

**Universidad Autónoma de Baja California
FACULTAD DE CIENCIAS QUÍMICAS
E INGENIERÍA**

FOLIO No. **233**

Tijuana, B.C.

04 DE MAYO DE 2007

C. ISMAEL VILLANUEVA MIRANDA

Pasante de INGENIERO EN COMPUTACION

Presente

El tema de trabajo y/o tesis para su exámen profesional, en la

Opción TESIS

es propuesto, por el C. M.C. LUIS ENRIQUE PALAFOX MAESTRE

quien será el responsable de la calidad de trabajo que usted presente, referido al tema

"Red de Servicios para Usuarios Móviles en el Campus Universitario"

el cual deberá usted desarrollar, de acuerdo con el siguiente orden:

- I.- RESUMEN
- II.- ABSTRACT
- III.- OBJETIVO
- IV.- INTRODUCCION
- V.- ANTECEDENTES
- VI.- PROTOCOLOS
- VII.- APLICACIONES DE REDES AD HOC
- VIII.- MOBILE CAMPUS AREA NETWORK (MCAN)
- IX.- CONCLUSIONES Y TRABAJO FUTURO
- X.- GLOSARIO
- XI.- REFERENCIAS

UNIVERSIDAD AUTÓNOMA
DE BAJA CALIFORNIA



FACULTAD DE CIENCIAS
QUÍMICAS E INGENIERÍA

M.C. RUBÉN GUILLERMO SEPÚLVEDA
MARQUÉS

Sub-Director Secretario

M.C. LUIS ENRIQUE PALAFOX MAESTRE

Asesor

MC. MARÍA EUGENIA PÉREZ MORALES

Directora



**UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
FACULTAD DE CIENCIAS QUÍMICAS E INGENIERIA**

**“Red de Servicios para Usuarios Móviles en el Campus
Universitario”**

TRABAJO DE TESIS

Presentada por

ISMAEL VILLANUEVA MIRANDA

Para obtener el título de

INGENIERO EN COMPUTACIÓN

Tijuana, Baja California

Mayo de 2007

INDICE

RESUMEN	6
ABSTRACT	6
OBJETIVO	7
INTRODUCCIÓN	8
1.- ANTECEDENTES	10
1.1.- LOS INICIOS	11
1.2 PRIMERAS CONEXIONES	12
1.3 PRIMERAS REDES	13
1.4 REDES DE AREA LOCAL	17
1.4.1 ARQUITECTURA TOKEN-RING	18
1.4.2 ARQUITECTURA ETHERNET	20
1.4.3 Redes de área local inalámbricas	22
1.4.4 NORMALIZACION IEEE DE WLAN	23
1.4.5 WLAN 802.11	24
1.4.6 WLAN 802.11b	24
1.4.7 WLAN 802.11g	24
1.4.8 WLAN 802.11a (Wi-Fi 5)	25
1.4.9 TECNOLOGIA ZIGBEE	25
1.4.10 PROTOCOLO ALOHA	26
1.4.11 ORIGEN DE REDES AD HOC	27
1.4.12 DESAFÍOS TÉCNICOS DE REDES AD HOC	28
2 PROTOCOLOS	30
2.1 PROTOCOLOS DE ACCESO AL MEDIO	31
2.1.1 PROTOCOLOS MAC (Media Access Control)	31
2.1.2 PROTOCOLO MACA (MULTIPLE ACCESS WITH COLLISION AVOIDANCE)	32
2.1.3 PROTOCOLO MACA-BI (MULTIPLE ACCESS WITH COLLISION AVOIDANCE BY INVITATION)	33
2.1.4 PROTOCOLO PAMAS (POWER AWARE MULTI-ACCESS PROTOCOL WITH SIGNALING)	34
2.2.- PROTOCOLOS DE RUTEO	37
2.2.1.- DYNAMIC SOURCE ROUTING (DSR)	38
2.2.2.- ZONE ROUTING PROTOCOL (ZRP)	40
2.2.3.- TEMPORALLY ORDERED ROUTING ALGORITHM (TORA)	42
2.2.4.- AD HOC ON DEMAND DISTANCE VECTOR (AODV)	43
2.2.5.- OPTIMIZED LINK STATE ROUTING PROTOCOL (OLSR)	45
2.2.6.- LOCATION AIDED ROUTING (LAR)	47
2.2.7. - POWER AWARE ROUTING (PAR)	51
2.2.8. - SOURCE TREE ADAPTIVE ROUTING (STAR)	53
2.2.9.- A SECURE ON DEMAND ROUTING PROTOCOL FOR AD HOC NETWORK (ARIADNE)	55
3 APLICACIONES DE REDES AD HOC	58
3.1 HAWKVISION	59
3.1.1 DESCRIPCION	59
3.1.2 DESARROLLO	60
3.1.3 OBSERVACIONES	62
3.2 PROXIMITY	63
3.2.1 DESCRIPCION	63
3.2.2 DESARROLLO	64

3.2.3 OBSERVACIONES	68
3.3 TDA (TARGETED DISTRIBUTED ADVERTISEMENTS)	69
3.3.1 DESCRIPCION.....	69
3.3.2 DESARROLLO.....	70
3.3.3 OBSERVACIONES	73
3.4 ZEBRANET PROJECT	74
3.4.1 DESCRIPCION.....	74
3.4.2 DESARROLLO.....	75
3.4.3 OBSERVACIONES	78
4 MOBILE CAMPUS AREA NETWORK (MCAN)	80
4.1 DESCRIPCION DE MCAN	81
4.1.1 COMPARTIR INFORMACION	81
4.1.2 ALMACENAMIENTO DE INFORMACION.....	82
4.1.3 CONSULTAS ESPECIALIZADAS	84
4.1.4 MENSAJERIA BASADA EN WEB	85
4.1.5 MENSAJERO INSTANTANEO	87
4.1.6 CLASES INTERACTIVAS	88
4.1.7 APUNTES	88
4.1.8 PREGUNTAS ALUMNO - MAESTRO Y MAESTRO - ALUMNO	89
4.1.9 EXÁMENES AUTOMÁTICOS	89
4.1.10 LISTA AUTOMÁTICA.....	90
4.1.11 LOCALIZACION GEOGRAFICA.....	92
4.1.12 KIOSCOS DE ACCESO A LA RED	94
4.2 HARDWARE	96
4.2.1 SERVIDORES.....	96
4.2.2 PUNTOS DE ACCESO (KIOSCOS).....	97
4.2.3 NODOS MÓVILES.....	98
4.3 MAPA.....	100
5 CONCLUSIONES Y TRABAJO FUTURO.....	102
6 GLOSARIO	105
REFERENCIAS	106

LISTA DE FIGURAS

FIG. 1 PRIMERAS COMPUTADORAS	11
FIG. 2 ANTIGUOS SISTEMAS DE COMUNICACIÓN	13
FIG. 3 EQUIPO DE LA ARPANET	14
FIG. 4 MAPA GEOGRAFICO DE ARPANET (1980)	15
FIG. 5 ARQUITECTURA TOKEN RING	19
FIG. 6 ARQUITECTURA ETHERNET	21
FIG. 7 REPRESENTACIÓN SIMBÓLICA DE UNA WLAN	22
FIG. 8 ESQUEMA REPRESENTATIVO DE UNA RED AD HOC	27
FIG. 9 RADIO DE ALCANCE DE UN NODO	28
FIG. 10 REPRESENTACIÓN DEL PROTOCOLO MAC	31
FIG. 11 EJEMPLO DE PROTOCOLO MACA	33
FIG. 12 EJEMPLO PROTOCOLO MACA-BI	34
FIG. 13 ESTADOS DEL PROTOCOLO PAMAS	35
FIG. 14 RED USANDO EL PROTOCOLO ZRP	41
FIG. 15 GRAFO ACÍCLICO DIRIGIDO (DAG)	43
FIG. 16 FUNCIONAMIENTO DE AODV	44
FIG. 17 FUNCIONAMIENTO DE OLSR	47
FIG. 18 ZONA ESPERADA (EXPECTED ZONE)	48
FIG. 19 ZONA DE PETICIÓN (REQUEST ZONE)	49
FIG. 20 ESQUEMA LAR 1	50
FIG. 21 ESQUEMA LAR 2	51
FIG. 22 EJEMPLO DE FUNCIONAMIENTO DE STAR	54
FIG. 23 ABSTRACCIÓN EN TRES CAPAS DEL PROYECTO	60
FIG. 24 DIAGRAMA DE SECUENCIA “HELLO”	66
FIG. 25 DIAGRAMA DE SECUENCIA “SEARCH PROFILE”	67
FIG. 26 INTERFAZ DE USUARIO PROXIMITY	68
FIG. 27 ARQUITECTURA DE TDA	72
FIG. 28 ESTADOS DE MOVIMIENTO DE LAS ZEBRAS	76
FIG. 29 DIAGRAMA DE BLOQUE DEL COLLAR ZEBRANET	77
FIG. 30 COMUNICACIÓN ENTRE USUARIOS CON INTERESES COMUNES	82
FIG. 31 ESQUEMA REPRESENTATIVO DEL PROCESO DE ALMACENAMIENTO DE INFORMACIÓN	83
FIG. 32 PROCESO DE ENVIAR Y CONTESTAR UNA CONSULTA	84
FIG. 33 MENSAJERÍA BASADA EN WEB	86
FIG. 34 MENSAJERÍA INSTANTÁNEA	87
FIG. 35 DIAGRAMA REPRESENTATIVO DE LISTA AUTOMÁTICA	91
FIG. 36 ETIQUETA RFID	92
FIG. 37 CALCULANDO LA UBICACIÓN DE UN NODO MÓVIL	93
FIG. 38 PROTOTIPO DE INTERFAZ GRÁFICA DEL KIOSCO	95
FIG. 39 CASSETAS DE ACCESO A LA RED	95
FIG. 40 SERVIDOR SUN FIRE T2000	96
FIG. 41 PUNTO DE ACCESO ORINOCO AP-4900M	97
FIG. 43 LAPTOP QUE PODRÁ SER USADA COMO NODO MÓVIL	98
FIG. 44 POCKET PC USADO COMO NODO MÓVIL	99
FIG. 45 DISTRIBUCIÓN GEOGRÁFICA DE LOS KIOSCOS Y SERVIDORES EN EL CAMPUS UABC TIJUANA	100

RESUMEN

Redes Ad Hoc es una área que se encuentra actualmente en un rápido desarrollo, y en consecuencia es un nuevo concepto que se aplica cuando un usuario desea comunicarse de alguna manera con una red temporal, sin necesidad de que exista una administración centralizada. Cada usuario que participa en la red actúa tanto como *terminal* y *enrutador*, por lo tanto puede reenviar paquetes de otros nodos.

Estas redes tienen ciertas características que imponen nuevas demandas sobre los protocolos existentes. La característica más importante es la movilidad de los nodos. Pueden cambiar de posición muy frecuentemente, por lo cual se necesitan protocolos que se puedan adaptar rápidamente a los cambios de la topología de la red. Otra característica que necesitan los protocolos es la adecuada administración de energía de los dispositivos de la red.

En este trabajo se propone una infraestructura que aprovecha las funcionalidades que ofrecen las redes Ad Hoc para beneficiar a la comunidad universitaria, brindando ciertas aplicaciones de comunicación que facilitarán la interacción de todos los usuarios dentro de los campus.

ABSTRACT

Ad hoc networks is an area that is at the moment in a fast development, and consequently is a new concept that is applied when a user wishes to communicate somehow with a temporary network, with no need of that exists a centralized administration. Each user who participates in the network acts as much as host and router, therefore he can re-send packages of other nodes.

These networks have certain characteristics that impose new demands on the existing protocols. The most important characteristic is the mobility of the nodes. They can change very frequently of position, thus are needed protocols that can be adapted quickly to the changes of the topology of the network. Another characteristic that needs the protocols is the suitable administration of energy of the devices of the network.

In this work an infrastructure sets out that takes advantage of the functionalities that offer the Ad hoc networks to benefit the university community, offering certain applications of communication that facilitated the interaction of all the users within the campuses.

OBJETIVO

El objetivo de este trabajo es presentar una investigación sobre un área muy importante de la computación, las redes, específicamente redes Ad Hoc. Se intenta dar un panorama amplio y profundo sobre el tema, abarcando la mayor parte de las características de las redes Ad Hoc.

A los lectores se les pretende introducir en el tema de una forma clara, sencilla y precisa, mostrando su importancia cuando todas ellas trabajan en conjunto y se obtiene un sistema o infraestructura de calidad.

El principal objetivo o meta del presente trabajo es dejar un material escrito que pueda servir como referencia para otras investigaciones, o que pueda ser motivo de inspiración para iniciar futuras investigaciones relacionadas con el área de redes ad hoc.

INTRODUCCIÓN

Existe mucha literatura del área informática que hace reseñas sobre los precursores de esta área que nos dan a conocer su vida y sus logros. A muchos nos nace la curiosidad de querer innovar e investigar al leer dichos textos ya que son una buena fuente de inspiración.

Al ver como la tecnología ha evolucionado, nos damos cuenta que dicha evolución ha sido en un tiempo muy corto comparado con otras tendencias por ejemplo el pensamiento humano que ha tardado siglos y aun no alcanza la perfección.

Al mismo tiempo, han nacido otras áreas igual de importantes, como las redes de computadoras. No solo era necesario que existieran computadoras más pequeñas y potentes, sino que deberían existir mecanismos mediante los cuales se pudieran comunicar para trabajar en conjunto y tratar de obtener un resultado en común.

Las redes de computadoras se han desarrollado con una velocidad impresionante, originándose en proyectos tales como el ARPANET, proyecto de la milicia americana, pasando por otras arquitecturas como TOKEN RING, LAN, WAN, WIFI hasta llegar a redes como las redes AD HOC.

Las redes AD HOC han tenido una gran cantidad de aplicaciones tanto para el beneficio humano como para la investigación. En el campo de desarrollo de aplicaciones para beneficiar las distintas actividades que los humanos realizamos comúnmente podemos mencionar varias, por ejemplo en centros comerciales se utilizan para dar mayor información sobre ciertos productos a los clientes. En la investigación, podemos mencionar proyectos relacionados con el censo de especies animales por ejemplo, el proyecto ZEBRA NET, que se enfoca en el estudio del comportamiento, migración y hábitos de especies como Zebras, Leones o cualquier otra.

De igual forma, en este trabajo se propone la implementación de un proyecto que beneficiaría a toda la comunidad universitaria, de esta manera se acerca un poco más la tecnología a todos los usuarios universitarios con la intención de que nuestra universidad cuente con sistemas de tecnologías recientes y esté a la vanguardia y al nivel de otras instituciones educativas en otros países de primer mundo.

CAPITULO

I ANTECEDENTES

Los avances tecnológicos que hoy en día nos impresionan, son gracias a varios personajes e instituciones que durante largos años han realizado investigaciones en diversas áreas informáticas.

Se dice que toda persona no tiene más de 5 ideas brillantes en toda su vida, y gracias a estas ideas vemos hoy como nuestra vida se ha plagado de muchas tecnologías nuevas y que hacen que nuestra vida diaria sea un poco más fácil de llevar.

Personajes como Bill Gates, Paul Allen, Steve Jobs, Linus Torvalds, Blaise Pascal, Steve Wozniak entre muchos otros son quienes han tenido esas grandes ideas que han revolucionado el mundo tecnológico. Estas personas han visto al mundo desde una perspectiva diferente a como muchos de nosotros lo vemos.

Debemos aprender de la historia para seguir mejorando la tecnología, ella nos ha enseñado que los cambios están siempre presentes, solo es cuestión de saberlos apreciar en el momento oportuno.

En este capítulo veremos como evolucionó la informática desde sus inicios hasta hoy en día, pasando por muchas etapas y áreas importantes como las redes de computadoras.

1.1.- LOS INICIOS

Al inicio, cuando surgieron las computadoras, éstas eran grandes, delicadas, caras, difíciles de operar y sobre todo poco eficientes. La ENIAC era un claro ejemplo, pesaba cerca de 30 toneladas y ocupaba el espacio equivalente a un cuarto de 10 m² (como se muestra en la fig. 1), su operación requería la cantidad de 174,000 W de potencia. Su costo era excesivo para la época, de forma que solo algunas instituciones (Universidad de Pensilvania en conjunto con el Departamento de Defensa) podían permitirse el lujo de tener y mantener una maquina de ese tipo.



Fig. 1 Primeras computadoras

A pesar de todas las desventajas que presentaban las máquinas, pronto le siguieron otras. La EDVAC (Electronic Discrete Variable Automatic Computer), solo existió como una

propuesta de diseño. Sin embargo, el Ferranti Mark I basado en un diseño de F.C. Williams y T. Kilburn de la Universidad de Manchester fue la primera computadora de uso general que se puso a la venta.

El EDSAC (Electronic Delay Storage Automatic Calculator), desarrollado por Maurice Wilkes de Cambridge, fue operativa por primera vez en Junio de 1949, siendo el inspirador de la primera computadora específicamente construida para aplicaciones de gestión, el LEO (Loans Electronic Office).

Tiempo más tarde surgieron el Whirlwind I y el IBM 701. En 1952 se construyeron dos computadoras idénticas en la Universidad de Illinois, una de ellas, el ORDVAC (Ordinance Variable Automatic Computer), fue destinada al Laboratorio de Investigaciones Balísticas de Aberdeen, un campo de pruebas del ejército. El otro, ILLIAC, fue retenido en la propia Universidad. En 1949 Eckert y Mauchly, los creadores de ENIAC, ponen en funcionamiento otra computadora, la BINAC (Binary Automatic Calculator).

1.2 PRIMERAS CONEXIONES

El contacto físico de los usuarios con las computadoras era bastante escaso, por lo que empezaron a generarse soluciones para acercarlos, empezó así el embrión de lo que sería el teleproceso y las redes, al empezar a utilizar algunos dispositivos físicamente alejados de las computadoras de las que dependían, enlazadas mediante líneas de muy diversos tipos.



Fig. 2 Antiguos sistemas de comunicación

Uno de los primeros servicios que se ofrecieron fue la impresión remota, donde la computadora enviaba los resultados a equipos de impresión en las oficinas y despachos de los usuarios. En la figura 2 se muestra un antiguo sistema de comunicación usado al inicio del desarrollo informático. Pronto apareció un antecesor de TELNET, un servicio que permitía ya el acceso a las computadoras mediante terminales remotas. Cuando la cantidad de computadoras en universidades y centros de investigación fue creciendo, se hizo evidente la necesidad de enviar datos directamente de una computadora a otra, con lo que nació FT (File Transfer), un sistema para que una computadora entendiera lo que enviaba otra, salvando las posibles diferencias particulares (modelo, lenguaje, formato interno de los datos, etc.).

1.3 PRIMERAS REDES

En diciembre de 1957 se marca otro hecho importante en el desarrollo de la computación, cuando en plena Guerra Fría, en respuesta al primer satélite soviético, el Departamento de Defensa (DoD) funda la ARPA, Agencia de Proyectos Avanzados de Investigación, para devolver a los EEUU la superioridad en el área de aplicaciones militares de la computación. Esta agencia sería la promotora de muchos proyectos científicos de gran trascendencia, entre los cuales se encuentra el lanzamiento del primer satélite artificial.



Fig. 3 Equipo de la ARPANET

En la figura 3 se muestra al equipo de científicos que colaboraron en el desarrollo de la ARPANET. Durante los años 60 y 70 se crearon muchas tecnologías de redes, cada una basada en un diseño específico de hardware. Algunas de estas redes, llamadas de área local LAN (Local Area Network), conectan equipos en distancias cortas mediante cables y hardware específico instalado en cada equipo. Otras redes más grandes, llamadas de área extensa WAN (Wide Area Network), conectaban equipos a distancias mayores utilizando líneas de transmisión similares a las empleadas en los sistemas telefónicos.

En 1959 en plena Guerra fría, los soviéticos lanzan con éxito su primer satélite artificial Sputnik, lo que induce a EEUU a redoblar sus esfuerzos científicos y técnicos por conseguir la supremacía tecnológico-militar. En 1960 el Departamento de Defensa ya poseía una red de computadoras uniendo sus centros estratégicos y de investigación (message-communication network, AUTODIN), aunque tenía conocidas deficiencias.

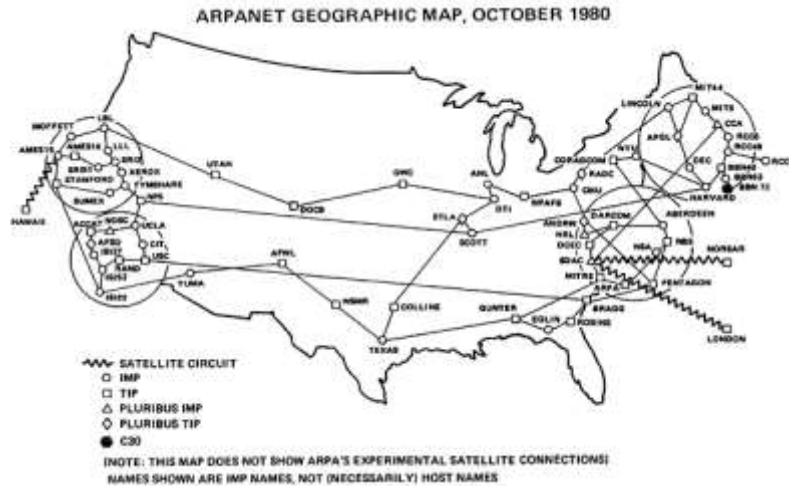


Fig. 4 Mapa geografico de ARPANET (1980)

En 1969 la Agencia ARPA crea ARPANet (Advance Research Proyect Agency Network), una red experimental de computadoras, basada en la tecnología de conmutación de paquetes. ARPANet era un proyecto para interconectar los diversos tipos de redes y permitir el libre intercambio de información entre los usuarios, independientemente de las máquinas o redes que utilizaran. Para ello, se agregaron equipos especiales, llamados enrutadores, que conectaban redes LAN y WAN de diferentes tipos. Los equipos interconectados necesitaban un protocolo en común. El nuevo protocolo de red propuesto por ARPA se denominó NCP y el sistema de esta red de redes interconectadas se llama hoy en día INTERNET.

La primera instalación real de una red de este tipo, se realizó dentro del edificio del Laboratorio Nacional de Física de Inglaterra en 1968, pronto se construirían modelos mucho mayores. Muy poco después el Pentágono deseaba construir en EEUU una red basada en los mismos principios, la tecnología de conmutación de paquetes se convierte rápidamente en la base del programa de redes de datos del Departamento de Defensa y se decide construir una primera red uniendo cuatro computadoras. En la figura 4 se muestra el mapa geográfico de cómo estaba constituida y distribuida la ARPANET.

Una compañía de Cambridge ganó el concurso para construir los conmutadores de paquetes IMP que utilizaría la red. En el mes de septiembre llega a la Universidad de UCLA el primer IMP. Pocas semanas después llegaron IMPs a las universidades de Stanford (Stanford Research Institute, SRI), Santa Bárbara de California (UCSB) y la Universidad de Utah en Salt Lake City. Cuando estos equipos estuvieron configurados, se conectaron a líneas telefónicas, y ARPANet empezó a funcionar con estos cuatro nodos en 1969.

Esta primera red (ARPANet) permitía a los investigadores trabajar conjuntamente en las súper computadoras de la época. Ofrecía básicamente tres servicios: Acceso a computadoras mediante terminal remota (TELNET), transferencia de archivos (FTP) e impresión remota.

ARPANet siguió creciendo. En 1971 ya constaba de quince nodos, en 1972 ya eran 37 los miembros de la red. Formar parte del club era por aquel entonces muy caro, una conexión costaba un cuarto de millón de dólares anuales.

En 1972, Robert Kahn hace la primera demostración pública de ARPANet, conectando 40 máquinas a lo largo y ancho de EEUU con la TIP (Terminal Network Group) en el vestíbulo del hotel Hilton en Washington, DC. ARPA cambia su nombre por DARPA (Defense Advanced Research Projects Agency). Se crea el INWG (International Network Working Group), entidad encargada de investigar protocolos comunes para la red.

En 1973 el crecimiento de la red se estimaba en un nuevo miembro cada veinte días y ARPANet se internacionaliza con la inclusión del University College de Londres y el Radar Real de Noruega. Sin embargo, el continuo incremento de tráfico militar en la red hizo que en Julio de 1975 la DCA (Defense Communications Agency) tomara el control sobre ARPANet.

En 1976 se materializa el proyecto de una red conmutada de paquetes vía satélite, SATNet (Atlantic packet Satellite Network), que enlaza los EEUU con Europa, aunque

sorprendentemente no usa satélites gubernamentales o militares, sino InTelSat (International Telecommunications Satellite Organization), una red de satélites de comunicaciones civiles.

En 1982 ARPANet instala oficialmente el protocolo TCP/IP como el oficial de la red, sustituyendo al protocolo original NCP (Network Control Protocol) con que había empezado su operación.

En enero de 1983, la DCA exige que adopten el protocolo TCP/IP a todos los sitios que desean seguir conectados a ARPANet. En este mismo año ARPANet se divide en MILNET, de uso preferencialmente militar y la nueva ARPANet de uso científico.

1.4 REDES DE AREA LOCAL

En los días anteriores a las computadoras personales, una empresa podía tener solamente una computadora central, accediendo los usuarios a esta vía terminales de computadora sobre un cable simple de baja velocidad. Las redes como SNA de IBM (la Arquitectura de Red de Sistemas) fueron diseñadas para unir terminales o computadoras centrales a sitios remotos sobre líneas alquiladas. Las primeras LAN fueron creadas al final de los años 70 y se solían crear líneas de alta velocidad para conectar grandes computadoras centrales a un solo lugar. Muchos de los sistemas fiables creados en esta época, como Ethernet y ARCNET fueron los más populares. El crecimiento CP/M y DOS basados en la computadora personal significó que en un lugar físico existieran docenas o incluso cientos de computadoras. La intención inicial de conectar estas computadoras fue, generalmente compartir espacio de disco e impresoras, tales recursos eran muy caros en este tiempo. Había muchas expectativas en este tema desde el año de 1983 en adelante y la industria informática declaró que el siguiente año sería “El año de las LAN”.

En realidad esta idea se vino abajo debido a la proliferación de las incompatibilidades de la capa física y la implantación del protocolo de red, y confusión sobre la mejor forma de

compartir los recursos. Lo normal es que cada vendedor tuviera tarjeta de red, cableado, protocolo y sistema de operación de red. Con la aparición de Netware surgió una nueva solución la cual ofrecía: soporte imparcial para los 40 o más tipos que existían de tarjetas y cables y sistemas operativos mucho más sofisticados que los que ofrecían la mayoría de los competidores. Netware dominaba el campo de las LAN de las computadoras personales desde antes de su introducción en 1983 hasta mediados de los 90, cuando Microsoft introdujo Windows NT Advance Server y Windows for Workgroups. De todos los competidores a Netware, sólo Banyan Vines tenía fuerza técnica comparable, pero Banyan se ganó una base segura. Microsoft y 3Com trabajaron juntos para crear un sistema de operaciones de red simple el cual estaba formado por la base de 3Com's 3+Share, el Gestor de redes Lan de Microsoft y el Servidor de IBM. Ninguno de estos proyectos fue especialmente satisfactorio. En este mismo período las terminales de trabajo de Unix de los fabricantes Sun Microsystems, Hewlett-Packard, Silicon Graphics, Intergraph, Next y Apolo estaban usando TCP/IP basado en protocolos de red. A pesar de que ahora el mercado en este aspecto esta muy reducido, la tecnología de desarrollo en este área continúa influenciado por Internet e incluso por redes Linux como por Apple Mac OS X].

1.4.1 ARQUITECTURA TOKEN-RING

La arquitectura Token-Ring es una implementación del estándar IEEE 802.5, en el cual se distingue más por su método de transmitir la información que por la forma en que se conectan las computadoras, en la figura 5 se puede apreciar un diagrama representativo de redes con arquitectura Token-Ring.

El primer diseño de una red de Token-Ring es atribuido a E. E. Newhall en 1969. IBM publicó por primera vez su topología de Token-Ring en marzo de 1982, cuando esta compañía presentó los artículos para el proyecto 802 del IEEE. IBM anunció un producto Token_Ring en 1984, y en 1985 este llegó a ser un Standard de ANSI/IEEE.



Fig. 5 Arquitectura Token Ring

Cuando una computadora desea mandar información debe esperar a que le llegue el token vacío, cuando le llega utiliza el token para mandar la información a otra computadora, entonces cuando la otra computadora recibe la información regresa el token a la computadora que envió con el mensaje de que fue recibida la información. Así se libera el token para volver a ser usado por cualquier otra computadora. Aquí, debido a que una computadora requiere el token para enviar información no hay colisiones, el problema reside en el tiempo que debe esperar una computadora para obtener el token.

Los datos en token-ring se transmiten a 4 ó 16 Mbps, depende de la implementación que se haga. Todas las estaciones se deben de configurar con la misma velocidad para que funcione la red. Cada computadora se conecta a través de cable par trenzado ya sea blindado o no a un concentrador llamado MAU (Media Access Unit), y aunque la red queda físicamente en forma estrella, lógicamente funciona en forma de anillo por el cual da vueltas el token.

Un MAU puede permitir hasta 72 computadoras conectadas y el cable del MAU a la computadora puede ser hasta de 100 metros utilizando Par Trenzado Blindado, o 45 metros sin blindaje. El

token-ring es eficiente para mover datos a través de la red. En redes pequeñas a medianas con tráfico de datos pesado el token-ring es más eficiente que Ethernet.

1.4.2 ARQUITECTURA ETHERNET

A finales de 1960, la Universidad de Hawai desarrolló una red de área amplia. La universidad necesitaba conectar varias computadoras que estaban esparcidas a través del campus. La pieza principal en el diseño de la red fue llamado Carrier-Sense Multiple Access with Collision Detection (CSMA/CD). Carrier-Sense significa que la computadora escucha el cable de la red y espera hasta un período de silencio para poder mandar su mensaje. Multiple Access se refiere a que múltiples computadoras pueden estar conectadas en el mismo cable de la red. Collision Detection es una protección contra mensajes chocando en el tránsito.

Este primer diseño de red fue la fundación de lo que hoy es Ethernet, en la figura 6 se puede ver un diagrama que representa una arquitectura de este tipo. En 1972, Xerox Corporation creó el experimental Ethernet, y en 1975 introdujo el primer producto Ethernet. La versión original de este producto de red fue diseñado como un sistema de 2.94 mbps conectando hasta 100 computadoras en un cable de un kilómetro.

El Ethernet de Xerox fue tan exitoso que Xerox, Intel y Digital crearon un estándar para Ethernet de 10 mbps. Este diseño fue la base de la especificación IEEE 802.3. El producto Ethernet se apega en la mayoría de las partes del estándar 802.3.

Las redes Ethernet pueden utilizar diferentes tipos de cableado, cada uno con sus beneficios y problemas. Los tres cableados más comunes son Thinnet, Thicknet, y Twisted Pair (Par trenzado).

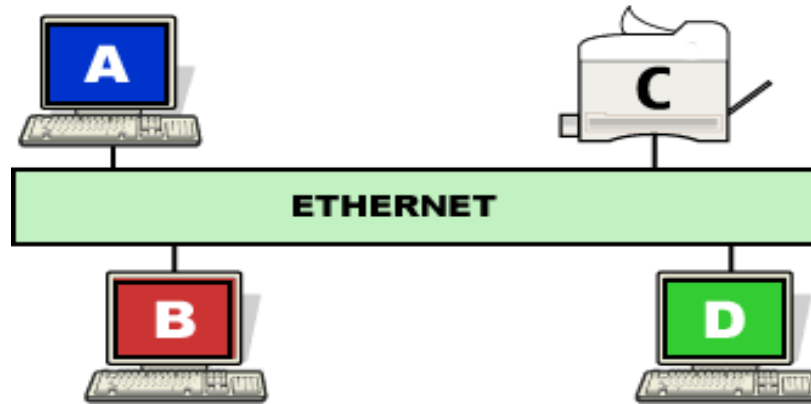


Fig. 6 Arquitectura Ethernet

Thinnet ó 10Base2 puede transmitir datos a 10mbps por banda base (señales digitales), pudiendo llegar el cableado hasta 185 metros. Se utiliza cable coaxial RG-58 el cual es bastante barato por lo que a esta red también se le conoce como CheapNet. Un mismo segmento de cable puede soportar hasta 30 computadoras. Es el más utilizado y recomendado para redes pequeñas. Utiliza la topología local bus, donde un mismo cable recorre todas y cada una de las computadoras.

Thicknet ó 10Base5 transmite datos a 10mbps por banda base en un cableado que puede alcanzar 500 metros. El cableado es grueso y es utilizado principalmente para largas oficinas o hasta todas las computadoras de un edificio. Del cable principal (backbone) salen cables usualmente Par Trenzado que se conectan directamente a cada una de las computadoras. Se pueden conectar hasta 100 computadoras con este cableado en un mismo segmento.

Twisted Pair ó 10BaseT transmite datos a 10mbps por Banda Base y utiliza un concentrador desde el cual con cable Par Trenzado se conecta cada una de las computadoras quedando en forma similar a estrella. El concentrador queda en el centro de la estrella y funciona como "repetidor". El cable desde el concentrador hasta la computadora no debe de medir más de 100 metros.

1.4.3 Redes de área local inalámbricas

Una WLAN es un sistema de comunicaciones de datos que transmite y recibe datos utilizando ondas electromagnéticas, en lugar del par trenzado, coaxial o fibra óptica utilizado en las LAN, y que proporciona conectividad inalámbrica de igual a igual (peer to peer), dentro de un edificio, de una área residencial o de un campus universitario.



Fig. 7 Representación simbólica de una WLAN

Las WLAN se encuadran dentro de los estándares desarrollados por el IEEE para redes locales inalámbricas. La figura 7 se muestra el diagrama representativo de una red WLAN interactuando con una LAN. Otras tecnologías como HyperLAN apoyada por el ETSI, y el nuevo estándar Homero para el hogar, también pretenden acercarnos a un mundo sin cables y, en algunos casos, son capaces de operar en conjunto y sin interferirse entre sí.

El origen de las LAN inalámbricas se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados por el IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema de espectro expandido (spread spectrum). En mayo de 1985, y tras cuatro años de estudios, la FCC (Federal Communications Comisión), la agencia federal del

Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-55,850 GHz para uso en las redes inalámbricas basadas en Spread Spectrum (SS), con las opciones DS (Direct Sequence) y FH (Frequency Hopping). La técnica de espectro expandida es una técnica de modulación que resulta ideal para las comunicaciones de datos, ya que es muy poco susceptible al ruido y crea pocas interferencias. La asignación de esta banda de frecuencias propició una mayor actividad en el seno de la industria y ese respaldo hizo que las WLAN empezaran a dejar ya el entorno del laboratorio para iniciar su camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando ya mas en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativos que superaban la velocidad de 1 Mbit/s, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN, con aplicación empresarial.

1.4.4 NORMALIZACION IEEE DE WLAN

La historia de las WLAN es bastante reciente, de poco más de una década. En 1989, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN, pero no es hasta 1994 cuando aparece el primer borrador, y habría que esperar hasta el año 1999 para dar por finalizada la norma.

En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencias para los sistemas PCS (Personal Communications Systems). En 1993 también se constituye la IrDA (Infrared Data Association) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos. En 1996, finalmente, un grupo de empresas del sector de computación móvil (Movil Computing) y de servicios forman el Wireless LAN Interoperability Forum (WLI Forum) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios inter

operativos. Por otra parte, WLANA (Wireless LAN Association) es una asociación de industrias y empresas cuya misión es ayudar y fomentar el crecimiento de la industria WLAN a través de la educación y promoción.

1.4.5 WLAN 802.11

En junio de 1997 el IEEE ratificó el estándar para WLAN IEEE 802.11, que alcanzaba una velocidad de 50 Mbit/s, con una modulación de señal de espectro expandido por secuencia directa (DSSS), aunque también contempla la opción de espectro expandido por salto de frecuencia, FHSS en la banda de 2.4 GHz, y se definió el funcionamiento y la interoperabilidad entre redes inalámbricas.

El 802.11 es una red local inalámbrica que usa la transmisión por radio en la banda de 2.4 GHz, o infrarroja, con regímenes binarios de 1 a 2 Mbit/s. El método de acceso al medio MAC (Medium Access Mechanism) es mediante escucha pero sin detección de colisión, CSMA/CA.

1.4.6 WLAN 802.11b

Un poco más tarde en 1999, se aprobó el estándar 802.11b, una extensión del 802.11 para WLAN empresariales, con una velocidad de 11 Mbit/s y un alcance de 100 metros, que al igual que Bluetooth y Homero, también emplea la banda de ISM de 2.4 GHz, pero en lugar de una simple modulación de radio digital y salto de frecuencia (FH/Frecuency Hopping), utiliza la modulación lineal compleja (DSSS). Permite mayor velocidad, pero presenta una menor seguridad, y el alcance puede llegar a los 100 metros, suficientes para un entorno de oficina o residencial.

1.4.7 WLAN 802.11g

El IEEE también ha aprobado en el 2003 en el estándar 802.11g compatible con el 802.11b, capaz de alcanzar una velocidad doble, es decir hasta 22 Mbit/s o llegar, incluso a 54

Mbit/s, para competir con los otros estándares que prometen velocidades de transmisión de datos mucho más elevadas pero que son incompatibles con los equipos 802.11.b ya instalados, aunque pueden coexistir en el mismo entorno debido a que las bandas de frecuencias que emplean son distintas. Por extensión también se le llama Wi-Fi.

1.4.8 WLAN 802.11a (Wi-Fi 5)

El IEEE ratificó en julio de 1999 el estándar en 802.11a, que con una modulación QAM-64 y la codificación OFDM alcanza una velocidad de hasta 54 Mbit/s en la banda de 5 GHz, menos congestionada y, por ahora, con menos interferencias, pero con un alcance limitado a 50 metros, lo que implica que montar más puntos de acceso que si se utilizase 802.11b para cubrir el mismo área, con el costo adicional que ello supone.

1.4.9 TECNOLOGIA ZIGBEE

ZigBee, también conocido como "HomeRF Lite", es una tecnología inalámbrica con velocidades comprendidas entre 20 kB/s y 250 kB/s y rangos de 10 m a 75 m. Puede usar las bandas libres ISM de 2,4 GHz, 868 MHz (Europa) y 915 MHz (EEUU).

Una red ZigBee puede estar formada por hasta 255 nodos los cuales tienen la mayor parte del tiempo el transceiver ZigBee dormido con objeto de consumir menos energía que otras tecnologías inalámbricas. El objetivo, es que un sensor equipado con un transceiver ZigBee pueda ser alimentado con dos pilas AA durante al menos 6 meses y hasta 2 años.

Como comparativa, la tecnología Bluetooth es capaz de llegar a 1 MB/s en distancias de hasta 10 m operando en la misma banda de 2,4 GHz, sólo puede tener 8 nodos por celda y está diseñado para mantener sesiones de voz de forma continuada, aunque pueden construirse redes que cubran grandes superficies ya que cada ZigBee actúa de repetidor enviando la señal al siguiente, etc.

Se espera, que los módulos ZigBee sean los transmisores inalámbricos más baratos jamás producidos de forma masiva, con un costo estimado alrededor de los 2 dólares. Dispondrán de una antena integrada, control de frecuencia y una pequeña batería. ZigBee ofrece una solución tan económica porque la radio se puede fabricar con muchos menos circuitos analógicos de los que se necesitan habitualmente.

El nombre del protocolo es un poco rebuscado, pero la idea vino de una colmena de abejas pululando alrededor de su panal y comunicándose entre ellas, algo así como la comunicación que se produce con el zumbido de las abejas.

1.4.10 PROTOCOLO ALOHA

Aloha, también llamado el Método Aloha, hace referencia a un esquema de comunicaciones simple en el que cada fuente (transmisor) en una red, envía datos siempre que haya un marco que enviar. Si el marco llega exitosamente al destino (receptor), el siguiente marco es enviado. Si el frame no es recibido exitosamente, es enviado nuevamente. Este protocolo fue originalmente desarrollado en la Universidad de Hawaii para el uso con sistemas de comunicaciones satelitales en el Pacífico.

Aloha trabaja perfectamente en sistemas wireless tipo broadcast o en sistemas half-duplex de dos vías. Pero como las redes se han venido haciendo más complejas, por ejemplo en un sistema Ethernet involucrando múltiples fuentes y destinos en el cual los datos viajan en diferentes rutas a la vez, el problema ocurre porque los marco de datos hacen colisiones. Mientras más pesado sea el volumen de las comunicaciones, peor es el problema de las colisiones, dando como resultado la pérdida de los datos.

Para minimizar el número de colisiones, optimizar la eficiencia de la red e incrementar el número de subscriptores que pueden usar dicha red, se ha desarrollado un esquema llamado Aloha ranurado. Este sistema emplea señales llamadas *beacons* que son enviados en intervalos precisos y le dicen a cada fuente cuando esta libre el canal para enviar un marco de datos.

Aloha se basa en dos principios básicos:

1. Si un nodo tiene un paquete que enviar, solo debe enviarlo.
2. Si el paquete sufre una colisión, deberá intentar enviarlo de nuevo.

1.4.11 ORIGEN DE REDES AD HOC

La idea de tener una red con poca infraestructura fue propuesta en 1970. DARPA tenía un proyecto conocido como PACKET RADIO, donde varias terminales inalámbricas podían comunicarse unas con otras sobre un campo de batalla. Packet radio fue una tecnología que extendió el concepto de conmutación de paquetes al dominio de Broadcast Radio Networks. Durante 1970, el proyecto ALOHA de la Universidad de Hawai, demostró la viabilidad de usar la propiedad de transmisión para enviar y recibir paquetes de datos en sistemas de radio de un solo salto. ALOHA más tarde llevó al desarrollo de una red de paquetes de radio multi-salto y multi-acceso (PRNET) bajo el patrocinio de ARPA.

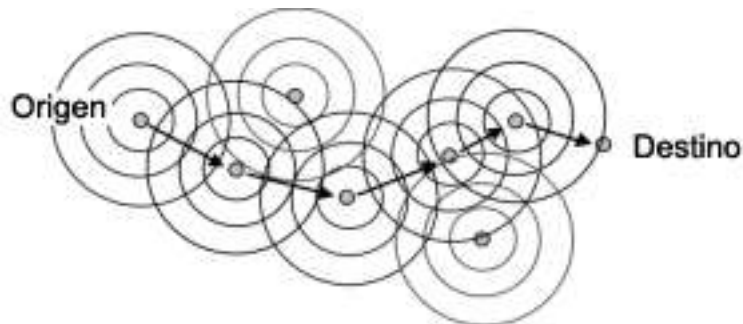


Fig. 8 Esquema representativo de una red AD HOC

Proyectos tales como ALOHA o PRNET permiten comunicaciones multi-salto a través de extensas áreas geográficas y varios fueron los pioneros que contribuyeron en el campo de la PRNET, tales como Robert Khan, Barry Leiner, Leonard Kleinrock y John Jubón.

Una de las cosas más atractivas de PRNET es su rápido despliegue. Una vez instalado, el sistema es auto-inicializable y auto-organizable. Esto implica que los nodos de la red son

capaces de descubrir conectividad entre nodos vecinos y organizar estrategias de ruteo basada en esta conectividad.

1.4.12 DESAFÍOS TÉCNICOS DE REDES AD HOC

PRNETs son muy diferentes en muchos aspectos respecto a redes cableadas. Estas tienen un backbone con menor infraestructura y cada nodo de la red actúa como un ruteador para enviar paquetes de un nodo a otro. Los ruteadores son conectados sin cables y estos pueden ser móviles.

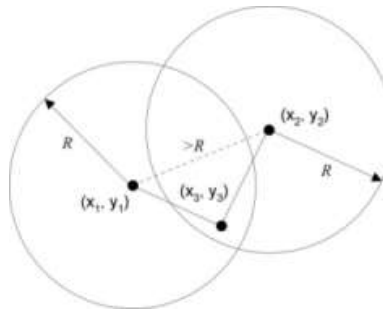


Fig. 9 Radio de alcance de un nodo

PRNET es la red que fue la responsable de unir las comunicaciones entre computadoras con las telecomunicaciones. Esto permitió que las redes fueran formadas y deformadas en cualquier momento de su uso, a través de innovadores y adaptivos protocolos de comunicación.

Los desafíos técnicos para PRNET pueden ser listados como:

- Control del flujo sobre comunicaciones inalámbricas multi-salto.
- Control de errores sobre enlaces inalámbricos.
- Mantenimiento de la información de la topología de red.
- Derivar el exacto ruteo de la información.
- Mecanismos para el manejo del ruteo móvil.
- Compartir canales de acceso para múltiples usuarios.

- Capacidad de procesamiento de las terminales.
- Tamaño y poder de requerimientos.

En este primer capítulo se habló sobre el origen de la computadora y los precursores en varias áreas de la computación tales como redes. Como vimos las primeras etapas informáticas fueron de gran importancia para el desarrollo computacional, creo que no nos podemos imaginar el presente informático si no hubiesen existido grandes genios como Pascal, Eckert, Mauchly y muchos más. Ellos marcaron la pauta para que nosotros podamos hoy usar los avances tecnológicos de los cuales gozamos.

Así mismo vimos como se fue desarrollando un área muy importante, el área de redes de computadoras, de nada serviría tener varias súper computadoras si no fueran capaces de comunicarse entre ellas para trabajar y tratar de dar algún resultado provechoso para la sociedad. Gracias a los grandes pioneros en esta área como el Departamento de Defensa de los Estados Unidos de Norteamérica que echó a andar el proyecto de ARPANET tenemos la posibilidad de disfrutar hoy en día servicios como el Internet, la gran red de moda. Sin embargo Internet no es la única red de gran utilidad, existen otros tipos LAN, WAN, AD HOC. Específicamente las redes Ad Hoc están teniendo gran impacto en la actualidad, y sus usos abarcan una gran cantidad de áreas.

Debido a la importancia de las redes Ad Hoc, en el siguiente capítulo se analizan los protocolos más importantes para estas redes, sus diferencias, eficiencias, historia y demás puntos importantes.

CAPITULO

II

P

ROTOCOLOS

La evolución de las redes de computadora ha sido de tal manera que hoy en día se puede contar con muchos servicios que facilitan gran cantidad de procesos tales como comunicación entre personas, monitoreo automático de campos de cultivos, seguridad privada en hogares entre muchos mas.

El funcionamiento de redes ad hoc se basa principalmente en aplicaciones distribuidas instaladas en cada nodo perteneciente a la red, en la cual se implementan diversos protocolos para cumplir con un objetivo en común.

Los protocolos se dividen en protocolos de acceso al medio y de enrutamiento. Estos protocolos tienen como fin hacer que las redes ad hoc sean eficientes, rápidas y ahorradoras de energía. En el desarrollo de redes ad hoc se debe considerar para su diseño tanto el propósito final de la red como elegir de forma óptima los protocolos a implementar.

necesariamente siguen el mismo tiempo. Un mecanismo de control mas distribuido es usado para coordinar el acceso al canal.

En la figura 10 se puede observar una representación básica del funcionamiento del protocolo MAC. Cuando el nodo A desea comunicarse con el nodo B, A envía un RTS (Request To Send) con el objetivo de indicarle a A que se desea comunicar con el. Todo esto ocurre si ambos nodos (A y B) están dentro de una misma región de alcance.

2.1.2 PROTOCOLO MACA (MULTIPLE ACCESS WITH COLLISION AVOIDANCE)

MACA fue originalmente propuesto por Phil Karn. Así mismo fue propuesto para resolver los problemas de la terminal oculta y el nodo expuesto.

MACA usa RTS-CTS-Data, como se puede ver en la figura 11. El nodo emisor primero envía un RTS al nodo receptor para reservar el canal. Esto bloquea a los nodos vecinos que pudieran actuar como emisores, evitando así que puedan transmitir datos. El nodo receptor entonces envía un CTS al emisor para indicarle que le permita la transmisión. Esto da como resultado que todos los nodos vecinos al emisor sean bloqueados evitando así colisiones. A partir de este momento, el emisor puede iniciar la transmisión de datos.

MACA tiene capacidades de ahorro de energía incorporadas. La principal característica de MACA es que inhibe a un transmisor cuando un paquete CTS es escuchado. Esto permite una reutilización de canales.

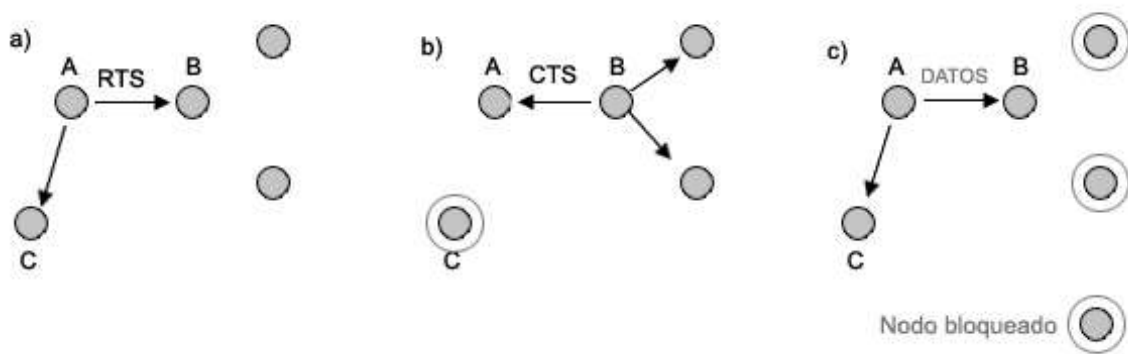


Fig. 11 Ejemplo de protocolo MACA

Pueden ocurrir colisiones en MACA, especialmente durante la fase RTS-CTS. Cada host móvil agrega una cantidad de tiempo aleatorio para el intervalo requerido de esperar después de que se ha escuchado un mensaje RTS o CTS. Por ejemplo si dos o más estaciones transmiten un RTS (Request to Send) concurrentemente, el resultado es una colisión, por lo tanto estas estaciones deberán esperar un intervalo aleatorio e intentar de nuevo. La estación que gana la competencia es la que recibirá un CTS (Clear to Send) de su responder, bloqueando así a otras estaciones garantizando la comunicación.

2.1.3 PROTOCOLO MACA-BI (MULTIPLE ACCESS WITH COLLISION AVOIDANCE BY INVITATION)

En protocolos tipo sender-initiated, el nodo emisor necesita cambiar a nodo receptor para obtener el CTS inmediatamente después de transmitir el RTS. Cada intercambio en el control de paquetes agrega un tiempo de vuelta, reduciendo el procesamiento total. MACA-BI es un protocolo del tipo receiver-initiated y reduce el número de intercambios de paquetes de control, se puede ver un ejemplo de su funcionamiento en la figura 12. En lugar de que el emisor espere para ganar el acceso al canal, MACA-BI requiere que el receptor le solicite al emisor que le envíe los datos, usando un paquete RTR (Ready To Receive) en lugar de los paquetes RTS y

CTS. Por lo tanto MACA-BI es un intercambio de dos vías (RTR-DATA) en contraste con el intercambio de tres vías (RTS-CTS-DATA) del protocolo MACA.

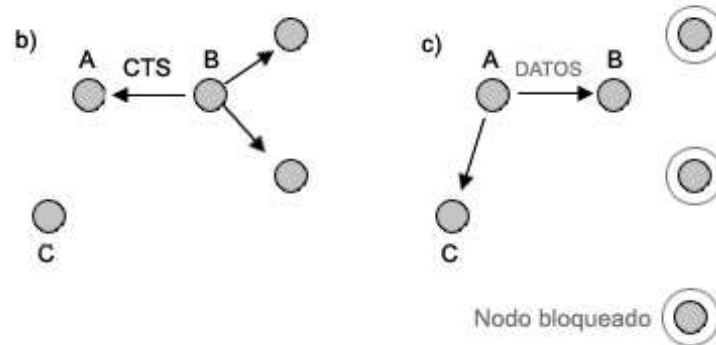


Fig. 12 Ejemplo protocolo MACA-BI

Debido a que el transmisor no puede enviar ningún dato antes de ser pedido por el receptor, tiene que haber un algoritmo para la predicción del tráfico implementado dentro del receptor, con el cual pueda saber cuando solicitar datos al emisor. La eficiencia de este algoritmo determina el rendimiento de procesamiento de la comunicación del sistema. El algoritmo propuesto lleva la información referente al paquete como longitud y llegada de los datos del emisor. Cuando el nodo receptor recibe estos datos, ya es capaz de predecir la ruta origen del emisor, para inmediatamente después de recibido enviar en consecuencia un paquete RTR. El nodo emisor cuenta con la capacidad para transmitir un paquete RTS, en el caso de que su buffer de entrada sufra de un desbordamiento. En tal caso, el sistema se auto-configura a MACA.

2.1.4 PROTOCOLO PAMAS (POWER AWARE MULTI-ACCESS PROTOCOL WITH SIGNALING)

El protocolo PAMAS es una combinación del protocolo MACA original y la idea de usar canales diferentes para datos y control. Con esto podemos asumir que los mensajes de control RTS-CTS son enviados por un canal independiente y separado al canal por donde se envían los

datos. La separación de canales permite a los nodos determinar cuando y por cuanto pueden apagarse por si mismos. En la figura 13 se muestra el diagrama de bloques de cómo funciona el protocolo PAMAS.

Un nodo trabajando bajo el protocolo PAMAS, puede estar en uno de seis estados: Idle, Await CTS, BEB (Binary Exponential Backoff), Await Packet, Receive Packet y Transmit Packet.

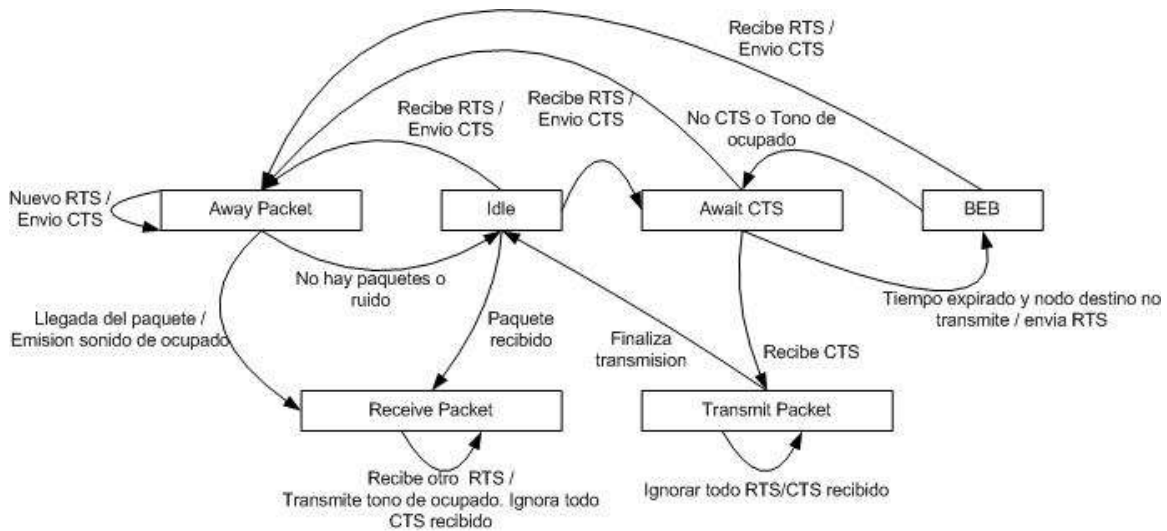


Fig. 13 Estados del protocolo PAMAS

Cuando un nodo no está transmitiendo o recibiendo un paquete, o no tiene ningún paquete para transmitir, o tiene paquetes que transmitir pero no lo puede hacer (debido a que los nodos vecinos están recibiendo una transmisión de datos) se encuentra en estado Idle. Cuando el nodo tiene un paquete para transmitir, envía un RTS y entra en estado de Await CTS. Si el mensaje CTS no le llega, entonces entrará en estado de BEB. En cambio, si llega un CTS, el nodo inicia a transmitir y entra en el estado de Transmit Packet. El nodo que transmite un paquete CTS entra en el estado Await Packet. Si se da el caso en que el paquete no llega en un tiempo de procesamiento, entonces el nodo entra en estado Idle. Si el paquete llega, se transmite por el canal de control un tono de ocupado, entrando así en estado Receive Packet.

Si un nodo en estado Idle recibe un RTS, responde con un CTS si el nodo vecino no está en estado Transmit Packet o Await CTS. Es fácil para el nodo determinar si cualquier nodo vecino está en el estado de Transmit Packet, solo es necesario que haga un censado al canal de datos. Sin embargo, no siempre es posible saber para un nodo cuando un nodo vecino esta en el estado Await CTS, porque pudo haber ocurrido una colisión del RTS con cualquier otra transmisión en el canal de control.

Si un nodo que está en estado Idle tiene que transmitir un paquete, envía un RTS y entra en estado Await CTS. Pero si el nodo vecino está recibiendo un paquete, ese nodo responde con un tono de ocupado que puede hacer colisión con la recepción del paquete CTA. Esto obliga al nodo emisor a entrar en estado BEB y no transmite el paquete. En caso contrario, la transmisión se efectúa normalmente y cambia a estado Transmit Packet.

PAMAS es un protocolo en el cual uno de sus objetivos principales es el ahorro de energía en los dispositivos en el cual es implementado. Los nodos consumen energía mientras transmiten o mientras están recibiendo datos. Desafortunadamente, en redes ad hoc se da frecuentemente el caso en que todos los nodos adyacentes a un nodo que está actuando en la fase de emisor escuchen dicha transmisión. En consecuencia todos estos nodos consumen energía de forma innecesaria.

Por lo tanto, para conservar energía y en consecuencia ampliar la vida del nodo, PAMAS requiere que los nodos se apaguen por si solos cuando se encuentren en una situación donde solo estén escuchando transmisiones.

Existen dos condiciones bajo las cuales es conveniente para un nodo apagarse por sí mismo:

1. Si un nodo no está recibiendo una transmisión de datos directamente, esto ocurre cuando dicho nodo solo esta escuchando una transmisión que no va dirigida a él.

2. Si no puede transmitir un paquete, debido a que el nodo que actuará como receptor está recibiendo datos de otro nodo.

Cada nodo de forma independiente toma la decisión de apagarse. Él sabe si su nodo vecino está transmitiendo porque puede oír la transmisión en el canal de datos. Igualmente, un nodo sabe si uno o más de sus vecinos está recibiendo datos, ya que el nodo receptor emite por el canal de control el tono de ocupado. Por todo lo anterior cada nodo fácilmente puede decidir cuando apagarse. Sin embargo, existen algunas cuestiones que se deben considerar:

¿Por cuánto tiempo un nodo debe permanecer apagado? Si el nodo solamente apaga la interfase de datos, pero siempre mantiene la interfase de los canales encendida, esto siempre permite al nodo conocer la longitud de la nueva transmisión y mantener la interfaz de datos apagada.

2.2.- PROTOCOLOS DE RUTEO

Los protocolos de enrutamiento son necesarios para que los paquetes de datos puedan llegar a su destino. Estos protocolos tienen dos funciones principales:

1. Selección de rutas para los paquetes.
2. Entrega correcta de paquetes a sus destinos.

Dependiendo de sus propiedades, los protocolos de ruteo pueden clasificarse en las siguientes categorías:

1. Centralizados / distribuidos.
2. Estáticos / adaptivos.
3. Reactivos / proactivos.

En protocolos centralizados todos los cálculos para el ruteo son hechos por un nodo central, mientras que en algoritmos distribuidos, el cálculo de las rutas es hecho por varios nodos de la red.

En los protocolos estáticos la ruta usada por un paquete es fija, sin importar las condiciones de tráfico en un momento determinado. Esta ruta fija, puede cambiar en caso de que un nodo ya no esté en su posición original o si la comunicación entre el nodo emisor y el nodo receptor falla. Mientras que en protocolos estáticos la ruta es fija, los adaptivos usan rutas que pueden cambiar dependiendo de la congestión de la red.

En protocolos proactivos continuamente se están evaluando rutas dentro de la red, así cuando un paquete debe ser enviado, se conoce de antemano la ruta exacta que debe seguir dicho paquete. En el caso de protocolos reactivos, se invoca un procedimiento para determinar una ruta, todo esto solo bajo demanda.

2.2.1.- DYNAMIC SOURCE ROUTING (DSR)

Este protocolo pertenece a la clase de protocolos reactivos, su implementación permite a los nodos descubrir rutas de forma dinámica a través de la red para que los paquetes lleguen a su destino correctamente. El nombre de este protocolo significa que cada paquete lleva en su cabecera una lista completa y ordenada de los nodos por los cuales debe pasar. Así mismo DSR utiliza ruteo de mensajes no periódico, reduciendo así el uso de ancho de banda y conservando energía.

DSR tiene dos modos básicos de operación: **DESCUBRIMIENTO DE RUTA** y **MANTENIMIENTO DE RUTA**.

DESCUBRIMIENTO DE RUTA

Cuando un nodo desea enviar datos a otro, primero verifica si tiene alguna entrada en su caché de rutas para dicho destino. Si tiene alguna entrada activa, envía los datos por medio del vecino que le indica la tabla.

Sin embargo, si el origen no dispone de una entrada activa, ya sea porque es la primera vez que se va a comunicar con él, o porque el plazo para esa destino ha expirado (al comprobar el campo *tiempo de vida* y la fecha de última modificación), se inicia un descubrimiento de ruta. Para ello se debe crear un paquete RREQ que contiene información relativa al nodo destino e información propia. Cada paquete RREQ es identificado unívocamente con un identificador propio, unido al originador del mensaje.

Este identificador se incrementa cada vez que se genera un nuevo RREQ y lo utilizan los nodos intermedios, para saber si deben retransmitir el paquete o, por el contrario, descartarlo porque ya lo retransmitieron con anterioridad. Dichos nodos, aún no siendo los destinatarios del RREQ, si mantienen una entrada para ese destino en su tabla de encaminamiento, contestarían al origen para evitar la propagación innecesaria de RREQ a través de la red. Incluso teniendo alguna entrada activa, es necesario que se cumpla que dicha ruta es más moderna que la última ruta recibida por el originador del RREQ. Aquí es donde entran en juego los números de secuencia. Cuando un nodo reenvía un RREQ, añade una ruta inversa en su tabla, que apunta al origen del RREQ (supone enlaces simétricos). Si este paquete llega al destinatario, éste devolverá un RREP al origen, a través del camino inverso por el que le llegó la petición.

MANTENIMIENTO DE RUTA

Este es un mecanismo que detecta si la topología de la red ha cambiado, si ha sucedido el cambio, entonces ya no se podrán utilizar las rutas que actualmente se tenían. Si una red ha

cambiado es debido a que un host listado en el ruteo fuente se ha movido del rango de transmisión o esta apagado haciendo que la ruta no se pueda utilizar. Cuando se detecta un problema con la ruta en uso, se envía un paquete de error hacia el nodo fuente. Una vez que el nodo fuente recibe este paquete, el salto en donde ocurrió el error es removido del caché de ruteo, y todas las rutas que tenían este salto son truncadas en ese punto.

2.2.2.- ZONE ROUTING PROTOCOL (ZRP)

El protocolo ZRP (Zone Routing Protocol) es una combinación de protocolos reactivos y proactivos, convirtiéndolo así en un híbrido. ZRP divide la red en diferentes zonas, en las cuales se definen dos protocolos que trabajan dentro y entre cada una de dichas zonas de enrutamiento.

El primero de los protocolos es IARP (Intrazone Routing Protocol), este opera dentro de la zona de enrutamiento y su función principal es la de aprender las distancias y rutas de todos los nodos dentro de la zona. El protocolo no está definido y puede incluir cualquier número de los protocolos proactivos, como el Distance Vector o Link-state Routing. Se puede ser flexible y en consecuencia, diferentes zonas pueden estar operando con diferentes protocolos intrazonas. Cuando ocurre un cambio en la topología de la red, inmediatamente se debe actualizar la información de los nodos y solo se propaga dentro de la zona afectada.

El segundo protocolo es el IERP (Interzone Routing Protocol), es de tipo reactivo y es utilizado para encontrar rutas entre las diferentes zonas. IERP es muy útil, sobre todo cuando un nodo destino no se encuentra dentro de la zona de ruteo. Es entonces cuando IERP envía un RREQ (Route Request) en forma de broadcast a todos los nodos fronterizos dentro de la zona, los cuales envían la solicitud si el nodo buscado no es encontrado dentro de esta zona. Dicho procedimiento se repite hasta que el nodo buscado es encontrado, es entonces cuando la ruta es enviada al nodo fuente. Cabe mencionar que IERP utiliza BRP (Border Resolution Protocol) que

esta incluido en ZRP, y que proporciona servicios de bordercasting. El bordercasting es el proceso de enviar data-gramas IP desde un nodo fuente a todos los nodos periféricos.

ZRP es un protocolo muy interesante ya que puede ajustar su operación a ciertas condiciones operativas de la red, como puede ser un cambio en el diámetro de la zona de enrutamiento. Esto no lo hace un protocolo dinámico, si no que por el contrario, se sugiere que este radio sea fijado por el administrador de la red o que venga por defecto por el fabricante. El funcionamiento óptimo de este protocolo depende en gran medida de esta decisión. En la figura 14 se muestra una red que utiliza ZRP con sus respectivas zonas.

Puesto que ZRP es un híbrido entre esquemas proactivos y reactivos, utiliza características de ambos. Las rutas pueden se encontradas mas rápidamente dentro de una zona, mientras que las rutas fuera de la zona son encontradas haciendo búsquedas en determinados nodos seleccionados eficazmente en la red.

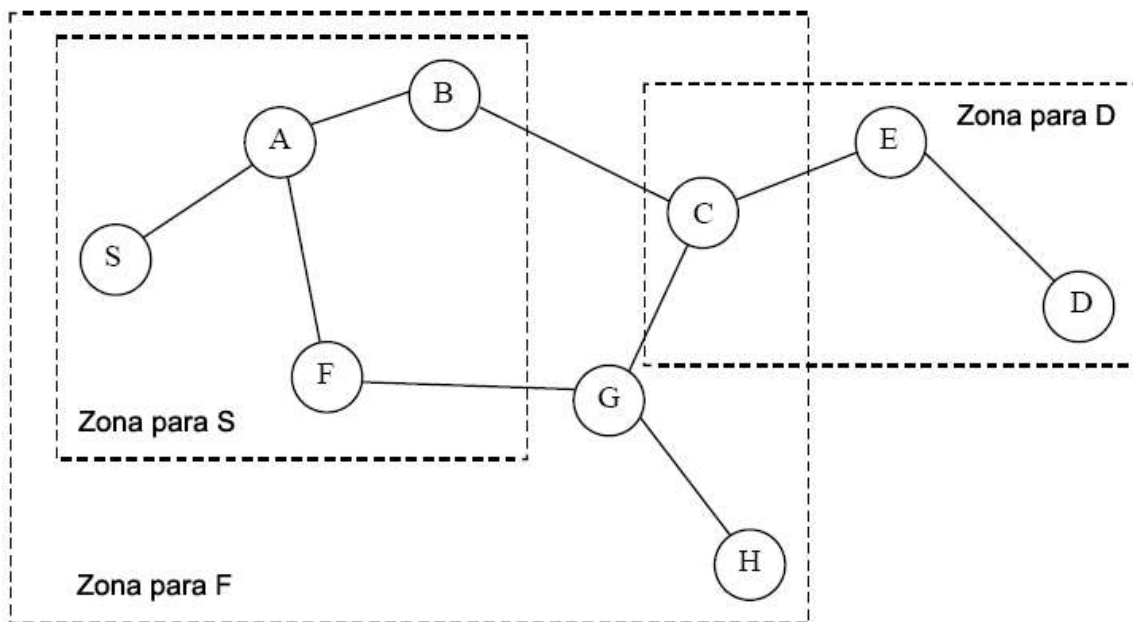


Fig. 14 Red usando el protocolo ZRP

Como se mencionó, en ZRP el protocolo de enrutamiento que actúa dentro de una zona no está definido, y esto es un problema, ya que se puede usar cualquier protocolo, por lo tanto se debe considerar

que los nodos deben tener la capacidad de soportar diferentes protocolos de ruteo. Esto es una desventaja, ya que sería mejor que todas las zonas fueran controladas por un solo protocolo, cuyo objetivo sería hacer un poco más estándar a la red entera.

2.2.3.- TEMPORALLY ORDERED ROUTING ALGORITHM (TORA)

TORA es un protocolo de enrutamiento distribuido, y está diseñado para minimizar la reacción ante cambios topológicos de la red. Se puede decir que la idea principal de este protocolo es el control de mensajes en pequeños grupos de nodos.

Esto garantiza que todas las rutas están libres de ciclos, y así mismo provee múltiples rutas para un mismo par de nodos fuente/destino. TORA se puede dividir en tres funciones básicas: creación de rutas, mantenimiento de rutas y borrado de rutas. La creación de rutas consiste básicamente en la asignación de direcciones a los enlaces en una red unidireccional o ciertas porciones de la misma, construyendo un grafo acíclico dirigido (DAG) como se muestra en la figura 15.

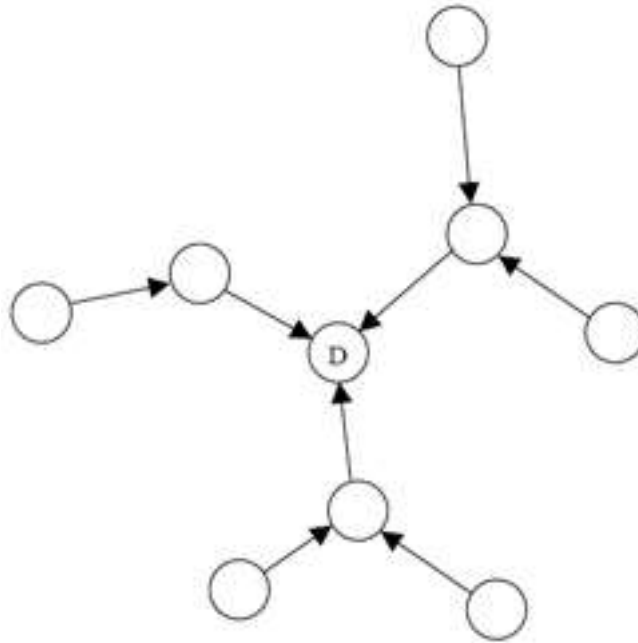


Fig. 15 Grafo acíclico dirigido (DAG)

TORA asocia cada nodo con un peso. Todos los mensajes en la red fluyen del nodo con mayor peso hacia el de menor peso. Aquí las rutas son encontradas usando paquetes del tipo QRY (Query) y UPD (Update). Cuando un nodo necesita una ruta hacia un destino, envía un paquete QRY en un broadcast. Este QRY se propagará a través de la red hasta que encuentre a un nodo que contenga una ruta o hasta que el nodo sea el destino al que debe llegar el paquete. Entonces el nodo ahora hará un broadcast de un paquete UPD que contendrá el peso del nodo.

Cada nodo que reciba este paquete UPD modificará su propio peso a un peso mayor que el especificado en el mensaje UPD. Ahora el nodo enviará su propio paquete UPD en forma de broadcast. Esto dará como resultado múltiples rutas entre nodo original y nodo final.

2.2.4.- AD HOC ON DEMAND DISTANCE VECTOR (AODV)

AODV fue creado por Charles E. Perkins como evolución de su anterior protocolo (DSDV). Mantuvo la idea de mantener números de secuencia y tablas de encaminamiento pero añadió el concepto de encaminamiento bajo demanda, es decir, solo se guarda información de

los nodos que intervengan en la transmisión de datos. La optimización primordial que se consiguió en relación a su anterior diseño fue el decremento del tiempo de proceso, disminución del gasto de memoria y reducción del tráfico de control por la red. Además AODV es muy cuidadoso con las rutas, manteniéndolas en caché mientras son necesarias e inhabilitándolas cuando su información no es útil.

El AODV mantiene tablas de enrutamiento en todos los nodos lo cual implica una mejora y por tanto los paquetes de datos no tienen que contener la totalidad de la ruta en sus encabezados. Las rutas son mantenidas solo entre nodos que necesitan comunicarse, por lo tanto usa tablas de ruteo tradicionales, una entrada por destino.

Dichas tablas son actualizadas cuando un nodo realiza una redifusión de un RREQ, al recibir dicho paquete actualizan la información con respecto al nodo de origen y establecen punteros que apunta hacia el nodo origen en su tabla de enrutamiento. A medida que avanza el RREQ, se va creando una ruta de retorno hacia el origen. Cuando el nodo destino recibe el RREQ, él contesta devolviendo un RREP, el cual es enviado hacia el nodo origen a través de la ruta de retorno que se creó durante el avance del RREQ.

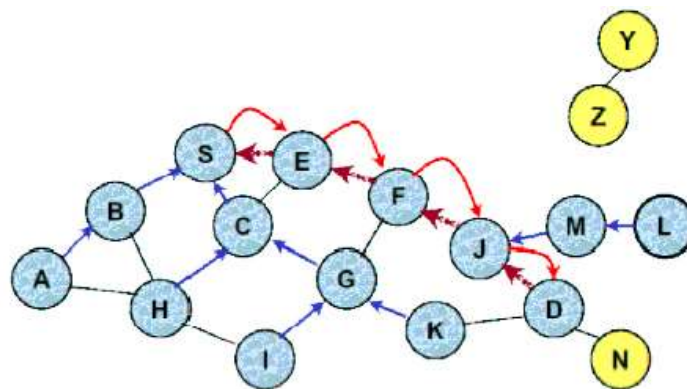


Fig. 16 Funcionamiento de AODV

Los enlaces hacia delante son fijados cuando el RREP viaja a través de la ruta de retorno. Una vez que el nodo de origen recibe un RREP, este puede comenzar a enviar paquetes de datos hacia el destino. A su vez, un nodo intermedio puede mandar un paquete RREP si este conoce un camino más reciente que el que conoce el origen. Los nodos intermedios que reenvían el RREP también guardan en su tabla punteros hacia el destino.

La entrada en la tabla de enrutamiento que mantiene el camino de regreso es borrada luego de un intervalo de tiempo. De la misma manera, la entrada en la tabla de enrutamiento que mantiene el camino directo es borrada si no se usa dentro de un tiempo determinado.

El AODV utiliza números de secuencia los cuales son mantenidos en cada destino para mantener la información de ruteo actualizada y prevenir ciclos de ruteo. Todos los RREQ llevan estos números de secuencia. Cuando la fuente recibe un RREP que contiene un número de secuencia mayor o igual pero con una cantidad de saltos menor, él puede actualizar la tabla de ruteo para ese destino y empezar a usar esta nueva ruta. En la figura 16 se puede ver representado el funcionamiento de AODV

2.2.5.- OPTIMIZED LINK STATE ROUTING PROTOCOL (OLSR)

OLSR es un protocolo de ruteo proactivo. Cada nodo envía periódicamente mensajes en broadcast con información a nodos específicos en la red, con el objetivo de intercambiar información sobre los nodos vecinos. Dicha información incluye la IP de los nodos, número de secuencia y una lista con información de distancias de los nodos. Una vez que se recibe esa información, cada nodo construye su propia tabla de ruteo. A partir de este momento el nodo puede calcular con el algoritmo de la ruta más corta la ruta a cualquier nodo con el que desee comunicarse.

Cuando un nodo recibe un paquete de información con el mismo número de secuencia dos veces, entonces lo desecha. En las tablas de enrutamiento, cada nodo almacena la ruta de cada nodo en la red, pero esa información solo es actualizada en los siguientes casos:

1. Cuando se detecta un cambio en los nodos vecinos.
2. Cuando una ruta hacia un nodo destino ha expirado.
3. Cuando una ruta mejorada es detectada.

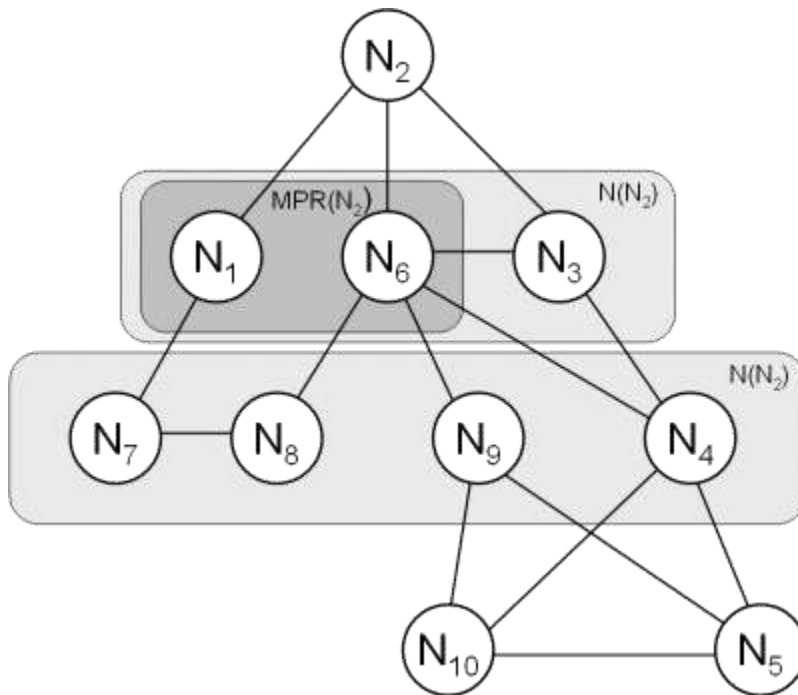


Fig. 17 Funcionamiento de OLSR

OLSR trabaja con multi-point relays (MPR) como se muestra en la figura 17. MPR es un nodo el cual es seleccionado directamente por un nodo vecino que se encuentra a un salto de distancia. La idea principal de los MPR es minimizar la inundación de la red con mensajes en broadcast. Entonces un paquete de información no debe ser enviado dos veces en la misma región de la red. MPR ayuda a optimizar y reducir ese problema.

2.2.6.- LOCATION AIDED ROUTING (LAR)

LAR es un protocolo sobre demanda, el cual esta basado en el DSR (Dynamic Source Routing). LAR utiliza información de localización la cual normalmente obtiene a través de GPS (Global Positioning System), todo esto con el objetivo de reducir la carga de enrutamiento en la red. Con la disponibilidad del GPS, las terminales móviles tienen la capacidad de conocer su localización física.

Para reducir la complejidad del LAR, asumimos que cada nodo conoce exactamente su posición, la diferencia entre la posición exacta y la posición calculada del GPS no son consideradas ya que todos los nodos se mueven solo en 2 dimensiones.

ZONA ESPERADA

Primero, consideremos que el nodo S (origen) necesita encontrar un camino hacia el nodo D (destino). El nodo S sabe que D estaba en la posición L, la "zona esperada" del nodo D, desde el punto de vista del nodo S, es la región donde el nodo S espera que este el nodo D. Cuando el nodo S sabe que el nodo D viaja con una determinada velocidad, esta velocidad es considerada por S para determinar la zona esperada de D como se muestra en la figura 18.

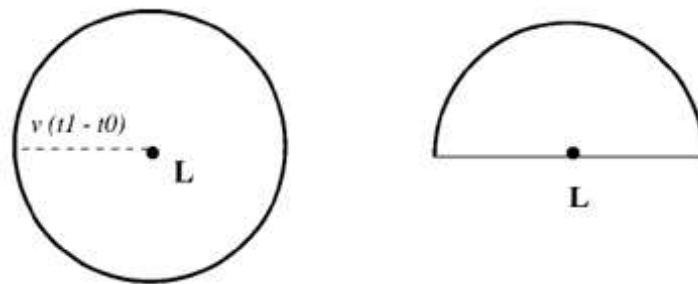


Fig. 18 Zona esperada (Expected Zone)

Cuando el nodo S no tiene información acerca de la posición de D, la región entera de la red es asumida como la zona esperada. Es aquí que el LAR se reduce al algoritmo de inundación básico. En general podemos decir, que mientras más conoce S acerca de D, es más pequeña la zona esperada.

REQUEST ZONE

Consideremos que un nodo S necesita encontrar una ruta hacia el nodo D. S define una zona de petición después que S envía una petición de ruta como en el algoritmo de inundación normal. Con la diferencia de que el nodo solo envía esta petición cuando esta en la zona de petición, este proceso se representa en la figura 19.

Existen dos razones diferentes, en las que regiones fuera de la zona esperada tienen que ser incluidas:

Cuando el nodo S no está en la zona esperada de D, entonces esta zona esperada tiene que ser expandida hasta la zona de petición.

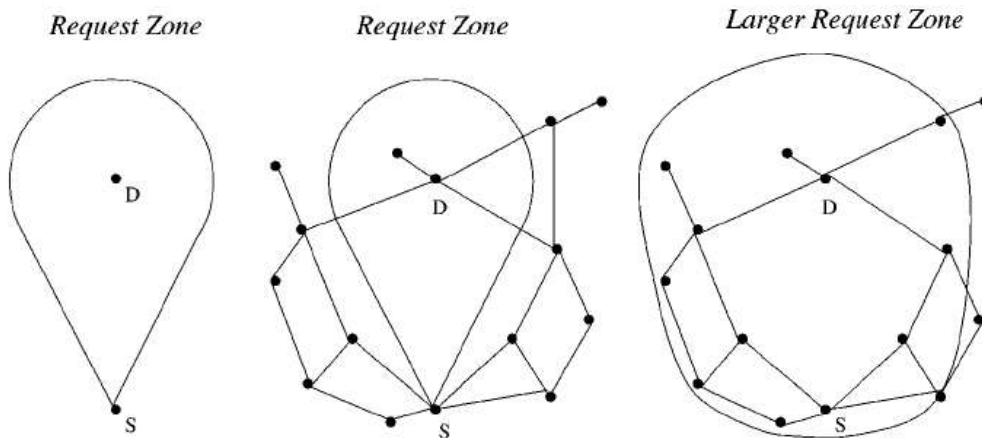


Fig. 19 Zona de petición (Request Zone)

Ahora nos debemos preguntar si esta zona de petición es una excelente zona. Considerando que todos los nodos entre S y D están fuera de la zona de petición, esto no nos garantiza que se podrá encontrar una ruta entre S y D. LAR permite expandir la zona de petición, todo esto para facilitar el proceso de encontrar una ruta. Pero tenemos que considerar, que cuando se incrementa la zona esperada, el tiempo para encontrar una ruta se incrementará.

DETERMINANDO SI UN NODO ES MIEMBRO DE LA ZONA DE REPETICIÓN.

LAR es esencialmente idéntico a los algoritmos de inundación, con la diferencia que un nodo que no se encuentra dentro de la zona de petición no reenvía la petición a sus vecinos de encontrar una ruta. Existen dos diferentes posibilidades para determinar si un nodo es miembro de la zona de petición.

Esquema LAR 1

Este primer esquema (figura 20) utiliza una petición que sea rectangular. El nodo S incluye las coordenadas de las cuatro esquinas de la zona de petición en su mensaje de petición. S sabe sus propias coordenadas, las cuales son proporcionadas por su propio GPS. Las coordenadas de la esquina opuesta son las de la esquina de la zona esperada. Con estos dos puntos, S ahora puede calcular un rectángulo y tendrá las cuatro esquinas de dicha zona rectangular.

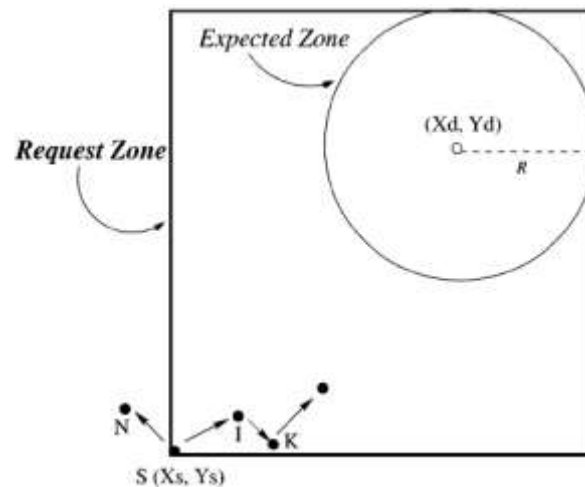


Fig. 20 Esquema LAR 1

Esquema LAR 2

En este esquema (figura 21), el nodo S, que debe encontrar una ruta hacia D, sabe la posición de D (X_d, Y_d). Con estas coordenadas, S calcula la distancia hacia D. Ambos, tanto las coordenadas y la distancia son incluidas en la petición de ruta. Ahora, cuando un nodo recibe la petición de ruta de S, calcula las distancias entre él mismo y D. Cuando esta distancia es demasiado grande en comparación con la distancia de S respecto a D, es descartada la petición de ruta. De otra manera, este nuevo nodo envía una petición de ruta a sus vecinos, incluyendo tanto distancia y coordenadas respecto a D.

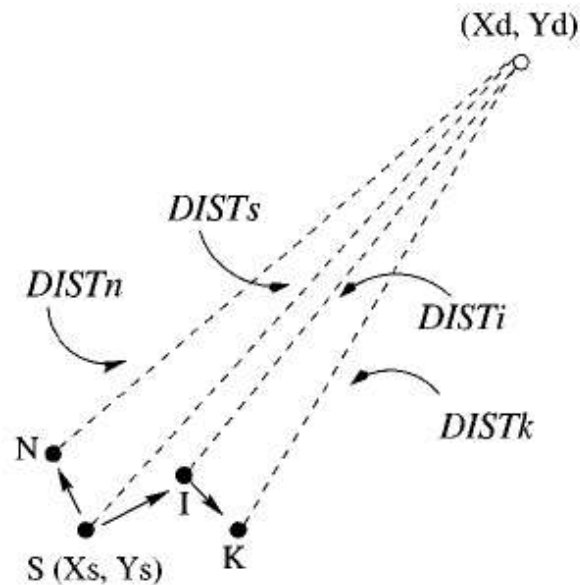


Fig. 21 Esquema LAR 2

2.2.7. - POWER AWARE ROUTING (PAR)

Los dispositivos móviles pueden tomar diferentes formas y algunas pueden demandar grandes cantidades de energía que otras. En PAR, la vida de la batería es tomada como una métrica de ruteo. De tal manera que PAR está enfocado para:

1.- Minimizar la energía consumida por paquete.

Esta es una de las métricas mas obvias que refleja nuestra intuición para conservar energía. Si asumimos que algún paquete j atraviesa los nodos n_1, \dots, n_k donde n_1 es el nodo fuente y n_k es el destino y así mismo denotamos $T(a,b)$ como la energía consumida en la transmisión y recepción de un paquete sobre un salto de a hacia b . Entonces podemos decir que la energía consumida por el paquete j es:

$$e_j = \sum_{i=1}^{k-1} T(n_i, n_{i+1})$$

El objetivo final es minimizar e_j .

2.- Maximizar el tiempo antes que la red sea particionada.

Esta métrica es muy importante en aplicaciones críticas como puede ser en redes sobre campos de batalla. Desafortunadamente, optimizar esta métrica es muy difícil si necesitamos simultáneamente mantener un retardo bajo y alto desempeño.

3.- Minimizar la variación en niveles de energía del nodo.

La idea detrás de esta métrica es que todos los nodos en la red tienen la misma importancia, por lo tanto ningún nodo deberá ser penalizado más que cualquier otro nodo. Esto asegura que todos los nodos en la red se mantengan activos y corriendo juntos por el mayor tiempo que sea posible.

4.- Minimizar el costo por paquete.

Si nuestro objetivo es maximizar la vida de todos los nodos en la red, entonces se tendrán que utilizar otras métricas de consumo de energía. Las rutas seleccionadas cuando se

usan estas métricas deben ser tal que los nodos con las reservas de energía agotadas no se usen para generar varias rutas.

5.- Minimizar el máximo costo por nodo.

La idea de esta métrica es minimizar el máximo costo del nodo después de rutear N paquetes a sus destinos y después de T segundos. Todas estas variaciones aseguran que ese nodo se tarde en fallar y como efecto la variación de energía en el nodo se reduce.

Por lo tanto podemos concluir que PAR selecciona rutas que permitan una larga vida de la batería en los dispositivos en el cual sea implementado.

2.2.8. - SOURCE TREE ADAPTIVE ROUTING (STAR)

El protocolo STAR fue el primer protocolo de enrutamiento proactivo que trabaja con información link-state y fue el más rápido de los protocolos denominados *bajo demanda*. STAR no toma rutas cortas para mantener el control de mensajes bajo. STAR identifica cada nodo con una dirección fija. Esto es una gran ventaja ya que no se requieren actualizaciones periódicas. En la figura 22 se muestra una red utilizando el protocolo STAR.

Después de iniciar el procedimiento, un árbol de fuentes contiene enlaces a cada nodo vecino. El siguiente paso es hacer la primera actualización, STAR envía su propio árbol inmediatamente como actualización a sus nodos vecinos. Así cada ruteador puede construir con su propio árbol y los recibidos un grafo topológico conteniendo la red completa.

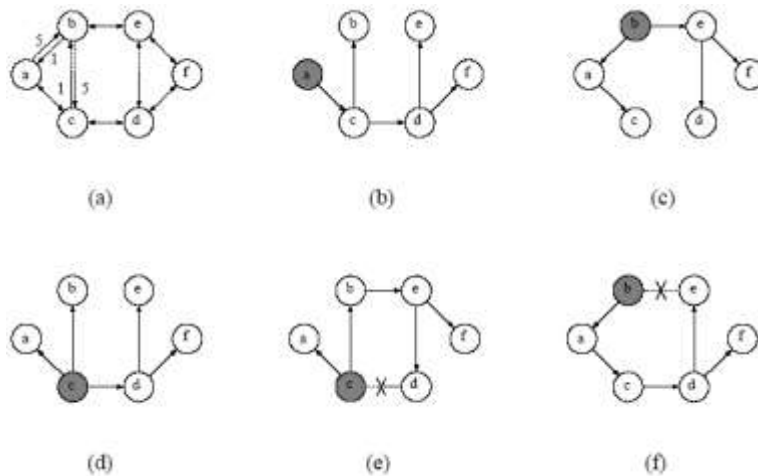


Fig. 22 Ejemplo de funcionamiento de STAR

Todas las actualizaciones de información son de tipo broadcast. En STAR se implementa LORA y las actualizaciones son enviadas cuando:

- El receptor no es alcanzable.
- Un nuevo receptor es detectado.
- Cuando los ciclos son construidos.
- La métrica de enlaces excede el límite de todos estos casos descubiertos.

STAR usa secuencia de números para validar actualizaciones. Las reglas para validar dichas actualizaciones son:

- a) Cuando una ruta esta al final de un ciclo.
- b) Cuando un nuevo sucesor de un enrutador tiene una dirección mayor al actual.
- c) Cuando la distancia al receptor sobre el sucesor elegido es más grande que el anterior.

Estas reglas son necesarias para prevenir ciclos.

2.2.9.- A SECURE ON DEMAND ROUTING PROTOCOL FOR AD HOC NETWORK (ARIADNE)

ARIADNE es un protocolo seguro de enrutamiento bajo demanda basado en DSR. ARIADNE asume la existencia de una llave secreta compartida entre dos nodos, y usa un MAC (Message authentication code) para autenticar mensajes punto a punto entre esos nodos.

Adicionalmente, ARIADNE emplea protocolo de autenticación TESLA para autenticar mensajes en modo broadcast, como por ejemplo las peticiones de ruta. En TESLA un emisor genera una llave unidireccional y define un calendario según la cuales se divulgarán las llaves de la cadena en orden inverso a la generación. Sin embargo, la sincronización a un tiempo es un requerimiento absoluto en la red para usar ARIADNE.

Cuando un nodo transmite una petición de ruta incluye su propia dirección, la dirección del nodo destino, un número que identifica la actual ruta de descubrimiento, un intervalo de tiempo TESLA que denota el tiempo de llegada esperado de la petición al nodo destino, un hash consistente de sus direcciones, la dirección destino, el ID, el tiempo de intervalo, y dos listas vacías, llamadas lista de nodo y lista MAC.

Un nodo vecino que recibe una petición de ruta verifica la validez del tiempo de intervalo del TESLA. Un tiempo de intervalo válido es uno que no está muy lejos en el futuro y su llave correspondiente aún no se ha divulgado. Un paquete con un intervalo inválido es descartado. De otra manera, el nodo actual inserta su dirección en la lista nodo, reemplazando el hash con uno nuevo, el cual consiste en la dirección actual más la dirección anterior, y agregando un MAC del paquete entero a la lista MAC. El MAC es calculado usando la llave TESLA que corresponda con el intervalo de tiempo de la petición. Es entonces cuando el nodo vecino hace un broadcast a la petición de ruta sobre sus propios vecinos.

El nodo destino verifica la validez de la petición de ruta una vez que la recibe. Una petición de ruta es considerada válida si las llaves del intervalo de tiempo especificado aún no han sido divulgadas, y si el hash incluido puede ser verificado. El nodo destino genera y envía en modo broadcast un paquete de respuesta replica de enrutamiento por cada petición de enrutamiento válida que recibe.

Una respuesta de ruta contiene los mismos campos que su correspondiente petición de ruta, y adicionalmente contiene un campo MAC objetivo y una lista vacía llama key list. El campo MAC objetivo es fijado al MAC calculado de los campos anteriores a la contestación de la ruta y de la llave que el destino comparte con el nodo iniciador. La contestación es enviada hacia el nodo inicial siguiendo la ruta inversa incluida en la lista nodo, como se especifica en el protocolo DSR. Un nodo intermedio que recibe la contestación, espera el intervalo de tiempo especificado, que permite divulgar la llave, la cual esta en la lista de llave y envía el mensaje al siguiente nodo. Una vez que se recibe una contestación de ruta, el nodo iniciador verifica la validez de cada llave contenida en la lista de llaves, de las MAC objetivo y de cada MAC contenido en la lista de MAC.

El protocolo ARIADNE especifica un mecanismo para un mantenimiento seguro de rutas, el cual se asegura de la validez de los mensajes de error concernientes a enlaces rotos en la red. Un nodo que genera un error de ruta incluye detalles en el mensaje de autenticación TESLA. Por lo tanto, cada nodo que remite el error de ruta hacia el nodo destino puede autenticarlo.

Los nodos intermedios almacenan el mensaje de error de ruta y su autenticación no ocurre hasta que el nodo que lo generó divulga la llave.

En este segundo capítulo analizamos los protocolos más importantes de las redes ad hoc. Estos a su vez están divididos en protocolos de acceso al medio y protocolos de ruteo. Los de acceso al medio son los encargados de manejar, coordinar y sincronizar todos los nodos de la red.

En cambio los protocolos de enrutamiento son los que se encargan como su nombre lo indica de encontrar rutas eficientes entre los distintos nodos, podemos decir que estos protocolos son los que definen en mayor parte la eficiencia de la red ad hoc.

Varios de estos protocolos son destinados de acuerdo a la aplicación que se vaya a implementar, puede ser que en un caso práctico se requiera el ahorro de energía en los nodos con el objetivo de extender la vida útil del dispositivo. Aunque en general, podemos afirmar que los objetivos de estos protocolos deben ser eficiencia, rapidez y ahorro de energía.

Al terminar este capítulo ya hemos analizado tanto historia como protocolos de redes ad hoc, en el tercer capítulo nos centraremos en describir algunos de los proyectos más importantes que se están desarrollando por algunos grupos de investigación en el mundo.

CAPITULO

III

APLICACIONES

Gracias a las redes ad hoc se han podido implementar una gran cantidad de proyectos enfocados a cubrir varias necesidades en diversos sectores tales como militares, de comunicación, comerciales y varios otros.

Es impresionante ver como a partir de una tecnología se pueden desarrollar muchas ideas realmente innovadoras, solo es necesario tener la visión y la motivación para generar nuevos proyectos a partir de una idea ya creada.

La mayoría de las veces se derivan varios proyectos a partir de uno que finalmente son una copia entre sí, pero lo mejor es generar varios proyectos basándose en una tecnología pero con la diferencia de que cada uno busca un resultado distinto. Es en este capítulo donde

analizaremos varios proyectos interesantes, detallando su implementación, uso y demás características.

3.1 HAWKVISION

3.1.1 DESCRIPCION

El proyecto es un Mapa Interactivo en Tiempo Real diseñado para ser usado en escenarios de combate urbano. Usa GPS para obtener la posición actual de todos los usuarios que estén usando la aplicación. Los usuarios pueden agregar objetos al mapa incluyendo edificios, enemigos, tanques y aviones solo por mencionar algunos. Los usuarios también pueden enviar mensajes instantáneos entre ellos y elegir la imagen de fondo. Así mismo, el sistema cuenta con un archivo (bitácora). Una de las últimas características del proyecto es Movie Record. Con esto los usuarios pueden crear una película de la actividad del mapa y visualizarla después para su análisis.

El proyecto fue dividido en 3 partes: Red, Aplicación e interfaz de usuario. En la capa de red, se detallan todos los paquetes y protocolos que se usan. También en esta capa se crea una bitacora de recuperación para manejar los fallos y reiniciar la aplicación. La capa de aplicación maneja la interacción entre el usuario y la capa de red. En esta capa es donde se encuentra el vector donde todos los objetos del mapa son almacenados. Se actualiza este vector cuando el usuario cambia cosas o cuando ocurre un cambio en la capa de red. La interfaz de usuario es lo que el usuario ve y con la cual interactúa.

La implementación de la capa de red se ha hecho en dos fases. La primera involucra diseño y pruebas en una red cableada multicast y la segunda fase involucra la integración de esta capa con la de aplicación. La aplicación de red ofrece importantes presentaciones. En términos de comunicación, se ofrecen capacidades de Mensajes de Broadcast y Mensajes Punto a Punto.

Debido a que este proyecto está orientado a la actividad militar, se ofrece una red que soporta persistencia de estado de información (persistence of state information), o lo que en otras palabras es que todo lo que pasa por la red es tolerante y resistente a fallas de hardware.

3.1.2 DESARROLLO

Para simplificar el problema se decidió dividir el proyecto en tres capas (figura 23). Estas tres capas son interfase de usuario, capa de aplicación y capa de red, a continuación se muestra un diagrama:

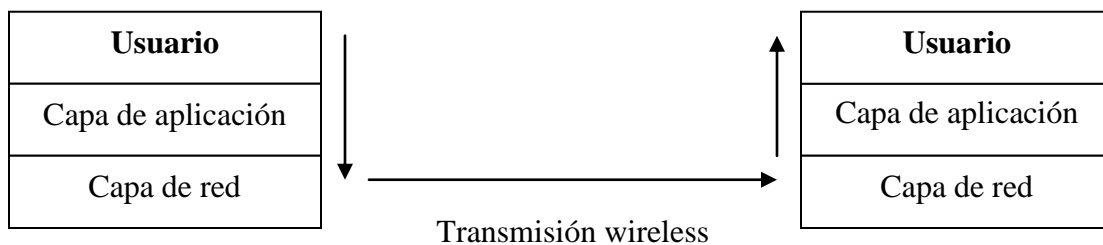


Fig. 23 Abstracción en tres capas del proyecto

En el nivel más alto se encuentra la interfaz gráfica que interactúa con el usuario. La capa básica de esta interfaz es un mapa que muestra la posición del usuario. Sobre esta capa un usuario puede agregar y remover objetos. También el mapa se actualiza en tiempo.

La capa de aplicación está entre la de red y usuario. Esta capa responde a solicitudes hechas tanto por la capa de red y de usuario. Los mensajes son generados basándose en los datos de entrada del usuario. Desde aquí los mensajes son enviados a la capa de red de donde son empaquetados y transmitidos. Los mensajes más comunes suelen ser GPS e identificadores de objetos. Una vez que los datos son recibidos por la capa de red, entonces la capa de aplicación se encarga de hacer las actualizaciones en la interfaz de usuario.

La capa de red es la parte del programa que inicia los sockets, envía y recibe mensajes aprovechándose de los protocolos TCP/IP. Esta capa recibe una gran cantidad de mensajes de la aplicación. Después de recibir los datos, esta capa les da el formato adecuado a los mensajes y los envía a los otros usuarios. Cuando los mensajes son recibidos, el tipo de mensajes es deducido, los campos necesarios son extraídos y los demás datos para su actualización deben ser pasados a la capa de aplicación.

HARDWARE REQUERIDO

En este proyecto se construyeron 3 unidades con el objetivo de realizar pruebas con el siguiente hardware:

- 3 computadoras portátiles (1 Linux, 2 Windows)
- 1 unidad externa GPS
- 1 tarjeta Prism 802.11b
- 2 enrutadores Wave Relay con unidad GPS integrada.

Para la computadora portátil con Linux, se planeó conectarle la tarjeta inalámbrica Prism 802.11b y luego usar un adaptador de USB a serial para configurar y conectar la unidad GPS externa. Esto proveerá a la computadora portátil la posibilidad de hacer un ruteo Wave Relay y de igual forma la posibilidad de obtener coordenadas GPS. Para las otras dos computadoras portátiles, se conectarán los enrutadores Wave Relay vía Ethernet, utilizando los mismos routers para enlazar la red. Aprovechando que los enrutadores están contruidos con tecnología GPS, se diseñó la capa de aplicación para obtener la dirección IP y la información de coordenadas de las unidades GPS.

INTERFAZ DE USUARIO

Se ha pensado en un diseño muy simple para la interfaz de usuario, se puede ver un ejemplo de la interfaz en la figura 24. Al usuario se le presentará un mapa que mostrará su ubicación actual si está activo, además la ubicación de cualquier otro miembro del equipo. En un lado del mapa habrá botones con las acciones más frecuentemente usadas, por ejemplo objetos que pueden ser arrastrados y pegados en diferentes localidades del mapa.



Fig. 24 Prototipo interfaz de usuario HAWKVISION

3.1.3 OBSERVACIONES

HAWKVISION es un proyecto muy ambicioso e interesante. Debido a la naturaleza de su aplicación, se puede considerar que tiene grandes probabilidades de éxito en la industria, en este caso la militar. HAWKVISION podrá ayudar en gran medida a los militares a tener una visión amplia y clara del área donde estén combatiendo o inspeccionando, reduciendo los peligros y contratiempos.

Una buena opción que se pudiera utilizar para reducir costos del proyecto sería utilizar Software Libre en todas las computadoras portátiles en lugar de tener que pagar licencias por Software

Propietario. En la capa de interfaz de usuario sería más eficaz si en lugar de introducir las órdenes, comandos o mensajes a otros usuarios de forma manual se hicieran utilizando la voz.

El mapa daría una mejor perspectiva si utilizara gráficos tridimensionales en lugar de usar bidimensionales. Esto ayudaría a los usuarios a tomar mejores decisiones porque verían un escenario más real. Hoy en día esto es más factible, y aprovechando el poder de cómputo ofrecido por las computadoras portátiles. Como ejemplo está la tecnología utilizada por Google Maps, en la cual en ciertas zonas ya se pueden ver regiones con irregularidades del terreno e incluso los edificios más importantes de esas zonas.

Analizando este proyecto, otra aplicación que se le pudiera dar además de la bélica, podría ser en áreas afectadas por desastres naturales, tales como huracanes, terremotos, tornados, etc. con el objetivo de crear un mapa del área devastada y planear las acciones que se requieran en el apoyo de personas afectadas.

3.2 PROXIMITY

3.2.1 DESCRIPCION

El objetivo de PROXIMITY es desarrollar una aplicación que emita una alerta a los usuarios si ellos están dentro de un rango de comunicación inalámbrica en los cuales están amigos o usuarios con intereses similares. Es entonces cuando la aplicación permitirá a los usuarios comunicarse mediante el envío de mensajes de texto.

Usando la aplicación el usuario (figura 26) puede hacer un perfil que contenga información que quiera compartir con otra gente. El perfil deberá ser estructurado en un orden estricto, pero puede contener un amplio rango de información, tales como nombre, intereses, películas favoritas, música, libros, entradas recientes de los blogs, etc. Para cada información el usuario

puede elegir el nivel de seguridad con la cual desea compartir su información: público, solo para amigos o solo para uso privado de ciertos usuarios.

Cuando un usuario se encuentra en movimiento, el sistema busca si existe algún usuario que este corriendo la misma aplicación, si esto ocurre la misma aplicación automáticamente intercambia el perfil del usuario de acuerdo a la política establecida por cada usuario. Adicionalmente, la aplicación incluye la funcionalidad de mensajería instantánea.

Los escenarios de uso del sistema son los siguientes:

1. CONFIGURACION INICIAL

- El usuario genera un nuevo certificado el cual representa su identidad.
- El usuario crea su perfil seleccionando una serie de categorías y llenando la información apropiada.
- El usuario selecciona las políticas para cada categoría.
- El usuario puede definir nuevas categorías.

2. FUNCIONAMIENTO DESATENDIDO

- La aplicación periódicamente envía un mensaje con el contenido "I'm here".
- La aplicación escucha en el grupo multicast en busca de otras personas. Cuando encuentra a alguna, obtiene la información pública de ese usuario y la almacena en un caché.

3. MODO EN LÍNEA

- La aplicación provee una lista de personas en línea y los usuarios pueden elegir si desean entrar en conversación con ellos.

3.2.2 DESARROLLO

PROXIMITY se basa en ciertos componentes:

1.- PERFIL DE USUARIO

Antes de entrar al sistema, un usuario debe definir su propio perfil. Este perfil contiene información tales como nombre, nombre de usuario, dirección de correo electrónico, localidad, intereses, amigos, etc. Son 3 tipos de elementos los cuales se definen en un perfil:

- CATEGORIA.- Es elemento básico que define un perfil; una categoría es definida por un nombre, descripción y valores (nombre, localidad, dirección de correo electrónico).
- GRUPO.- Un grupo de interés (música, deportes, etc.), cualquier usuario puede unirse a un grupo, solo debe agregarlo. Por omisión viene el grupo GENERAL.
- AMIGO.- Define un amigo directo.

Cada categoría y grupo deberán tener una política que defina como será transferida la información hacia otro usuario. Existen 4 tipos de políticas:

- PUBLIC.- La información puede ser accesada por cualquier usuario.
- FFRIEND.- La información está disponible solo para amigos directos o amigos de amigos.
- FRIEND.- La información solo está disponible para amigos directos.
- DISABLED.- La información no está disponible para nadie.

2.- DIAGRAMA DE SECUENCIA “HELLO”

El primer contacto entre dos aplicaciones (APP1 y APP2) se realiza como se muestra en la figura 24. La explicación del diagrama es el siguiente:

- La aplicación APP1 hace un broadcast “Hello” a la aplicación APP2 con el objetivo de indicarle que desea comunicarse.
- APP2 verifica el perfil de APP1 para saber si ya esta en sus repositorios.
- Si no esta el perfil de APP1 en los repositorios de APP2, APP2 le pide el perfil a APP1.
- APP1 obtiene y prepara su perfil lo prepara para enviárselo a APP2.
- APP1 entonces le envía el perfil a APP2.
- APP2 es ahora entonces que almacén el perfil de APP1 en sus repositorios de perfiles.

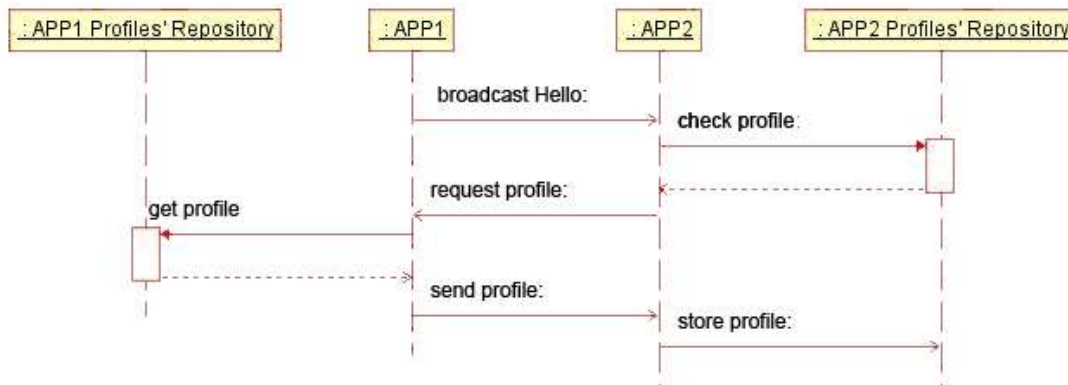


Fig. 24 Diagrama de secuencia “HELLO”

3.- DIAGRAMA DE SECUENCIA “SEARCH PROFILE”

Si un usuario está interesado en cierto usuario, este puede definir en su configuración que ese usuario sea buscado periódicamente. El intercambio de mensajes se muestra en la figura 25 y ocurre de la siguiente manera:

- APP1 envía un mensaje pidiendo el perfil de usuario a APP2.
- APP2 va, busca y obtiene el perfil en sus repositorios.
- APP2 ahora envía el perfil de usuario a APP1.
- APP1 almacena en sus repositorios el perfil de usuario de APP1.

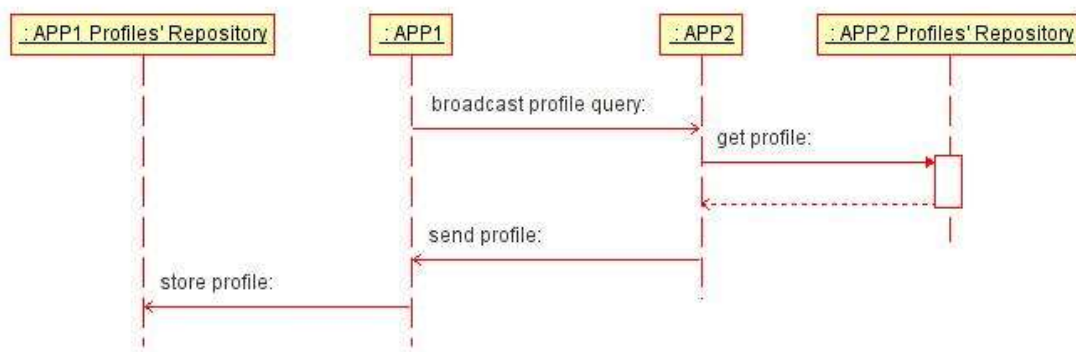


Fig. 25 Diagrama de secuencia “SEARCH PROFILE”

Para la implementación del sistema se utiliza el lenguaje JAVA, y puede ser soportado por cualquier red ad hoc, ya sea inalámbrica o alámbrica. Utiliza infraestructura Peer to Peer. La criptografía soportada está basada en Boundy Crypto API, una API criptográfica ligera que aprovecha dos presentaciones: AES y RSA. Las comunicaciones se basan en UDP multicast y TCP punto a punto. El UDP multicast es usado para enviar periódicamente mensajes HELLO e intercambiar información de los perfiles, mientras que TCP es usado para hacer el intercambio de mensajes instantáneos más sencillos de manejar.

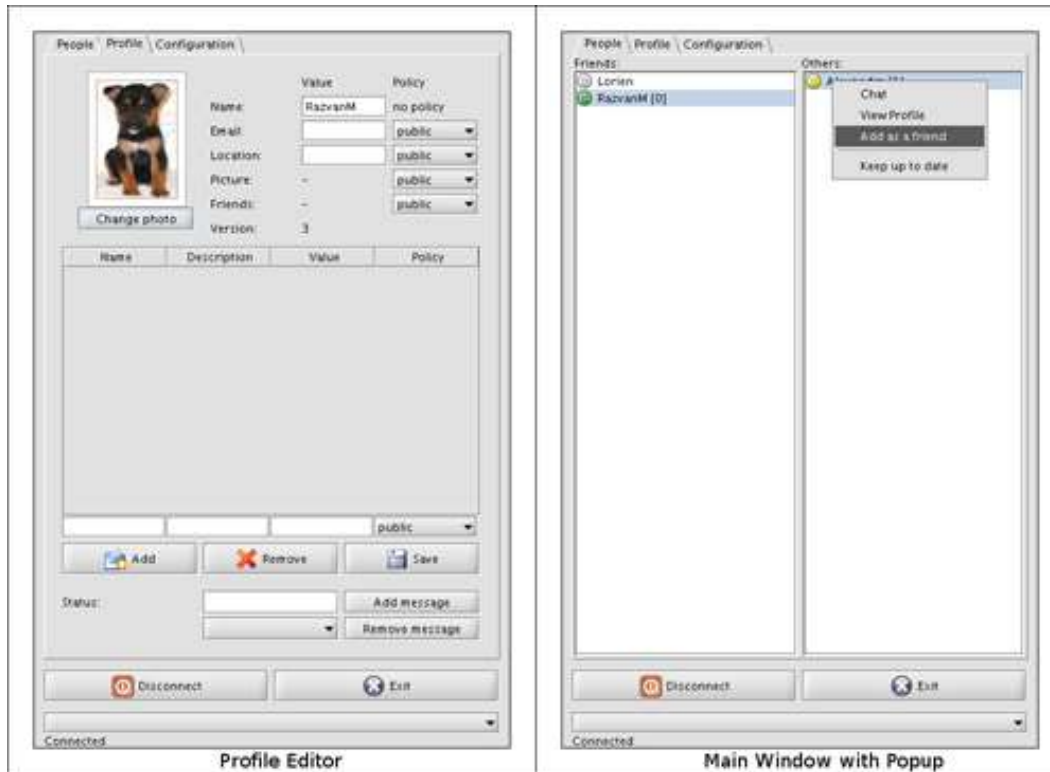


Fig. 26 Interfaz de usuario PROXIMITY

3.2.3 OBSERVACIONES

PROXIMITY es un proyecto que vendrá a modificar nuestras costumbres de comunicación. Actualmente podemos ver esta idea en clientes de mensajería instantánea que funcionan sobre Internet, sin embargo PROXIMITY nos permitirá estar en comunicación aunque no tengamos acceso a Internet.

No obstante, veo un punto en contra. PROXIMITY solo podrá interactuar con usuarios que estén dentro de su rango de alcance inalámbrico, pero imaginemos que dos usuarios (A y B) que se encuentren comunicándose o compartiendo archivos, empiecen a moverse, y en cierto tiempo salgan de su radio de alcance. En ese instante de tiempo perderán contacto y todo lo que estuvieran compartiendo fallaría en su entrega.

Para solucionar ese inconveniente, se podrían aprovechar los recursos de otros usuarios. Esto sería por ejemplo, si estos mismos dos usuarios (A ó B) salen de su radio de alcance, utilizar los

equipos de otros usuario para avisarles a A y B que han perdido comunicación y que deben buscar de nuevo al usuario (A o B) con el que estaban en contacto, o bien solo avisarles que han perdido comunicación.

Aunque de esta manera aumentaría el tráfico en la red, pero creo que se puede justificar con el hecho de que PROXIMITY no solo abarcaría un determinado rango, si no todo lo contrario, más haya del rango establecido.

Otra mejora que se puede implementar a PROXIMITY es la utilización de GPS. No usarlo en exceso, sería solo para obtener las coordenadas de la posición exacta de un usuario. Esto ayudaría a localizar amigos dentro de una determinada zona y facilitar la comunicación. Para prevenir y proteger la confidencialidad de los usuarios, ésta opción podría ser activada y desactivada por ellos mismo, así solo podrán ser localizados por GPS solo cuando el usuario así lo desee.

3.3 TDA (Targeted Distributed Advertisements)

3.3.1 DESCRIPCION

TDA consiste en un sistema de sensores, pantallas y una base de datos que en conjunto forman una red ad hoc 802.11. El objetivo de TDA es mostrar anuncios publicitarios a los clientes en un ambiente similar a tiendas tomando en cuenta sus preferencias de compras. Los movimientos de los clientes son seguidos por una serie de sensores que se localizan a través de las tiendas y los cuales detectan dispositivos móviles de los clientes (celulares, PDAs, etc.) que están en modo abierto.

Cada dispositivo Bluetooth tiene un identificador semi único que es usado para compararlo con los terminales Bluetooth, e identificar a que tiendas entran los usuarios, y cuanto tiempo duran en cada una de ellas.

Este seguimiento de información es continuamente actualizado por los sensores y enviado a una base de datos centralizada para su almacenamiento. Esta base de datos contiene una colección de todos los anuncios posibles, que son asociados a palabras claves dependiendo del tipo de tienda en la cual se vayan a desplegar, por ejemplo “women”, “shoes”, “outdoors”, etc. Así mismo, una vez que un cliente ha realizado sus compras, estas se almacenan en la base de datos, con el objetivo de hacer una lista personalizada de anuncios para dicho cliente.

Los anuncios son presentados en pantallas, las cuales están localizadas a través de toda la tienda. Cada pantalla contiene un dispositivo Bluetooth que puede detectar cuando un dispositivo Bluetooth de un cliente está en rango (entre 30-50 pies).

Otra opción potencial del TDA es poder hacer una conexión entre un dispositivo Bluetooth de un cliente y la pantalla cuando ambos estén en el mismo rango de comunicación para poder descargar cupones o información de ciertos productos.

3.3.2 DESARROLLO

Las dos partes principales de este proyecto son los componentes que actúan como sensores de la tienda para monitorear los hábitos de compras de los clientes y los dispositivos usados para desplegar los anuncios a los clientes. La parte central de estos componentes es la interfaz de sensores que implementan la funcionalidad de localizar los identificadores de los clientes.

El servidor principal se interfasa con la base de datos para actualizar y obtener los datos apropiados, la cual es entonces analizada usando el algoritmo *cosine similarity* para desplegar la mejor publicidad para un cliente en particular.

La publicidad es desplegada con un applet de java, la mejor publicidad es mostrada el 50% del tiempo, la segunda mejor un 20% del tiempo y la tercera mejor un 10% del tiempo.

Este proyecto se ha desarrollado en JAVA, en el cual se han desarrollado las 4 interfaces siguientes:

- **StoreSensor:** Esta clase es necesaria para las tiendas que esperan participar en TDA. Su propósito es escanear a los clientes y actualizar datos en el servidor central con los identificadores de los clientes obtenidos por SensorDeviceInterface.
- **SensorDeviceInterface:** Busca dispositivos disponibles y relaciona sus identificadores y su señales de identificación respectivas.
- **AdDisplay:** Esta clase inicializa el software y hardware. Inicia escaneando en busca de dispositivos Bluetooth usando SensorDeviceInterface y abre conexiones hacia el servidor central para actualizar la base de datos y buscar en ella los anuncios a mostrar.
- **Viewer:** Esta clase implementa el applet de java que despliega al cliente los anuncios.

La arquitectura genera de TDA se muestra en la figura 27, y se considera la siguiente secuencia de operación:

- 1.- El sensor Bluetooth descubre el identificador del dispositivo de clientes cercanos.
- 2.- El sensor Bluetooth envía la dirección sobre una conexión WAP al Sensor/Ad Server.
- 3.- Ad Server verifica en la base de datos y procesa la información para asegurarse cual es la publicidad que se va a mostrar.
- 4.- El identificador de la publicidad apropiada es enviada a las pantallas para su desplegado.

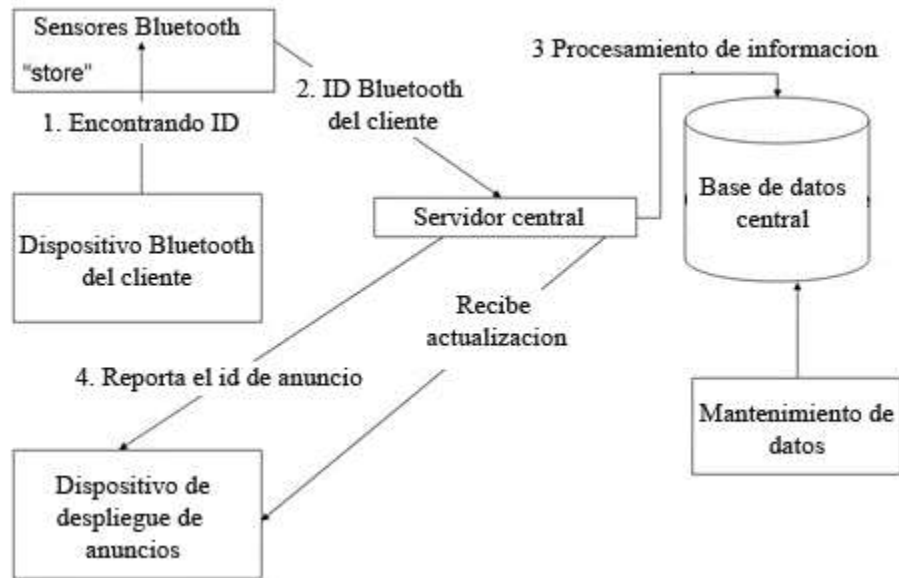


Fig. 27 Arquitectura de TDA

Observando la arquitectura, podemos ver que existen diferentes componentes:

- **Sensores de la tienda:** Pueden ser computadoras portátiles con Bluetooth y capacidades wave relay. Debe correr DiscoveryListener.java utilizando una antena Bluetooth para detectar la presencia de clientes con dispositivos Bluetooth. Cuando el cliente se mueve fuera del rango de un sensor, el sensor envía datos al servidor central vía wave relay. El sensor llama un método remoto en el servidor central que debe insertar/actualizar los datos del cliente en la base de datos.
- **Dispositivo de desplegado:** Puede ser computadoras portátiles con el mismo equipamiento que los sensores de la tienda. Este dispositivo debe almacenar toda la publicidad localmente a través de un mapeado entre cada anuncio y su identificador único. El Display deberá estar a la escucha de entradas de señales Bluetooth. Si el Display sensa a un cliente, éste llama un método remoto en el servidor central el cual regresa un ID ad.
- **Servidor Central:** Puede ser una laptop solo con wave relay. Contendrá la base de datos central. Y ese servidor es el que ejecutará los métodos remotos que se mencionaron anteriormente.

- **Base de datos:** Se planea usar MySQL para la implementación de la base de datos. Se busca que la base de datos contenga tres tablas: store type, customer y ad. La tabla store type será usada para especificar un tipo de tienda, por ejemplo: Kellis Liquors pertenecerá a Liquor store. La tabla customer contendrá un identificador único para cada cliente, una lista de tiendas visitadas y el tiempo que permaneció en dicha tienda. La tabla ad tendrá una combinación lineal de tipos de tiendas con funciones similares.
- **Dispositivo Bluetooth:** Cualquier dispositivo Bluetooth con el modo descubrimiento habilitado.

3.3.3 OBSERVACIONES

TDA es un excelente y prometedor proyecto que ayudará en gran medida a la venta de distintos productos. Principalmente los comercios tendrán un mejor perfil de los usuarios que los visitan, esto auxiliará a los comercios a conocer las preferencias de cada uno de sus clientes, aumentando la calidad del servicio ofrecido.

Hablando respecto a las ventajas que tendrá el cliente, se puede decir que van a ser muchas, no obstante, se considera que también habrá ciertas desventajas. Analizando las ventajas hay que mencionar que existirá un aumento en la eficiencia de compra, pues se anunciarán productos que tal vez incluyan algún descuento atractivo, así el cliente no tendrá que buscarlo y compararlo con otro similar. Una de las desventajas es saber que tanta privacidad tendrá el cliente. Puede ser que para un cliente no sea de su completo agrado que estén monitoreando sus compras, y se sienta un poco observado o vigilado. Se deben crear criterios muy específicos, por ejemplo se pudiera crear una limitante, la cual sería que el cliente pudiera elegir si desea que el sistema lo monitoree o no.

Una mejora que se pudiera añadir al proyecto es que los clientes pudieran usar su identificador único para poder hacer compras u ordenes a través de un sistema Web. Por ejemplo, que un

cliente pudiera acceder desde su casa o algún otro lugar a la Web del TDA. Una vez dentro el cliente pueda elegir que productos necesita más frecuentemente y crear una lista de compra. Esta lista estaría disponible la próxima vez que el cliente visite la tienda y a través de la red de sensores de TDA avisar cuando dicho cliente vaya entrando a la tienda. Es entonces que la tienda le tendrá lista para entregar la compra al cliente, ahorrando tiempo de esta manera. De tal manera que el cliente solo ira a recoger sus productos.

3.4 ZEBRANET PROJECT

3.4.1 DESCRIPCION

ZebraNet fue fundado por iniciativa del Nacional Science Foundation a través de su Information Technology Research (ITR). ZebraNet es un proyecto que explora los protocolos inalámbricos desde una perspectiva de eficiencia de energía.

El proyecto es un esfuerzo interdisciplinario de Biología y Sistemas Computacionales. Del lado de la computación, ZebraNet está estudiando los sistemas power-aware, position-aware. Es decir, el objetivo es desarrollar, evaluar, implementar y probar sistemas que integren comunicaciones inalámbricas y almacenamiento no volátil con GPS y otros sensores. En el lado de la Biología, el objetivo es usar dichos sistemas para realizar estudios sobre las migraciones de animales e interacción entre distintas especies.

Los objetivos principales de ZebraNet son:

- Que la posición GPS sea tomada cada tres minutos.
- Se haga una bitácora de actividad detallada de tres minutos cada hora.
- Sea capaz de operar sin intervención humana mínimo un año.
- La operación se pueda realizar sobre grandes rangos de zonas abiertas (cientos o miles de kilómetros cuadrados).

- Para el collar de Zebras el peso límite es de 3-5 libras. Para animales más pequeños los límites son menores.

3.4.2 DESARROLLO

Los modelos de movilidad son de gran importancia a la hora de diseñar redes móviles. Estos modelos ayudan a abstraer que tan rápido y que cantidad de usuarios se mueven, en qué dirección, y con qué fuerza de atracción o repulsión. Para el diseño de ZebraNet, se necesitó entender como se moverían los nodos, como esto afectaría el hardware, que protocolos usar y en general todo lo necesario para hacer el diseño. Al final, se espera desarrollar collares ZebraNet para un amplio rango de especies que compartan el mismo ecosistema: zebras, leones, elefantes, etc.

Los movimientos de las zebras puede ser categorizados en términos de tres estados principales (figura 28): pastando, pastando-caminando y moviéndose rápido. Las zebras gastan el mayor tiempo pastando, tanto el día como la noche.

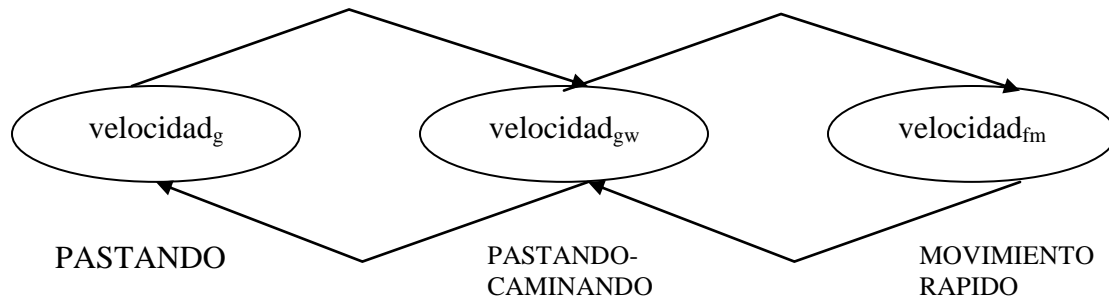


Fig. 28 Estados de movimiento de las zebras

La probabilidad de transición entre cada estado está derivada de las siguientes circunstancias, según lo señalan los biólogos:

- **Distancia recorrida:** La distancia total recorrida se define como la distancia recorrida desde el inicio del intervalo de los tres minutos hasta el final. Esto es, si una zebra se mueve diez metros de su posición original y luego regreso al mismo lugar, todo esto en tres minutos, la distancia total es cero.
- **Cambio de ángulo:** Similar a la distancia recorrida, el cambio de ángulo es definido como el valor absoluto del ángulo entre el inicio del intervalo de tiempo y el final. Si una zebra se mueve 360 grados dentro de los tres minutos, el cambio de ángulo debe ser cero.
- **Fuentes de agua y bebederos:** Las zebras son herbívoros dependientes de agua, por lo tanto frecuentemente están en busca de fuentes de agua. Basados en la observación, los modelos de movilidad asumen que las zebras buscan fuentes de agua al menos una vez por día. En este modelo de movimiento se asume que las fuentes de agua están distribuidas aleatoriamente.
- **Dormir:** Las zebras tienden a no tener largos períodos de sueño, ya que a diferencias de los carnívoros, las zebras entran en un estado de observación y pendientes a predadores. De tal manera que este modelo de movimiento asume que las zebras mantienen su patrón de movilidad 24 horas al día.

El diseño del collar consta de un prototipo para evaluarse, esta constituido por un GPS, Flash RAM y un CPU, el diagrama de bloques puede verse en la figura 29. El GPS es receptor de 12 canales con capacidad de obtener la posición actualizada cada segundo. El procesador de 32 bits es un Hitachi SH1 de 20 Mhz con soporte I/O. Este procesador se utiliza para la captura de datos y el control del protocolo. La memoria Flash es de 1 MB, de los cuales solo 640 KB están disponibles para datos del usuario, mientras que el resto almacena el firmware.

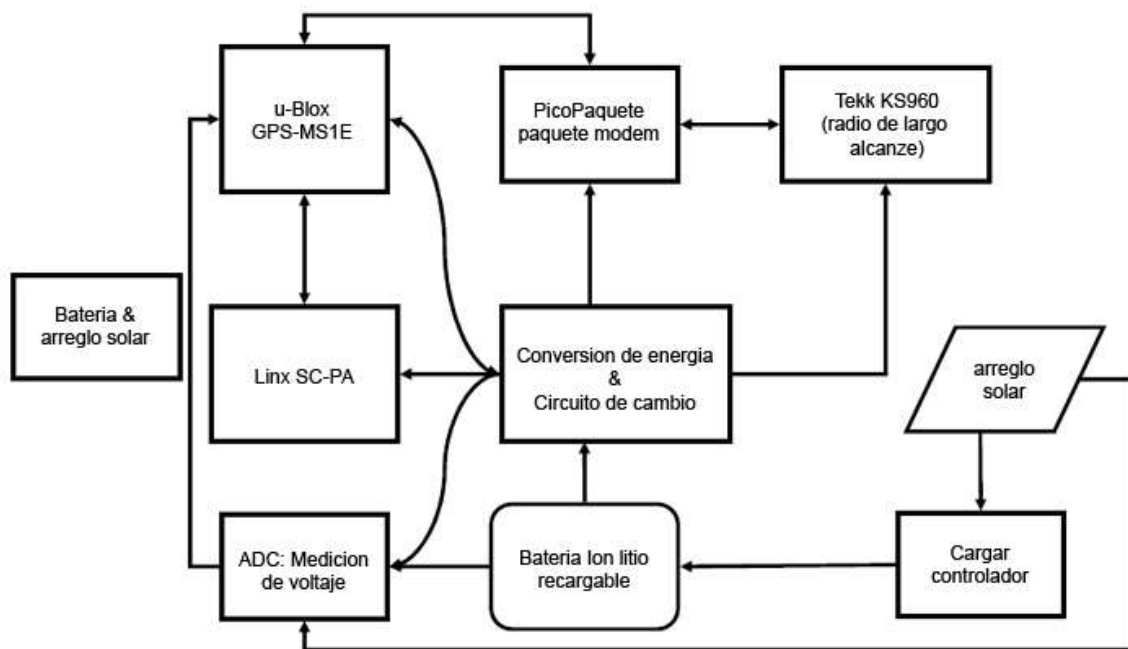


Fig. 29 Diagrama de bloque del collar ZebraNet

El diseño del protocolo se ha hecho considerando que el objetivo de ZebraNet es recolectar datos en cada collar y enviarla a una estación base. Debido a que cada collar no está en rango respecto a la estación base, los datos no pueden ser enviados directamente. Por lo tanto, debe ir saltando encontrando una ruta a través de otros collares hasta la estación base.

En ZebraNet, todos los nodos excepto la estación base son fuentes de datos. Además todos los nodos son móviles. La estación base también puede ser móvil, dependiendo si los investigadores están recolectando información.

El protocolo de inundación (Flooding Protocol) es aprovechado en ZebraNet. Una idea simple para mover datos hacia la estación base es mandar datos a todos los vecinos. La estación base no necesariamente necesita estar en contacto con todos los nodos del sistema, solo con que este en contacto con algunos es suficiente. A pesar de esto, la estación base debe ser capaz de interferir o identificar a nodos que han estado en contacto con la mayor cantidad de otros nodos. Estos nodos contienen entonces una cantidad substancial de información.

3.4.3 OBSERVACIONES

ZebraNet es un proyecto muy ingenioso, sobre todo en la forma en que se ha diseñado. Una de las características más notables es la capacidad de trabajar en forma independiente por un año sin la intervención de personas, esto es una ventaja ya que de esta manera ZebraNet es muy efectivo en un largo plazo.

Una desventaja es que los nodos son un poco grandes, que en este caso son en forma de collares. Creo que sería mejor que los nodos fueran mucho más pequeños, por ejemplo que midieran pocos milímetros para que puedan ser insertados por debajo de la piel de los animales y de esta manera no interfieran mucho con la vida de ellos.

Las ventajas son muchas más que las desventajas. ZebraNet se podría extender mas allá que a zebras y animales similares. Como ejemplo sería a aves, solo que para este caso sería necesario disminuir el tamaño de los nodos como se mencionó anteriormente. O también se podría usar en especies marinas, tales como focas, ballenas, tiburones, delfines, etc. Pero se tendría que mejorar el diseño de los nodos para que fueran resistentes al agua y a la presión de las profundidades oceánicas.

En este tercer capítulo se han descrito una serie de proyectos que una vez terminados tendrán un gran impacto social y tecnológico. Como todo avance tecnológico, las redes ahora han encontrado una aplicación en el área militar haciendo más eficientes las guerras lamentablemente.

Sin embargo existen aplicaciones que serán de mucha ayuda en diversas actividades cotidianas de los usuarios. Por ejemplo el proyecto PROXIMITY ayudará a comunicar usuarios con intereses comunes fomentando de esta manera el intercambio de ideas y experiencias. En otros casos como el proyecto TDA nos ayudará a realizar compras más eficientemente y a su vez permitiendo a los comerciantes ofrecer servicios personalizados a sus clientes, provocando un aumento en las ventas.

Como estos, existe una gran cantidad de proyectos en desarrollo para hacernos la vida más fácil de tal manera que podremos enfocar más tiempo en otras actividades de mayor prioridad.

Tratando de hacer más eficaz la vida estudiantil, en el siguiente capítulo expondré un proyecto enfocado a satisfacer diversas necesidades de comunicación dentro del campus universitario.

CAPITULO

IV

MOBILE CAMPUS AREA NETWORK

Las redes ad hoc proporcionan grandes ventajas en las comunicaciones a través de dispositivos móviles, los cuales se pueden utilizar para mejorar el desarrollo de procesos en el ambiente universitario.

Gracias a esto, se ha podido visualizar un proyecto que ayudará a la comunidad universitaria a tener una mejor comunicación entre alumnos, maestros, personal administrativo y directores. Los dispositivos que constituirán la red abarcan servidores, puntos de acceso, dispositivos móviles y un software especialmente diseñado para ser instalado en los nodos.

En este capítulo se analizará el desarrollo del proyecto propuesto, describiendo detalladamente todas sus características físicas y de uso.

4.1 DESCRIPCION DE MCAN

La propuesta se enfoca en el desarrollo de una infraestructura que permita la implementación de una red Ad Hoc, cuyo objetivo es cubrir varias necesidades que se tienen en las actividades académicas del campus universitario. Estas necesidades son principalmente de comunicación entre alumnos, maestros y personal administrativo.

Son varios los servicios que se van a ofrecer tanto a usuarios universitarios como a usuarios visitantes como por ejemplo a estudiantes de preparatoria que vayan a realizar su primer trámite de inscripción, a docentes visitantes de otras escuelas, a investigadores con estancias en la universidad, etc..

A continuación se describirán los servicios:

4.1.1 COMPARTIR INFORMACION

Uno de los servicios principales será el compartir información entre usuarios con intereses comunes. Estos intereses pueden ser por ejemplo cursos, gustos, actividades, etc. La información que se compartirá tendrá distintos niveles de clasificación con el objetivo de guardar la privacidad de cada usuario. Los niveles se clasificarán en público, personal y restringido.

El nivel público se le dará a la información que el usuario quiera compartir con todos los usuarios que estén cerca de él. El nivel personal se asignará a información que el usuario no quiera compartir en un momento determinado pero que en un futuro si se le podrá asignar cualquiera de los otros dos niveles. Finalmente el nivel restringido es para la información que el usuario quiera compartir con usuarios específicos que él decida (amigos, profesores, etc.).



Fig. 30 Comunicación entre usuarios con intereses comunes.

Para que la información pueda ser compartida es necesario que varios usuarios estén dentro de un mismo rango de transmisión y que la red se autoconfigure, un ejemplo puede verse en la figura 30. En el instante en que un usuario se aproxime a otro usuario el software iniciará las negociaciones para tratar de establecer una conexión. Una vez realizada dicha conexión lo siguiente es identificar la información que se va a compartir en ambos nodos y ver cual es su clasificación.

4.1.2 ALMACENAMIENTO DE INFORMACION

Otro servicio que se ofrecerá mediante la red será el almacenamiento de información. Se tendrán servidores de almacenamiento distribuidos en todo el campus universitario para distribuir la carga de trabajo entre ellos y hacer el acceso y almacenamiento más eficientes, el diagrama de la figura 31 ejemplifica este proceso. Debido a que la información tiene que ser la misma en todos los servidores se tiene que actualizar casi en tiempo real. Por ejemplo si en un servidor un usuario sube algunos datos, esos datos se tienen que retransmitir automáticamente a los demás servidores para que estén disponibles en todo el campus.

Cada usuario de la red tendrá un espacio en disco en los servidores para que puedan almacenar sus datos. Al igual que en cada dispositivo de usuario, en los servidores también habrá diferentes categorías para clasificar la información.

Los dispositivos que actuarán como apoyo a la red y a los servidores serán unos puntos de accesos (Kioscos) que al igual que los servidores serán distribuidos estratégicamente a través de todo el campus universitario para dar una amplia cobertura.

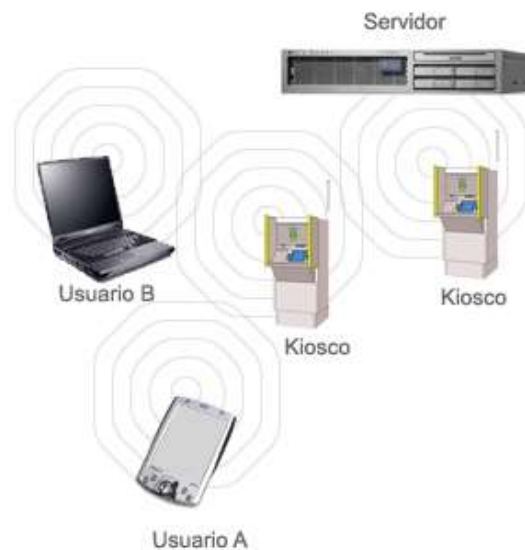


Fig. 31 Esquema representativo del proceso de almacenamiento de información.

Cuando un usuario se aproxime a un kiosco, se conectará al servidor y tendrá varias opciones a realizar tales como subir datos, descargar datos, cambiar la clasificación de la información o solo consultarla.

En caso de que un usuario no esté cerca de un kiosco para subir información, se aprovechará la infraestructura de la red ad hoc para encontrar una ruta hasta un kiosco y de ahí ya de forma automática se enviará la información a todos los servidores.

4.1.3 CONSULTAS ESPECIALIZADAS

Un servicio muy útil que se ofrecerá serán las consultas especializadas sobre temas específicos. Usuarios que tengan un mayor conocimiento sobre ciertos temas podrán especificar en el software que son capaces de responder consultas a otros usuarios.

El procedimiento que se debe realizar para solicitar una consulta es estar en el rango de comunicación con el usuario al que se quiere consultar, en la figura 32 se puede ver un ejemplo de este proceso. Si esto ocurre entonces el software avisará que ese usuario esta en línea. En este momento al usuario que se desea consultar el software le avisará que algún otro usuario desea consultarlo.



Fig. 32 proceso de enviar y contestar una consulta.

El usuario a consultar podrá decidir si acepta la consulta en ese momento, la pone en estado pendiente para contestarla en un futuro o la manda a un foro personal donde el otro usuario podrá publicar su pregunta para que posteriormente sea respondida.

En caso que el usuario a consultar quiera responder la consulta inmediatamente entonces la comunicación entre usuarios será mediante el envío y recepción de mensajes y en un tiempo especificado por el usuario experto.

Si la consulta se pone en estado pendiente, el usuario experto se obliga a responder la consulta antes de que abandone la sesión actual y la comunicación se hará mediante envío y recepción de mensajes y en un rango de tiempo predefinido.

Finalmente si la consulta se canaliza al foro, el usuario experto se comprometerá a responderla en un tiempo mínimo para que el servicio refleje seriedad y calidad.

4.1.4 MENSAJERIA BASADA EN WEB

Un gran problema que existe en el campus universitario es la deficiencia de comunicación entre alumnos, maestros y personal administrativo. Muchas veces se difunden noticias o comunicados pero no son muy bien difundidos a toda la comunidad interesada.

Lo que se planea solucionar con este sistema de mensajes es la eficiente entrega de noticias, comunicados o cualquier otro tipo de información que le interese a la comunidad universitaria. Es aquí donde entra en acción la mensajería basada en Web.



Fig. 33 Mensajería basada en Web.

El funcionamiento de este sistema se basa en un software multiusuario que se instalará en un servidor, en la figura 33 se puede ver el uso básico de este sistema. Cuando un usuario (personal administrativo o maestro) quiera publicar alguna información tendrá que seguir el siguiente procedimiento:

- Entrar al sistema introduciendo su usuario y contraseña.
- Una vez dentro del sistema escribir el mensaje y configurarlo (fecha en que se publicará, a quienes, tiempo activo que durará el mensaje publicado, etc.)
- Enviarlos a los servidores que estarán distribuidos en el campus.

A partir de aquí, todos los mensajes ya estarán disponibles para la comunidad universitaria. De tal manera que cuando un usuario esté cerca de un kiosco, el software instalado en su dispositivo móvil será capaz de identificar esos mensajes y notificárselos al usuario, todo esto si se da el caso de que el usuario sea parte del grupo al que van dirigidos las noticias.

El mantenimiento de mensajes será automático, de tal manera que los mensajes se borrarán cuando el tiempo de vida haya expirado. Esto es de mucha ventaja porque el sistema dependerá de forma mínima de la intervención de los usuarios.

4.1.5 MENSAJERO INSTANTANEO

Otro servicio de utilidad será el mensajero instantáneo, el cual permitirá que usuarios dentro de la red se comuniquen. Los usuarios estarán disponibles siempre y cuando estén en el alcance de la red no importando si hay o no comunicación directa entre los dispositivos móviles de los usuarios.



Fig. 34 Mensajería instantánea

Si dos usuarios están dentro de un radio de alcance donde sus dispositivos móviles puedan interactuar directamente, entonces los mensajes serán enviados de nodo a nodo sin ser necesario que sean auxiliados por otros dispositivos. En el caso en que dos usuarios no se puedan comunicar directamente, será posible hacer la comunicación mediante el apoyo de los kioscos, no importando la ubicación física de los usuarios, este proceso se puede apreciar en la

figura 34. Por ejemplo supongamos que el usuario A desea comunicarse con B pero ambos no están cerca, ambos usuarios podrán saber que están dentro de la red gracias a que la identificación será posible gracias a los kioscos.

Dentro de la configuración del Mensajero Instantáneo se podrán activar o desactivar diversas opciones como:

- Si desea ser visto por otros usuarios.
- Una lista personalizada de usuarios creada por el usuario mismo.
- Si desea que su ubicación geográfica sea pública.

4.1.6 CLASES INTERACTIVAS

Una idea que surgió gracias a la experiencia como estudiante fueron las clases interactivas, las clases normales que hoy en día se toman en la mayoría de las veces hay poca interactividad entre alumnos y maestros. Esto hace que por parte de los estudiantes la clase sea poco provechosa y aburrida.

La propuesta de clases interactivas se enfocará específicamente en varias actividades que se desarrollan dentro del salón de clases. Dichas actividades se mencionan a continuación:

4.1.7 APUNTES

La mayoría de los maestros entran al salón de clases e inician impartiendo su clase dictando o escribiendo en el pizarrón el tema del día. Esto hace que el tiempo real de clase disminuya y se desperdicie, puesto que ese tiempo que se dedica al dictado se pudiera aprovechar para resolver dudas del alumno. Aquí es donde entra el concepto de clases

interactivas, el maestro tendrá que preparar con anterioridad su clase, y crear algún tipo de documento que al momento de iniciar la clase, la red sea capaz de redistribuir ese documento a todos los alumnos que pertenecen a la clase. Esto se realizará a partir del dispositivo móvil del maestro que entrará en comunicación con los dispositivos de los alumnos y se propagará a todos ellos. Para evitar que el dispositivo del maestro se sature, si un alumno ya recibió dicho documento, su dispositivo actuara como emisor y tratará de reenviar la información a otros alumnos que estén a su alrededor.

4.1.8 PREGUNTAS ALUMNO - MAESTRO Y MAESTRO - ALUMNO

Las preguntas que realicen los alumnos serán mediante su dispositivo móvil, entonces el maestro las recibirá y podrá dedicar una cierta cantidad de tiempo de la clase para dar respuesta a las preguntas. De esta manera además de saber que alumno hizo la pregunta, será guardada en un historial para en un futuro el maestro pueda saber que alumno está mas atrasado y en que temas. Ahora, si el maestro es quien desea hacer preguntas el las podrá redactar o haberlas redactado con anterioridad y lanzarlas cuando el decida o cuando hayan sido programadas. Con esto las clases serán un poco más ágiles y eficientes.

4.1.9 EXÁMENES AUTOMÁTICOS

La forma que actualmente se usa para aplicar exámenes puede ser considerado obsoleta para la época que vivimos. Además de que se sigue utilizando papel siendo esto un gasto innecesario para la Universidad. Es por esto que se propone la utilización de la red MCAN para que realice la función de aplicar exámenes de forma semiautomática. El funcionamiento sería básicamente que el maestro publicaría mediante la Mensajería descrita párrafos arriba el día y hora en que el examen será aplicado. Al mismo tiempo el examen se programaría automáticamente. Llegado el día del examen, solo los alumnos suscritos a la materia y

permitidos por el maestro podrán hacer el examen. Pero una de las restricciones es que los alumnos deben estar cerca del Dispositivo móvil del maestro para poder hacer el examen. Esto para evitar que el examen sea resultado fuera del alcance del maestro. La cercanía de los alumnos respecto al maestro será calculada gracias a la herramienta de localización geográfica que se describirá posteriormente. Otra característica es que todos los alumnos serán avisados 10 minutos antes de que el examen inicie, esto para que cada uno de ellos tome su tiempo para llegar a tiempo al salón de clases. El examen tendrá por defecto un tiempo de duración, para evitar que los alumnos abusen y lleguen más tarde al examen, de tal forma que el maestro evitará problemas con ellos. Terminado el tiempo, el sistema dará los resultados casi de forma instantánea a los alumnos y serán procesados ahorrando tiempo de captura y revisión al maestro.

4.1.10 LISTA AUTOMÁTICA

Este servicio consta específicamente en que el sistema será capaz de tomar lista de asistencia automáticamente. Los alumnos deben estar localizados dentro del salón de clases para que sean registrados como asistentes de la clase, de caso contrario se marcará como falta, el diagrama de la figura 35 muestra como se lleva a cabo este proceso. El sistema dará 15 minutos de margen para que el alumno asista a la clase, este tiempo puede ser modificado por el maestro de acuerdo a su punto de vista.

En la configuración, el maestro tendrá dos opciones:

- Que el sistema de forma automática y considerando el horario de clases del maestro se active e inicie con el tomado de lista. Con esta opción el maestro en la mañana antes de que inicie sus labores tendrá que especificar al sistema que durante todo ese día desea que la lista sea de forma automática.

- La segunda opción es que el maestro active de forma manual la toma de lista. Aquí se tiene que activar unos minutos antes de que inicie la clase para que el sistema inicie el conteo de los 15 minutos que los alumnos tienen como margen para llegar a la clase.

Considerando que puede suceder la situación en que varios alumnos no cuenten con su dispositivo móvil (PDA, LAPTOP, etc.) se propone alternativamente la utilización de etiquetas RFID.

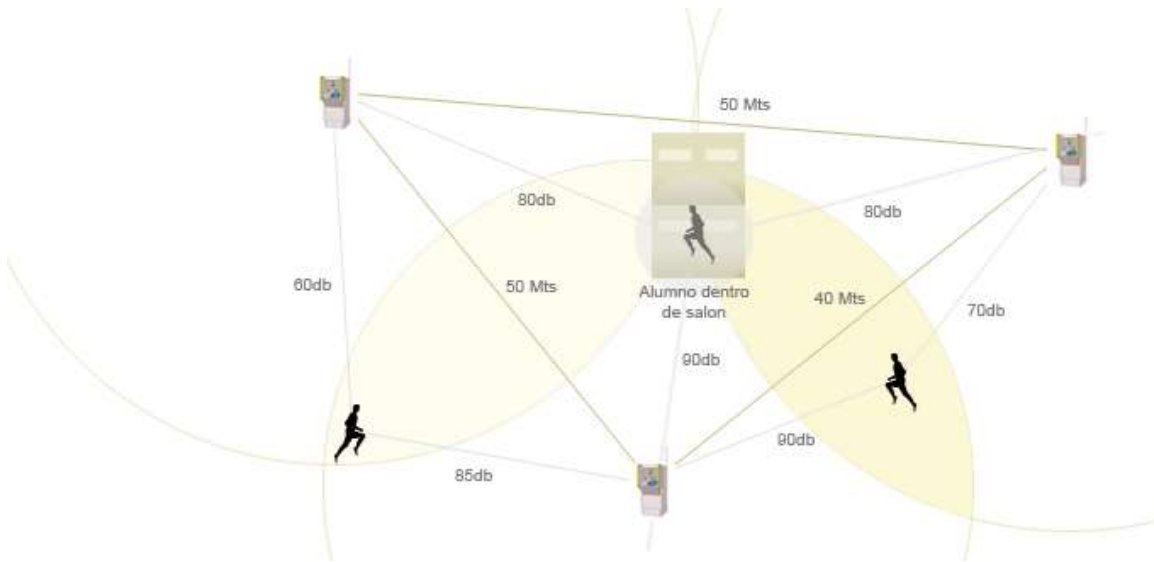


Fig. 35 Diagrama representativo de lista automática

RFID (siglas de Radio Frequency IDentification) es un método de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas o tags RFID, en la figura 36 se observa una tarjeta de este tipo. Una etiqueta RFID es un dispositivo pequeño, como una calcomanía, que puede ser adherida o incorporada a un producto, animal o persona. Las etiquetas RFID contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren.

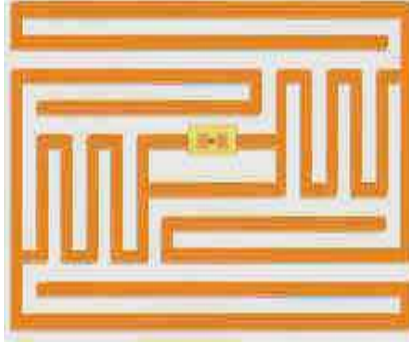


Fig. 36 Etiqueta RFID

Como las etiquetas pasivas son mucho más baratas de fabricar y no necesitan batería, la gran mayoría de las etiquetas RFID existentes son del tipo pasivo. Las etiquetas tienen un precio desde 0,40\$, en grandes pedidos. Observando estos precios, podemos asegurar que es una opción muy viable de utilizar en el Campus Universitario.

4.1.11 LOCALIZACION GEOGRAFICA

Una propuesta interesante dentro de MCAN es la posibilidad de localizar a los usuarios en la zona geográfica del campus. Así, la ubicación se podrá calcular tomando en cuenta varios aspectos que abarcan la posición de los kioscos, dispositivos móviles de los usuarios, intensidad de la potencia de la señal de los kioscos, en la figura 37 se puede ver el proceso mencionado.

El proceso de cálculo de cierta ubicación consiste en medir la potencia de la señal de varios kioscos a través de los dispositivos móviles de los usuarios, entonces una vez conociendo esta potencia se pueden realizar las estimaciones pertinentes para la ubicación.

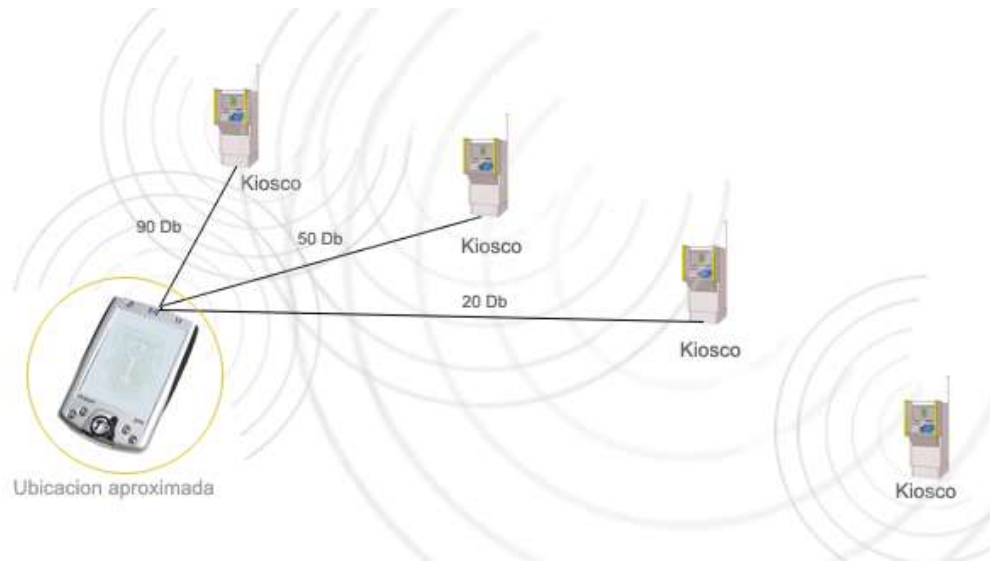


Fig. 37 Calculando la ubicación de un nodo móvil.

Específicamente existe un método para hacer localización de nodos llamado LOCAL POSITIONING SYSTEM (LPS) y puede ser usado por cualquier nodo que se localice dentro de la red. LPS es un método para obtener la posición solo de los nodos a lo largo de una trayectoria de la red, cuidando que el tráfico de la red no aumente demasiado. De tal manera que cada nodo que sea encontrado en la ruta gasta tiempo de cálculo para determinar su propia posición. Al hacer esto, se optimiza el uso de la red, puesto que al gastar tiempo de cálculo se ahorra comunicación evitando que circule por la red datos que se pueden procesar localmente.

LPS asume que cada nodo en la red tiene un eje principal sobre el cual se reportan todos los ángulos, y la capacidad para calcular con precisión la dirección con la cual los nodos vecinos envían la información. Cuando dos nodos vecinos interactúan, uno de ellos puede encontrar el ángulo entre su propio eje y la dirección de donde proviene la señal.

Si creamos un escenario en donde interactúan 3 nodos: A, B y C, el nodo A ve a los nodos vecinos como unos ángulos $\angle AC$ y $\angle AB$ y tiene la capacidad de inferir un ángulo del triangulo $\angle ABC = \angle AC - \angle AB$. Para mantener la consistencia se asume que todos los ángulos están

medidos en dirección trigonométrica. Una vez obtenida esta triangulación ya es posible calcular de forma precisa la ubicación de un nodo.

Se debe observar que LPS es eficiente en el sentido que trata de disminuir el tráfico en la red al momento de estar calculando posiciones y también es eficiente en el ahorro de energía en los nodos, ya que se gasta menos energía haciendo los cálculos localmente que enviar datos vía inalámbrica.

4.1.12 KIOSCOS DE ACCESO A LA RED

En todo el campus universitario se instalarán casetas que ofrecerán acceso a la red tanto de manera inalámbrico como por cable. Esto para dar acceso a todos lo usuarios incluyendo a aquellos que no tengan tarjetas inalámbricas.

Los servicios que estarán ofreciendo estas casetas serán: acceso alámbrico e inalámbrico a la red, verificación de mensajes enviados a la comunidad universitaria, lectura del correo universitario, cargar datos al espacio personal, descargar datos al dispositivo del usuario, la interfaz gráfica propuesta se puede ver en la figura 38.



Fig. 38 Prototipo de interfaz gráfica del kiosco

Debido a que estas casetas estarán libres a todos los usuarios, tendrán un control de sesión con un tiempo predeterminado y así evitarán el uso prolongado de un usuario. Con esto se habilitará que la caseta sea usada por el mayor número posible de usuarios. En la figura 39 se puede ver el prototipo de un kiosco.

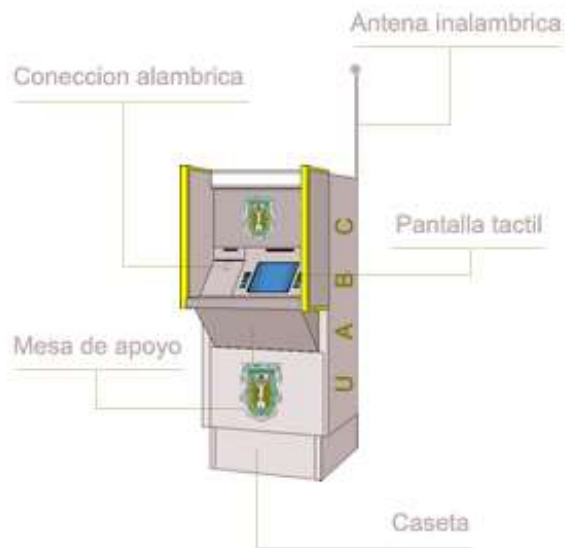


Fig. 39 Casetas de acceso a la red

Las características físicas de las casetas son:

- Acceso inalámbrico para usuarios que cuenten con tarjeta inalámbrica en sus dispositivos.
- Una ranura para conexión alámbrica mediante un cable de red. Así mismo la caseta contara con un cable de red para los usuarios que no cuenten con el cable.
- Pantalla táctil sobre la cual se podrá hacer uso de los distintos servicios ofrecidos en las casetas.
- Una mesa sobre la cual se podrá poner el dispositivo móvil del usuario.

4.2 HARDWARE

En esta propuesta tecnológica se tiene planeado utilizar hardware de calidad y lo más económico posible, con el objetivo de hacerlo un proyecto viable. La lista de hardware a utilizar se lista a continuación:

4.2.1 SERVIDORES



Fig. 40 Servidor SUN FIRE T2000

Como servidores se proponen los de la compañía SUN MICROSYSTEM, específicamente el Sun FIRE T2000. Estos servidores son de alto rendimiento y eficiencia debido al uso del procesador de multiprocesamiento masivo UltraSPARC T1 (figura 40) el cual ofrece:

- Un rendimiento hasta 3 veces mas rápido que la tecnología de servidor existente
- Eficiencia energética y de refrigeración que reduce los costos de funcionamiento en un 75%.
- Diseño compacto con solo 1 o 2 unidades de rack.
- Alta compatibilidad con aplicaciones existentes.

4.2.2 PUNTOS DE ACCESO (KIOSCOS)

El hardware elegido para implementar los puntos de acceso fueron los de la empresa ORINOCO específicamente el ORINOCO AP-4900M (figura 41). Estos puntos de acceso ofrecen alto rendimiento y escalabilidad. Soporta redes Wi-Fi tanto 4.9 Ghz pública y 2.4 Ghz metropolitana.



Fig. 41 Punto de acceso ORINOCO AP-4900M

Las características que presenta este dispositivo son:

- Radio dual, sistema de mallas multibandas
- Quad-mode (4.9 GHz, 802.11a, 802.11b, and 802.11g) y dual radio AP-to-AP
- Escalabilidad – antena externa para incrementar la distancia de transmisión y máximo sistema de ganancia para configuraciones repetitivas.
- Salida de operación 802.11g y 802.11a/4.9 GHz
- Nuevo nivel de detección y prevención de intrusos
- Pre-estandar IEEE 802.11e QoS soportado para aplicaciones de latencia sensitiva.

Estos puntos de acceso tienen la característica de que pueden ser configurados de tal manera que todos pueden comunicarse entre sí, sin la necesidad de cables. Esto es de gran ayuda en esta propuesta ya que al tener este modo de configuración se prescindiría de cables y la red sería Wi-Fi en su mayor parte.

4.2.3 NODOS MÓVILES

Los dispositivos móviles ideales que se podrán usar en esta red pueden ser computadoras portátiles (figura 43), PDA's (figura 44) o cualquier otro dispositivo que comparta estas características. A continuación se listan algunos posibles a usar:

Computadora portátil con tarjeta inalámbrica integrada con soporte para los estándares IEEE 802.11b y/o IEEE 802.11g. Adicionalmente se recomienda un procesador @ 800 Mhz, 256 Mb de RAM, unidad de CD ROM o DVD ROM.



Fig. 42 Laptop que podrá ser usada como nodo móvil.

Los PDA al igual que las laptops deben soportar los estándares IEEE 802.11b y IEEE 802.11g. La velocidad de procesador se recomienda como mínimo de 400 Mhz, 64 Mb de memoria ram.



Fig. 43 Pocket PC usado como nodo móvil.

4.3 MAPA

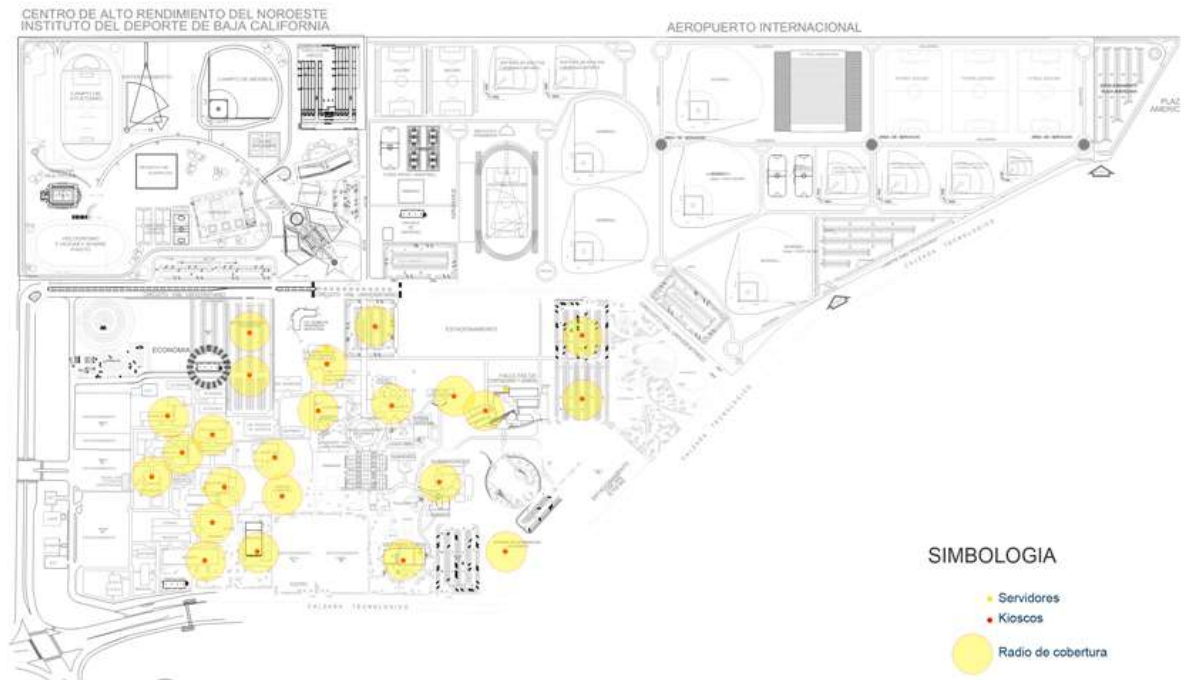


Fig. 445 Distribución geográfica de los kioscos y servidores en el campus UABC Tijuana.

Como se observa en la figura 45, se propone una distribución de servidores y kioscos en todo el campus universitario, con el fin de tener una mayor cobertura. Para hacer esta distribución se tomaron en cuenta los siguientes aspectos:

- Los servidores se distribuyeron considerando que zonas tendrán mayor tráfico, con esto se pretende dar un servicio mas rápido a la peticiones que se hagan.
- Los kioscos igualmente, se les distribuyo en lugares que se cree que van a tener un mayor uso, por ejemplo en biblioteca, cafetería, edificio 44, vicerrectoría.

En este capítulo se presentó la propuesta tecnológica MCAN que ofrecerá una serie de servicios para la comunidad universitaria. MCAN intentará agilizar varias actividades que se realizan diariamente por los diversos grupos de la comunidad. Se tiene como objetivo ir cambiando la cultura hacia un modo más automático y hacer uso de la tecnología más actual.

MCAN presenta un modelo de uso muy atractivo para todos, es innovador y sobre todo es una muy buena propuesta que se puede tomar como referencia para iniciar proyectos similares relacionados con el mejoramiento de la educación, no importando el nivel. MCAN no solo queda delimitado por los servicios propuestos en este trabajo, al contrario su funcionalidad puede ser extendida en muchos aspectos más.

CAPITULO

V Conclusiones y trabajos futuros

En el presente trabajo se presentó historia, protocolos, aplicaciones y una propuesta tecnológica relacionada con las redes ad hoc. Sin embargo, estamos concientes que en este trabajo queda mucho por hacer, se puede extender mucho más, proponer nuevas aplicaciones, mejorar las aplicaciones que se expusieron, describir nuevos protocolos o elegir nuevo hardware.

Tomando en consideración lo anterior, podemos definir trabajos futuros que se pueden desarrollar a partir de este:

- Proponer aplicaciones adicionales.- Se pueden proponer nuevas aplicaciones que faciliten la realización de las actividades universitarias.

- Configurar e implementar la infraestructura de la red.- La configuración e implementación es un trabajo muy importante y que aun falta por hacer.
- Instalar y configurar los servidores.- Este trabajo es muy importante y debe hacer de tal manera que queden muy eficientes para que cumplan con su objetivo. En esta parte se deben tomar en cuenta factores muy importantes, tales como seguridad de la información y seguridad en las transacciones de la información.
- Documentación detallada de MCAN. La documentación es una parte importante y aun falta hacer una buena documentación de las aplicaciones que se desarrollaran y que son mencionadas en este trabajo.

MCAN intenta ser un proyecto innovador que intentara poner a nuestra universidad en un nuevo nivel tecnológico, situándose en un mejor nivel, e incluso se podrá comparar con universidades de primer mundo.

La tecnología que se propone utilizar en MCAN suena un tanto irrealista, sin embargo la mayoría de esta ya esta disponible en el mercado. Tal vez unos inconvenientes que se puedan presentar durante la implementación de MCAN, sean los precios de los dispositivos, puesto que son tecnologías nuevas, sus precios son aun altos, pero en algunos casos esto no es así, por ejemplo en las tarjetas RFID sus precios son bajos si se compran en mayoreo.

Un caso en el que MCAN pudiera tener un poco de dificultad para ser implementado, es la cuestión de que la mayoría de estudiantes no cuentan con un dispositivo móvil, esto no afectara el funcionamiento de MCAN mas bien el aspecto que se verá afectado será el uso. Esto es que MCAN estará funcionando al 100% pero no todos lo usuarios gozaran de su uso al no contar con el dispositivo móvil necesario.

En el transcurso del tiempo, después que se haya implementado MCAN, tal vez se detecten puntos que se pueden optimizar tomando en consideración nuevo hardware que salga a la venta, o la optimización de software considerando nuevas técnicas o protocolos.

Se espera que este trabajo sirva para entusiasmar a nuevos estudiantes a innovar y crear nuevas tecnologías a favor de nuestra comunidad.

Las redes ad hoc en un futuro no muy lejano, pienso podrán ser parte de nuestra vida cotidiana, haciendo mas fácil las actividades que realizamos diariamente. Aunque hoy en día esta tecnología aun se encuentra en desarrollo, ya tiene aplicaciones en producción, principalmente aplicaciones desarrolladas en universidades.

El alcance que pueden llegar a tener las redes ad hoc es inmenso, desde aplicaciones industriales, educación, sociales hasta aplicaciones espaciales que ayuden a colonizar ciertas zonas del espacio. Como toda nueva tecnología, el limite esta restringido por el ingenio humano, hasta donde se quiera explotar y que es lo que se desea lograr, por esto, las redes ad hoc son una gran herramienta para el futuro.

6 GLOSARIO

Blog: Es un sitio Web periódicamente actualizado que recopila cronológicamente textos o artículos de uno o varios autores donde el más reciente aparece primero, con un uso o temática en particular, siempre conservando el autor la libertad de dejar publicado lo que crea pertinente.

Multicast: Es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen.

Peer to peer: Se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan a la vez como clientes y como servidores de los demás nodos de la red.

API: Es un conjunto de especificaciones de comunicación entre componentes de software. Representa un método para conseguir abstracción en la programación, generalmente (aunque no necesariamente) entre los niveles o capas inferiores y los superiores del software. Uno de los principales propósitos de una API consiste en proporcionar un conjunto de funciones de uso general.

Firmware: Es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria tipo ROM, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

Protocolo: Conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.

Wave Relay: Técnica utilizada para el intercambio automático de señales.

REFERENCIAS

- [1] Tony Larsson, Nicklas Hedman. Routing Protocols in Wireless Ad-hoc Networks - A simulation study. 1998, tesis de Maestria.
- [2] Charles E. Perkins, Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing," wmcasa, p. 90, Second IEEE Workshop on Mobile Computer Systems and Applications, 1999.
- [3] Vikram Srinivasan, Pavan Nuggehalli, Carla F. Chiasserini, Ramesh R. Rao. Cooperation in Wireless Ad Hoc Networks. INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE. 3 April 2003
- [4] Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, Robert Morris. Capacity of Ad Hoc Wireless Networks. International Conference on Mobile Computing and Networking archive Proceedings of the 7th annual international conference on Mobile computing and networking table of contents, Rome, Italy, Pages: 61 – 69, Year of Publication: 2001, ISBN:1-58113-422-3
- [5] Margaret Martonosi. The Princeton ZebraNet Project: Sensor Networks for Wildlife Tracking.
- [6] Antonis Dimakis, Linhai He, John Musacchio, Hoi-Sheung Wilson So, Teresa Tung, Jean Walrand. Adaptive Quality of Service for a Mobile Ad Hoc Network. Jul-2003. IEEE
- [7] YihChun Hu, Adrian Perrig, David B. Johnson. Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc Networks. 2005 - Springer
- [8] Patroklos G. Argyroudis, Donal O'Mahony. Secure Routing for Mobile Ad hoc Networks. 2004 European PKI Workshop – Springer.
- [9] Chunlong Guo, Lizhi Charlie Zhong, Jan. M. Rabaey. Low Power Distributed MAC for Ad Hoc Sensor Radio Networks. Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE, 2001, Volume: 5, On page(s): 2944-2948 vol.5.
- [10] Hakan Cuzdan. WIRELESS MULTIPLE ACCESS CONTROL PROTOCOLS. IEEE Internet Computing, July-August 2002.

- [11] Sunil Kumar, Vineet S. Raghavan and Jing Deng. MEDIUM ACCESS CONTROL PROTOCOLS FOR AD-HOC WIRELESS NETWORKS: A SURVEY. Elsevier Ad-Hoc Network Journal 1994.
- [12] Yuan Xue, Baochun Li. A Location-aided Power-aware Routing Protocol in Mobile Ad Hoc Networks. Global Telecommunications Conference, 2001. GLOBECOM'01.
- [13] Young-Bae Ko and Nitin H. Vaidya. Location-Aided Routing (LAR) in mobile ad hoc networks. Wireless Networks, 2000 – Springer.
- [14] Mike Woo, Suresh Singh and C.S. Raghavendra. Power-Aware Routing in Mobile Ad Hoc Networks. international conference on Mobile computing and networking, 1998.