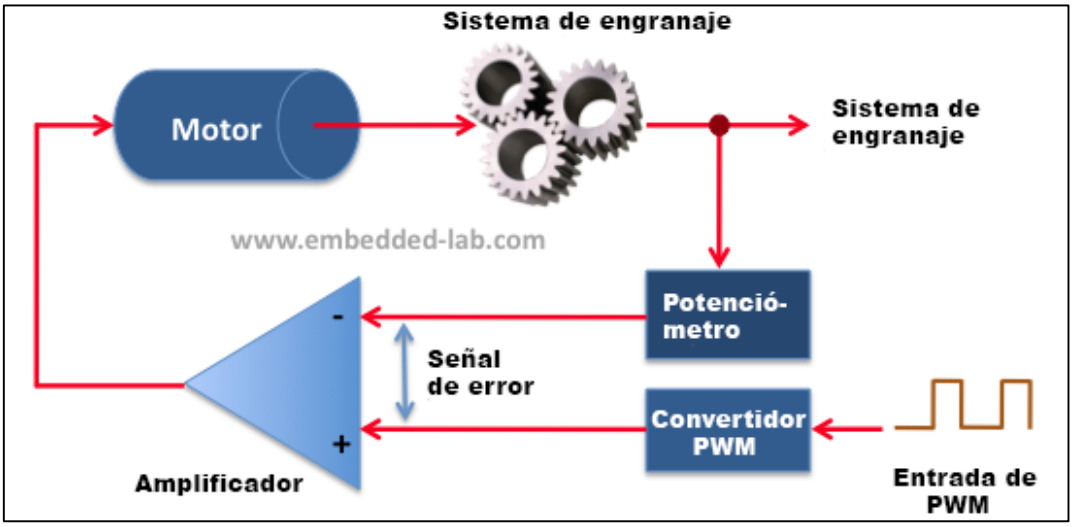


Figura.2.11. Diagrama general de funcionamiento de un servomotor [29].

2.5.2 Servomotor A0090 de Sparkfun

Los servomotores son un tipo de motor de corriente continua, que se caracteriza por posicionarse de forma muy precisa en un determinado rango de operación, para llegar a dicha posición el servomotor espera un tren de pulsos que corresponde a la posición que tomará el servomotor. El A0090 es un servo, de uso general estándar, de bajo costo, analógico de potencia, de alta definición, en la figura 2.12 se puede observar el aspecto físico de este servomotor.

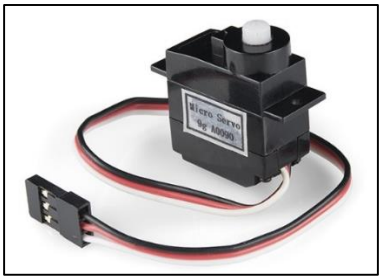


Figura.2.12. Servomotor A0090 [30].

En la tabla 2.3 se detallan sus características.

Tabla 2.3. Especificaciones técnicas servomotor A0090 [30].

Características	**Especificación**
Peso	43g
Dimensiones	40.7x15.5x39.5mm
Voltaje	4.4V~6.0V
Torque	4.4kg.cm
Velocidad	0.12sec/60°
Tipo de engranes	Plásticos
Temperatura almacenamiento	-20℃~55℃
Ancho de banda	≤4us

2.6 Control remoto mediante una tarjeta de propósito específico.

El control programado remoto es el encargado de controlar a distancia, algunas acciones en el vehículo como son el encendido y activación o desactivación de la alarma, para lo cual se puede auxiliar de Internet como puente de comunicación para la interacción con el protocolo SSH (Secure SHell). (Véase Apéndice D). A continuación se desglosan algunas de las características de Internet que son importantes para el desarrollo del sistema propuesto.

Para coordinar y controlar los nodos y servomotores se han empleado diversas tarjetas electrónicas que son capaces de procesar, almacenar, transmitir y recibir datos. En esta sección abordaremos los aspectos técnicos generales de la tarjeta Raspberry Pi, debido a que esta tarjeta cuenta con las capacidades antes señaladas.

La Raspberry Pi modelo B es una de las tarjetas más versátiles en el mercado de las computadoras de propósito específico, una de las principales razones por las que se decidió su uso, fue por su alta capacidad de procesamiento, ya que cuenta con un procesador ARM11 a 700 MHz que puede llegar hasta 1 GHz, cuenta con dos puertos USB uno de los cuales fue empleado para implementar la tarjeta de comunicación hacia Internet, otra característica de hardware fue el puerto GPIO el cual establece una comunicación directa entre procesador y dicho puerto; La comunicación con el procesador se realiza mediante la programación en Python (Véase Apéndice C).

Un problema al elegir esta tarjeta fue su nula disponibilidad en el país por lo que se decidió importarla, proceso que duró alrededor de cuatro meses, sin embargo el precio de 35 usd aumento los beneficios que se podrían obtener de esta tarjeta, cabe mencionar que tarjetas de uso común como Arduino o similares no cubren ni una pequeña parte de las características con las que cuenta la Raspberry Pi, incluida su conexión a Internet directa mediante un puerto RJ45, y sus 2 puertos USB, ya que por dichos puertos se puede hacer la adaptación de una antena WiFi de tipo USB , todo lo anterior llevó a la elección de la tarjeta. Además que permitió reducir drásticamente el costo de fabricación del prototipo al solo usar una tarjeta y no varias, en la figura 2.13 se observan las partes principales de la Raspberry Pi.

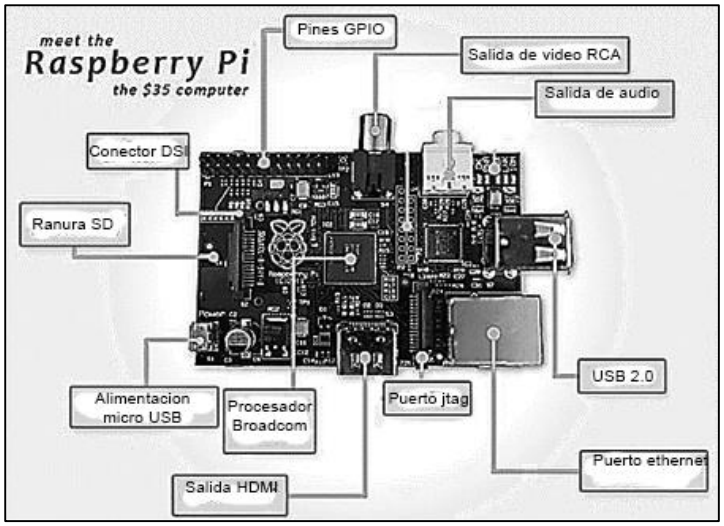


Figura. 2.13. Componentes principales de la Raspberry Pi [31].

2.7 Comunicación inalámbrica

Se le llama comunicación inalámbrica a aquella en que el emisor como el receptor no utiliza cables para su transmisión física, sino ondas electromagnéticas moduladas, como en todos los modos de comunicación, la comunicación inalámbrica también posee protocolos de transmisión, dichos protocolos poseen diversas especificaciones de acuerdo al uso que se le requiera. Los estándares de las comunicaciones inalámbricas sirven para crear dispositivos y software capaz de satisfacer ciertas características, que hacen eficiente o no a un protocolo.

A continuación se describen algunas de las características de los protocolos inalámbricos más populares.

2.7.1 Bluetooth

Bluetooth [32] proporciona una vía de interconexión inalámbrica entre diversos aparatos que cuentan con esta tecnología, como teléfonos celulares, computadoras de mano (Palm, Pocket PC), cámaras, computadoras portátiles, impresoras.

La especificación de Bluetooth define un canal de comunicación máxima de 720Kb/seg con rango óptimo de 10 metros (opcionalmente 100m).

La frecuencia de radio con la que trabaja está en el rango de 2.4 a 2.48 Ghz con amplio espectro y saltos de frecuencia con posibilidad de transmitir en Full Duplex con un máximo de 1600 saltos/seg. Los saltos de frecuencia se dan entre un total de 79 frecuencias con intervalos de 1Mhz, lo que le permite dar seguridad y robustez.

La potencia de salida para transmitir a una distancia máxima de 10 metros es de 0dBM (1 mW), mientras que la versión de largo alcance transmite entre -30 y 20dBM (100 mW).

Para lograr alcanzar el objetivo de bajo consumo y bajo costo, se ideó una solución que se implementar un chip utilizando circuitos CMOS. De esta manera, se logró crear una solución de 9x9mm y que consume aproximadamente 97% menos energía que un teléfono celular común.

2.7.2 Zig Bee

ZigBee [33] proviene de la familia de protocolos 802.15, la diferencia entre 802.15.4 y ZigBee., es que la primera es un estándar de radio bajo la familia Área de red personal inalámbrica (por sus siglas en inglés WPAN) y ZigBee es la especificación definiendo las aplicaciones de red capaces de soportar esos dispositivos.

ZigBee está diseñado para operaciones de baja potencia. Un dispositivo ZigBee puede dejarse sin utilizarse por un periodo largo de tiempo sin necesidad de volver a cargar la batería de ese dispositivo.

Características del sistema:

Bandas en las que opera: 2.4 Ghz, 915 MHz y 868 MHz.

Métodos de transmisión: DSSS, se focaliza en las capas inferiores de red (Física y MAC).

Velocidad de transmisión: 20 kbit/s por canal.

Rango: 10 y 75 metros.

2.7.3 WiFi

Wi-Fi [34] es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11. Es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de

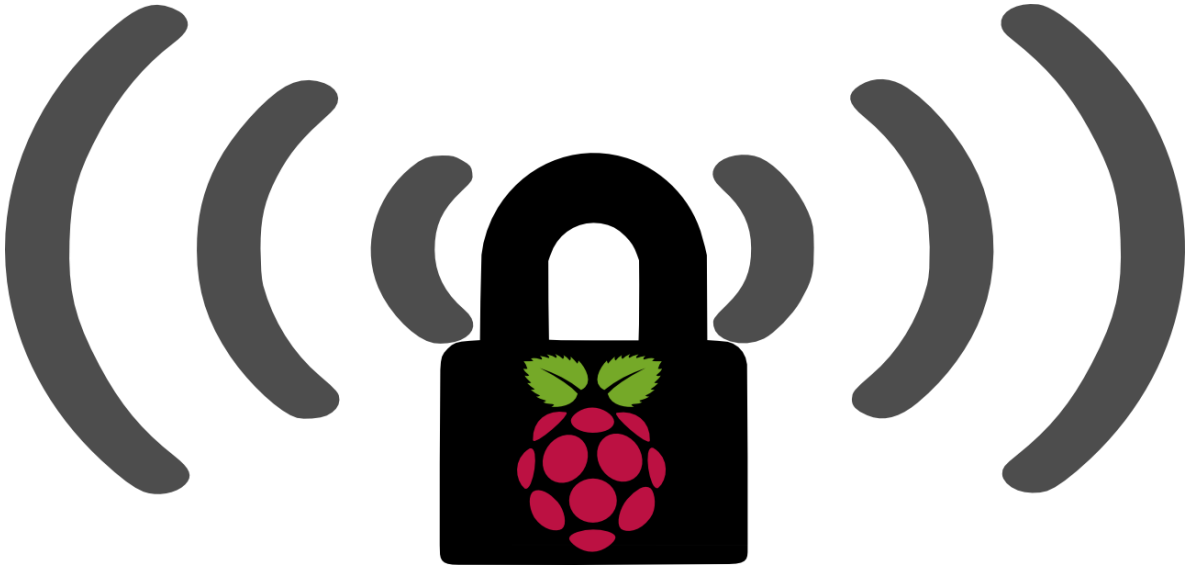
enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local. Wi-Fi, o 802.11b, es un estándar robusto, maduro y bien establecido que continúa creciendo y evolucionando. Se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad también se utilice para acceder a Internet desde casi cualquier tipo de dispositivo. Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la Wireless Ethernet Compatibility Alliance), la organización comercial que prueba y certifica que los equipos cumplen los estándares IEEE 802.11x. En la actualidad son 3 las diferentes versiones comerciales con las que se comercializan dispositivos con WiFi dichas versiones son B,G y N.

WiFi B y G son los más tradicionales y llevan bastante tiempo en el mercado, mientras que el N lleva pocos años de existencia.

Una conexión Wireless B, puede transferir 11,000 Mbit/s o 1.375 megas por segundo, la conexión Wireless G, puede transferir 54,000 Mbit/s o 6.750 megas por segundo y la conexión Wireless N, puede transferir 200,000 Mbit/s o 25.00 megas por segundo. En cuanto al rango los protocolos Wireless B & G, tienen un rango de 30 metros, y el Wireless N, tiene un rango de 50 metros.

CAPÍTULO 3

DISEÑO DEL SISTEMA PISECURITY CAR



CAPÍTULO 3 Diseño del Sistema Pisecurity car

En el presente capítulo de detallará el proceso de diseño de un sistema de monitoreo y control en tiempo real de un automóvil mediante internet utilizando redes de sensores y actuadores, así mismo se describirán las diferentes etapas que conforman el proyecto y los elementos que la conforman.

3.1 Requisitos del sistema

Para que el sistema propuesto sea competitivo con otros sistemas similares ya existentes debe de satisfacer de la mejor manera posible los siguientes aspectos:

- No invasivo. Implica que el sistema sea lo menos agresivo posible en los componentes originales del vehículo, desde la instalación hasta la colocación final se debe de evitar hacer modificaciones al chasis y a la estructura del vehículo.

- Poseer un alcance inalámbrico de al menos 25 metros. Para satisfacer este requisito es necesario incluir en el sistema una tarjeta inalámbrica que tenga un largo alcance.

- Sistema inteligente. Una vez activado el sistema tiene que ser capaz de realizar una acción de manera autóma ante una posible amenaza de intrusión no autorizada, aun cuando el usuario no este supervisando el estado de su vehículo.

- Bajo costo. Su costo debe ser competitivo frente a otros sistemas similares existentes en el mercado.

- Difícil de corromper. Implica que el sistema debe poseer la suficiente seguridad como para mantener la autenticidad del propietario del vehículo, esto significa que solo el usuario conocerá la forma de activar y desactivar el sistema y asi mantener la fiabilidad del sistema.

3.2 Diseño del sistema

El sistema constara de cuatro etapas principales: sensado, procesamiento, comunicación y control. Cada una de las etapas realizará una acción muy específica y en conjunto garantizarán el monitoreo del automóvil, el control del sistema de encendido, así como de informar al usuario a través de Internet del estado del automóvil.

3.2.1 Diagrama a bloques

En esta sección se presenta el diseño del sistema por medio de un diagrama a bloques que se encuentra en la Figura. 3.1. El diagrama a bloques es un explicación gráfica que denota las principales funciones de acción para poder lograr el objetivo de controlar y monitorear vía remota un automóvil.

En el diagrama es posible observar las diferentes etapas y cómo interactúan entre si; la información proveniente de la etapa de sensado, es enviada a la etapa de procesamiento, que es la encargada de tomar las acciones necesarias, la información una vez procesada pasa a la etapa de comunicación, esta etapa envía y recibe datos provenientes de la etapa de procesamiento y del usuario a través de Internet, por último la etapa de control, tiene como objetivo activar o desactivar el sistema de encendido dependiendo de la información ya procesada de la etapa de sensado, la información recibida y procesada del usuario a través de la red y de ser necesario de rutinas programadas en el caso de que no exista una respuesta del usuario ante un intento de robo.

En las siguientes secciones se describirá con mayor detalle cada una de las etapas que conforman el sistema.

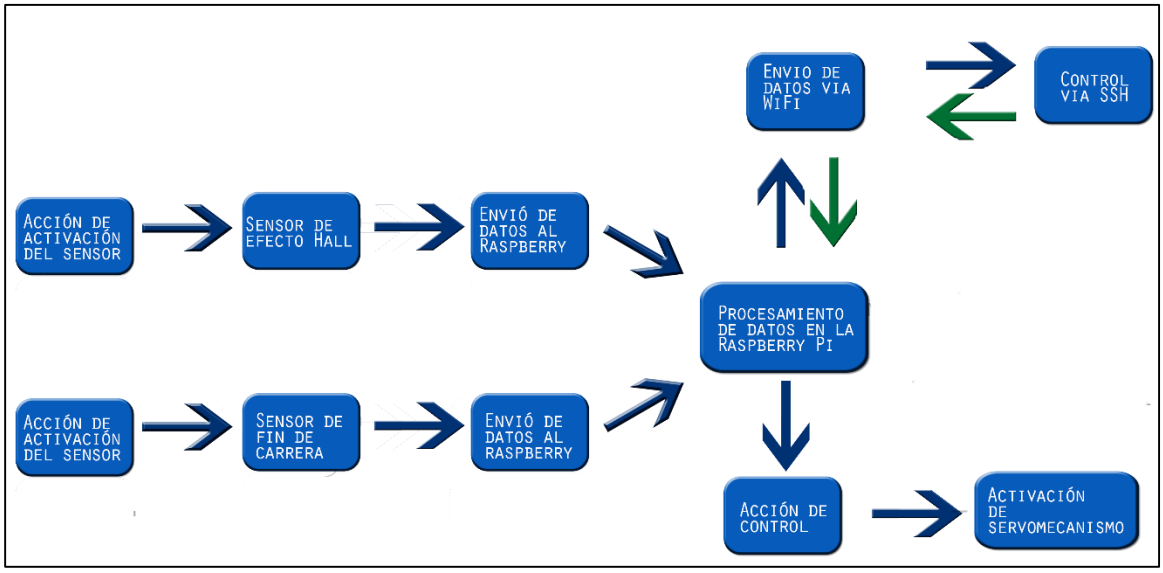


Figura.3.1.Diagrama a bloques.

3.3 Etapa de sensado

Esta etapa se encarga de conectar los diversos sensores que serán utilizados para el monitoreo del automóvil, en esta sección se mostrará la forma en la que se conectan los sensores al sistema y su disposición en el vehículo. La figura 3.2 muestra la función básica del proceso de sensado y el tipo de sensor que va ser utilizado en cada sección del automóvil, los cuales están descritos con mayor detalle en la sección 2.3.

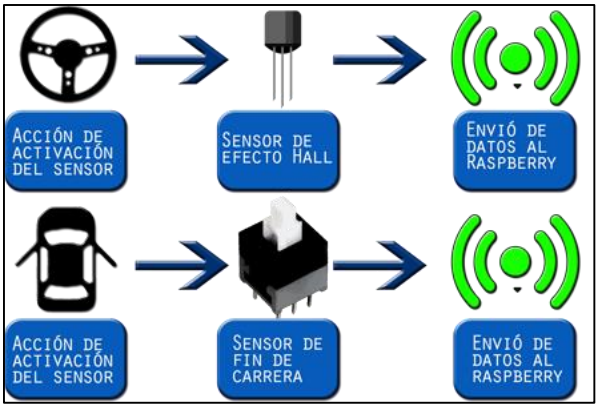


Figura.3.2 Diagrama de la etapa de sensado.

3.3.1 Sensores de fin de carrera

Se les denomina de fin de carrera o interruptor de límite a los sensores que se activan al contacto con un límite, que acciona de forma mecánica el interruptor para enviar una señal de tipo eléctrica.

Los sensores de fin de carrera elegidos para el sistema son genéricos y no poseen una matrícula específica siendo sus únicas referencias su tamaño, el voltaje y la corriente que toleran, este tipo de sensores fueron elegidos ya que soportan de forma muy eficiente el maltrato físico que ejercerá la puerta donde serán colocados.

Los sensores serán instalados en cada una de las puertas del automóvil, en la Figura. 3.3 se muestra la disposición de los sensores en el automóvil. Dichos sensores estarán desactivados mientras las puertas estén completamente cerradas, al intentar forcejear o abrir la puerta mandará una señal, es decir, el sensor se activará.

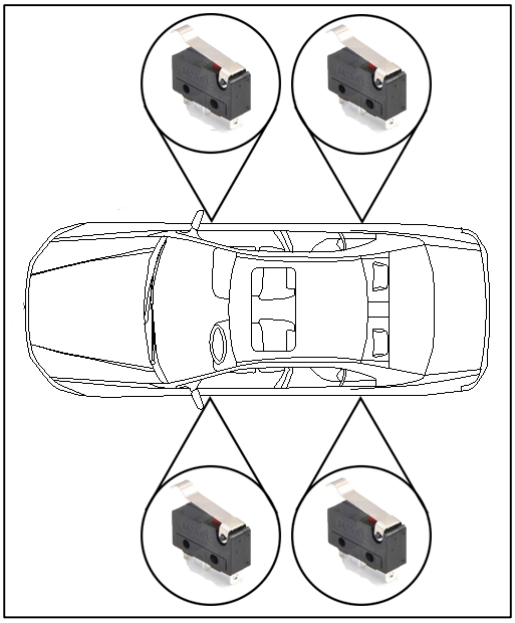


Figura.3.3 Disposición de los cuatro sensores de fin de carrera en las puertas del vehículo.

Para la utilización de los sensores de fin de carrera, se decidió conectarlos directamente a 4 pines del puerto GPIO de la Raspberry PI (descrito en la sección 3.4), como se muestra en la Figura. 3.4, se coloca un por cada puerta del vehículo (tomando en cuenta que por lo regular los automóviles poseen 4 puertas), al estar conectados directamente los sensores al puerto GPIO, el puerto recibe de forma inmediata los datos provenientes de los sensores, una vez que el puerto GPIO recibe por lo menos una señal de activación de alguno de los sensores de fin de carrera, significará que alguna puerta ha sido abierta o se está intentando abrir. La señal proveniente de los sensores es un pulso del mismo voltaje y corriente al suministrado que es de +5v a 600 mA, posteriormente la señal llegará al puerto GPIO para su posterior procesamiento y manejo de la información.

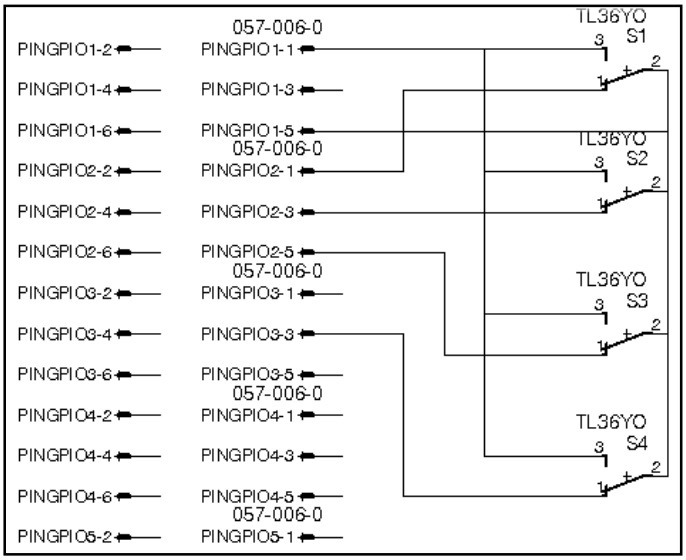


Figura. 3.4 Conexión de los sensores de fin de carrera al puerto GPIO de la Raspberry.

3.3.2 Sensor efecto Hall

El sensor de efecto Hall basa su funcionamiento en la detección de campos magnéticos, convierte una variación en el campo magnético, cercano a su zona de detección, en una corriente eléctrica. Es decir, al detectar un campo magnético se activa.

El sensor de efecto Hall es el encargado de detectar el giro del volante, en cualquier sentido. El sensor seleccionado para realizar esta tarea es el US2881KUA mostrado en la figura. 3.5 de la marca Melexis [35], es de tipo switch, lo que significa que la variación en el campo magnético cercano a su zona de detección, activa el sensor dependiendo del polo magnético que este cerca a dicha zona.

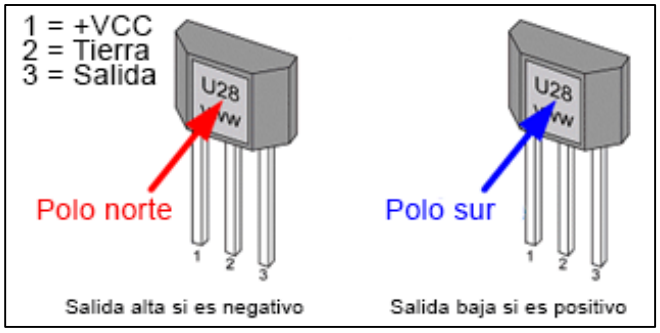


Figura. 3.5 Funcionamiento sensor efecto Hall.

En la tabla 3.1 se presentan las características eléctricas del sensor US1881KUA, mismas que son apropiadas para la conexión directa del sensor al puerto GPIO de la Raspberry Pi, ya que solo es necesaria una resistencia eléctrica como protección.

Tabla 3.1 Características del sensor de efecto Hall.

Parámetros eléctricos	Mínimos	Máximos
Voltaje	3.5v	24v
Corriente	60mA	80mA
Punto de operación	0.5mT	9.5mT

El sensor de efecto Hall es conectado al puerto GPIO como se muestra en la figura. 3.5, para que la información del sensor sea posteriormente procesada por la tarjeta Raspberry Pi.

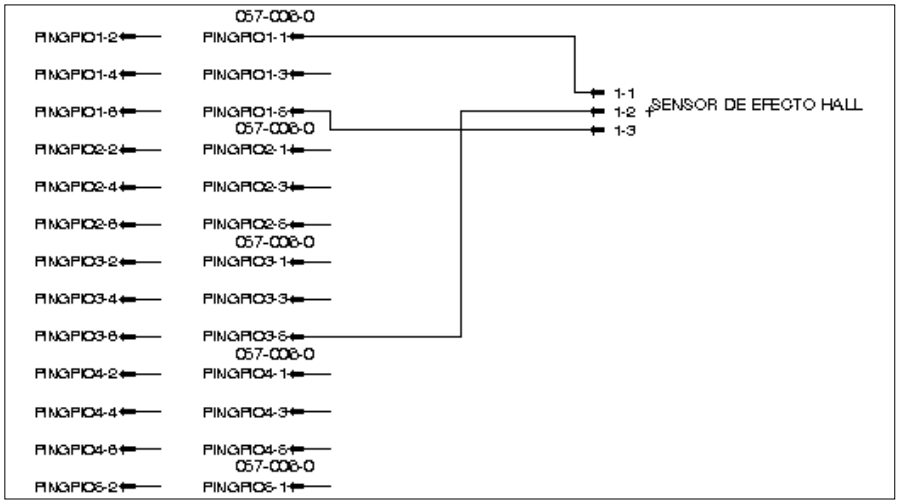


Figura.3.6. Diagrama esquemático del sensor de efecto Hall.

Se decidió colocar un arreglo de 3 imanes cerámicos o ferritas, que son los encargados de dar la variación al campo magnético en la zona de detección del sensor de efecto Hall y con esto activar los sensores, se eligieron estos imanes por su estabilidad y su bajo costo, además de su bajo coeficiente magnético.

La configuración elegida para los imanes se puede observar en la figura. 3.7, dicha configuración ofrece la capacidad de detectar el giro del volante, mediante el sensado de un polo magnético; al detectar otro polo el sensor se activará y enviará una señal al puerto GPIO, dicha señal representará un movimiento posición original del volante.

Figura. 3.7. Configuración de imanes en el volante.

El sensor de efecto Hall será montado en la base del volante. Al volante se le colocará un imán con polo norte (N) alineado con el sensor de efecto hall, además de otros dos imanes con el polo sur (S) en cada lado del volante que servirán para corroborar el estado del sensor para que al momento de ser desalineados se active el sensor, esta configuración se muestra en la figura. 3.8.

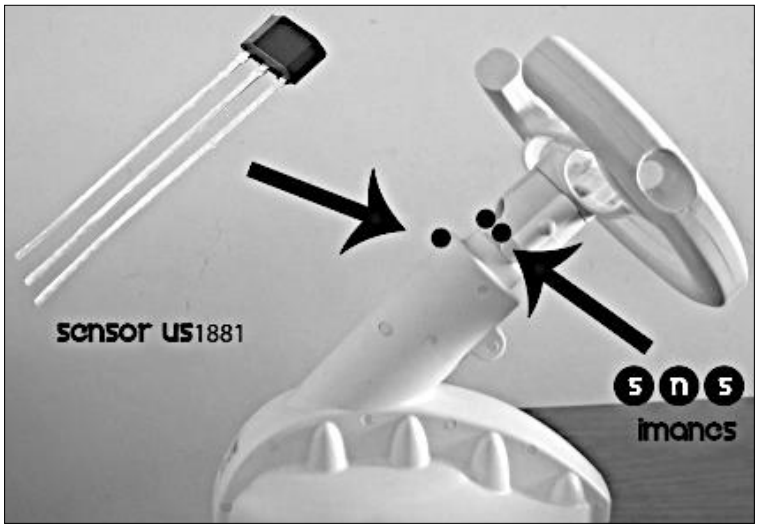


Figura. 3.8 Posicionamiento de sensor de efecto Hall e imanes.

3.4 Etapa de procesamiento

Es la etapa más importante del sistema ya que en ella se encuentra el cerebro del sistema que es la Raspberry Pi, en esta etapa se toman todas las decisiones que ejecuta sistema. Recolecta la información proveniente de la etapa de sensado, y las ordenes provenientes

de la etapa de comunicación, esta etapa también se encarga de dar las órdenes que ejecutará la etapa de control. La figura. 3.9 muestra un esquema de la etapa de procesamiento, así como de la Raspberry Pi, pieza central y cerebro que dota de autonomía sistema.

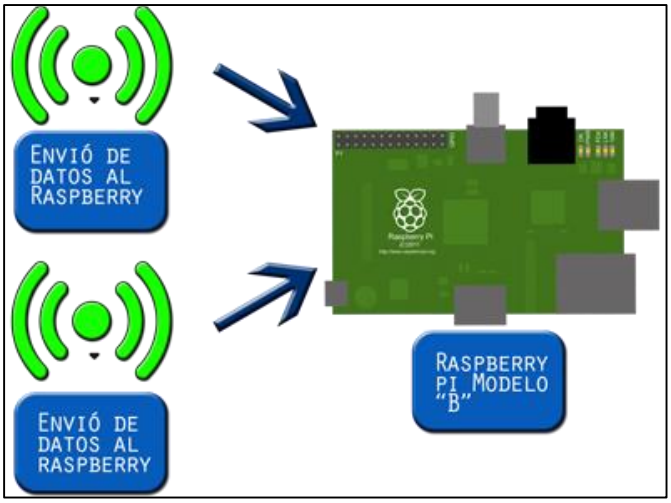


Figura. 3.9 Diagrama de la etapa de procesamiento.

3.4.1 Raspberry Pi

La Raspberry Pi es una mini computadora del tamaño de una tarjeta de crédito que puede conectarse a un monitor de TV y a un teclado de tipo USB. Es una mini computadora muy capaz ya que puede ser usada como una computadora genérica de escritorio, es capaz procesar hojas de cálculo, textos, juegos, etc. También puede reproducir videos de alta definición y procesar grandes volúmenes de datos [36].

En la figura. 3.10 se muestran los componentes principales de la Raspberry Pi modelo B.

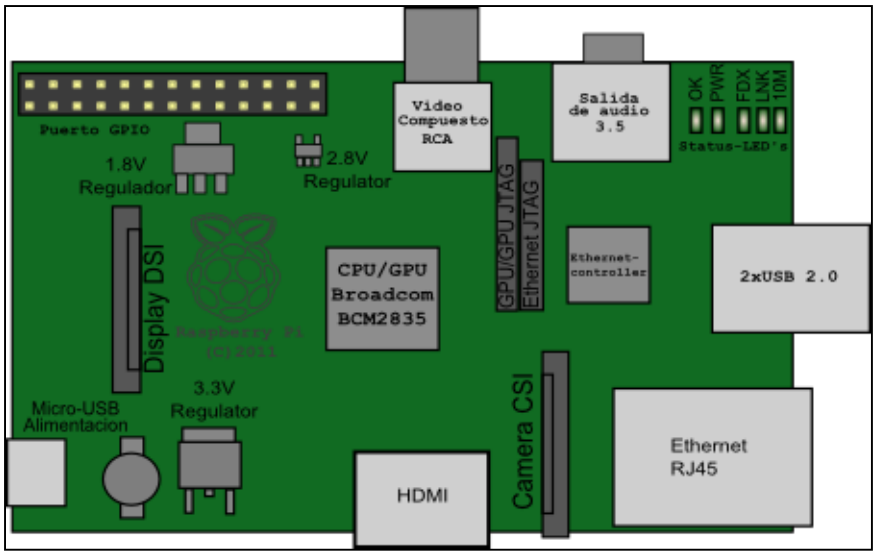


Figura. 3.10 Raspberry Pi modelo B [36].

La Raspberry Pi modelo B posee un sistema llamado “System-on-a-chip” que básicamente reúne el CPU, el GPU y la memoria RAM en un solo chip, las características del chip Broadcom BCM2835 son las siguientes: contiene un procesador central (CPU) ARM1176JZF-S a 700 MHz, un procesador gráfico (GPU) VideoCore IV, y 256 MB de memoria RAM. Se alimenta mediante una entrada micro USB de 5 volts, su almacenamiento está dado por una tarjeta SD, en dicha tarjeta se almacena el sistema operativo GNU/Linux y los diferentes programas que vienen agregados a él, tiene un puerto de Ethernet RJ45, dos puertos USB 2.0, salida de audio de 3.5, puerto HDMI, salida de video compuesto RCA, leds indicadores del status de la computadora y un puerto GPIO muy característico de la Raspberry Pi y que es parte fundamental para el desarrollo del proyecto.

3.4.2 Manejo de datos

La tarjeta Raspberry Pi puede comunicarse con dispositivos externos mediante el conector GPIO (General Purpuse Input Output) que tiene incorporado, figura 3.11. En dicho conector se integran pines de alimentación (+5 y +3.3 V), tierra y 8 pines de entradas/salidas capaces de implementar diferentes protocolos, estos 8 pines poseen un nivel lógico de 3.3V [37].

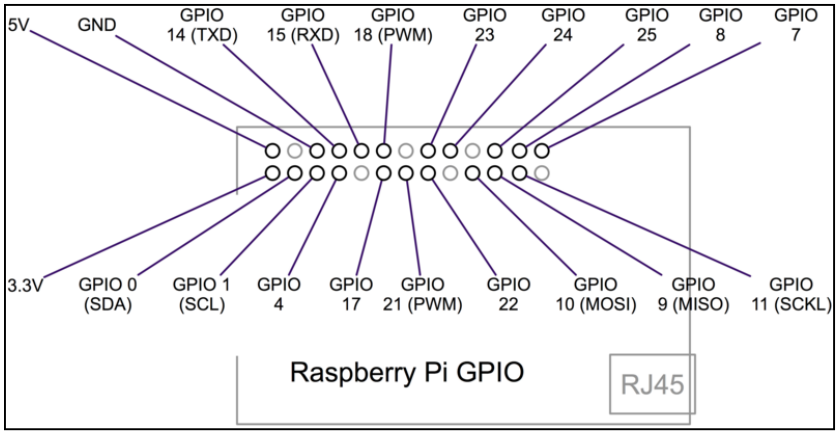


Figura. 3.11 Puerto GPIO de la Raspberry Pi [38].

Es importante saber que a nivel software se tiene que saber con qué pin se requiere comunicar. Además de los pines correspondientes a +5V, +3.3V y tierra, el puerto GPIO (General Purpuse Input Output) tiene 8 pines de uso genérico donde se puede conectar dispositivos de hardware.

Es muy importante resaltar que cualquier manipulación errónea, conexionado equivocado o descarga de estática sobre las pines GPIO (General Purpuse Input Output) puede dañarlas de forma permanente. Por esta razón es recomendable tener sumo cuidado al manipular los dispositivos que se le conecten a este puerto.

En los sistemas operativos GNU/Linux se referencia casi todo lo que maneja en forma de ficheros, y los pines del puerto GPIO (General Purpuse Input Output) no son la excepción. Aunque el núcleo de GNU/Linux sabe de la existencia de dicho puerto, el resto del sistema no, por esa razón se tiene que informar (vía software) a la Raspberry Pi de la presencia del

puerto GPIO que sea reconocido. Para ello se utilizan librerías que hacen la función de intérpretes, para este sistema se utilizara la librería general del lenguaje de programación Python (Véase apéndice C), llamada GPIO.py versión 0.0.3.a, dicha librería posee las herramientas necesarias para la comunicación directa entre el procesador y el puerto, es decir, con esta librería se puede programar de manera directa el procesador para que pueda interpretar los datos provenientes de la etapa de sensado.

Para poder utilizar los pines de entrada/salida del puerto GPIO(General Purpuse Input Output) se realizará un programa en Python que permitirá utilizar el puerto como salida y entrada de datos. La figura. 3.12 muestra la importación de la librería GPIO(General Purpuse Input Output) de Python y las sentencias para entrada y salida de datos.

```
import RPi.GPIO as GPIO                 #Para utilizar el Puerto GPIO
GPIO.setup (pinx , GPIO.IN)             #Para entrada de datos
GPIO.setup (piny , GPIO.OUT)            #Para salida de datos
```

Figura. 3.12 Sentencias de manejo puerto GPIO.

Las líneas anteriores muestran cómo se maneja el flujo de datos entre el puerto GPIO y un programa en Python, el procesamiento depende de la información recibida por el puerto GPIO y del algoritmo implementado en Python.

Para ello solo se manejan los estados de los puertos con valores booleanos (“1” o “0”), uno para cuando el pulso es alto y cero para cuando el pulso es bajo.

3.5 Etapa de comunicación

Esta etapa recibirá los datos obtenidos por la etapa de sensado y los enviará de igual forma a las etapas de comunicación y control. Esta última etapa regirá una interfaz que será activada automáticamente, a su vez, la etapa de comunicación puede enviar una orden adicional, dependiendo de la decisión tomada por el usuario. Por ejemplo, bloquear o permitir el acceso al encendido. La figura. 3.13 muestra de forma esquemática la interacción de los componentes de esta etapa.

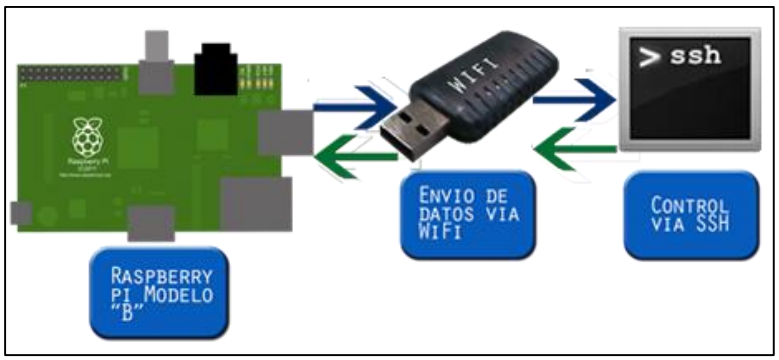


Figura.3.13 Diagrama de la etapa de comunicación.

La comunicación es una de las ventajas más sobresalientes de este sistema con respecto a dispositivos similares ya existentes en el mercado, ya que el presente sistema cuenta con la capacidad de monitorear y controlar de manera remota un automóvil mediante una terminal esto es, un teléfono celular o algún otro dispositivo que cuente con comunicación a Internet. La comunicación depende de dos sub-etapas, las cuales son un módulo Wifi y terminal SSH o interfaz de operación remota.

3.5.1 Modulo WiFi

Esta sub-etapa tiene como función enviar los datos de la etapa de procesamiento a la web por medio de una conexión de ejecución segura.

Para realizar esto se envían los datos obtenidos por los sensores vía WiFi a un router que esté conectado al Internet, una vez realizado esto se puede acceder a los datos o modificarlos por medio de una interfaz de conexión remota esta conexión será gestionada por medio de un cliente de SSH (Secure SHell).

La necesidad de enviar y recibir datos fuera de la Raspberry Pi, lleva a buscar diversas opciones para comunicarse remotamente a un dispositivo móvil. La Raspberry Pi trae por default una conexión Ethernet lo cual lo confina a estar siempre conectado a un cable para tener acceso a Internet. Sin embargo, existen en el mercado diversas soluciones para realizar conexiones inalámbricas que van desde el RF (Radio Frecuencia), Bluetooth, Zig Bee hasta el WiFi.

Se eligió la solución WiFi dado que el Gobierno del Distrito Federal tiene previsto realizar una infraestructura que haga llegar el WiFi a toda la ciudad. Además de esto el servicio de WiFi se puede contratar por un módico precio a uno de los proveedores de servicio existentes.

En este caso el módulo WiFi que será utilizado es el DWA-140 Range Booster de la marca D-Link Figura. 3.14, dicho módulo se conecta a la Raspberry Pi por medio de su puerto USB 2.0.

Figura. 3.14. Módulo WiFi USB modelo DWA-140.

Para que el módulo WiFi funcione es necesario verificar que este tenga el chipset Realtek RTL81CUS en cualquiera de sus familias, para el caso específico del módulo DWA -140 es necesario descargar el paquete de la versión 1.53 del firmware de GNU/Linux. Una vez descargado se procede a ser descomprimido. A continuación se procede a copiar y

reemplazar el archivo *rt2870.bin* de las librerías del firmware de la Raspberry Pi y en su lugar colocar el archivo del mismo nombre del paquete descargado en el nuevo firmware.

La instalación del módulo WiFi se realiza mediante la ejecución del script que ejecuta la función de instalador y configurador del sistema. Dicho script debe contener el archivo de configuración inicial, así como los comandos de instalación para los diferentes tipos de seguridad de red existentes. Un ejemplo de ellos es el paquete WPA-suplicant que realiza la solicitud de conexión a una red con seguridad WPA o WPA2, además este script debe buscar el chipset específico modificado, analizar las interfaces de red disponibles y colocar la configuración inicial dependiendo el tipo de seguridad y gestionar los datos de la red como el SSID(identificador de red, por sus siglas en inglés Service Set IDentifier) y el Password.

3.5.2 Interfaz de operación remota (SSH)

Debido a que el envió de datos se puede hacer con una red pública es necesario garantizar en la medida de lo posible la seguridad con la que los datos van a ser transmitidos, para ello se utiliza una conexión SSH (Secure Shell) ya que esta garantiza que los datos en datagramas enviados (ordenes ejecutables y paquetes) pasaran por un túnel “directo” a la IP (Internet Protocol) deseada.

Para la operación remota del dispositivo se tendrá que seleccionar un cliente de SSH (Secure Shell) ya que la mayoría de los dispositivos como computadoras, Smartphones y tablets tienen la posibilidad de correr una aplicación que le permita hacer la función de SSH (Ver sección 4.2.2).

Una vez elegido el cliente SSH se prosigue a realizar la configuración con los datos de la Raspberry Pi, como se puede observar en la figura. 3.15, dichos datos son: la descripción, el host o IP, el puerto de conexión, el *login* y el *password*.

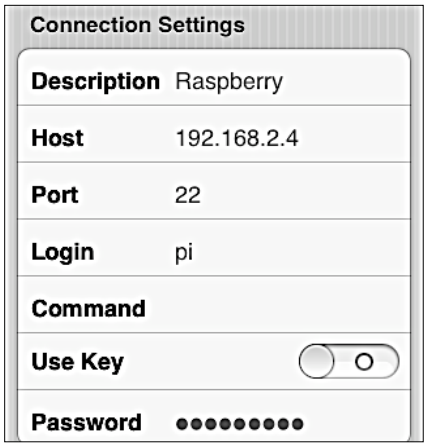


Figura. 3.15 Configuración de datos del cliente SSH [39].

Una vez realizada la conexión se pueden ejecutar los dos programas de seguridad cargados en la memoria de la Raspberry Pi, uno de activación y otro de desactivación del

sistema, una muestra de ejecución del programa activación se ilustra en la figura 3.16 (a) y (b).

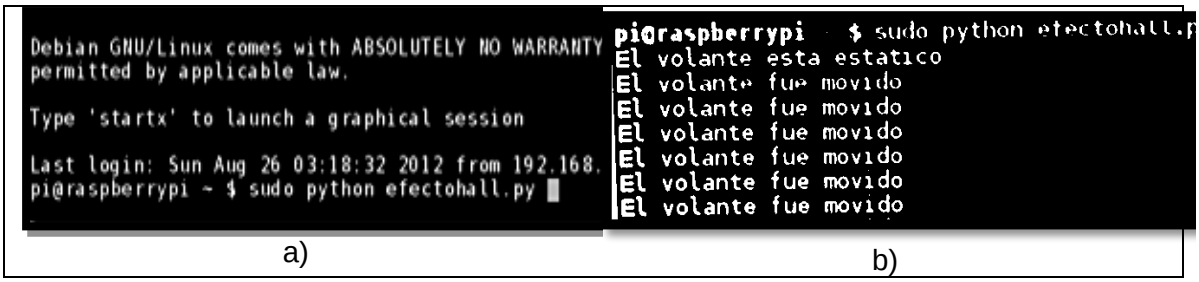


Figura.3.16. Programa de activación cargado en la Raspberry Pi. a) Comando de ejecución del programa, b) Programa ejecutado.

3.6 Etapa de control

Esta etapa constara de una interfaz para la activación de un zumbador y un servomecanismo de control, que será regido mediante las órdenes provenientes del puerto GPIO de la Raspberry Pi, en la figura. 3.16 se muestra de manera esquemática la interacción de los elementos de la etapa.

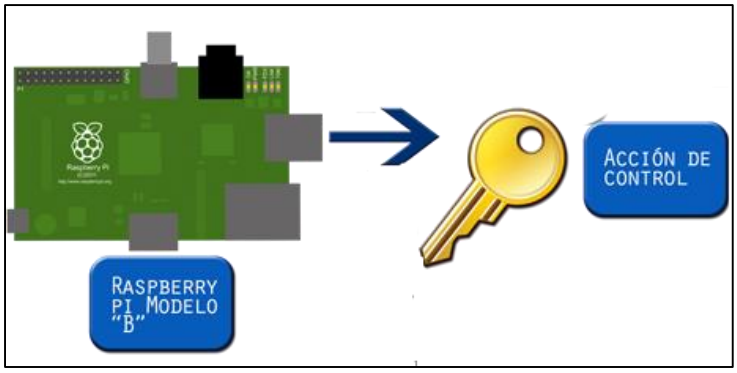


Figura. 3.17 Diagrama de la etapa de control.

3.6.1 Zumbador

Una vez que la Raspberry Pi ha procesado la información proveniente de la etapa de sensado y ha detectado la activación de un sensor de fin de carrera, accionará un zumbador que generará un sonido con el objetivo de desalentar al intruso.

El zumbador elegido para este sistema no tiene una matrícula y sólo puede diferenciarse de otros por sus características. Ver Tabla 3.2.

Tabla 3.2. Características del zumbador.

Parámetros eléctricos	Mínimo	Máximo
Voltaje	5.3v	7.2v
Corriente	60mA	80mA
Sonido	0 dB	75 dB

3.6.2 Servomotor

Para solventar la problemática del robo es importante que al detectar una intrusión se realice una acción contundente para evitar el robo del automóvil, dicha acción es cortar la energía al sistema de encendido, esto se puede realizar mediante la acción de un servomotor, que consiste en desconectar la alimentación del sistema de encendido del vehículo mediante un bloqueo mecánico, impidiendo la alimentación del vehículo , con esta acción se impide el arranque del motor del automóvil en la figura 3.18 se muestra un diagrama de lo antes descrito.

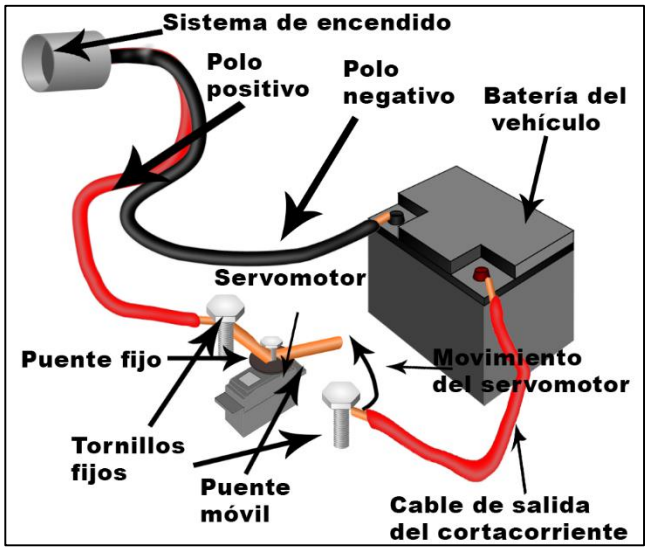


Figura.3.18. Esquema del cortacorriente.

La conexión del servomotor se realiza mediante un pin genérico de entrada/salida al puerto GPIO, el diagrama de conexión se muestra en la figura. 3.19. Así como la conexión del zumbador al mismo puerto, cabe mencionar que el servomotor puede generar corrientes parasitas que pueden afectar al microprocesador de la Raspberry Pi, por lo que es necesario utilizar un transistor como protección.

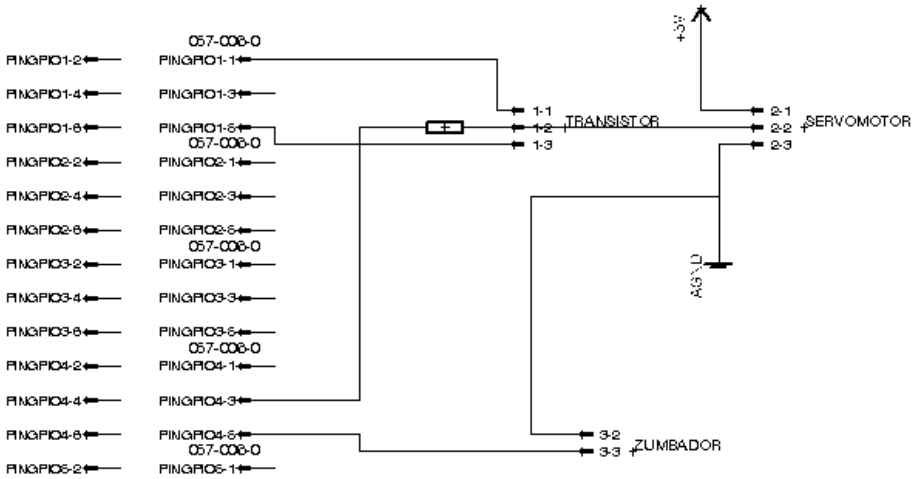


Figura.3.19. Diagrama de conexión del servomotor y el zumbador.

La etapa de control requiere de mayor potencia eléctrica que las demás etapas por lo que es necesaria una fuente externa, ya que la fuente de alimentación que trae por defecto la Raspberry Pi de 5 volts no soporta la corriente demandada por el servomotor que es 700mA como mínimo. Por otro lado, se deberá conectar una resistencia de 1 KΩ en la terminal positiva de la fuente al colector del transistor con el fin de aumentar la intensidad de la señal proveniente del puerto GPIO, ya que el servomotor por utilizar un embobinado demandará más corriente.

3.7 Diagrama de flujo del sistema propuesto

El inicio del diagrama comienza con la activación del sistema vía SSH, las órdenes son enviadas a la Raspberry Pi para que comience a censar el estado de los sensores, si alguno de los sensores presenta o no una alteración enviara la información de su estado para que sea procesada a través del puerto GPIO hacia la Raspberry Pi, una vez procesada la información de los sensores esta tomara dos caminos, en la figura 3.20 se muestra la primera parte del diagrama.

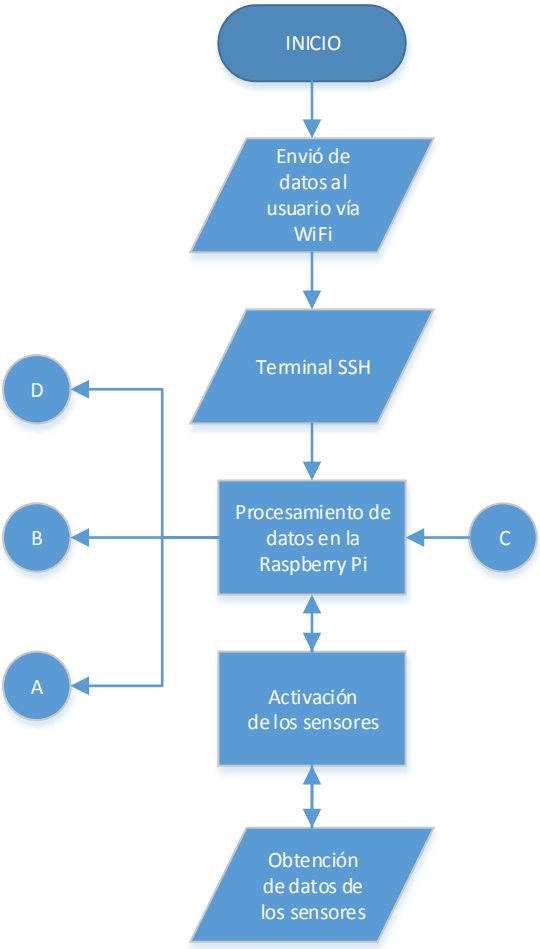


Figura.3.20. Primera parte del diagrama de flujo

En el primer camino en caso de que no exista una intrusión seguirá verificando el estado de los sensores, en caso de una intrusión enviara una orden de activación al servomotor lo que provocara que acción de bloqueo del encendido del vehículo, en la figura 3.21 se muestra la etapa “A” del diagrama de flujo.

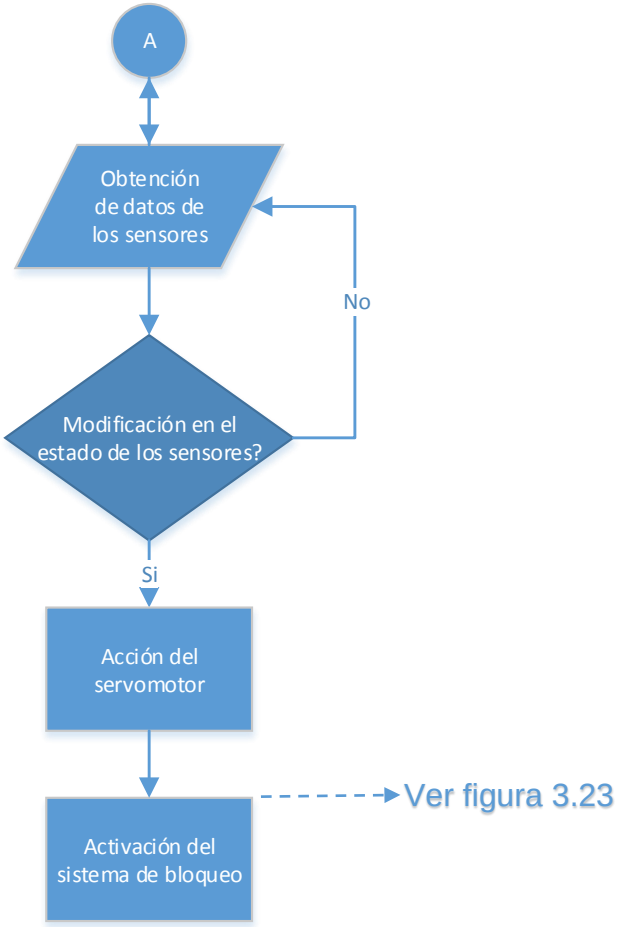


Figura.3.21. Etapa “A” del diagrama de flujo

En el segundo camino la información procesada provenientes de los sensores es enviada por la Raspberry Pi al usuario por medio de una conexión WiFi, el usuario puede acceder a ella por medio de una terminal remota SSH, en esa terminal remota que puede ser un smartphone, una tablet o una computadora, el usuario puede verificar el estado del sistema y en caso de que sea una falsa intrusión no autorizada puede desbloquear el sistema, en la figura 3.22 se muestra la etapa “B” del diagrama de flujo.

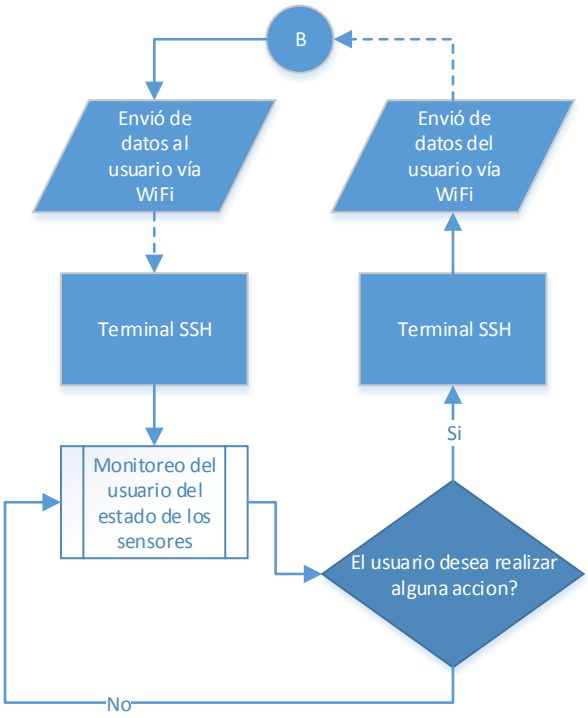
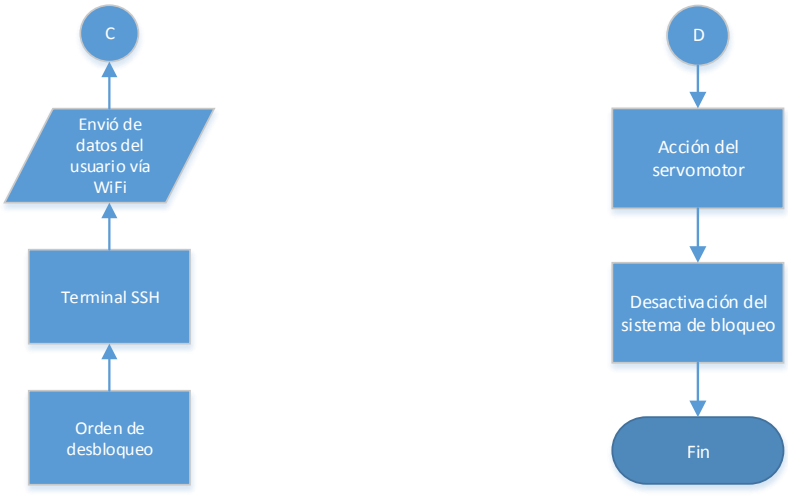


Figura.3.22. Etapa “B” del diagrama de flujo

Para volver a activar el sistema de encendido del automóvil, después de un bloqueo, es necesario que el usuario ejecute una restauración del sistema por medio de SSH, dicha orden será procesada por la Raspberry Pi (ver figura 3.23 a), la orden procesada por la Raspberry Pi la cual enviara una señal al servomotor lo que provocara que se desactive el sistema de bloqueo, con lo cual el encendido del vehículo regresara a su estado original. La restauración también reinicia el sistema por lo que el sistema propuesto estará nuevamente en funcionamiento.



a b

Figura.3.23. Restauración del sistema. a) Diagrama de flujo etapa “C” b) Diagrama de flujo etapa “D”

3.8 Software requerido

La Raspberry Pi cuenta con un sistema operativo nativo llamado Raspbian que tiene como base el sistema operativo Debian Wheezy con algunas mejoras de rendimiento para el procesador ARM, que es un sistema que consume pocos recursos computacionales existen versiones de 32 y 64 bits, cabe mencionar que se puede utilizar cualquier sistema operativo diseñado para procesadores ARM, como Raspbian, Arch Linux ARM, etc.

Para el manejo de puerto GPIO es necesario instalar la librería RPi.GPIO, para este particular caso se está utilizando la versión 0.3 (Véase Apéndice E).

Una vez instalada la librería es necesario instalar Python desde la terminal de la Raspberry Pi, se utilizará Python 3-dev por su estabilidad y mayor información disponible. El siguiente comando es el encargado de la instalación de descargar Python para su posterior instalación dentro de la Raspberry Pi.

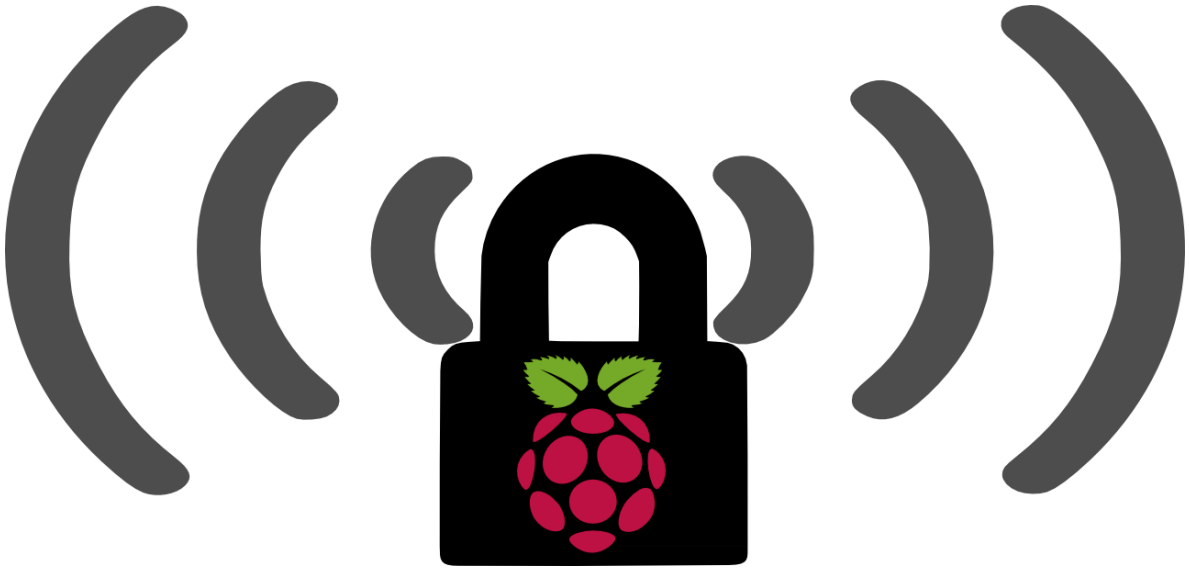
```
sudo apt-get install python3-dev
```

Ya que se ha descargado Python se procede a ejecutarlo e instalarlo, para ese propósito se utiliza el siguiente comando. Todo lo anterior se realiza en la terminal de la Raspberry Pi con el sistema operativo Debian Wheezy.

```
sudo python3 setup.py install
```

CAPÍTULO 4

INSTRUMENTACIÓN, INTEGRACIÓN Y PRUEBAS



CAPÍTULO 4 Instrumentación, integración y pruebas

En este capítulo se detallara la implementación de hardware y software necesario para la puesta en marcha del sistema propuesto, se describirá ampliamente el proceso de instalación de hardware, así como la implementación de software necesario para el monitoreo y control del sistema a través de internet.

4.1. Implementación de hardware.

El hardware son todos elementos físicos imprescindibles para el funcionamiento del sistema, dichos elementos son regidos por las ordenes y comandos que se generan en el software. Para la implementación del sistema en el vehículo es necesario acoplar componentes mecánicos a este para que funcione adecuadamente.

Para la implementación del sistema se utilizó un automóvil estándar Volkswagen Bora modelo 2009, cabe mencionar que el sistema puede ser implementado en cualquier automóvil sin importar el tamaño, el número de puertas, marca o modelo.

Para que el sistema funcionara eficientemente se optó por tomar dos variables muy importantes en un automóvil, la primera es el estado de las puertas del vehículo y la segunda el estado de giro en el volante, a continuación se describe el proceso de instalación del sistema.

Debido al constante sometimiento de fuerza y la gran cantidad de golpes que deben soportar los sensores de fin de carrera, se deben de colocar en puntos estratégicos en cada una de las puertas del vehículo, lo sensores tienen que ser colocados de tal manera que los golpes de la puerta no afecten su funcionamiento y además no deben ser fácilmente detectables.

En la figura 4.1 se muestra la colocación final de los sensores en la puerta del automóvil, cabe señalar en cada una de las puertas la disposición será la misma.

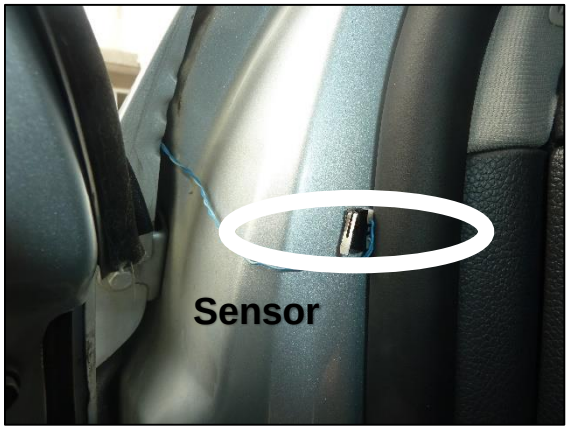


Figura. 4.1. Disposición de sensor de fin de carrera en la puerta de automóvil.

La sujeción de los sensores a la puerta del automóvil debe ser lo mejor posible ya que si no es así se puede comprometer el correcto funcionamiento del sistema.

Para la colocación del cableado de los sensores se utilizó alambre de calibre 22 debido a no exige un significativo consumo de corriente y también es capaz de soportar la acción de apertura y cierre de la puerta.

En la figura 4.2 se muestra la colocación final del cableado en la puerta del vehículo, dicho cableado se posiciono por debajo de la vestidura pasando por la bisagra de la puerta hasta llegar al interior del cofre del automóvil donde se encuentra el cerebro del sistema Pisecurity car.

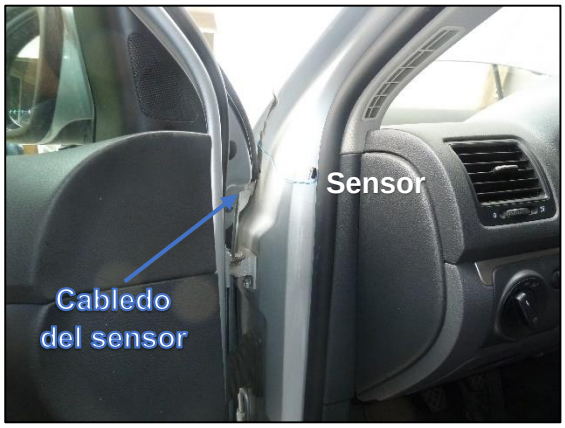


Figura. 4.2. Cableado del sensor de fin de carrera en la puerta del automóvil.

Otra de las variables que se monitorea en el automóvil es el estado de giro del volante, como se puede ver en la figura 4.3 esto se logra mediante la colocación de un sensor de efecto Hall en la base del volante y un conjunto de tres imanes de 1 cm de diámetro dispuestos en el borde del volante.

(a) (b)

Figura. 4.3 Disposición del sensor de efecto Hall e imanes dentro del automóvil. A) Vista frontal. B) Vista lateral.

La colocación idónea del sensor de fin de carrera se consiguió colocándolo entre la base metálica del volante y el protector de este, debido a su tamaño tan pequeño se acoplo de manera óptima a una espacio muy reducido, el cableado del sensor se colocó por debajo

de la tapicería del vehículo hasta llegar al interior del cofre del automóvil donde se encuentra el cerebro del sistema.

Para que el cableado de los sensores al cerebro del sistema fuera lo más sencillo posible, se optó por colocar el cerebro a un lado de la batería del automóvil, esto con la finalidad de facilitar la colocación de la etapa de control del sistema. Ver figura 4.4

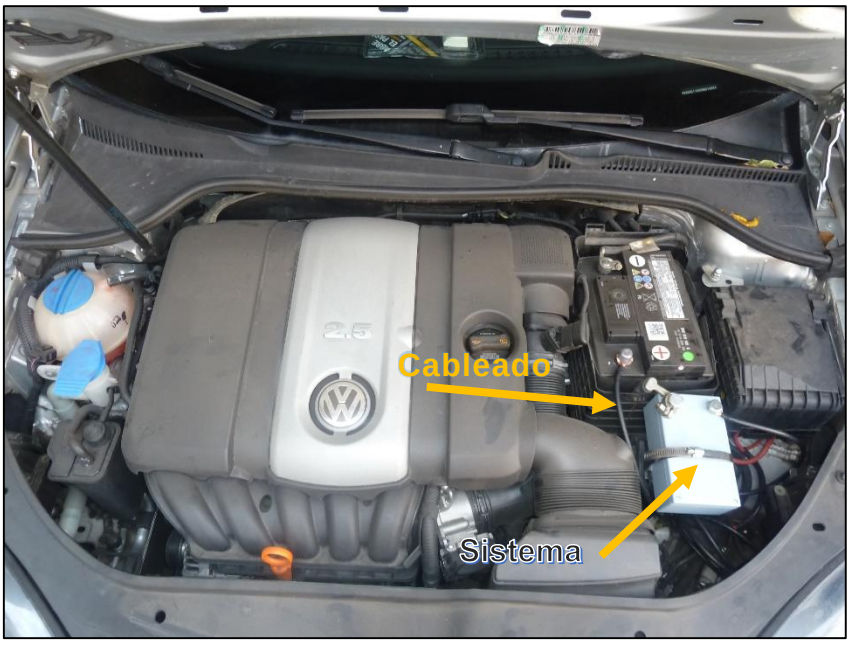


Figura. 4.4 Colocación del cerebro del sistema y cableado.

Para la implementación de la etapa de control se colocó en el cerebro del sistema dos tornillos que fungirán como terminales eléctricas, en uno de ellos se colocara con un cable la terminal positiva de la batería del automóvil, y en la otra se colocara la terminal positiva de alimentación del sistema principal de encendido, esto provocara que al ser alterado el estado de giro del volante el servomotor se activara y desalineara las terminales eléctricas del vehículo dejando sin alimentación de corriente el sistema de encendido del automóvil, en la figura 4.5 se puede observar las terminales eléctricas del prototipo del sistema .

Figura. 4.5 Prototipo del sistema vista exterior.

En la figura 4.6 se puede observar el interior del prototipo, en él está el servomotor, la tarjeta Raspberry Pi y la tarjeta inalámbrica.

Figura. 4.6 Prototipo del sistema vista interior.

Para conseguir unir todos los componentes del sistema tanto de hardware como de software se requirió de una pequeña placa que fungiera como interfaz entre el hardware y la Raspberry Pi, dicha placa permitió el correcto acople y protección a la tarjeta Raspberry Pi, porqué el hardware podría fácilmente dañar dicha tarjeta.

En la figura 4.7 se muestra el diseño del circuito requerido como interfaz para la tarjeta Raspberry Pi, la figura 4.8 se puede observar la placa ya terminada con la que se enlazan los elementos de hardware y la Raspberry Pi mediante el puerto GPIO.

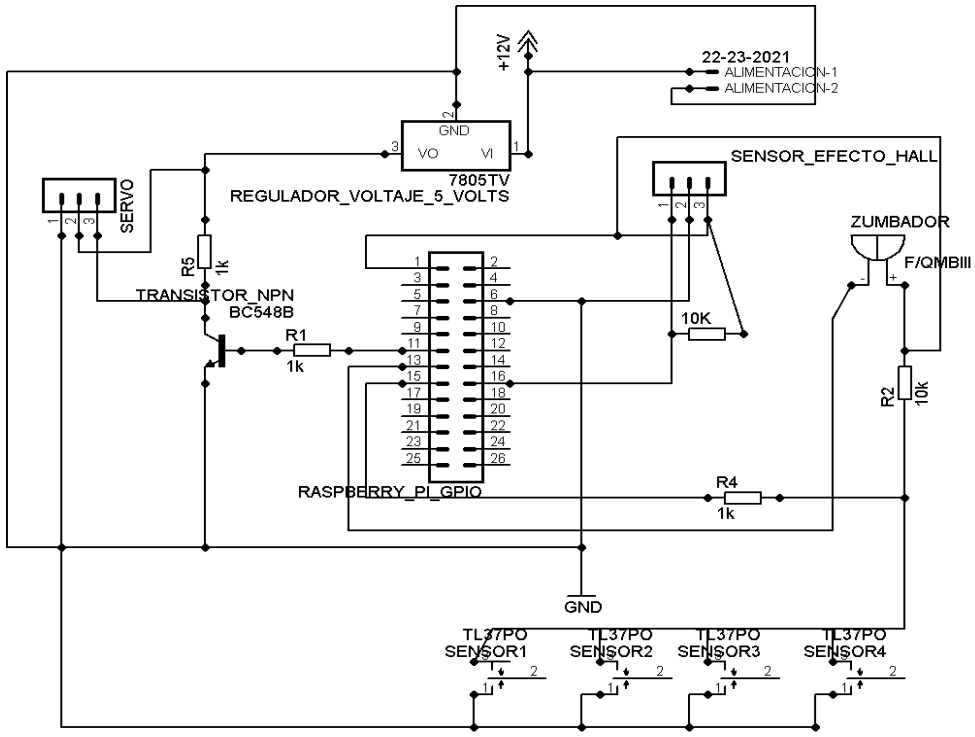


Figura. 4.7 Diagrama esquemático de la interfaz de acoplamiento entre la Raspberry Pi y el hardware.

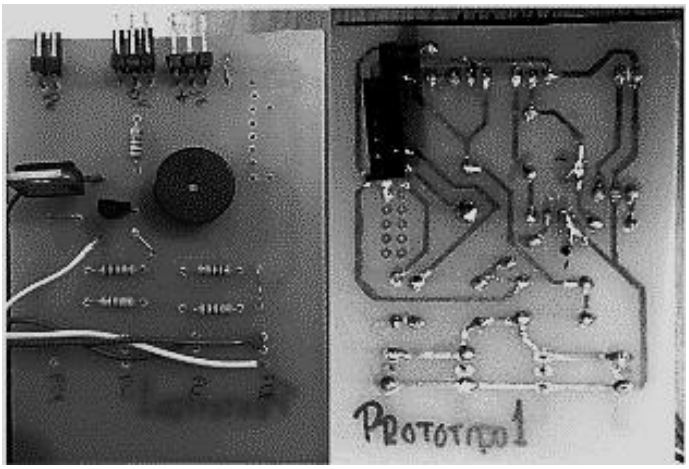


Figura. 4.8. Montaje físico de los componentes del prototipo.

Para llevar a cabo el concentrado final se requiere de una ubicación específica, las diversas pruebas llevaron a la colocación del concentrado a un costado de la batería, que resultó ser el lugar donde las interferencias provenientes del motor afectan de menor forma a todo el sistema. En el concentrado se conectan los 5 sensores y el servomotor de la etapa de control y la Raspberry Pi ya con la conexión de la etapa de envió de datos, en la figura 4.9 se muestra la disposición final de los sensores y el cerebro del vehículo (cortacorriente).

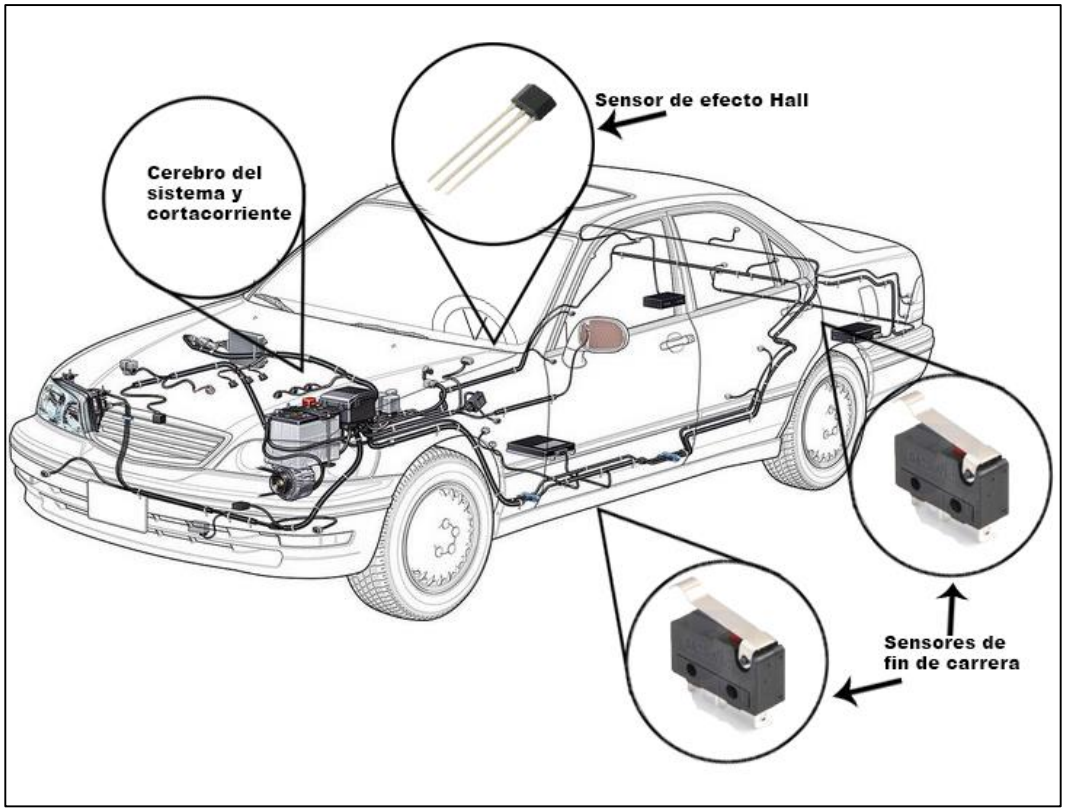


Figura.4.9. Disposición de los sensores, sistema de bloqueo y cerebro en el vehículo

4.2. Desarrollo de software.

La segunda etapa a instrumentar para la puesta en marcha del sistema, es la instrumentación del software que permitirá el correcto funcionamiento de la interfaz entre el sistema e Internet para la comunicación remota.

Al comenzar proyecto y revisar las especificaciones del puerto GPIO de la Raspberry Pi, se llegó a la conclusión de que las pruebas y resultados en la etapa de sensado y la etapa de control, no podían ser realizadas directamente en la placa Raspberry Pi, ya que esta no posee ningún tipo de protección contra corto circuito en el microprocesador, y cualquier error en el cálculo o fallo de algún dispositivo podría ocasionar un daño irreversible en la placa y un retraso muy importante en el tiempo de desarrollo del proyecto.

Por esta razón, solo se realizaron pruebas en el desarrollo del software ya que en la parte del hardware se tenía que ser muy minucioso en el valor de los dispositivos para no cometer ningún error.

Para la realización del sistema se utilizó Python como lenguaje de programación base; Python es un lenguaje muy flexible en cuanto su manejo, por lo tanto es capaz de manejar datos obtenidos por medios externos, modificarlos o interpretarlos como mejor se considere, es por esta razón que se puede simplificar el trabajo y reducir el número de programas o bibliotecas ejecutadas simultáneamente.

En las 4 etapas que se fusionaron en este proyecto se creó un programa que conjunta todas las acciones que realiza el sistema, para hacerlo funcionar en conjunto. Aunque las cuatro etapas estén ligadas, la etapa de comunicación no es propiamente una etapa programada, como se explicará en la sección 4.2.2. en dicha etapa se hará la activación del sistema y la visualización del monitoreo del sistema

En la figura 4.10 se muestra un diagrama general de la unión entre las etapas, como se puede visualizar, la etapa de procesamiento está implicada en 2 etapas de las 3 etapas restantes, eso se debe a que se tuvo que realizar una programación conjunta en la etapa de procesamiento, también se puede observar que si bien la etapa de comunicación no está incluida dentro de la etapa de procesamiento, es por esta etapa es la que se encarga de activar, desactivar y visualizar los datos provenientes de la etapa de procesamiento; otra de las cosas que se pueden comprobar es que las etapas de sensado y control, se encargan de introducir y extraer datos respectivamente.

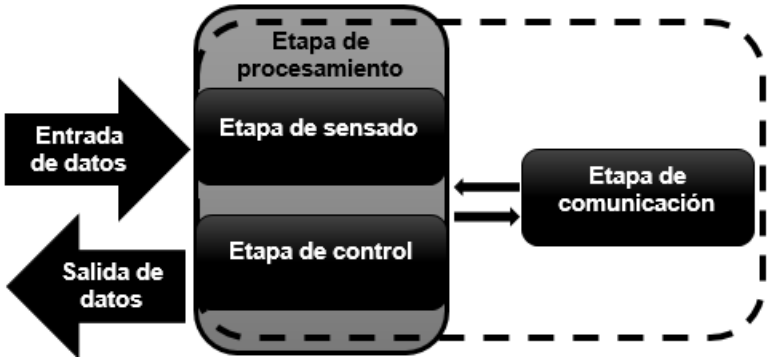


Figura.4.10.Diagrama general de la unión de las etapas del proyecto.

La primera elección que se tuvo que hacer en el software, fue la elección de la versión de Python con la que se trabajaría, aunque la Raspberry Pi trae instalado por default Python 2.7 y Python 3 es imprescindible tomar una buena decisión, lo que se tomó a consideración es la velocidad de respuesta de las dos versiones, en Python 2.7 se pueden manejar grandes cantidades, mientras que en Python 3 se pueden manejar datos a muy alta velocidad. Otra decisión importante es la elección de la librería GPIO con la que se trabajará, después de diversas pruebas con las versiones 0.2.0 y 0.3.0.a donde la salida de los datos no era la esperada y los sensores no respondían como se requería se eligió la librería Rpi.GPIO. 0.4.2ª por ser la más completa y la que menos errores tiene.

En las etapas de sensado y control se probaron las 2 diferentes formas de obtención y salida de datos, dichas formas son:

Dichas formas son: GPIO.setmode (BOARD) y GPIO.setmode (BCM). En la primera GPIO.setmode (BOARD) , implica que se usen los pines con los números de pines físicos en el conector GPIO; y en la segunda, implica que se usará la designación de canal SOC de Broadcom .

Para que el sistema funcione óptimamente es necesario combinar las dos formas, ya que hay funciones que son requeridas para los dos modos ya que la entrada de datos se requiere utilizar el modo BOARD y la salida el modo BCM. En el momento en que se realizó este proyecto (Agosto del 2012) aún no existía una versión de librería Rpi.GPIO que conjuntará y depurará los errores en los retardos de cada uno de los modos de entrada y salida.

A continuación en la figura 4.11 se muestra un diagrama más específico del funcionamiento del sistema propuesto en sus cuatro diferentes etapas y la unión que existe entre estas. Dichas etapas son: sensado, procesamiento, comunicación y control.

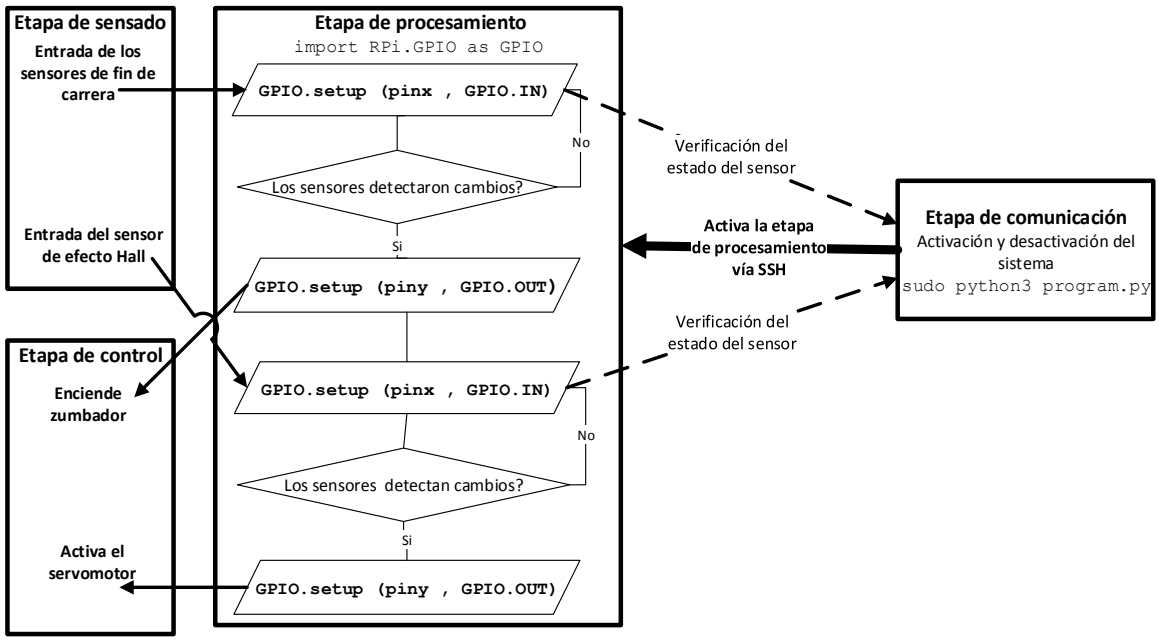


Figura.4.11. Diagrama de funcionamiento del sistema.

Como se puede observar la parte principal del proyecto es la etapa de procesamiento, dicha etapa sirve para entrelazar y contener las etapa de sensado y de control. Ver figura 4.9. El programa global es la etapa de procesamiento, para comenzar se agrega la librería de control del puerto GPIO con la sentencia *import RPi.GPIO as GPIO* después de haber agregado la librería se comienzan a introducir los comandos de entrada que se efectúan con la sentencia *GPIO.setup (pinx , GPIO.IN)* y que están simbolizados con las flechas del lado izquierdo del diagrama, que entran a la etapa de procesamiento.

Por medio de ciclos y decisiones la etapa de procesamiento une las etapas de sensado y la etapa de control, a continuación se agregan las sentencias que fungirán como salida de datos para la etapa de control, dicha sentencia es *GPIO.setup (piny , GPIO.OUT)* dichas acciones están simbolizadas con las flechas del lado izquierdo del diagrama, que salen de la etapa de procesamiento. En la sección 4.2.1 se detalla un poco más las fases que componen la etapa de procesamiento.

La etapa de comunicación es básicamente un acceso a la terminal del dispositivo Raspberry Pi por medio de una conexión de tipo SSH, se eligió este tipo de conexión ya que además de ser segura, se puede utilizar uno o varios clientes gratuitos (aplicaciones en el caso de móviles y programas en el caso de equipos de escritorio) para la mayoría de los smartphones, tabletas electrónicas y equipos de escritorio.

Por medio del cliente SSH se realiza el acceso al sistema, una vez en el se procede a activar o desactivar el sistema, mediante la sentencias *sudo python3 activa.py* , *sudo python3 desactiva.py*, esta acción está representada en el diagrama del lado derecho, con la flecha negra de un grosor diferente que entra a la etapa de procesamiento. Otra de las cosas que se realizan en la etapa de comunicación es la visualización de los estados de los sensores, dichos estados cuando sean alterados mandaran un aviso a la interfaz del programa SSH que se esté utilizando, cabe destacar que en el diagrama las visualizaciones se representan con líneas punteadas ya que estas pueden o no ser vistas por el usuario, independientemente si son supervisadas o no el sistema actuará de forma automática en caso de una intrusión, en la sección 4.2.2 se explica más a detalle el funcionamiento de esta etapa.

4.2.1. Etapa de procesamiento

El procesamiento al no ser una implementación física, todas las pruebas se realizaron ejecutando el programa (desarrollado en Python), dichas pruebas consistían en la ejecución del programa bajo las diferentes situaciones que se podrían presentar en el intento de robo de un automóvil y verificar que la interacción entre las señales de entrada proveniente de los sensores y las señales de salida enviadas al servomecanismo, fueran congruentes con los criterios de seguridad establecidos con anterioridad, todo lo anterior se logró con aproximadamente 200 pruebas de ejecución bajo diferentes entornos, lo que dio como resultado una correcta interacción además de eficiente, rápida y segura.

En la figura 4.12 se muestra la terminal del sistema operativo Debian Wheezy funcionando en la Raspberry

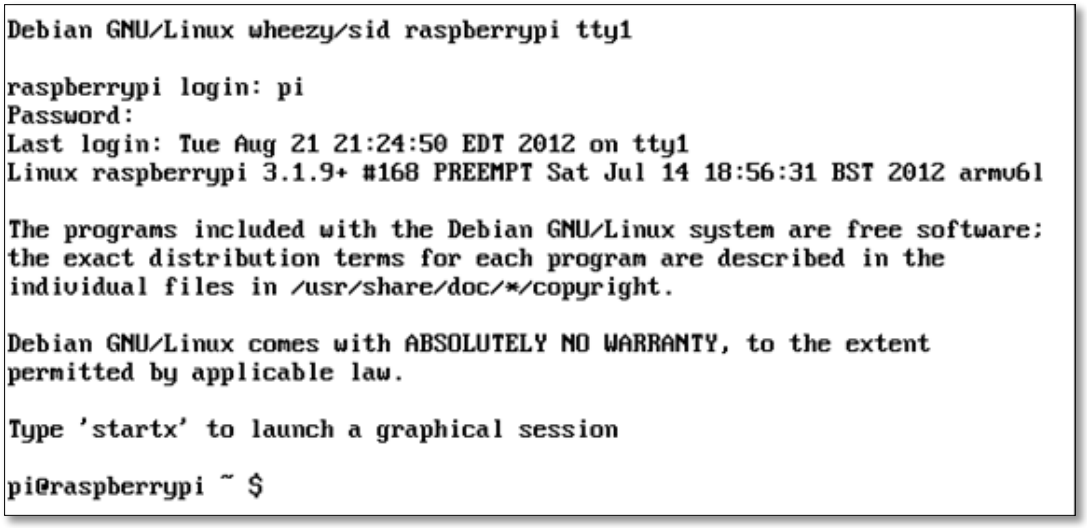


Figura.4.12.Terminal de ejecución de la Raspberry Pi con el sistema operativo Debian.

En la primera fase se realizó un programa cuya función es detectar el cambio de estado en el sensor de efecto Hall, una vez que se obtuvo una notificación de la activación del sensor en la terminal, se prosiguió a incluir el segundo sensor que es el sensor de fin de carrera. El sensor a nivel programación tiene el mismo comportamiento que el sensor de efecto Hall por lo tanto para implementarlo solo bastó con repetir el código del sensor de efecto Hall, ya que los dos dispositivos fungen como interruptores.

En la segunda fase se le añadió líneas del código al programa de los sensores, dichas líneas interpretaban el cambio de estado en los sensores, una vez que se detecta un cambio de estado, se prende y apaga un zumbador dependiendo el estado de los sensores, dicho zumbador pertenece a la etapa de control.

En la tercera fase se agregaron líneas de código que permitieran el manejo de un servomotor, dicho servomotor se encarga de la fase de control.

En la cuarta fase se agregaron librerías de conexión SSH por medio de sripts, dichas librerías se encargarían de realizar un enlace entre el programa y una terminal de control SSH.

4.2.2. Etapa de comunicación.

La etapa de comunicación a diferencia de las otras etapas del proyecto, es una etapa que se encuentra totalmente separada, ya que físicamente está constituida por una tarjeta de red inalámbrica y una conexión WiFi.

En la parte de software se realiza una conexión de tipo SSH entre el dispositivo Raspberry Pi y un cliente SSH, dicho cliente puede estar construido en cualquier sistema operativo, a continuación se muestran diferentes clientes de SSH para cuatro sistemas operativos diferentes.

A continuación se muestra el cliente de SSH llamado PuTTY dicho cliente es compatible con los sistemas operativos Windows XP, Vista, Seven así como los sistemas operativos basados en UNIX y GNU/Linux. En la figura 4.13 se muestra la interfaz de dicho programa.

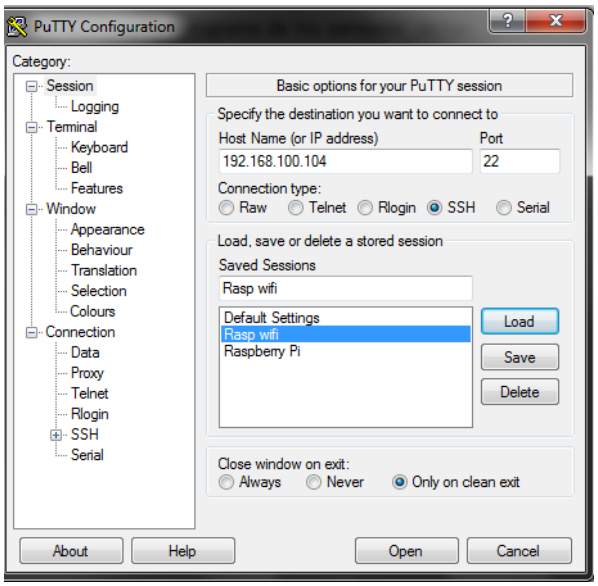


Figura.4.13. Cliente de SSH PuTTY [40].

Para los sistemas operativos móviles también existen diversos clientes de SSH, para el caso del sistema operativo móvil Apple IOS, el cliente ISSH se eligió para realizar las pruebas de operación y funcionamiento del sistema, en la figura 4.14 se muestra la pantalla de configuración del cliente previamente mencionado.

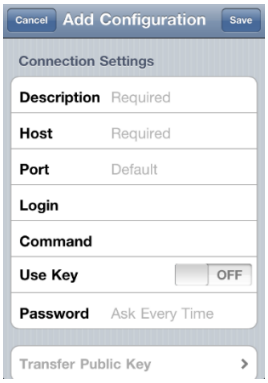


Figura.4.14. Cliente de SSH ISSH [39].

Para el sistema operativo móvil Android se eligió el cliente SSH Tunnel, para realizar las pruebas de operación y funcionamiento del sistema, en la figura 4.15 se muestra la ventana de configuración de dicho cliente.

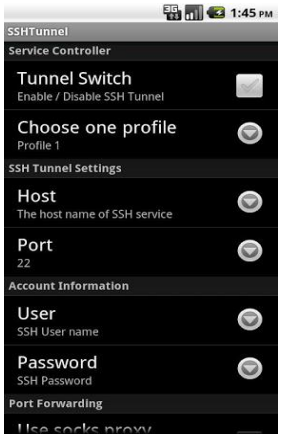


Figura.4.15. Cliente SSH Tunnel [41].

Una vez que se seleccionó el cliente SSH con el que se desea realizar la conexión se procede a llenar los datos de la conexión, a continuación se muestra un ejemplo del llenado de los datos para el cliente SSH:

Descripción: Raspberry

Host o IP: 192.168.100.104

Puerto: 22

Usuario: pi

Contraseña: raspberry

Una vez que se agregan los datos se realiza una conexión como la que se ilustra en la figura 4.16.

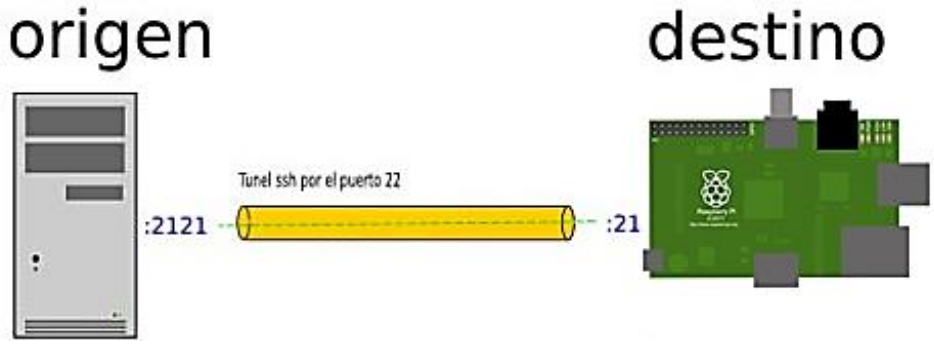


Figura. 4.16. Explicación grafica de una conexión SSH.

Una vez realizada la conexión se muestra la terminal tty1 del dispositivo Raspberry Pi, dentro de la terminal se procede a la activación del sistema, para ello se utiliza el comando *sudo python3 activa.py*, una vez activado el sistema este trabajará de forma autónoma y realizará las acciones programadas de acuerdo al estado de los sensores.

Ya que el sistema se encuentra activado el usuario puede verificar el estado de los sensores para ver si han sido modificados, para la desactivación se utiliza el comando *sudo python3 desactiva.py.*

4.2.3 Opiniones de los usuarios

El sistema propuesto fue implementado en un automóvil Volkswagen Bora 2009,se realizaron pruebas de operación del sistema propuesto, se hizo una simulación de intrusión en el vehículo antes mencionado, se probó el funcionamiento de cada uno de los cinco sensores instalados en el vehículo.

El escenario donde se probó el funcionamiento del sistema fue el estacionamiento del propietario del vehículo.

Después de haber concluido con las pruebas de funcionamiento del sistema, con el usuario que es el propietario del vehículo se tomó su opinión respecto al sistema.

- Precio: El sistema propuesto tiene un precio accesible de $1400 lo cual resulta muy atractivo respecto a otros sistemas de seguridad similares existentes en el mercado.

- Invasión: La invasión del sistema al automóvil no es agresiva como el de otros sistemas de seguridad como alarmas y geo-localizadores, ya que este sistema no requirió de modificaciones a la carrocería o el chasis del vehículo.

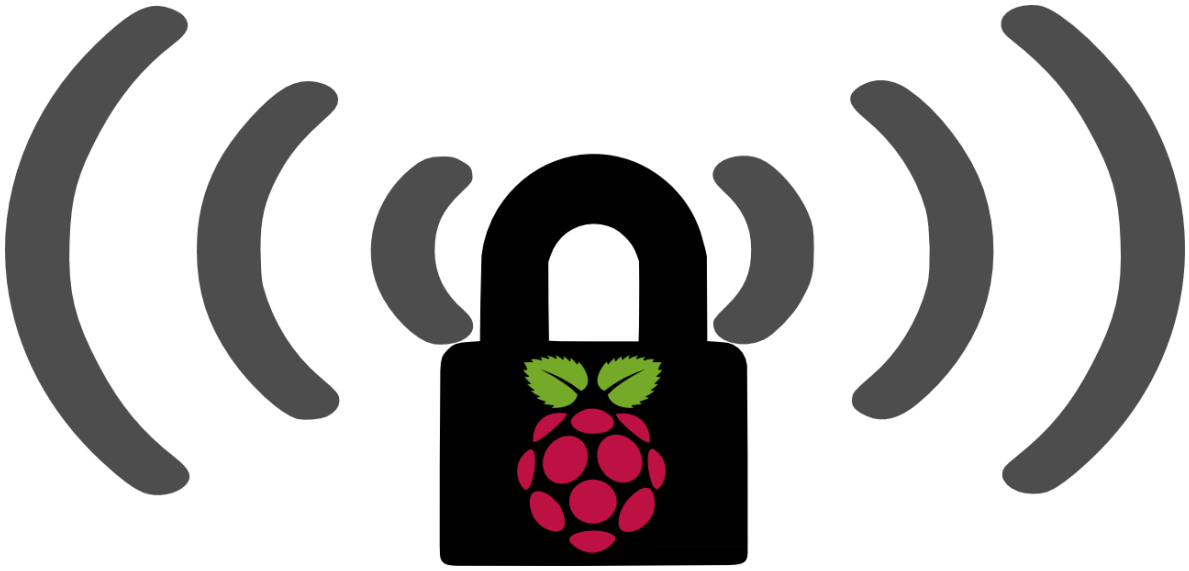
- Instalación. Es complicada si lo hace el propietario del vehículo ya que la colocación del cableado tiene que ser muy precisa y minuciosa ya que los cables pasan a través de los orificios de cableado que se encuentran en las bisagras del vehículo.

- Accesibilidad. Es casi nula ya que al ser un prototipo carece de distribución.

- Ventajas sobre otros sistemas similares. El sistema es innovador, aunque recurre a técnicas de bloqueo de encendido ya existentes ningún sistema actual puede activarse o desactivarse por medio de una conexión a internet, eso resulta muy conveniente ya que en la actualidad la mayoría de las personas cuentan con un dispositivo capaz de conectarse a internet, otra de las grandes ventajas es la doble verificación en el sistema ya que se requiere de un usuario y una contraseña para accesar al sistema.

- Desventajas. La interfaz es poco amigable con el usuario ya que es solo en modo texto.

CONCLUSIONES



CONCLUSIONES

Se realizó esta tesis con la finalidad de mejorar los sistemas existentes en el mercado, integrando una tarjeta SBC a un sistema de seguridad que inmoviliza el vehículo para impedir el robo. La parte más destacable del proyecto es la tarjeta SBC llamada Raspberry Pi que dota de inteligencia al sistema y que por medio de una tarjeta WiFi lo comunica con el usuario, esta característica hace que la tarjeta Raspberry Pi sea superior frente otro tipos de tarjetas desarrolladoras.

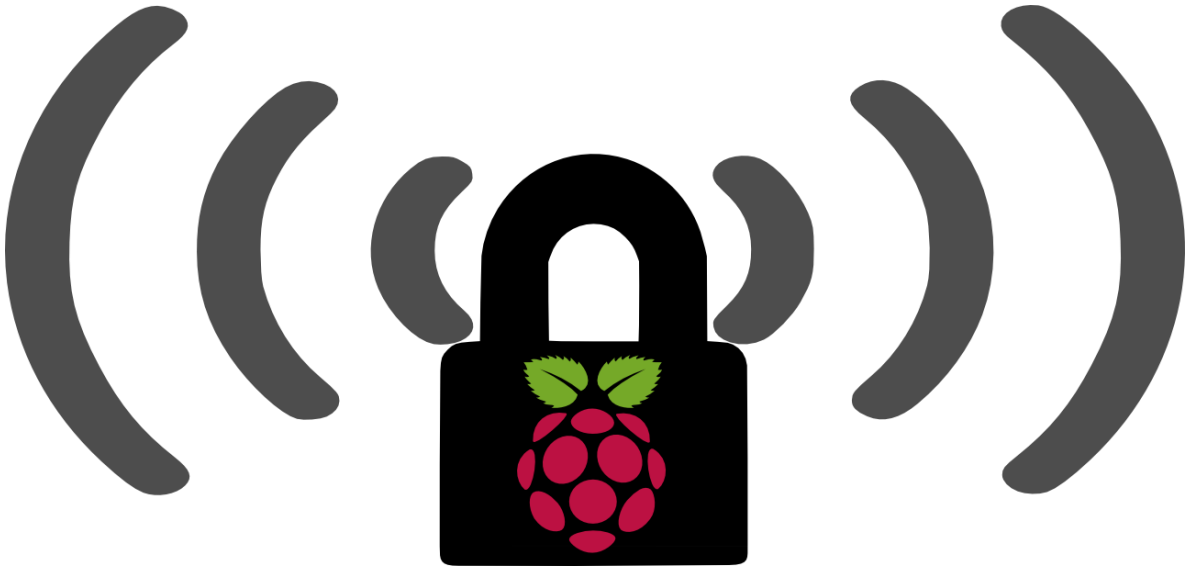
Para diseñar el sistema Pisecurity car se requirió del conocimiento y la aplicación de disciplinas como el control, la electrónica, la computación y la electricidad, además de los sistemas del automóvil para la implementación en el mismo, dando como resultado un sistema capaz de reaccionar de forma autónoma ante un intento de robo; Esto lo hace superior a sistemas antirrobo existentes en el mercado que solo alertan al usuario pero no realizan ninguna acción por evitar el siniestro.

Las pruebas de operación mostraron que el sistema cumplía satisfactoriamente con el objetivo principal de esta tesis que es monitorear y controlar el sistema de encendido de un vehículo, sin embargo cabe destacar que una debilidad del sistema, es que solo es funcional cuando el automóvil se encuentra estacionado, ya que una vez encendido el alternador del automóvil le proporcionará la energía suficiente para que el vehículo siga funcionando.

Para corregir esta debilidad que presenta el sistema y mejorar su funcionamiento cuando el automóvil este en movimiento, se tendría que realizar significativos cambios en la arquitectura fundamental del automóvil como el cableado de las bujías, en un trabajo a futuro podría implementar dicha mejora, además se le podría integrar un módulo GPS que tendría la capacidad de rastrear la ubicación del automóvil, un módulo 3g/GSM para que el sistema pueda realizar acciones en el vehículo como: activar el sistema enviando un mensaje SMS al dispositivo. Se podrían cambiar los sensores utilizados por sensores inalámbricos y con ello se podría solventar el problema del cableado del sistema.

La relevancia de esta tesis es la integración de la tecnología SBC a los sistemas de seguridad, para dotarlos de mejores funciones e integrar elementos tecnológicos que estaban reservados solo para las computadoras, como sistemas de comunicación WiFi.

RECOMENDACIONES



RECOMENDACIONES

Después de haber realizado las pruebas de operación se formularon las siguientes recomendaciones:

- Se recomienda ser paciente en la instalación de los sensores y su cableado ya que se tiene que ser muy meticuloso para el posicionamiento óptimo de los mismos.

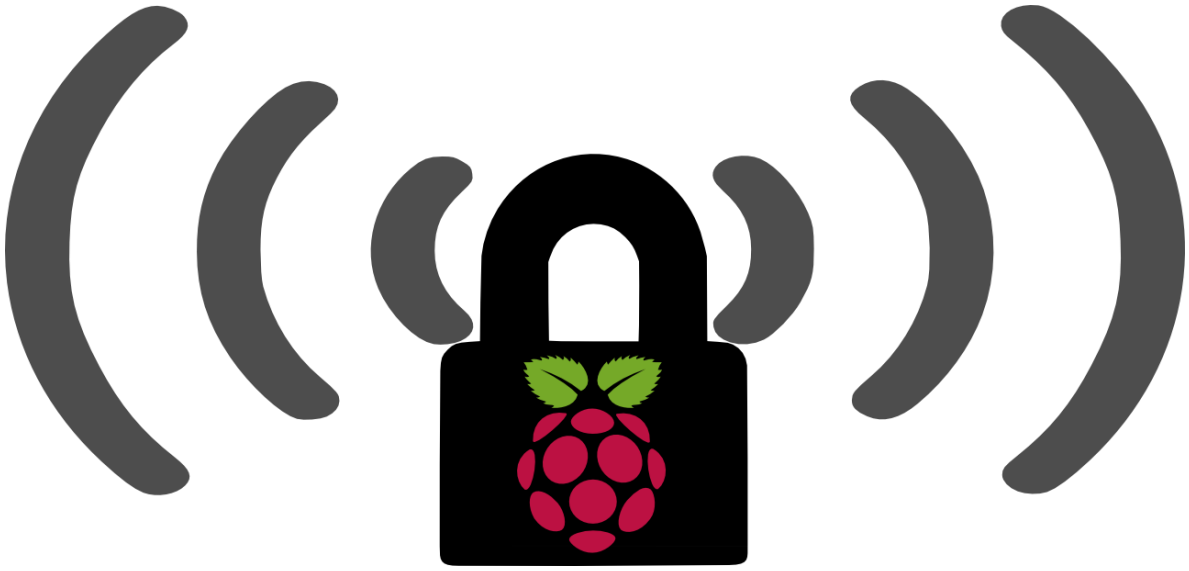
- Al conectar cualquier dispositivo como transistores, capacitores o resistencias al puerto GPIO de la Raspberry Pi se tiene que ser precavido ya que dicho puerto no posee ningún tipo de protección y tiene comunicación directa con el microprocesador.

- Es muy importante verificar las versiones del software utilizado, ya que una versión de la librería incorrecta provocaría que el puerto GPIO sea irreconocible para la Raspberry Pi. Por otro lado la versión de Python también tiene que verificar ya que no todas las versiones de Python trabajan con las mismas librerías GPIO.

- Se debe de poner suma atención cuando se instale el módulo WiFi ya que si la información no corresponde a la red se tendrá que reconfigurar.

- Existen dos lugares donde se puede colocar el sistema, una es dentro del cofre, la segunda es esconderlo dentro del vehículo como por ejemplo colocarlo debajo de algún asiento, sin embargo se recomienda que la instalación del prototipo sea dentro del cofre ya que de esta forma el sistema será menos accesible al maleante.

APÉNDICES



APENDICE A. GLOSARIO DE TERMINOS

Concepto	Significado
Actuador	Dispositivo capaz de realizar una acción como respuesta a un estímulo eléctrico.
Codec	Archivo necesario para poder decodificar archivos en un formato específico.
Contraseña	Conjunto de letras, números y/o símbolos que solo conoce el usuario, y que le dan acceso a algo.
Debian Wheezy	Sistema operativo que utiliza el núcleo Linux y las herramientas GNU, Wheezy es su séptima versión.
Framework	Palabra inglésa que se define marco de trabajo, es un conjunto estandarizado de conceptos y criterios que se tienen como plantilla para realizar trabajos en línea.
GPIO	Acrónimo en inglés de General Purpuse Input and Output, es un puerto de uso genérico que posee entradas y salidas de un sistema.
GPS	Acrónimo en inglés de Global Positioning System que significa Sistema de Posicionamiento Global,
GPU	Acrónimo en inglés de Graphics Processing Unit, es la unidad de procesamiento gráfico de una computadora.
Host	En informática es un dispositivo o computadora que funciona como el punto de inicio y final de las transferencias de datos.
Interfaz	Programa creado para permitir la comunicación entre dos o más aplicaciones diferentes, o entre el usuario y las aplicaciones.
IP	Acrónimo en inglés de Internet Protocol, conjunto de números mediante el cual un dispositivo se identifica en una red.
Login.	Palabra inglesa que se define como la acción de acceder a un ordenador que tiene el acceso restringido.
Paradigma	En programación son las reglas que se tienen que seguir para que un programa funcione eficientemente.
Protocolo	Conjunto de normas que es necesario seguir y de mensajes que es necesario intercambiar para establecer una comunicación en un sistema informático. El protocolo determina cómo se realiza el intercambio de datos entre dos ordenadores, y también el formato y la transmisión de los datos dentro de dicha red.

Puerto	Conexión física o virtual en el cual se puede realizar una conexión
RJ-45	Conector estándar para cables de tipo CAT usados usualmente para la instalación de redes estructuradas.
SBC	Acrónimo en inglés de Single Board Computer, es una computadora con todos sus componentes montados en una sola tarjeta, frecuentemente dicha tarjeta es de un tamaño muy compacto.
Script	Es programa que da una serie de instrucciones para ser realizadas por otros programas o dispositivos
Sensor	Dispositivo capaz de transformar una magnitud física en un voltaje eléctrico.
Servomotor	Dispositivo dotado de un motor de corriente continua que puede ubicarse en cualquier posición dentro de su rango de operación de 180 grados, utiliza un tren de pulsos para llegar a dicha posición.
SSH	Acrónimo en inglés Secure Shell, método de conexión remota de un dispositivo a otro
SSID	Acrónimo en inglés Service Set IDentifier, nombre de una red para que todos los paquetes enviados por la misma puedan ser identificados.
Transpondedor	Es un tipo de dispositivo utilizado en telecomunicaciones cuyo nombre viene de la fusión de las palabras inglésas *Transmitter* (Transmisor) y *Responder* (Contestador/Respondedor).
Usuario	Es quien ordinariamente usa algo.
WAP	Acrónimo en inglés de Wireless Aplication Protocol, es un protocolo estandarizado para transferir datos en Internet sobre una red inalámbrica.
WiFi	Acrónimo en inglés de Wireless Fidelity, es un método de conexión inalámbrica.

APENDICE B. Raspberry Pi

Existen en el mercado varias computadoras de uso específico llamadas “computadora mono-placa” o SBC (Single Board Computer) cuyo diseño se centra en un sólo microprocesador con la memoria RAM, E/S y todas las demás características de un computador funcional en una sola tarjeta, pero en un tamaño reducido. Entre este tipo de computadoras se encuentran la MK802 de la empresa APC, OVERO de la empresa Gumstix y Raspberry Pi (Figura 1.B) que fue desarrollada por la Universidad de Cambridge [36].

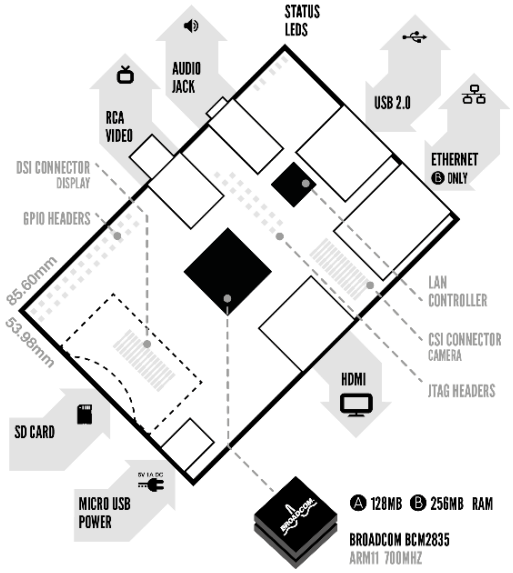


Figura.1.B. Computadora Raspberry Pi Modelo B [31].

La Raspberry Pi es una computadora del tamaño de una tarjeta de crédito que se puede le puede conectar una TV o un monitor, un teclado y un mouse para poder ser una computadora 100% funcional. Como se puede ver en la figura 2.B es una PC en miniaturización con procesador ARM1176-JZFS que se puede utilizar para muchas de las cosas que un PC de escritorio puede hacer, como hojas de cálculo, procesador de textos y videojuegos.

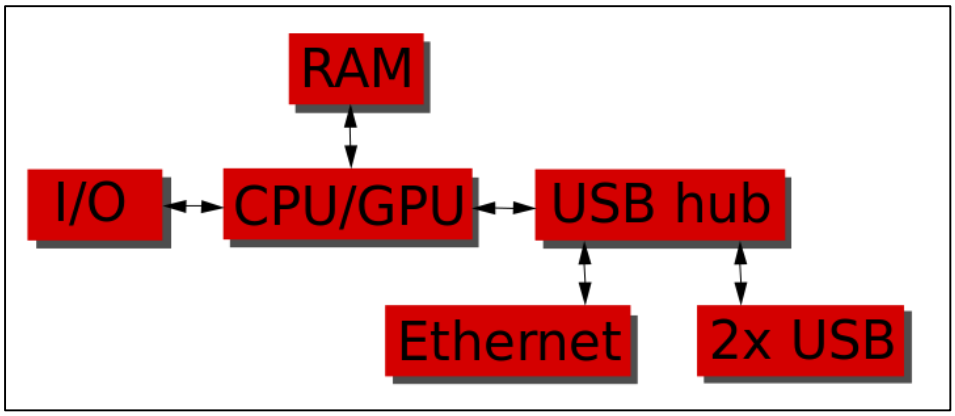


Figura.2.B.Conexión de procesos en la Raspberry Pi [36].

La Raspberry Pi es capaz de funcionar con diversos sistemas operativos GNU/Linux como Debian, Fedora, Arch Linux, Qton, Risc OS, Raspberry PWN, además de su propia versión Debian modificada llamada Raspbian.

El diseño de la tarjeta y la explotación del microprocesador permite reproducir video y audio con calidad Blu-ray usando el códec H.264 a 40Mbits/s y decodificación de perfil alto 1080p 30 Tiene un núcleo 3D que puede ser accedido mediante las librerías OpenGL ES2.0 y Open VG. La GPU (*Graphics Processing Unit***)** es capaz de mostrar 1Gpixel/s, 1.5 Gtexel/s o llegar a 24 GFLOPS de cálculos de propósito general.

Dicha computadora fue creada por la fundación Raspberry que es auspiciada por la Universidad de Cambridge y la compañía fabricante de circuitos integrados Broadcom, dicha placa surge con un objetivo en mente que es: *Desarrollar el uso y entendimiento de los computadoras en los niños*. La idea es conseguir computadoras portables y económicas que permitan a los niños usarlos sin miedo, abriendo su mentalidad y educándolos en la ética del "ábrelo y mira cómo funciona". El ideólogo del proyecto, David Braven, un antiguo desarrollador de videojuegos, afirma que su objetivo es que los niños puedan llegar a entender el funcionamiento básico de la computadora de forma divertida, y sean ellos mismos los que desarrollen y amplíen sus dispositivos.

Especificaciones técnicas.

Tabla 1.B.Especificaciones técnicas de la Raspberry Pi Modelo B [36].

Característica	**Especificación**
CPU	700MHz ARM1176JZFS
GPU	Broadcom Videocore 4
Memoria	256 Mb LPDDR2-800
Video	HDMI, Compuesto
Audio	HDMI, Analógico Stereo
USB	2 X USB 2.0 (Modelo B)
Almacenamiento	Tarjeta SD
Red	10/100 Ethernet
Alimentación	5V micro USB 700 mA

Puerto GPIO.

La tarjeta Raspberry Pi puede comunicarse con dispositivos externos mediante el conector GPIO incorporado.

El puerto GPIO (General Purpose Input/Output) es una de las partes más importantes de ya que permite comunicarse de una manera muy dinámica con el exterior ya que mediante

diversas librerías como GPIO.py (librería en python) el puerto posee una comunicación directa con el microprocesador.

El GPIO es un puerto genérico cuyo comportamiento está regido por el software con el que se comunica con el microprocesador. Como se puede ver en la figura 3.B, el puerto de la Raspberry Pi tiene 26 pines en DIP en un formato de 2 X 13 , este proporciona 8 pines que pueden ser utilizadas como salidas o entradas, así como 3 salidas de voltaje una de 3.3v, dos de 5v y una salida a GND.

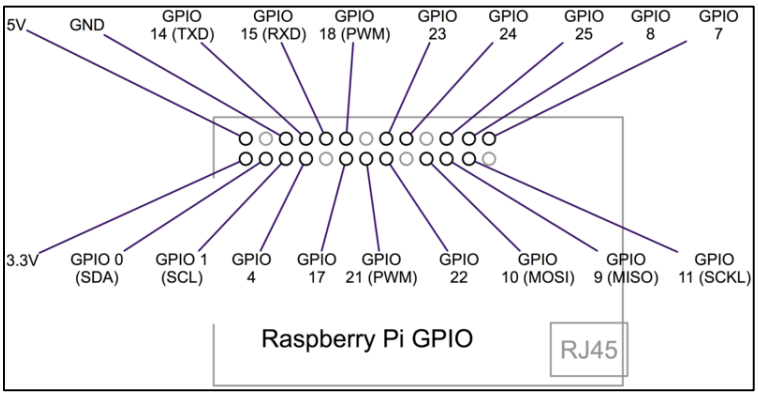


Figura. 3.B. Esquema del puerto GPIO de la Raspberry Pi [38].

Algo muy importante que se puede ver en la figura 4.B, es que se debe de tomar en cuenta al manipular el puerto GPIO es el orden de los pines, ya que físicamente es diferente en software y en hardware

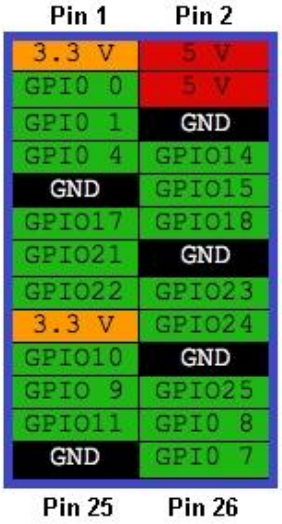


Figura.4.B.Nomenclatura de los pines del puerto GPIO.

Cuando una computadora, un microprocesador o cualquier dispositivo microcontrolador, efectúa un control vía I/O el software se comunica con un dispositivo hardware externo, y las posibilidades de hacerlo son, típicamente, dos:

OUTPUT: genera una salida lógica (escribe) en un pin configurado como SALIDA.
INPUT: obtiene un entrada lógica (lee) en un pin configurado como ENTRADA.

Usos y aplicaciones.

Dadas sus excelentes características la Raspberry Pi en relación con su tamaño y precio, comienza a ser utilizada como alternativa para las aplicaciones cotidianas por encima de otras placas de desarrollo. A continuación se enlistan algunas de las aplicaciones conocidas.

- Trazado vehicular (agregando un módulo GPS)
- Caja de streaming de radio por Internet
- Network Attached Storage setup (NAS)
- Servidor Proxy
- Sistema de alarma
- Webcam de seguridad (con un sensor de movimiento)
- Computadora de coche
- Cerebro para Arduino

APENDICE C. Lenguaje de programación Python

Python [42] es un lenguaje de programación interpretado cuya filosofía hace hincapié en una sintaxis muy limpia y que favorezca un código legible.

Es un lenguaje de scripting independiente de plataforma multiparadigma ya que soporta orientación a objetos, programación imperativa y, en menor medida, programación funcional. Python preparado para realizar cualquier tipo de programa, desde aplicaciones Windows a servidores de red o incluso, páginas web.

Python viene por default en la mayoría de la distribuciones GNU/Linux, este lenguaje se puede escribir directamente en una consola de comandos, y aunque existen diversos intérpretes de este lenguaje, no existe ningún compilador ya que la computadora interpreta este lenguaje por medio de la Shell de Python.

Es administrado por la Python Software Foundation. Posee una licencia de código abierto, denominada Python Software Fundation License, que es compatible con la Licencia pública general de GNU a partir de la versión 2.1.1, e incompatible en ciertas versiones anteriores.

Características y paradigmas

Python es un lenguaje de programación multiparadigma. Esto significa que más que forzar a los programadores a adoptar un estilo particular de programación, permite varios estilos: programación orientada a objetos, programación imperativa y programación funcional. Otros paradigmas están soportados mediante el uso de extensiones.

Propósito general. Se pueden crear todo tipo de programas. No es un lenguaje creado específicamente para la web, aunque entre sus posibilidades sí se encuentra el desarrollo de páginas por medio de frameworks.

Multiplataforma. Hay versiones disponibles de Python en muchos sistemas informáticos distintos. Originalmente se desarrolló para Unix, aunque cualquier sistema es compatible con el lenguaje siempre y cuando exista un intérprete programado para él.

Orientado a Objetos. La programación orientada a objetos está soportada en Python y ofrece en muchos casos una manera sencilla de crear programas con componentes reutilizables.

Interpretado. Quiere decir que no se debe compilar el código antes de su ejecución. En ciertos casos, cuando se ejecuta por primera vez un código, se producen unos bytecodes que se guardan en el sistema y que sirven para acelerar la compilación implícita que realiza el intérprete cada vez que se ejecuta el mismo código.

Interactivo. Python dispone de un intérprete por línea de comandos en el que se pueden introducir sentencias. Cada sentencia se ejecuta y produce un resultado visible, que puede ayudar al programador a entender mejor el lenguaje y probar los resultados de la ejecución de porciones de código rápidamente.

Funciones y librerías. Dispone de muchas funciones incorporadas en el propio lenguaje, para el tratamiento de cadenas, números, archivos, etc. Además, existen muchas librerías que se pueden importar en los programas para tratar temas específicos como la

programación de ventanas, sistemas en red, funciones web y administración de archivos entre otros.

Sintaxis clara. Cabe destacar que Python tiene una sintaxis muy visual, gracias a una notación identada (con tabulaciones) de obligado cumplimiento. En muchos lenguajes, para separar porciones de código, se utilizan elementos como las llaves o las palabras clave begin y end. Para separar las porciones de código en Python se debe tabular hacia dentro, colocando un margen al código que iría dentro de una función o un bucle. Esto ayuda a que todos los programadores adopten unas mismas notaciones y que los programas de cualquier persona tengan un aspecto muy similar.

Una característica importante de Python es la resolución dinámica de nombres; es decir, lo que enlaza un método y un nombre de variable durante la ejecución del programa (también llamado ligadura dinámica de métodos).

Python usa tipado dinámico y conteo de referencias para la administración de memoria.

Otro objetivo del diseño del lenguaje es la facilidad de extensión. Se pueden escribir nuevos módulos fácilmente en C o C++.

En la figura 1.C puede observarse la sintaxis y el entorno de trabajo Python.

```
def add5(x):
   return x+5

def dotwrite(ast):
   nodename = getNodename()
   label=symbol.sym_name.get(int(ast[0]),ast[0])
   print '    %s [label="%s' % (nodename, label),
   if isinstance(ast[1], str):
      if ast[1].strip():
         print '= %s"];' % ast[1]
      else:
         print '"]'
   else:
      print '"];'
      children = []
      for  in n, childenumerate(ast[1:]):
         children.append(dotwrite(child))
      print ,'    %s -> {' % nodename
      for  in :namechildren
         print '%s' % name,
```

Figura.1.C.Ejemplo de la sintaxis en Python.

APENDICE D. Comunicación

TCP/IP

Antecedentes.

La red Arpanet, nombre de la organización militar Advances Research Project Agency (Arpa) nació en 1969. Fue creada por el Department od Defense (DoD) de los EE.UU para conectar distintos sitios informatizados y en primer lugar conecto cuatro institutos universitarios. Se conectaron una serie de centros militares y de investigación, públicos y privados, que participaron progresivamente de esta implementación [43].

A principios de los años 70, Bob Kahn, del Defense ARPA (DARPA), ex ARPA, trabajaba con Vinton Cerf, investigador del Stanford Institute, sobre nuevos protocolos que permiten conectar redes. Así nace el TCP/IP. En 1976, Arpanet emigra hacia TCP/IP. En 1978, se conecta una segunda red Arpanet que utiliza las líneas telefónicas y toma el nombre de Internet.

Protocolos

La familia TCP/IP implica decenas de protocolos comunicación y aplicación, que se utilizan para conectar sistemas heterogéneos, independientes de la capa física y que se define en un modelo de cuatro capas de red, como se muestra en la figura 1.D.

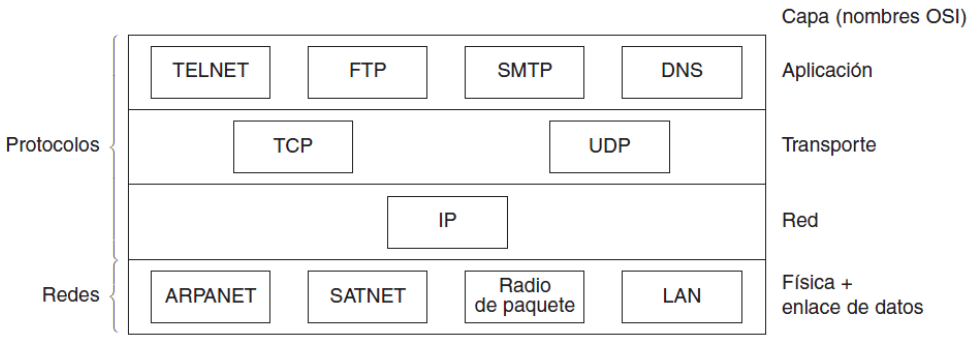


Figura. 1.D. Protocolos y redes en el modelo TCP/IP inicialmente [44].

Capa de interred (IP)

La capa de interred(IP) [44] es la pieza clave que mantiene unida a la arquitectura. Su trabajo es permitir que los hosts inyecten paquetes dentro de cualquier red y que éstos viajen a su destino de manera independiente (pudiendo ser en una red diferente). Aunque los paquetes lleguen en un orden diferente al que fueron enviados, las capas más altas del modelo deberán ordenarlos, si se desea una entrega ordenada. El concepto “interred” se utiliza en un sentido genérico, aun cuando esta capa se presente en Internet.

La capa de interred define un paquete de formato y protocolo oficial llamado IP (Protocolo de Internet). El trabajo de la capa de interred es entregar paquetes IP al destinatario. Aquí, el enrutamiento de paquetes es claramente el aspecto principal, con el propósito de evitar la congestión.

TCP

La capa que está arriba de la capa de interred en el modelo TCP/IP se llama capa de transporte o TCP [44].

Está diseñada para permitir que las entidades iguales en los *hosts* de origen y destino puedan llevar a cabo una conversación. Aquí se han definido dos protocolos de transporte de extremo a extremo. El primero, TCP (Protocolo de Control de Transmisión), es un protocolo confiable, orientado a la conexión, que permite que un flujo de bytes que se origina en una máquina se entregue sin errores en cualquier otra máquina en la interred. Divide el flujo de bytes entrantes en mensajes discretos y pasa cada uno de ellos a la capa de interred. En el destino, el proceso TCP receptor reensambla en el flujo de salida los mensajes recibidos. TCP también maneja el control de flujo para asegurarse de que un emisor rápido no sature a un receptor lento con más mensajes de los que puede manejar.

El segundo protocolo de esta capa, UDP (Protocolo de Datagrama de Usuario), es un protocolo no confiable y no orientado a la conexión para aplicaciones que no desean la secuenciación o el control de flujo de TCP y que desean proporcionar el suyo. También tiene un amplio uso en consultas únicas de solicitud-respuesta de tipo cliente-servidor en un solo envío, así como aplicaciones en las que la entrega puntual es más importante que la precisa, como en la transmisión de voz o vídeo.

Capa de aplicación

El modelo TCP/IP no tiene capas de sesión ni de presentación. Arriba de la capa de transporte está la capa de aplicación [44]. Contiene todos los protocolos de nivel más alto. Los primeros incluyeron una terminal virtual (TELNET), transferencia de archivos (FTP) y correo electrónico (SMTP), como se muestra en la figura 1.D. El protocolo de terminal virtual permite que un usuario en una máquina se registre en una máquina remota y trabaje ahí. El protocolo de transferencia de archivos proporciona una manera de mover con eficiencia datos de una máquina a otra. El correo electrónico era originalmente sólo un tipo de transferencia de archivos, pero más tarde se desarrolló un protocolo especializado (SMTP) para él. Con el tiempo, se han agregado muchos otros protocolos: DNS (Sistema de Nombres de Dominio) para la resolución de nombres de *host* en sus direcciones de red; NNTP, para transportar los artículos de noticias de USENET; HTTP, para las páginas de World Wide Web, SSH como una intérprete de ordenes segura y muchos otros.

SSH

SSH™ [45] (Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP (File Transfer Protocol) o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través de la shell de comando, tales como telnet o rsh (remote shell). Ya que estas aplicaciones antiguas no encriptan contraseñas entre el cliente y el servidor, evite usarlas mientras le sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas reduce los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.

Características de SSH

El protocolo SSH proporciona los siguientes características tipos de protección [45]:

Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.

El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.

Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.

El cliente tiene la posibilidad de reenviar aplicaciones X11 (X11 se refiere al sistema de visión por ventanas X11R6.7, tradicionalmente llamado Sistema de ventanas X o simplemente X. Red Hat Enterprise Linux contiene XFree86, un sistema de ventanas X de código abierto.) desde el servidor. Esta técnica, llamada reenvío por X11, proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

Ya que el protocolo SSH encripta todo lo que envía y recibe, se puede usar para asegurar protocolos inseguros. El servidor SSH puede convertirse en un conducto para convertir en seguros los protocolos inseguros mediante el uso de una técnica llamada reenvío por puerto, como por ejemplo POP, incrementando la seguridad del sistema en general y de los datos.

APENDICE E. Librerías GPIO

En este apéndice se muestra la evolución de la librería GPIO.py [46], desde su comienzo hasta última versión disponible, cabe destacar que cuando se inició este trabajo la última versión disponible era la versión 0.0.3a.

- 0.5.2a
  - Adicionado software para PWM(experimental)
  - Adicionado parámetro de número de canales para eventos
  - Restauración interna de fábrica

- 0.5.1a
  - Reparadas las llamadas múltiples en el GPIO

- 0.5.0a
  - Adicionado nuevo límite de detección de eventos (interrupt handling) Adicionando Added add_event_detect() - Added remove_event_detect() - Added add_event_callback() - Added wait_for_edge()
  - Cambio de eventos detectados para nueva funcionalidad de límite
  - Input () ahora regresa 0/LOW == False o 1/HIGH == True en lugar de False or True (booleanos).
  - Cambio de SetupException a RuntimeError
  - Mejorado docstrings en funciones

- 0.4.2a
  - Reparación en la instalación en Arch Linux en Python 3.3
  - Valor inicial cuando se coloca un canal como salida

- 0.4.1a
  - Adicionada VERSION
  - Permiso de input() en canal de output() (Eric Ptak <trouch@trouch.com>)

- 0.3.1a
  - Reparado el fallo crítico con el intercambio de estados de salida high/low
  - Adicionado pull-up/pull-down setup y funcionalidades para entradas

- 0.3.0a
  - Reescrita la extensión de C
  - Ahora se usan los registros de /dev/mem y SoC en vez de /sys/class/gpio
  - Llamados de GPIO.setmode() obligatorios
  - Adicionado las constantes GPIO.HIGH y GPIO.LOW

- 0.2.0
    - Cambio de estado de alfa a beta
    - Adicionado setmode() puede usar BCN GPIO 00.nn numero de canal
    - Renombrado InvalidPinExeption a InvalidChannelException

- 0.1.0
    - Reparación de fallo de dirección
    - Adicionado MANIFEST.in
    - Cambios en el número de pines en el canal GPIO
    - Probado y funcionando

- 0.0.3a
    - Aún no completamente probada
    - Reparación de algunos fallos críticos
    - Re fabricada
    - Adicionada tabla GPIO

- 0.0.2a
    - Re-configuración de fábrica. Aún no completamente probada.

- 0.0.1a
    - Primera versión. No fue completamente probada.

APENDICE F. Publicaciones

VII CONGRESO NACIONAL ESTUDIANTIL DE INVESTIGACIÓN
CONGRESO DE INVESTIGACIÓN POLITÉCNICA
II JORNADA DE PROTOTIPOS
NOVIEMBRE 15 Y 16, 2012

El Instituto Politécnico Nacional

Otorga la presente

Constancia

a

RAMÍREZ CARDONA JUAN CARLOS

Por su valiosa participación en la modalidad de ***Prototipo***, con el tema:

SISTEMA DE CONTROL Y MONITOREO DEL ENCENDIDO DE UN AUTOMÓVIL

en el VII Congreso Nacional Estudiantil de Investigación, el VII Congreso de Investigación Politécnica y la II Jornada de Prototipos, celebrado los días 15 y 16 de noviembre de 2012, en las instalaciones de la Coordinación General de Formación e Innovación Educativa.

México, D.F. a 16 de noviembre de 2012.

Dra. Yoloxóchitl Bustamante Díez
Directora General del
Instituto Politécnico Nacional

SOMI XXVII

Congreso de Instrumentación

Culiacán, Sinaloa, del 29 al 31 de octubre de 2012

El Centro de Ciencias Aplicadas y Desarrollo Tecnológico
de la Universidad Naciona Autónoma de México y
el Instituto Tecnológico de Culiacán

Otorgan la presente

CONSTANCIA

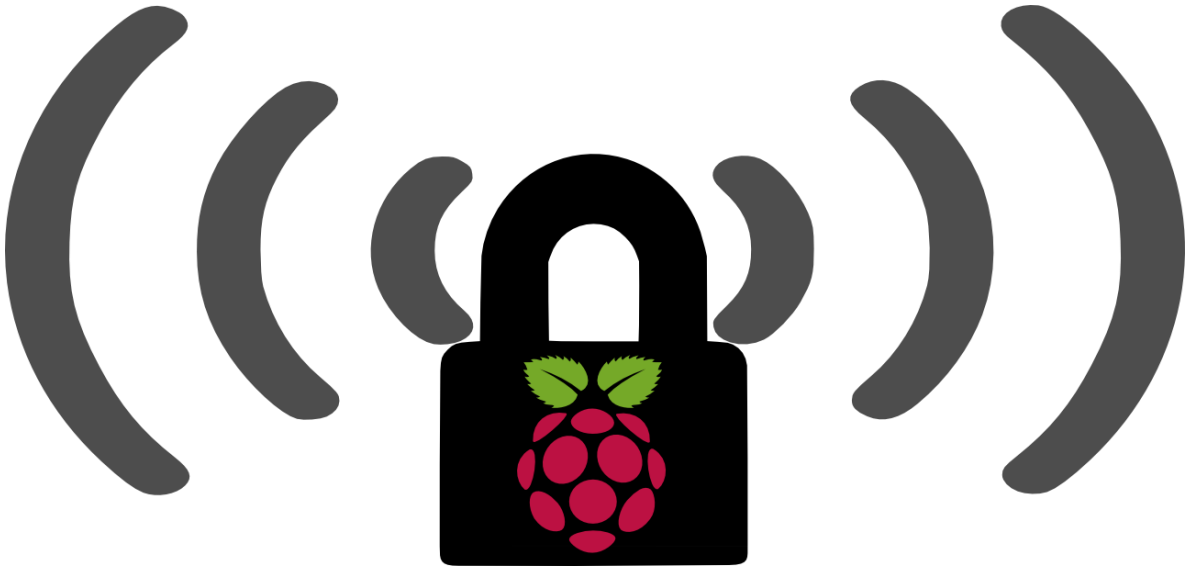
a: Jovany Gil García, Juan Carlos Ramírez Cardona, María Aurora Molina Vilchis

Por haber presentado en el SOMI XXVII Congreso de Instrumentación su trabajo:

SISTEMA DE SEGURIDAD DE ACCESO A UN VEHÍCULO
CON CONTROL REMOTO POR INTERNET

Dr. José Manuel Saniger Blesa
PRESIDENTE DEL COMITÉ ORGANIZADOR

REFERENCIAS



REFERENCIAS

[1] Consejo Ciudadano, «Consejo Ciudadano,» [En línea]. Available: http://www.consejociudadanodf.org.mx/alerta.php. [Último acceso: 10 Agosto 2013].

[2] F. Gutierrez Rostro, «Estado de Mexico y D.F. encabezan robo automoviles,» El economista, 31 Julio 2013. [En línea]. Available: http://eleconomista.com.mx/finanzas-personales/2013/07/31/edomex-df-encabezan-robo-automoviles. [Último acceso: 10 Agosto 2013].

[3] Gobierno del Distrito Federal; Secretaria de Seguridad Publica, «Informe anual de resultados 2011,» PGJDF, Ciudad de Mexico, 2011.

[4] Reforma (periodico), «Animal politico,» 24 Octubre 2011. [En línea]. Available: http://www.animalpolitico.com/2011/10/robo-de-autos-los-puntos-mas-peligrosos-del-df-segun-la-ssp/#axzz2fsLJGoD1. [Último acceso: 5 Septiembre 2013].

[5] Notimex, «CNN Expancion,» 31 Julio 2013. [En línea]. Available: http://www.cnnexpansion.com/economia/2013/07/31/robo-de-autos-crece-266-en-seis-anos. [Último acceso: 1 Sepriembre 2013].

[6] D. R., «Tecno coche,» [En línea]. Available: http://www.tecnococoche.com/marca/general/antirobo_coche.html. [Último acceso: 15 Septiembre 2013].

[7] Dani meganeboy., «Aficionados a la mecanica,» 2011. [En línea]. Available: http://www.aficionadosalamecanica.com/inmovilizador.htm. [Último acceso: 16 Septiembre 2013].

[8] Tecnologias integrales, «Tecnologias integrales,» 2012. [En línea]. Available: http://www.tecnicosintegrales.cl/cortacorriente.html. [Último acceso: 16 Septiembre 2013].

[9] A. Mackay Barriga, P. Contreras Meriño y A. Mackay Juhl, «Good Lock,» 2012. [En línea]. Available: http://www.goodlock.cl/. [Último acceso: 16 Septiembre 2013].

[10] E. V. Ramírez y M. Weiss, Introducción a los microprocesadores: equipo y sistemas, Limusa, 1986.

[11] Intel Corporation, «The Story of the Intel® 4004,» Intel Corporation, [En línea]. Available: http://www.intel.com/content/dam/www/public/us/en/images/photography/museum-microprocessor-4004-921x307-3-1.jpg. [Último acceso: 17 Septiembre 2013].

[12] F. E. Valdés Pérez y R. Pallas Areny, Microcontroladores fundamentos y aplicaciones con pic, Alfaomega; Marcombo, 2007.

[13] E. Santamerina, Electrónica digital y microprocesadores., Universidad Pontificia Comillas, 1993.

[14] R. Oviedo, *"Sistema minimo de propósito general" Tesis,* Oaxaca, México: Universidad Tecnológica de la Mixteca, 2007.

[15] Wikipedia, «List of single-board computers,» Wikipedia, 25 Septiembre 2013. [En línea]. Available: http://en.wikipedia.org/wiki/List_of_single-board_computers. [Último acceso: 27 Septiembre 2013].

[16] M. A. Mares, «Robo de vehículos, ¡$35,000 millones!,» El economista, 13 Enero 2013. [En línea]. Available: http://eleconomista.com.mx/columnas/columna-especial-empresas/2013/01/16/robo-vehiculos-35000-millones. [Último acceso: 23 Septiembre 2013].

[17] M. Fernandez Barcell, «Introducción a las redes de sensores inalámbricas,» [En línea]. Available: http://www.mfbarcell.es/conferencias/wsn.pdf. [Último acceso: Febrero 2012].

[18] L. Orozco-Barbosa, T. Olivares, R. Casado y A. Bermudez, Wireless Sensor and Actor Networks, Albacete,Espana: Springer, 2007.

[19] I. Wigmore, «Sensor,» Whatls, julio 2012. [En línea]. Available: http://whatis.techtarget.com/definition/sensor. [Último acceso: 20 Septiembre 2013].

[20] «Sensor,» Wikipedia, 21 Septiembre 2013. [En línea]. Available: http://en.wikipedia.org/wiki/Sensor. [Último acceso: 21 Septiembre 2013].

[21] J. . L. Molina Marticorena, «QUÉ ES UN SENSOR,» [En línea]. Available: http://www.profesormolina.com.ar/tecnologia/sens_transduct/que_es.htm. [Último acceso: Noviembre 2012].

[22] J. Caniparoli, «Sensores de final de carrera,» [En línea]. Available: http://www.slideshare.net/JavierCaniparoli/sensores-de-final-de-carrera. [Último acceso: 23 Septiembre 2013].

[23] «Sensores de proximidad,» Galeon, [En línea]. Available: http://sensoresdeproximidad.galeon.com/carrera2.jpg. [Último acceso: Septiembre 2013].

[24] R. L. Boylestad, Introduccion al analisis de circuitos, Mexico: Pearson educacion, 2004.

[25] Diego, «Actuadores electricos,» [En línea]. Available: http://www.slideshare.net/diego5wh/actuadores-electricos-presentation. [Último acceso: Octubre 2012].

[26] Universidad de Castilla-La mancha, «El servomotor,» [En línea]. Available: http://www.slideshare.net/diego5wh/actuadores-electricos-presentation. [Último acceso: 24 Septiembre 2013].

[27] J. Noble, Programing Interactivity, Estados Unidos de Norteamerica: O'Reilly Media Inc, 2009.

[28] V. R. Gonzalez, «Servomotores,» Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado, 2003. [En línea]. Available: http://platea.pntic.mec.es/vgonzale/cyr_0204/ctrl_rob/robotica/sistema/motores_servo.htm. [Último acceso: 27 Septiembre 2013].

[29] Embedded Lab, «Lab 21: Servo motor control,» 7 Abril 2012. [En línea]. Available: http://embedded-lab.com/blog/wp-content/uploads/2012/04/ServoMEchanism.png. [Último acceso: 22 Septiembre 2013].

[30] Sparkfun, «Servo - Generic (Sub-Micro Size),» [En línea]. Available: https://www.sparkfun.com/products/9065. [Último acceso: Enero 2013].

[31] Raspberry Pi Foundation, «Raspberry Pi Quick guide,» Marzo 2012. [En línea]. Available: http://www.raspberrypi.org/quick-start-guide. [Último acceso: Julio 2012].

[32] Electronika2, «Bluetooth,» [En línea]. Available: http://electronika2.tripod.com/info_files/bluetooth.htm. [Último acceso: Diciembre 2012].

[33] UNAM, «Control inalambrico Zig Bee,» 2011. [En línea]. Available: http://redyseguridad.fi-p.unam.mx/proyectos/control_inalambrico_zig_bee.html. [Último acceso: Diciembre 2012].

[34] Metrologic Instruments, Inc. , «Estándares Inalámbricos,» 2009. [En línea]. Available: http://www.metrologicmexico.com/contenido1/informacion_tecnica/estandares_inalambricos.php. [Último acceso: Febrero 2013].

[35] Melexis Microelectronic Systems, «US1881 Hall Latch – High Sensitivity,» 2011. [En línea]. Available: http://www.melexis.com/Hall-Effect-Sensor-ICs/Hall-Effect-Latches/US1881-140.aspx. [Último acceso: Marzo 2013].

[36] Wikipedia, «Raspberry Pi,» 23 Septiembre 2013. [En línea]. Available: http://es.wikipedia.org/wiki/Raspberry_Pi. [Último acceso: 25 Septiembre 2013].

[37] «Raspberry Pi y GPIO (1),» 16 Abril 2013. [En línea]. Available: http://www.diverteka.com/?p=1370. [Último acceso: 10 Septiembre 2013].

[38] S. Monk. [En línea]. Available: http://learn.adafruit.com/assets/3059. [Último acceso: Mayo 2013].

[39] Zingersoft, «iSSH,» Febrero 2013. [En línea]. Available: http://www.zinger-soft.com/iSSH_features.html. [Último acceso: Abril 2013].

[40] «Putty,» Marzo 2013. [En línea]. Available: http://www.putty.org/.

[41] «SSH Tunnel,» Marzo 201. [En línea]. Available: http://code.google.com/p/sshtunnel/. [Último acceso: Marzo 2013].

[42] Python Foundation, «Python,» Septiembre 2012. [En línea]. Available: http://python.org/. [Último acceso: Julio 2012].

[43] P. Atelin y J. Dordoigne, TCP/IP y protocolos de internet, Ediciones ENI, 2007.

[44] A. S. Tanenbaum, Redes de computadoras, Mexico: Pearson Educacion, 2003.

[45] RedHat, «SSH,» 2010. [En línea]. Available: http://www.gb.nrao.edu/pubcomputing/redhatELWS4/RH-DOCS/rhel-rg-es-4/ch-ssh.html. [Último acceso: Octubre 2012].

[46] Google, «raspberry-gpio-python,» Septiembre 2013. [En línea]. Available: [https://code.google.com/p/raspberry-gpio-python/downloads/list?can=1&q=&colspec=Filename+Summary+Uploaded+ReleaseDate+Size+DownloadCount]. [Último acceso: Agosto 2013].