DISEÑO E IMPLEMENTACIÓN DE UNA RED INALAMBRICA PARA SUFRAGIO ELECTRÓNICO BASADA EN EL ESTÁNDAR ZIGBEE (IEE802.15.4)

Borja Santiago, Ing.
Andrango Wilmer,Ing.

Debido a los altos costos, lentitud y riesgo de manipulación en el tratamiento de los resultados al llevar a cabo un proceso de elecciones, se ha hecho palpable la necesidad de solucionar este problema mediante la implementación del voto electrónico.

Actualmente, existen diversas tecnologías inalámbricas que definen la transmisión en tasas altas para voz, video y redes de computadoras personales. Sin embargo, estas tecnologías tienen características sobredimensionadas para aplicaciones donde el ancho de banda no es esencial como es el caso de la votación electrónica. ZigBee fue creado para cubrir la necesidad del mercado de un sistema a bajo costo, un estándar para redes Wireless personales de pequeños paquetes de información, bajo consumo, seguro y fiable.

Entre las principales características de este estándar se puede mencionar las siguientes:

- Bandas de trabajo 2,4 GHz, 868 MHz (Europa) y 915 MHz (EEUU).
- Alcance de hasta 75m
- Velocidad 20 a 250kbps
- Topología Maestro/Esclavo.
- Bajo consumo y administración de energía.
- Incorporación de algoritmos de seguridad.

SISTEMA DE VOTACIÓN

En la actualidad, cada proceso electoral demanda una gran inversión económica debido a los suministros, personal, transporte y otros recursos que se demandan. Además se hace necesario un gran planeamiento logístico para coordinar el evento y llegar al sitio adecuado en el momento que se necesite. Por último, los procesos actuales tienen un gran riesgo en la seguridad de la información, debido a la posible manipulación de los datos, especialmente en la tabulación de resultados en la cual se ven involucradas diferentes personas que podrían actuar fraudulentamente, cambiando el resultado real.

En los últimos años, han surgido y han sido implementados sistemas electrónicos que han hecho más sencillo y seguro el proceso electoral. Dichos sistemas tienen como ventaja principal almacenar los datos de forma digital para su futura tabulación, evitando la manipulación de los resultados.

Existen diversas formas de votación electrónica que varían según el grado de sofisticación técnica con el que se cuenta y el procedimiento utilizado. El elector puede usar su propia computadora (EE.UU) o, como en el caso de Brasil, el voto electrónico deberá ser emitido por él desde el lugar de votación que le fuera asignado. Pero más allá de las múltiples modalidades que hay, todas las formas de voto electrónico coinciden en brindar ciertas ventajas: bajo costo de implementación, rapidez en el recuento de los votos (apenas unos minutos son necesarios para

conocer el resultado de cada urna), simplicidad del sistema (el voto electrónico no debería presentar especiales dificultades ni siquiera para aquellas personas que no están familiarizadas con las nuevas tecnologías), etc.

Sin embargo, además de esos ventajosos aportes, el sistema debe -fundamentalmente- ser seguro. Se tiene que garantizar un correcto funcionamiento. De hecho, la gran crítica al uso del voto electrónico en una elección pasa, justamente, por la desconfianza que brinda. Es necesario, dada la importancia del acontecimiento, que las redes por las que circulan los datos electorales den tranquilidad al elector. Los ataques cibernéticos a los servidores donde se alojan los resultados del escrutinio deben evitarse de cualquier manera.

Motivados por esta tendencia, el proyecto describe la creación de un sistema de votación electrónico con la principal característica de que se implementa en base a una red inalámbrica de bajo costo, bajo consumo de potencia y alta seguridad. El sistema se encuentra dirigido a cubrir un proceso electoral que consulte a un grupo humano reducido (colegios de profesionales, entidades educativas, etc.). Con ciertas adecuaciones, el mismo puede ser utilizado por encuestadoras, consultoras o empresas de servicio para receptar datos provenientes del público, y con ello diagnosticar y mejorar los servicios que prestan.

DESCRIPCIÓN DEL PROYECTO

El sistema de votación elaborado es una red prototipo que consta de tres nodos (un coordinador o maestro y dos terminales o esclavos) que se comunican inalámbricamente, y un ordenador que se comunica de forma serial con el nodo maestro.

El coordinador tiene la tarea de iniciar y mantener la red Zigbee, y de recibir los datos provenientes de los esclavos (terminales de votación) para transferirlos al ordenador para su tabulación.

Para la comunicación con el usuario cada terminal dispone de dispositivos de entrada/salida (teclado/display de cristal líquido), cuya interacción con el usuario es sencilla y requiere de la mínima asistencia por parte de personas ajenas al votante, quienes podrían influir en su decisión

El ordenador posee una base de datos con tablas de información de los votantes (similar al padrón electoral) y de registro de los votos. El software implementado autentifica al votante, recoge su selección y la tabula junto al resto de votos al finalizar el evento electoral.

Los procesos de votación no manejan un flujo continuo, ni periódico de información ya que en determinado momentos cada nodo puede ser requerido por un gran número de usuarios y en otros no presentar demanda alguna.

En consecuencia el tráfico a generarse es de tipo intermitente, ya que los terminales transmiten información sólo cuando el usuario

está en proceso de votación, caso contrario el dispositivo entra en estado de reposo para maximizar el ahorro de energía.

Al ser un modelo prototipo se planteó como objetivo demostrar la factibilidad y sencillez de formar una red Zigbee a través de la implementación de una red básica, razón por la cual se utilizó una topología tipo estrella.

Redes con topologías más complejas como árbol y malla pueden ser implementadas, las cuales soportan un número de nodos mayor y tienen un mayor alcance. Sin embargo, requiriendo para ello de un mejor coordinador y ruteadores que necesitan mayores capacidades de memoria para almacenar la información sobre la red.

La seguridad es un área fundamental en un sufragio, es importante garantizar la integridad física de los equipos, identificar y autorizar a los nodos a participar en la red, autentificar y autorizar a los votantes, garantizar la veracidad de la información, proteger la privacidad de los datos, entre otros aspectos. Es importante resaltar que las medidas de seguridad se deben implementar en cada capa de la arquitectura Zigbee

A continuación se señalan las soluciones de seguridad implementadas, y consejos para ser tomados en cuenta para llevar a cabo durante un evento electoral.

A nivel físico, se debe precautelar el acceso al coordinador y a los terminales mediante personal o agentes de control que cuidarán su integridad y realizarán la autentificación mediante la solicitud de la documentación del posible votante. Se recomienda el uso de un UPS para enfrentar problemas o sabotaje del suministro de energía para el coordinador y el servidor. Adicionalmente, el servidor debe encontrarse física y lógicamente aislado de redes públicas o privadas inseguras que incrementen la probabilidad de un ataque cibernético.

A nivel de capa RED, se utiliza listas de acceso de direcciones para autorizar datos provenientes únicamente de los terminales de votación.

A nivel de aplicación el sistema verifica la validez de los datos, autentifica al usuario mediante su cédula de identidad y contraseña ingresadas, restringiendo la repetición de la votación de parte de un mismo usuario.

Una limitación a nivel de autentificación es la realización dentro de un mismo terminal de los procedimientos de identificación y de selección de voto (a diferencia de sistemas electrónicos utilizados en procesos electorales de gran escala). Como solución, cada usuario debe ingresar una contraseña que es verificada con la clave existente en la base de datos del ordenador/servidor.

El suministro de energía DC a cualquiera de los terminales se lo realiza mediante una batería o una fuente regulada del mismo voltaje. En cambio, el coordinador sólo utiliza una fuente regulada.

Para reducir el consumo de potencia, se da empeño en poner a los diferentes módulos terminales en modo de reposo (sleep) cuando no se encuentren en comunicación con el coordinador o con el usuario.

El ordenador utilizado como servidor funciona con 110V de alimentación AC, se recomienda su respaldado y del coordinador mediante una fuente de emergencia o UPS para caso de fallas de la alimentación en la red eléctrica.

El sistema ha sido diseñado para ser utilizado dentro de un área abierta o en recintos amplios (el hall del edificio de la Escuela de Ingeniería Eléctrica de la EPN, por ejemplo) donde no se encuentren obstrucciones (muros, paredes, etc.) y fuentes de interferencia que limiten el alcance de forma significativa. En un área abierta, se ha alcanzado una cobertura de hasta 60m.

Dicho rango cubre el suficiente espacio para ubicar en un recinto el suficiente número de terminales para desarrollar un proceso electoral de baja a media escala.

El computador utilizado en el sistema debe cumplir con algunos requerimientos básicos:
Disponer de un puerto serial DB9 con interfaz RS232, para la comunicación con el coordinador.
Trabajar con sistema operativo Windows 98 o superior para la ejecución del programa a crear.
Debe respaldarse de un sistema contra fallas de energía (UPS) para evitar errores de comunicación con el coordinador por caídas en el suministro eléctrico.

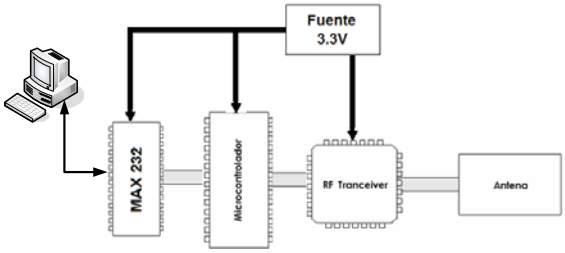
HARDWARE

Tiene las siguientes responsabilidades:

- Incluir dispositivos para la transmisión y recepción de datos formando una red inalámbrica bajo el estándar Zigbee.
- Permitir la interacción de los terminales con el usuario mediante el uso de dispositivos de entrada/salida.
- Permitir la comunicación serial entre el computador y el coordinador Zigbee.
- Proporcionar el interfaz necesario para la programación del software requerido por los nodos.
- Suministrar la energía requerida para el funcionamiento de los distintos módulos.

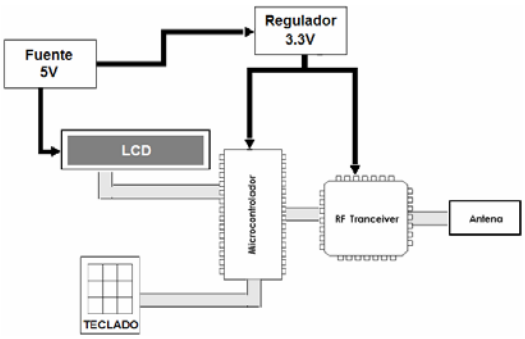
Los principales elementos que se pueden destacar en los terminales son los siguientes:

Coordinador



- Microcontrolador PIC 18LF4620
- Transceiver RF
- Conversor MAX 232

Nodo terminal/esclavo



- Microcontrolador PIC 18LF4620
- Transceiver RF
- Display LCD
- Teclado

El software desarrollado tiene como objetivos:

- Manejar la base de datos, permitiendo el ingreso de datos provenientes del sistema de votación.
- Controlar la seguridad e integridad de los datos: identificando a los votantes, evitando reintentos de sufragio, y reconociendo selecciones inválidas de parte del usuario.
- Presentar resultados y estadísticas del proceso electoral.
- Monitorear el funcionamiento del sistema para controlar su buen funcionamiento y advertir cualquier falla en la comunicación de los módulos para su pronta solución.

Adicionalmente se utilizaron varias herramientas para desarrollo y evaluación del sistema.

- Kit de desarrollo PICDEM Z. Es un kit de desarrollo para permitir a los desarrolladores experimentar y crear aplicaciones con las herramientas de la empresa Microchip para el protocolo Zigbee.
- MPLAB ICD2. Es un programador que permite cargar el código de máquina sin necesidad de desmontar el PIC del circuito, con la principal ventaja de ayudar a la depuración del código al permitir la ejecución paso a paso del mismo.
- MPLAB IDE. Es un entorno de desarrollo que permite crear aplicaciones basadas en microcontroladores Microchip. Que utilizado el lenguaje C para la programación.
- ZENA. Es un programa que genera los archivos de configuración del stack.
- Microchip Software Stack for Zigbee. Librería para la implementación de Zigbee en uC PIC 18
- Application Maestro. Conjunto de librerías de funciones para control de periféricos (entre ellos el LCD).

PROCEDIMIENTO DE VOTACIÓN

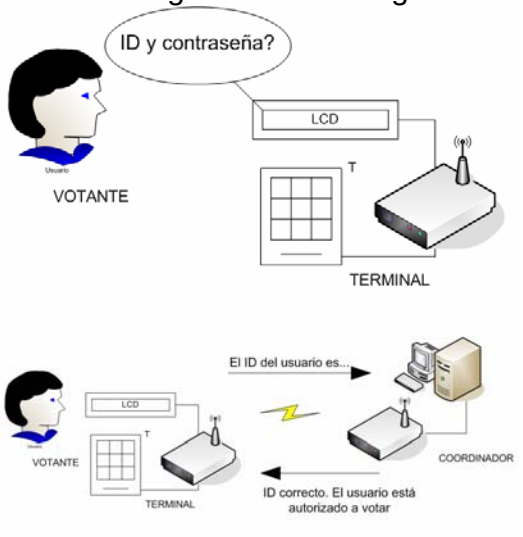
A continuación se describe el procedimiento general para que un individuo lleve a cabo la votación dentro del sistema, se analizan los posibles problemas a los que podría enfrentarse y se plantean soluciones contra ellos.

- El posible votante se identifica ante un agente (persona) de control, el cual verificará la validez de su

documento de identificación y autorizará su votación. El agente tiene como misión controlar el buen uso del sistema como medida de seguridad y prevenir sabotajes a nivel físico.

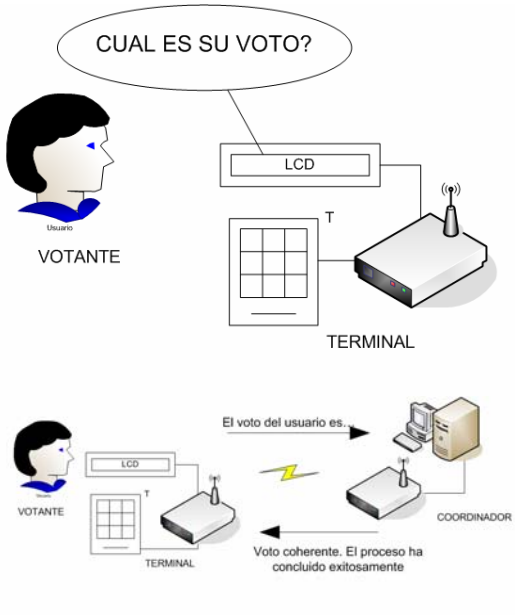
Autentificación ante el agente

- Una vez autorizado, el usuario se acerca al terminal, presiona la tecla INICIO para activar el sistema e ingresa su número de identificación y contraseña para ser verificado por la red. El dispositivo pedirá al usuario confirmar los datos ingresados para permitirle corregir errores de digitación.



Autentificación ante el terminal y verificación del servidor.

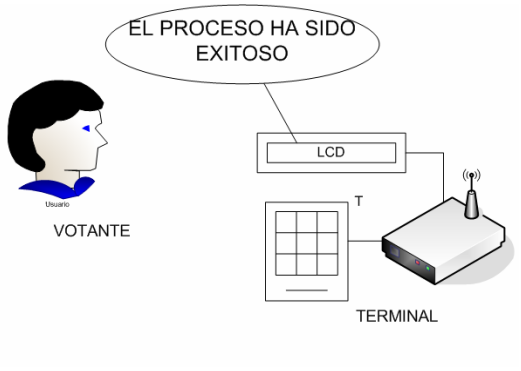
- Ya autentificado por la red, el usuario procede con la votación. Mediante el LCD se identifica la dignidad, y enumerará las opciones. Se permite al usuario el ingreso del número que represente la opción de su preferencia y se pedirá una confirmación de su voto antes de enviarlo. En caso negativo en la confirmación, tendrá la oportunidad de ingresar el voto nuevamente. Si ingresase una opción inexistente y lo confirmará, se le enviará un mensaje informándole de ello y el voto será considerado nulo. Se repetirá este último procedimiento, en caso de elección de más dignidades.



Recolección y procesamiento del voto

- Finalmente se despliega un mensaje informando sobre el éxito del proceso (Por ejemplo: “Su voto ha sido procesado”). Una vez concluido este proceso, el votante será marcado en la base de datos para evitar un posible reintento de votación

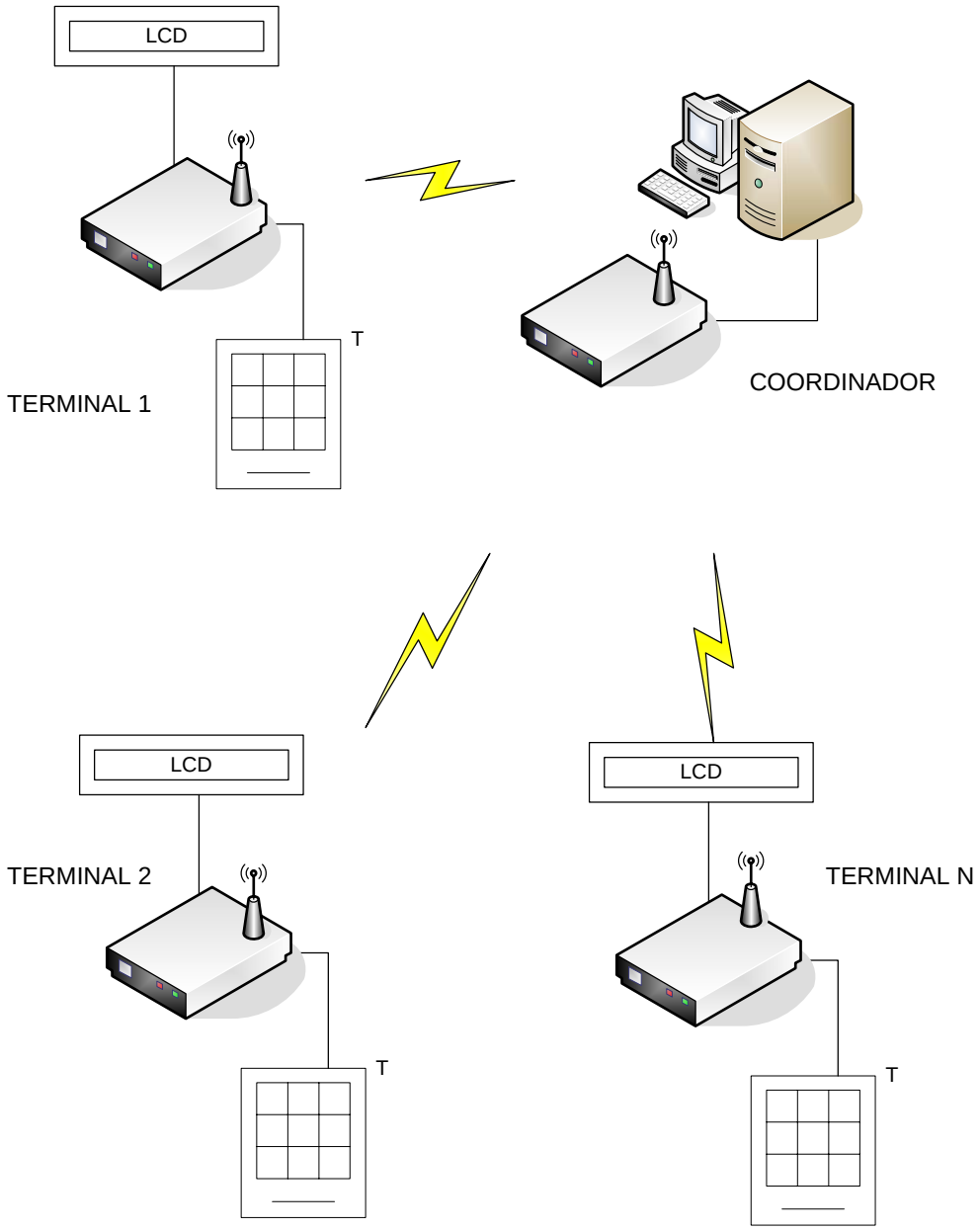
que podría afectar la credibilidad del proceso.



Informe de éxito del proceso

Adicionalmente, como ayuda al administrador del evento electoral, se implementó un sencillo programa para configurar el número de dignidades y las listas de candidatos a elegir. Este programa genera un archivo para ser cargado en la memoria del microcontrolador con el fin de que conozca estos datos y despliegue los nombres de las candidaturas en la pantalla del LCD ante el votante, al tiempo que actualiza la base de datos a ser utilizada por el programa de control de sufragio.

El sistema de administración además de mostrar en pantalla las estadísticas del proceso electoral; también muestra una ventana con los logs del sistema, fundamental para monitorear el proceso y corregir fallas en el mismo, en caso de presentarse.



Representación de la red implementada en el proyecto

El presente proyecto puede ser mejorado, y adecuado para procesos electorales de mayor magnitud, mediante la utilización de elementos con mayores capacidades, consiguiendo con ello redes más complejas y de mayor alcance, sin dejar de tomar en cuenta la facilidad del elector al llevar a cabo el proceso de votación.

e-mail: santiborja@msn.com